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

# Contents

**Introduction** 

#### **Prerequisites**

**Requirements** 

Components Used

#### **Background Information**

Wi-Fi 6E Security

WPA3

Level Set: WPA3 Modes

Cisco Catalyst Wi-Fi 6E APs

Clients Supported Security Settings

#### **Configure**

Network Diagram

**Configurations** 

Base Configuration

#### <u>Verify</u>

Security Verification
WPA3 - AES(CCPM128) + OWE
WPA3 - AES(CCPM128) + OWE with Transition Mode
WPA3-Personal - AES(CCMP128) + SAE
WPA3-Personal - AES(CCMP128) + SAE + FT
WPA3-Enterprise + AES(CCMP128) + 802.1x-SHA256 + FT
WPA3-Enterprise + GCMP128 cipher + SUITEB-1X
WPA3-Enterprise + GCMP256 cipher + SUITEB192-1X
Security Conclusions
Troubleshoot
Related Information

# 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/WPA3 Encryption -		
AES(CCMP128)	CCMP256	
GCMP128	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.

<ul> <li>Protected Management Frame –</li> </ul>	
PMF	Required 🔻
Association Comeback Timer*	1
SA Query Time*	200

### **Authentication Key Management**

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

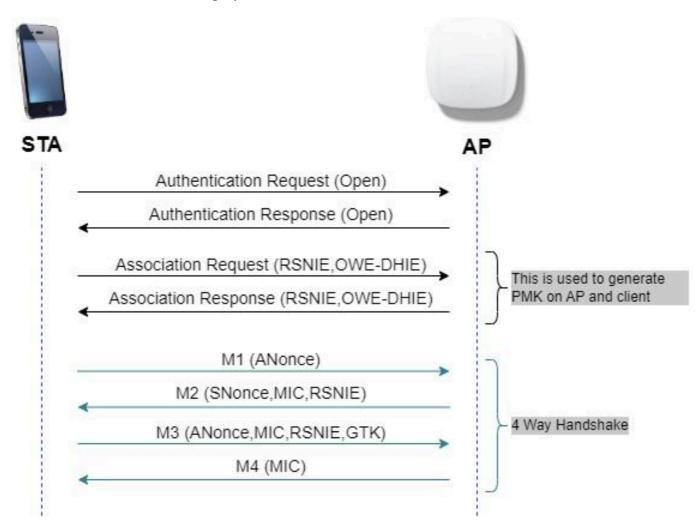
Auth Key Mgr	nt	
SAE	O	FT + SAE
OWE		FT + 802.1x
802.1x- SHA256	D	
Anti Cloggir	ng Threshold*	1500
Max Retries	*	5
Retransmit	Timeout*	400
PSK Format	t	ASCII
PSK Type		Unencrypted v
Pre-Shared	Key*	
SAE Passw	ord Element 🚯	Both H2E and HnP ▼

AKM Options

### OWE

Opportunistic Wireless Encryption (OWE) is an extension to IEEE 802.11 that provides encryption of the wireless medium (<u>IETF RFC 8110</u>). The purpose of OWE based authentication is avoid open unsecured wireless connectivity between the AP'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).

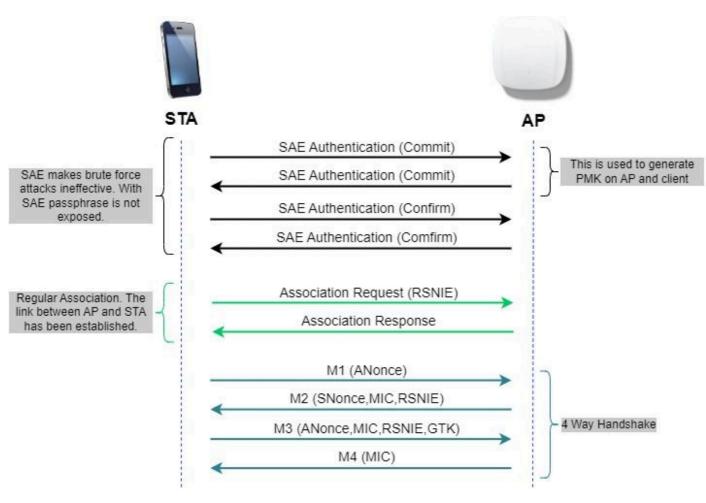
SAE with H2E is mandatory for WPA3 and Wi-Fi 6E.

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)

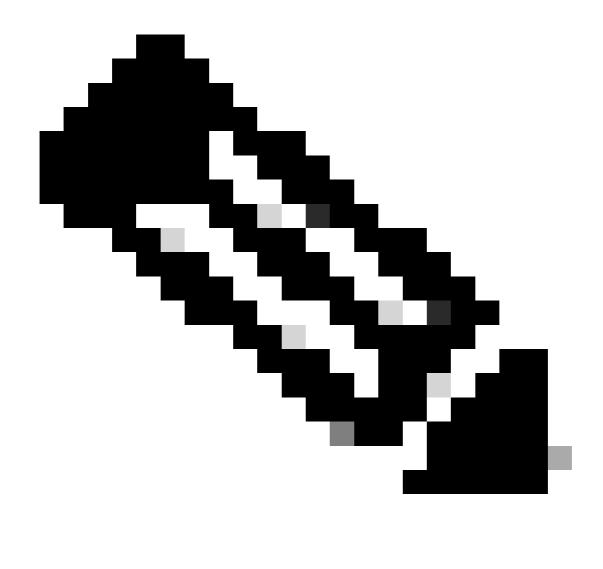
Hash-to-Element (H2E) is a new SAE Password Element (PWE) method. In this method, the secret PWE used in the SAE protocol is generated from a password.

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:

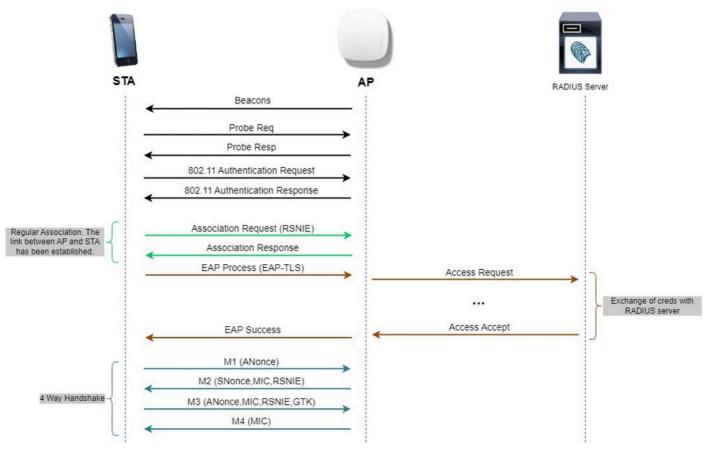
- Derivation of a secret intermediary element (PT) from the password. This can be performed offline when the password is initially configured on the device for each supported group.
- Derivation of the PWE from the stored PT. This depends on the negotiated group and MAC addresses of peers. This is performed 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 "192-bit" mode aligned with Commercial National Security Algorithm (CNSA)
    - More than just for the federal government
    - Consistent cryptographic cipher suites to avoid misconfiguration
    - Addition of GCMP & ECCP for crypto and better hash functions (SHA384)
    - PMF Required
    - WPA3 192-bit security shall be exclusive for EAP-TLS, which shall require certificates on both the supplicant and RADIUS server.

• To use WPA3 192-bit enterprise, the RADIUS servers must use one of the permitted EAP ciphers:

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 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 <u>WPA3 Deployment Guide</u>.



### 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:

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 802.11a 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:
Authentication and cipher supported in infrastructure mode:
OpenNoneOpenWEP-40bitOpenWEP-104bitOpenWEPWPA-EnterpriseTKIPWPA-PersonalCCMPWPA-PersonalCCMPWPA2-EnterpriseTKIPWPA2-EnterpriseCCMPWPA2-EnterpriseCCMPWPA2-PersonalCCMPWPA2-PersonalCCMPWPA2-PersonalCCMPWPA2-PersonalCCMPWPA2-PersonalCCMPOpenVendor definedWPA3-PersonalCCMPVendor definedWPA3-EnterpriseWPA3-EnterpriseCCMPWPA3
WPA3-Enterprise TKIP Number of supported bands : 3 2.4 GHz [ 0 MHz - 0 MHz] 5 GHz [ 0 MHz - 0 MHz] 6 GHz [ 0 MHz - 0 MHz] IHV service present : Yes IHV adapter OUI : [00 00 00], type: [00] IHV extensibility DLL path: C:\WINDOWS\System32\DriverStore\FileRepository\netwtw6e.inf_amd64_eda979fbdedea064\IntelIHVRouter12.dll

Windows output of \_netsh wlan show driver\_for client AX211

Netgear A8000:

### Interface name: A8000\_NETGEAR

Driver :	NETGEAR A8000 WI	Ed & E &E Adapter
	NETGEAR Inc.	ri v a oc Adapter
	MediaTek, Inc.	
	11/25/2022	
	1.0.0.108	
	oem9.inf	
	Native Wi-Fi Dri	
		802.11g 802.11n 802.11ac 802.11ax
FIPS 140-2 mode supported :		
802.11w Management Frame Pr	otection supporte	d : Yes
Hosted network supported :	No	
Authentication and cipher s	upported in infra	structure mode:
	Open	None
	Open	WEP-40bit
	Open	WEP-104bit
	Open	WEP
	WPA-Enterprise	TKIP
	WPA-Enterprise	CCMP
	WPA3-Personal	CCMP
	OWE	CCMP
	WPA-Personal	TKIP
	WPA-Personal	CCMP
	WPA2-Enterprise	TKIP
	WPA2-Enterprise	CCMP
	WPA2-Personal	TKIP
	WPA2-Personal	CCMP
Number of supported bands :		
number of supporced ballus :	2.4 GHz [ 0 MHz -	_ 0 NU7]
	5 GHz [ 0 MHz	
was sound as an example	6 GHz [ 0 MHz	- e nazj
	Yes	
	[00 00 00], type	
IHV extensibility DLL path:		
IHV UI extensibility ClSID:		
		888-8888-888888888888888888888888888888
Wireless Display Supported:	Yes (Graphics Dr	iver: Yes, Wi-Fi Driver: Yes)

Windows output of \_netsh wlan show driver\_for client Netgear A8000s

Android Pixel 6a:

9243 18

÷

0 B

# None

Enhanced Open

WEP

WPA/WPA2-Personal

WPA3-Personal

WPA/WPA2-Enterprise

WPA3-Enterprise

WPA3-Enterprise 192-bit



88





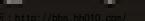
2 3 4 5 6 7 .8





Ş,

0



: 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.

### WPA3 - AES(CCPM128) + OWE

This is the WLAN Security configuration:

Search Menu Items	Configuration * > Tags & Profiles * > WLANs		Edit WLAN			
Dashboard	+ Add X Delens	Frable WLAN	A Changing WLAN parame	ters while it is enabled will result in loss	of connectivity for clients conn	lected to it.
Monitoring >	Selected WLANs : 0		General Security Advanced	Add To Policy Tags		
Configuration >	O Status Y Name	di T	Layer2 Layer3 AAA			
	MacFilter     dot1x	1	O WPA + WPA2 O WPA2	+ WPA3	O Static WEP	O None
Administration >	O O wih6E_test	5	MAC Filtering O			- There
Troubleshooting			Lobby Admin Access	2 O Stati Over Read	the DS ssociation Timeout * Key Mgmt	Disabled 0 20 FT + SAE
			GCMP128     GCM     Protected Management Frame     PMF     Association Comeback Timer*     SA Query Time*	Required  Tran	and the second se	FT + 802.1x

**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.

wan bss	id 00:df	1 Ididdi 7di 38 or wlan. fc. type,	subtype == 0x00	01d				
io. Ti	ine	Delta Source	Destination	Protocol	Length Ch	annel Signalistre	Info	> Frame 158: 355 bytes on wire (2040 bits), 355 bytes captured (2040 bits) on interface \Device\WFF_(D4578905-2998-4456-8C33-C343166
155 2		0.020504 Cisco_dd:7d:38		882.11	355		Beacon frame, SH+1850, FN+0, Flag1+C, HI+100, SSID+"wifi66_test"	Ethernet II, Src: Cisco_62:97:47 (74:11:02:02:97:47), Ost: Universa_07:cf:06 (00:30:08:07:cf:06)
		0.001919 IntelCor_90:58:		892.11	168		Probe Request, SN+201, FN+0, Flagt+C, SSID+Hildcard (Broadcast)	> Internet Protocol version 4, Src: 192.168.1.15, Dst: 192.168.1.121
		0.001115 Cisco_dd:7d:38		882.11	312		Probe Response, SN#13, FN#0, Flags+C, 01+100, SSID+"wif168_test"	> User Datagram Protocol, Src Port: 5555, Ost Port: 5000
		0.019059 Cisco dd:7d:30		802.11	312		Probe Response, SN+1852, FN+0, Flags+C, 81+100, SSID+"xifi68_test"	AiroPeek/OmiPeek encapsulated IEEE 802.11
		0.019972 Cisco dd:7d:38		802.11	332		Probe Response, SN+1853, FN+0, Flags+C, #I+100, SSID+"wifi68 test"	1 > 802.11 radio information
		0.019006 Cisco dd:7d:30		802.11	312		Probe Response, SN+1054, FN+0, Flags+C, BI+100, SSID+"wifi6E test"	> IEEE 802.11 Beacon frame, Flags:C
		0.021793 Cisco dd:7d:38		002.11	312		Probe Response, SN+1855, FN+0, Flags+C, B1+100, SSID+"wifi68_test"	✓ IEEE 802.11 wireless Hanagement
		0.015704 IntelCor 98:58:			96		Authentication, SN=24, FN=0, Flags+C	> Fixed parameters (12 bytes)
		0.000000 192.168.1.15	192,160,1,1		76		Acknowledgement, Flags+C	<ul> <li>Tagged parameters (253 bytes)</li> </ul>
		0.002000 Cisco dd:7d:38			355		Beacon frame, SN+1856, FN+0, Flags+C, 8I+100, SSID+"wifi6E_test"	> Tag: SSID parameter set: "wifi64_test"
		0.001687 Cisco_dd:7d:38			96		Authentication, SN+11, FN+0, Flags+C	> Tag: Supported Rates 4(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Mbit/sec]
		0.000000 192.160.1.15			76		Acknowledgement, FlagsC	> Teg: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
		0.000061 IntelCor_98:58:			204		Association Request, SN=25, FN=0, Flags=	> Tag: Country Information: Country Code na, Environment Global operating classes
		0.000053 192.168.1.15	192.168.1.1		76		Acknowledgement, FlagsC	> Tag: Power Constraint: 6
		0.010940 Cisco_dd:7d:35			275		Association Response, SNu0, FNu0, FlagsC	> Tar: TPC Report Transmit Power: 16, 11mR Margin: 4
		0.000000 192.168.1.15			26		Acknowledgement, FlagsC	v fag: #SN Information
		0.000019 IntelCor_98:58:			93		Action, SN+26, FN+0, Flags+C	Tag Number: RSN Information (48)
		0.000000 192.168.1.15	192.168.1.1.		76		Acknowledgement, flags+C	Tag length: 26
		0.000388 Cisco_dd:7d:38			221		Key (Nessage 1 of 4)	RSN Version: 1
			192.160.1.1.		26		Acknowledgement, #lags+C	> Group Cipher Suite: 40:0f:ac (Ieee 802.11) AES (CCM)
		0.003360 IntelCor_98:58:			227		Key (Nessage 2 of 4)	Fairwise Cipher Suite Count: 1
		0.000000 192.168.1.15	192,168.1.1		26		Acknowledgement, Flags+C	> Pairwise Cloher Suite List 00:0f:ac (leee 802.11) AES (CCM)
								Auth Key Mahagement (ADM) Suite Count: 1
		0.001564 Cisco_dd:7d:38			295		Key (Nessage 3 of 4)	<ul> <li>Auth Key Management (AoN) List 40:0fiac (Ieee 802.11) Opportunistic wireless Encryption</li> </ul>
		0.000000 192.168.1.15	192.168.1.1.		26		Acknowledgement, flags+C	✓ Auth Key Hanagement (AKH) Suite: 00:0f:ac (Ieee 802.11) Opportunistic wireless Encryption
		0.000642 Cisco_dd:7d:38			312		Probe Response, SN+1857, Fise0, Flags+C, BI+100, SSID+"wifi6E_test"	auth Key Management (AON) OUI: 00:0f:ac (Icee 802.11)
		0.000075 IntelCor_98:58:			199 76		Key (Hessage 4 of 4)	Auth Key Management (AOM) type: Opportunistic Mireless Encryption (18)
		0.000226 192.168.1.15	192.168.1.1.				Acknowledgement, FlagsC I. N(R)+62, N(S)+42: DSAP 0x5e Individual, SSAP 0x00 Command	v Six Capabilities: #x00es
		0.005613 Cisco_5c:f5:24			183			
		0.000000 192.168.1.15 0.000000 Cisco Scif5:24	192.168.1.1.		111		Acknowledgement, flagswC U F. funcwSABME: DSAP exdB Individual, SSAP ex64 Response	
			192,168,1,1		283		<pre>u v, runceseme; user exes individual, sawr exe+ sesponse Acknowledgement, flags+C</pre>	
		0.000000 192.168.1.15			312			
		0.014642 C1sco_dd:7d:38		002.11	312		Probe Response, SN=1858, FN=0, Flags=C, BI=100, SSID="wifi66_test"	+ Anagement Frame Protection Required: True
		0.020414 Cisco_dd:7d:38					Probe Response, SN=1859, FN=0, Flags=C, 81=100, SSID="wifi66_test"	Hanagement Frame Protection Capable: True
		0.020397 Cisco_dd:7d:38		802.11	312		Probe Response, SN=1860, FN=0, Flags=C, BI=100, SSID="wifi66_test"	
		0.022546 Cisco_dd:7d:38		802.11	355		Beacon frame, SN+1861, FN+0, flags+C, BI+100, SSID+"wifi6E_test"	
		0.000000 IntelCor_98:58:		LLC	114		I P, N(R)=25, N(S)=115; DSAP Exd6 Group, SSAP SNA Path Control Command	
		0.018546 Cisco_dd:7d:38		802.11	312		Probe Response, SN=1862, FN=0, Flags=C, BI=100, SSID="wifi6E_test"	Prkip Counti e
		0.001647 192.168.1.15	192.168.1.1		- 76		Acknowledgement, Flags+C	PORTD List
		0.018786 Cisco_dd:7d:38		\$92.11	312		Probe Response, SN+1863, FN+0, Flags+C, #I+100, SSID+"wif16E_test"	) Group Hanagement Cipher Suite: 00:0f:sc (Seee 802.11) 81P (128)
		0.020471 Cisco_dd:7d:38		\$82.11	312		Probe Response, SN+1864, FN+0, Flags+C, BI+100, SSID+"wif166_test"	> Tag: CBSS LOAD EINMART BD: THE CCA VERSION
		0.009165 192.168.1.15	192.168.1.1.		76		Acknowledgement, Flags+C	> Tag: RH Enabled Capabilities (S octets)
		0.013528 Cisco_dd:7d:38		002.11	312		Probe Response, SN+1865, FN+0, Flags+C, BI+100, SSID+"wifi66_test"	> Tag: Extended (apabilities (1) octets)
		0.000648 192.168.1.15	192.168.1.1		76		Acknowledgement, flags+C	) Tag: Tx Power Service
		0.009719 Cisco_dd:7d:38		802.11	355		Beacon frame, SN×1866, FN×0, Flags+C, B1×100, SSID+"wifi6E_test"	Tag: Tx Power Envelope
		0.020366 Cisco_dd:7d:38		802.11	312		Probe Response, SN×1867, FN+0, Flags+C, BI×100, SSID+"wifi6E_test"	Fit Teg: Nultiple BSDD Configuration
		0.000004 192.168.1.15	192.168.1.1.		26		Acknowledgement, flags+C	> ixt mg: m cooblities
		0.020353 Cisco_dd:7d:38		882.11	312		Probe Response, SN+1868, FN+0, Flags+C, BI+100, SSID+"wifi6E_test"	> Ext Tag: H Operation
		0.001927 192.168.1.15	192.168.1.1.		26		Acknowledgement, Flags+C	
348.2	.78346B	A. #18662 /isco.dd:7d:18	Renadcast	887,11	352	<li>K1 . 16 dkn</li>	Prohe Reconne. Stall69, Flat, Flate	

OWE beacon frame

If you look at RSN capabilities field, you can see AP is advertising both Management Frame Protection (MFP) capabilities and MFP required bit set to 1.

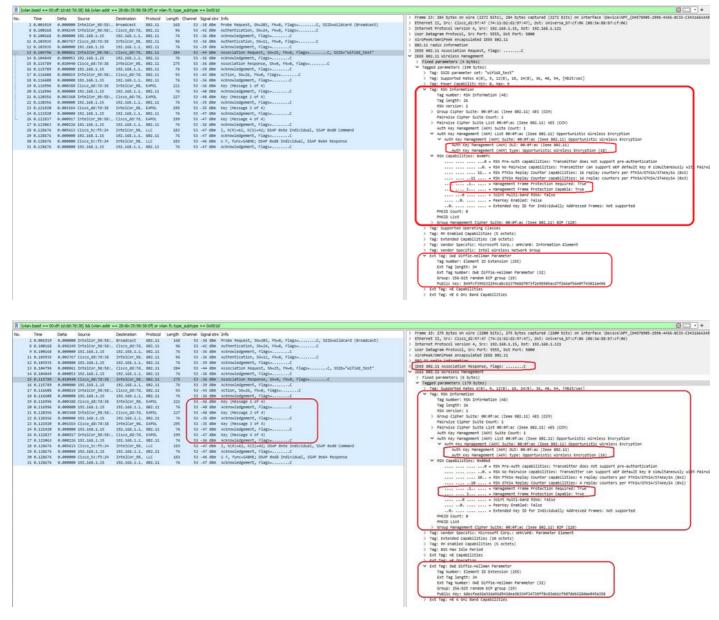
### **OWE** Association

You can see the UPR sent in broadcast mode and then the association itself.

The OWE starts with the OPEN authentication request and response:

(wlan.bssid == 00	0:df:1d:dd:7d:38) && (v	n.addr == 28:6b:35:5	8:58:0f) or w	lan.fc.type_su	btype == 0x001	d	
o, Time	Delta Source	Destination	Protocol	Length Ch	annel Signalistr	10%0	> Frame 8: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface \Device\WFf_(D4578985-2998-4456-8C33-C34316643498), 1
	0.000000 IntelCo					Probe Request, SN+203, FN+0, Flags+C, SSID+Wildcard (Broadcast)	Ethernet II, Src: Cisco_d2:97:47 (74:11:b2:d2:97:47), Dst: Universa_b7:cf:06 (08:3a:88:b7:cf:06)
	0.090249 IntelCon			96		Authentication, SNx24, FNx0, FlagisC	Internet Protocol Version 4, Src: 192.168.1.15, Ost: 192.168.1.121
	0.000000 192.168			76		Acknowledgement, Flags+C	> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
	0.003767 Cisco_d			26		Authentication, SN+11, FN+0, Flagi+C	> AiroPeek/OmniPeek encapsulated IEEE 802.11
							> S02.11 radio information
	0.000000 192.168			76		Acknowledgement, Flags=C	> IEEE 802.11 Authentication, Flags:C
	0.000861 IntelCo					Association Request, SN+25, FN+0, Flags+C, SSID+"wifi64_test"	IEEE 802.11 Wireless Management
	0.000053 192.168					Acknowledgement, flags+C	Fixed parameters (6 bytes)
	0.010940 Cisco_d					Association Response, SN=0, FN=0, Flags=C	Authentication Algorithm: Open System (0)
	0.000000 192.168			76		Acknowledgement, Flags+C	Authentication Sig: exceed
	0.000819 IntelCo					Action, SN=26, FN=0, Flags=C	Status code: successful (exemple)
	0.000000 192.168					Acknowledgement, Flags+C	
	0.000388 Cisco_d			221		Key (Message 1 of 4)	
	0.000000 192.168			76		Acknowledgement, Flags+C	
	0.003360 IntelCo			227		Key (Message 2 of 4)	
22 0.120356	0.000000 192.168	.15 192.168.1	1. 002.11	76	53 -35 dBm	Acknowledgement, Flags+C	
23 0.121920	0.001564 Cisco_d	7d:38 IntelCor_1	B. EAPOL	295	53 -35 dBm	Key (Message 3 of 4)	
24 0.121920	0.000000 192.168	.15 192.168.1	1. 802.11	76	53 -47 dBm	Acknowledgement, Flags+C	
26 0.122837	0.000917 IntelCod	98:58: Cisco_dd::	d_ EAPOL	199	53 -47 dBm	Key (Message 4 of 4)	
27 0.123063	0.000226 192.168	.15 192.168.1	1. 802.11	76	53 -36 dBm	Acknowledgement, Flags+C	
28 0.128676	0.005613 Cisco_5	f5:24 IntelCor 1	8. LLC	183		I, N(R)=62, N(S)=42; DSAP 0xSe Individual, SSAP 0xd0 Command	
	0.000000 192.168			76		Acknowledgement, Flags+C	
	0.000000 Cisco_5			183		U F, func+SABHE; DSAP exd8 Individual, SSAP ex64 Response	
	0.000000 192.168			76		Acknowledgement, FlagsC	
							11
	3:dfi 1d:dd: 7d:38) && (r						Ø
(elan.bssid == 00			8:58:0f) or w	lan.fc.type_su		8	> Frame 11: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface \Device\NPF_{D4578905-2998-4456-8C33-C343166A3498},
(wlan.bssid == 00	odfi schidd: 7d: 38) && (v Delta Source	n.addr == 28:6b:35:5 Destination	8:58:0f) or w Protocol	lan.fc.type_si	btype == 0x001 annel Signal str	4	> Frame 11: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface \Device\WF_[04578985-2998-4456-8C33-C3436643498], > Ethernet II, Src: Cisco_d2:97:47 (74:13:1b2:d2:97:47), Dst: Universa_b7:cf:06 (08:3a:88:b7:cf:06)
(wlan.bssid == 00 . Time 2 0.001919	0:dfild:dd:7d:38) && (v Delta Source e.000000 IntelCor	n.addr == 28:60:35: Destination 98:58:Broadcast	8:58:0f) or w Protocol 892.11	lan.fc.type_si	btype == 0x001 annel Signalistr 53 -38 dim	d 19f0 Prote Request, Sw200, Plueb, Flagr	> Frame 11: 56 bytes on wire (N& Dits), 56 bytes captured (N& Dits) on interface (Derice(W#D04578906-2598-4456-8C33-C3411643348), > Bthermet 11, Src: (Dico_d259747 (NillDitd):97/47), Dot: Universa_Dricf46 (08:1a:08:07:6746) > Intermet Protocol Version, Src: 03:348-135, Dot: 30:146-13.121
(wlan.bssid == 00 Time 2 0.001919 8 0.100168	0:df:1d::dd:7d:38) && (v Delta Source e.exexes IntelCor e.exexes IntelCor	n.addr == 28:60:35:5 Destination 98:58:Broadcast 98:58:Cisco_dd:7	8:58:0f) or w Protocol 842.11 d. 842.11	lan.fc.type_su Length Ch 168	8type == 0x001 annel Signal str 53 -38 d8m 53 -42 d8m	d Info Probe Request, Sun20, Plus, FlagsC, SSID-wildcard (Broadcast) Authentication, Sun24, Plus, FlagsC	> Former 11: 46 bytes on wire (TAB bits), M bytes cabtered (TAB bits) on interface Unrice/br/(DAT2006-2008-A466-623)-CA436643400), > Ethernet Trobocol version 4, Sec: 392.466.155, Dott 108.166.121 > Discrement Protocol, Versi SSS5, D Strett 1860
(wlan.bssid == 00 . Time 2 0.001919 8 0.100168 9 0.100168	Delta Source e.eeeeee IntelCor e.eeeeee IntelCor e.eeeeee 192.166	n.addr == 28:6b:35:5 Destination 98:58:_ Broadcast 98:58:_ Cisco_ddr: 15 192.168.1	8:58:0f) or w Protocol 802.11 d. 802.11 1. 802.11	lan.fc.type_su Length Oh 168 96 76	btype == 0x001 annel Signal str 53 -38 dim 53 -42 dim 53 -36 dim	d Info Prob Reputst, Sin200, Find, FlagsC, SSID-Mildcard (Broadcast) Authentication, Sin24, Find, FlagsC Automolegement, FlagsC	> Frame II: 96 bytes on wire (748 bits), 96 bytes captured (748 bits) on interface Unvice(WF(04570805-2998-4456-453)-C3416643488), b thermet II, Src: (156.0,01974) (74111111010197407), 0511 universa_D7cfr366 (881381807cfr36) ) thermet Protocol wrston & Src: 192.586.135, 051 192.146.1.121 ) user Datagram Frotocol, Src Port: SSS, 051 Fort: 5680 ) AurroBerkynnerke mcopulated IEEE B02.11
(wlan.bssid == 00 Time 2 0.001919 8 0.100168 9 0.100168 11 0.103935	Doff Ldvidd: 7dr38) && (v           Delta         Source           0.0000000         IntelCor	n.addr == 28:6b:35: Destination 98:58:Broadcast 98:58:Cisco_ddi: 15 192.168.1 76:38 IntelCor_1	8:58:0f) or w Protocol 802.11 d. 802.11 1. 802.11 8. 802.11	lan.fc.type_su Length Oh 168 96 76 95	btype == 0x001 annel Signal str 53 -38 dbm 53 -42 dbm 53 -36 dbm 53 -36 dbm	d 196 Prote Reputst, SW-201, Find, flagsC, SSID-wildcard (Broadcast) Authentication, Sw-24, Find, flagsC Authentication, Swist, Find, flagsC	> Prome 31: 96 bytes on wire (THE Bits), H0 bytes captored (THE BIts) on interface Unvice/byt (DH37886-2988-A458-4C33-C48166A3488), > thermet II, Sorci Sica, Sarkovite (THE BITS), Bott Interface Unvice/byt (DH37886-2988-A458-4C33-C48166A3488), > Internet Protocol unvice of the Size (Size (S
(wlan.bosid == 00 Time 2 0.001919 8 0.100168 9 0.100168 11 0.180905 12 0.181905	Defi Idridd: 7d:38) 88 (v Defia Source e.eeeeee Intelco e.eeeeee Intelco e.eeeeee 192.168 e.eeeeee 192.168	n.addr == 28:60:13:1 Destination 98:58:Broadcast 98:58:Ciscodd: 15 192.168.1. 76:38 Intelcor1 15 192.168.1.	8:58:0f) or w Protocol 802.11 d. 802.11 1. 802.11 1. 802.11 1. 802.11	lan.fc.type_su Length Oh 168 96 76 96 76	btype == 0x001 annel Signal str 53 -38 die 53 -42 die 53 -36 die 53 -36 die 53 -39 die	d Sofo Prote Repett, SN-200, Pinek, FlagsC, SSID-wildcard (Broadcast) Arbentization, SN-3K, Pinek, FlagsC Arbentization, Pinek, Pinek, FlagsC	> Frame 11: 96 bytes on wire (CHE bits), 96 bytes captured (HE bits) on interface Unvice/byt_[0472082-2008_4456_4C3)-CAU166A1408), > Buterent Trotocol wrw.ion 4, Sec: 352.166.1.55, Dat: 352.166.1.121 > Loss Fatagen Protocol, 3cr event 1585, Dat: 352.167.157.167.167.167.167.167.167.167.167.167.16
(wlan.bssid == 00 . Trme 2 0.001919 8 0.100168 11 0.100168 11 0.100395 12 0.100395 13 0.104796	Dedf Ldudd: 7d:38) && ( Delta Source e.000000 IntelCor e.000249 IntelCor e.000249 IntelCor e.000000 192.163 e.000000 192.163	n.addr == 28:60:35: Destination 90:58:Broadcast 15 92.368.1 76:38 IntelCor_ 15 92.168.1 15 92.168.1 15 92.168.1	8:58:0f) or w Protocol 802.11 d. 802.11 1. 802.11 8. 802.11 d. 802.11 d. 802.11	lan.fc.type_su Length Oh 168 96 76 95 76 284	btype == 0x00 annel Signal str 53 -38 die 53 -42 die 53 -36 die 53 -36 die 53 -39 die 53 -44 die	d tofo Probe Request, Suc20, Find, Flags	> Prome 11: 46 bytes on wire (NM bits), wh bytes captored (NM bits) on interfact (Device/DFF_(C015080-1998-4454-623-C4016443488), > Ethernet Trotocol version 4, Src: 193.146.155, Dat: 193.146.121 > Lose Patager Protocol, Ye Prot: 555, of Src: 1980 > Lorenet Patager Protocol, Ye Prot: 555, of Src: 1980 > Aircheek/Dm/Deek excessibled 2008 182.13 > Deel Datager Protocol, Ye Prot: 1958, of Src: 1980 > Aircheek/Dm/Deek excessibled 2008 182.13 > Deel Datager Protocol, Ye Prot: 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot: 1958, of Src: 1980 > Deel Datager Protocol, Ye Prot: 1958, of Src: 1980 > Deel Datager Protocol, Ye Prot: 1958, of Src: 1980 > Deel Datager Protocol, Ye Prot: 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot: 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, Deel Datager Prot. 1958, Deel Datager Prot. 1958, Deel Datager Protocol, Ye Prot. 1958, Deel Datager Protocol, Ye Prot. 1958, Deel Datager Prot. 1958, Deel Data
(wlan.bssid == 00 Time 2 0.001919 8 0.100160 11 0.100160 11 0.101935 12 0.101935 13 0.104756 14 0.104569	Delta         Sauce           Delta         Source           e.ceeseese         IntelCor           e.ceeseese         IntelCor           e.ceeseese         IntelCor           e.ceeseese         IntelCor           e.ceeseese         192.164           e.ceeseese         192.164           e.ceeseesi         192.164	n.addr == 28:60:35: Destination 90:50:Broadcast 90:50:Cisco_dd:: 15 192.160.1 15 192.160.1 90:50:Cisco_dd:: 15 192.160.1	8:58:0f) or w Protocol 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11	lan. fc. type_su Length Ch 168 96 76 96 76 284 76	btype == 0x001 annel Signal str 53 -38 dim 53 -42 dim 53 -42 dim 53 -46 dim 53 -36 dim 53 -36 dim 53 -36 dim 53 -36 dim	d 106 Probe Request, Swa20, Flue, FlagsC, Athentication, Swa24, Flue, FlagsC Athentication, FlagsC Athentication Request, Swa25, FlagsC Association Request, Swa25, FlagsC, Association Request, Swa25, FlagsC, Association Request, Swa25, FlagsC	> Frame 11: 96 bytes on wire (CNE bits), 96 bytes captured (CNE bits) on interface Unvice/MF_[CMST089-2008-4466-4513-CH316641888), > Biterret Trotcol WF106 4, Seci 352.661.153, Dati 352.864.151 > Disterret Trotcol WF106 4, Seci 352.661.153 > Disterret Trotcol WF106 4, Seci 353.661.153 >
(wlan.bssid == 00 Time 2 0.001919 8 0.100160 9 0.100160 11 0.109395 13 0.104796 14 0.104399 15 0.115789	Defa         Source           0.0000000         IntelCor	n.addr == 28:60:35: Destination 98:58:Broadcast 98:58:Cisco_ddi: 15 192.168.1. 78:38 Intel2cor_1 15 192.168.1. 193:38 Intel2cor_1	8:58:0f) or w Protocol d. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 8. 802.11 8. 802.11	Aan.fc.type_su Length Oh 168 96 76 284 76 275	btype == 0x001 annel Signal str 53 -38 dBn 53 -42 dBn 53 -36 dBn 53 -36 dBn 53 -36 dBn 53 -36 dBn 53 -36 dBn 53 -36 dBn	d bofe Probe Report, Swaddy, Findy, Flags	> Prome 11: 46 bytes on wire (NM bits), wh bytes captored (NM bits) on interfact (Device/DFF_(C015080-1998-4454-623-C4016443488), > Ethernet Trotocol version 4, Src: 193.146.155, Dat: 193.146.121 > Lose Patager Protocol, Ye Prot: 555, of Src: 1980 > Lorenet Patager Protocol, Ye Prot: 555, of Src: 1980 > Aircheek/Dm/Deek excessibled 2008 182.13 > Deel Datager Protocol, Ye Prot: 1958, of Src: 1980 > Aircheek/Dm/Deek excessibled 2008 182.13 > Deel Datager Protocol, Ye Prot: 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot: 1958, of Src: 1980 > Deel Datager Protocol, Ye Prot: 1958, of Src: 1980 > Deel Datager Protocol, Ye Prot: 1958, of Src: 1980 > Deel Datager Protocol, Ye Prot: 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot: 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, OF Src: 1980 > Deel Datager Protocol, Ye Prot. 1958, Deel Datager Prot. 1958, Deel Datager Prot. 1958, Deel Datager Protocol, Ye Prot. 1958, Deel Datager Protocol, Ye Prot. 1958, Deel Datager Prot. 1958, Deel Data
(wlan.bosid == 00 . Time 2 0.001919 8 0.100168 9 0.100168 11 0.100736 12 0.100736 14 0.104736 14 0.104736 14 0.104739 16 0.115739	Defa         Source           0.000000         Tratelco           0.0000000         Tratelco	n.add == 28:60:35: Destination 98:58: Broadcast 98:58: Cisco_dd: 15 192.166.1. 15 192.166.1. 15 192.166.1. 15 192.166.1. 15 192.168.1.	8:58:0f) or w Protocol 802.11 d. 802.11 1. 802.11 0. 802.11 d. 802.11 d. 802.11 1. 802.11 1. 802.11 1. 802.11	Aan.fc.type_su Length Oh 166 96 76 284 76 284 76 284 76 275 76	btype == 0x001 annel Signal str 53 -42 ditt 53 -36 ditt	d sofe Probe Request, Sun20, Flue, FlagsC, SSID-wildcard (Broadcast) Actomologenert, FlagsC Actomologenert, FlagsC Accomologenert, FlagsC Association Response, Sube, FlagsC Association Response, Sube, FlagsC Association Response, Sube, FlagsC	> Frame 11: 96 bytes on wire (VM bits), 96 bytes captured (VM bits) on interface Unvice/WF.[CMXT089-2008-4464-451-CH316644888), > thterent IT, Src: (Sice.2019/0716 (VHIS1001629797), Ditt Universa, 2016748 (M812818076768)) > biterent Protocol years Protocol, year (VHIS1001610, Ditt 1930-1841-121) > User Datager Protocol, year (VHIS1001610, DItt 1930-1841-1841-1841-1841-1841-1841-1841-184
(wlan-bosid == 00	bidfild:dd:7d:38) 8.8. (v           Defa         Source           0.000000         IntelCo           0.000000         1012.163           0.000000         1012.163           0.000000         102.164           0.000000         102.163           0.000000         102.164           0.000000         132.164           0.0000000         132.164           0.0000000         132.165           0.0000000         132.164	n.addr == 28:60:35: Destrution 98:58: 15: 12:168: 15: 12:168: 16: 12:168: 16: 12:168: 16: 12:168: 16: 12:168: 16: 12:168: 17:	8:58:07) or w Protocol 802.11 1. 802.11 8. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 3. 802.11	lan.fc.type_su Length Ch 168 96 76 95 76 284 76 275 76 93	btype == 0x00) samel Sgnal str 53 -38 dim 53 -42 dim 53 -36 dim 53 -39 dim 53 -34 dim	d Sofe Proce Report, SN-201, Plush, FlagsC, SSID-wildcard (Broadcast) Arbentication, Sn-3k, Plush, FlagsC Automotogener, FlagsC Association Report, Sn-3k, FlagsC	> Frame II: 46 bytes on wine (NM Bits), 40 bytes captored (NM Dits) on interfact (Device/UM*_(DOTSB0-1998-4454-633-CMB1664A386), > Ethernet Trotocol version 4, Src: 193.184.155, DET: 193.184.121 > Loss Potagram Protocol, 2rc Port: 1956, 01 France, Direct Segue > AutrebrackComplexe executive 2188.213 > User Potagram Protocol, 2rc Port: 1956, 01 France, Direct Segue > AutrebrackComplexe executive 2188.213 > Best: Interfact Interface Interface 2188.213 > Best: Interface Interface 2188.214 > Best: Interface Regenet V Fixed parameters (& Dyte) AutrebrackComplexe (& Dyte)
(wlan.bssid == 00 Time 2 0.001919 8 0.100166 11 0.100166 11 0.100195 12 0.100195 13 0.104796 14 0.10439 15 0.115789 15 0.115789 17 0.116608	hoff: Ldsdd: 7d:38)         84. (f)           Defta         Source           0.0000000         Intelico           0.000000         192.162           0.000000         192.162           0.000000         192.162           0.000001         192.162           0.000001         192.162           0.000001         192.163           0.000001         192.164           0.000001         192.163           0.000001         192.164           0.000001         192.164           0.000001         192.164	n.addr == 28:60:35: Destination 9:54: Broadcast 9:54: Disco.ddi 9:54: Disco.ddi 9:54: Disco.ddi 9:54: Disco.ddi 9:54: Disco.ddi 15 19:2.168.1 9:54: Disco.ddi 15 19:2.168.1 9:55: Disco.ddi 15 19:2.168.1 9:55: Disco.ddi 15 19:2.168.1	8:53:07) or w Protocol 802.11 d. 802.11 1. 802.11 1. 802.11 1. 802.11 8. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11	An fc.type_si Length Ch 168 96 76 284 76 275 76 93 76 93 76	btype == 0x00 annel Signal str 53 -38 dbm 53 -34 dbm 53 -36 dbm	d tob robe request; Sun20, Fine, FlagsC Acconsidgement, FlagsC Acconsidgement, FlagsC Acconsidgement, FlagsC Acconsidgement, FlagsC Acconsidgement, FlagsC Acconsidgement, FlagsC Acconsidgement, FlagsC Acconsidgement, FlagsC Acconsidgement, FlagsC	> Frame 11: 46 bytes on wine (TAB bits), 46 bytes captured (TAB bits) on interface Unvice/WF.[CASTB08-2008-4464-453-CAB1664A800], > Itherent Trotocol warior (TAB bits), 46 bytes (TAB bits) on interface Unvice/WF.[CASTB08-2008-4464-453-CAB1664A800], > Interent Trotocol warior (TAB bits), 45 bytes (TA
(wian-basid == 00 Time 2 0.001519 9 0.100168 10 0.100355 10 0.100355 10 0.100355 10 0.100355 10 0.100355 10 0.100355 10 0.115789 10 0.116698 10 0.11698 10 0.11688 10 0.116888 10 0.116888 10 0.1168	>:dfild:dd:7d:38) 8& (b           Obis         Source           0:00000         IntelCo           0:00000         12:182           0:00000         12:182           0:00000         12:182           0:00000         12:182           0:00000         12:182           0:00000         12:182           0:00000         12:182           0:00000         12:182           0:00000         12:182           0:00000         12:182           0:00000         12:182           0:00000         12:182           0:00000         12:182           0:00000         12:182	n.add == 28:60:35: Destination Performance	8:58:50°) or w Protocol 002.11 d. 002.11 d. 002.11	lan fc. type_su Length Oh 368 96 76 284 76 275 76 93 76 93 76 93 76 221	btype == 0x001 annel Signal sty 53 -38 dim 53 -42 dim 53 -36 dim	d profit Prote Reports, Shu28, Flue, FlagsC, SSID-wildcard (Breadcast) Atthentication, Shu28, Flue, FlagsC Attoentication, Shu28, Flue, FlagsC Association Report, Shu29, FlagsC Association Report, FlagsC	> Frame 11: 46 bytes on wire (TAB bits), 46 bytes captured (TAB bits) on interface Unvice/byt_(DAST888-2898-4468-453)-CM3166434888), > Itterent Trotocol werlion 4, 5rc: 393.1461.155, Dat: 183.2467.1588 (BB:18:07:07:08) > Discretarger Potocol, 5rc cort: 5555, Dit Tab.1461.151 > Unvice/Barger Potocol, 5rc cort: 5555, Dit Tab.1461.151 > Base: Tab.2587 (Potocol, 5767 (Potocol, 5777 (Potocol, 5777 (Potocol, 5777 (Potocol, 5777 (Potocol, 57
(wlan.basid == 00 5. Tme 2 0.00151 9 0.100166 9 0.100166 1 0.100305 1 0.100305 1 0.100305 1 0.100305 1 0.100305 1 0.115789 1 0.116698 1 0.116996 2 0.116996	bidf 1d:dd:7d:38) 8& (           Dels Source           0.00000 IntelCo	n.addr == 28:60:35: Destination 9:54: Elroc.doi: 15 192.164.1 15 192.164.1 15 192.164.1 15 192.164.1 15 192.164.1 15 192.164.1 15 192.164.1 15 192.164.1 15 192.164.1 15 192.164.1	8:58:07) or w Protocol 002.11 1. 802.12 1. 802.13 1. 802.13 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.13 1. 802.13 1. 802.13	Ann. Sc. type _su length On 168 96 76 284 76 275 76 275 76 275 76 221 76 221	Brype         ==         0x00           53         -38         dbn           53         -38         dbn           53         -42         dbn           53         -42         dbn           53         -36         dbn	d Info Probe Request, SN-283, Fine, flagsC, SSID-wildcard (Broadcast) Actonologenert, FlagsC Actonologenert, FlagsC Actonologenert, FlagsC Actonologenert, FlagsC Actonologenert, FlagsC Actonologenert, FlagsC Actonologenert, FlagsC Actonologenert, FlagsC Actonologenert, FlagsC Actonologenert, FlagsC	> Frame 11: 46 bytes on wire (TAB bits), 46 bytes captured (TAB bits) on interface Unvice/byt_(DAST888-2898-4468-453)-CM3166434888), > Itterent Trotocol werlion 4, 5rc: 393.1461.155, Dat: 183.2467.1588 (BB:18:07:07:08) > Discretarger Potocol, 5rc cort: 5555, Dit Tab.1461.151 > Unvice/Barger Potocol, 5rc cort: 5555, Dit Tab.1461.151 > Base: Tab.2587 (Potocol, 5767 (Potocol, 5777 (Potocol, 5777 (Potocol, 5777 (Potocol, 5777 (Potocol, 57
(wlan.bosid == 00 . Tree 2 0.401515 2 0.100146 9 0.100146 1 0.100155 12 0.100155 12 0.100756 14 0.100756 14 0.101709 15 0.115709 16 0.115709 16 0.115709 16 0.116996 20 0.116996 20 0.116996 20 0.116995	Defi ididi 74:38) 84. (s           Deta Surre           0.00000 IntelCo	n.add == 28:60:35: Destination Performance	8:58:00) or w Protocol 0:02.11 1. 002.11 1. 002.11	Ann fc: type _pu Length _Oh 168 96 96 96 96 96 98 76 284 76 275 93 76 93 76 221 76 221 76 221 76 222	Boyoe         ==         Dx000           sand         Sg -33         dill           S1         -42         dill           S1         -34         dill           S1         -42         dill           S1         -36         dill           S1         -46         dill           S1         -46         dill           S1<-46	d info Probe Request, Swa20, Flue, FlagsC, Actonicagement, FlagsC Actonicagement, FlagsC Actonicagement, FlagsC Association Report, Swa29, FlagsC Association Report, Swa29, FlagsC Association Report, Swa29, FlagsC Association Report, Swa29, FlagsC Action, Swa39, FlagsC	> Frame 11: 46 bytes on wire (TAB bits), 46 bytes captured (TAB bits) on interface Unvice/byt_(DAST888-2898-4468-453)-CM3166434888), > Itterent Trotocol werlion 4, 5rc: 393.1461.155, Dat: 183.2467.1588 (BB:18:07:07:08) > Discretarger Potocol, 5rc cort: 5555, Dit Tab.1461.151 > Unvice/Barger Potocol, 5rc cort: 5555, Dit Tab.1461.151 > Base: Tab.2587 (Potocol, 5767 (Potocol, 5777 (Potocol, 5777 (Potocol, 5777 (Potocol, 5777 (Potocol, 57
(wlan.basid == 00 5. Time 2 0.80159 3 0.100168 9 0.100168 1 0.100305 1 0.100305 1 0.104756 1 0.104756 1 0.104756 1 0.115789 1 0.115789 1 0.115789 1 0.116688 2 0.116966 2 0.1120356	Control 12:00 Tel:00 Te	n.add == 28:60:35: Destination 90:56:	8:58:00) or w Protocol 802.11 1. 802.11 1. 802.11	An fc.type_pu Length Oth 168 96 76 284 76 225 76 227 76 221 76 221 76 227 76	btype == 0x00 saved Sgoal st 53 -38 dan 53 -36 dan 53 -44 dan	d Sofo Proce Resets, Senado, FlagsC, SSIDwildCard (Broadcast) Proce Resets, Senado, FlagsC Authonicignems, FlagsC Autocolognems, FlagsC	> Frame 11: 46 bytes on wire (TAB bits), 46 bytes captured (TAB bits) on interface Unvice/byt_(DAST888-2898-4468-453)-CM3166434888), > Itterent Trotocol werlion 4, 5rc: 393.1461.155, Dat: 183.2467.1588 (BB:18:07:07:08) > Discretarger Potocol, 5rc cort: 5555, Dit Tab.1461.151 > Unvice/Barger Potocol, 5rc cort: 5555, Dit Tab.1461.151 > Base: Tab.2587 (Potocol, 5767 (Potocol, 5777 (Potocol, 5777 (Potocol, 5777 (Potocol, 5777 (Potocol, 57
(wlan.bosid == 00 . Tree 2 0.001515 2 0.001515 2 0.1001515 1 0.1001515 1 0.1001515 1 0.1001515 1 0.1001515 1 0.1001515 1 0.1101515 1 0.1101515 1 0.1101515 1 0.1101515 1 0.1101515 1 0.110155 1 0.11055 1 0.110555 1 0.11055 1 0.110555 1 0.110555 1 0.110555	Defa idada 7d-38) 8.4 ( Defa Source 0.000000 IntelCo 0.001200 IntelCo 0.001200 IntelCo 0.000000 IS2.168 0.000000 IS2.168	n add == 28:60:35: Desination 98:58: Eroadcast 98:58: Cisco,60: 16: 192:16:1. 16: 192:16:1. 19: 19: 19:16:1. 19: 19:16:16:10:10:16:10:10:10:10:10:10:10:10:10:10:10:10:10:	8:58:00°) or w Protocol 802.11 1. 802.12 1. 802.12 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 2. 84POL 1. 84POL	An fc. type_gu Length Oh 148 96 96 96 96 98 96 284 76 284 76 293 76 93 93 76 221 76 222 76 222 76 93 93 26 225	Boyos         men         Dx000           S0         31         ddll           S1         -32         ddll           S1         -32         ddll           S1         -32         ddll           S1         -36         ddll           S1         -35         ddll           S1<-35	d info Probe Request, Sun20, Flue, FlagsC, SSID-wildcard (Broadcast) Attontication, Sun24, Flue, FlagsC Attontication, Sun24, Flue, FlagsC Attontication, Sun24, FlagsC Attonnel agenert, FlagsC Association Response, Sune, FlagsC Attonnel agenert, FlagsC Key (Densage 1 of 4) Key (Densage 1 of 4) Attonnel agenert, FlagsC	> Frame 11: 46 bytes on wire (TAB bits), Ho bytes (aphored (TAB bits) on interface Unvice/byt_(DAT2085-2008-AASE-4C3)-CA0166ALMAG), > Itherent Trobocol werlaw (A, Src: 392.166.1.55, Dat: 392.166.1.51) > Interent Trobocol werlaw (A, Src: 392.166.1.55, Dat: 392.166.1.51) > User Datagram Protocol, Src Cort: SSM, Of the Tori SBMD > Marchenk/Mmilterk respuisited IEEE B02.11 > B02.1 Engementer() (A) DatagramC > Werlaw (A) Amander (A) DatagramC > Werlaw (A) Amander (A) DatagramC > Werlaw (A) Datagram
[ulan.basid == 00 b. Time 2 0.001919 8 0.100164 9 0.100164 10 0.100155 12 0.100305 13 0.100469 14 0.100469 15 0.115789 17 0.116698 18 0.116996 20 0.116996 20 0.116996 21 0.120556 22 0.122558 24 0.121558	Defi idado 7d:30) && ( c. composition of the second of th	n.add == 28:66:35: Destination PESEL: (incodeta) PESEL: 15 12:164.1 15 12:164	8:58:00°) or w Protocol 802.111 1. 802.121 1. 802.	lan fc type _su Length Ot 168 96 76 284 76 275 76 225 76 221 76 227 76 227 76 227 76 235 76	btype == 0x00 annel Signal sty 51 - 42 dill 53 - 42 dill 53 - 45 dill 53 - 45 dill 53 - 46 dill 53 - 44 dill 53 - 44 dill 53 - 55 dill 53 - 55 dill 53 - 55 dill	d profit Prote Reports, Sku209, Fludy, FlagsC, SSID-wildcard (Breadcast) Atthetication, Sku20, Fludy, FlagsC Attoenciesterer, FlagsC Association Reports, Sku29, FlagsC Association Reports, FlagsC Association Reports, FlagsC Association Reports, FlagsC Association Reports, FlagsC Association Report, FlagsC Association Reports, FlagsC Association Report, FlagsC Association Report, FlagsC Kay Dessage 3 of 4) Association Report, FlagsC	> Frame 11: 46 bytes on wine (TAB bits), 46 bytes captured (TAB bits) on interface Unvice/WF.[CASTB08-2008-4464-453-CAB1664A800], > Itherent Trotocol warior (TAB bits), 46 bytes (TAB bits) on interface Unvice/WF.[CASTB08-2008-4464-453-CAB1664A800], > Interent Trotocol warior (TAB bits), 45 bytes (TA
(wlan-busid == 00 b. Time 2 0.4001519 8 0.100148 11 0.1001515 12 0.1001515 13 0.1001515 13 0.100151 14 0.115789 14 0.115789 15 0.115789 16 0.115789 16 0.115789 16 0.115789 16 0.115996 10 0.116996 10 0.11696 10 0.1166 10 0.1166 1	bdf.1d.dd 7d130 & & (* 0.00000 17d130 & & (* 0.00000 17d1200 0000 17d1200 0.000000 17d1200 0000 17d1200 0.000000 17d1200 17d1200 0.000000 17d1200 17d1200 0.000000 17d1200 17d1200 0.000000 17d1200 17d1200 0.000000 17d1200 17d1200 0.000000 17d1200	n add == 28:60:35: Destination 80:581. Broadcast 80:581. Class_doi: 10:102.163.1. 10:102.1.	8:58:07) or w Protocol 802.11 d. 802.11 1. 802.11 1. 802.11 d. 802.11 d. 802.11 1. 802.11 1. 802.11 1. 802.11 d. 802.11 d. 802.11 d. 802.11 d. 802.11 d. 802.11 d. 802.11 d. 802.11	Ann. Sc. type LengthOn 168 96 284 275 76 284 275 76 221 76 221 76 221 76 221 76 221 76 221 76 93 93 76 221 76 93 93 93 76 221 76 93 93 76 221 76 93 76 76 93 76 76 93 76 93 76 93 76 93 76 93 76 94 76 93 76 93 76 93 76 93 76 93 76 93 76 93 76 93 77 93 76 93 76 93 76 93 76 93 76 93 77 93 76 93 77 93 76 93 77 93 76 93 77 93 76 93 77 94 77 93 76 93 77 93 77 76 76 77 76 76 76 76 76 76 76 76 76	bbype         ==         0x000           snred         Signal str         Si         -32 dim           Si         -42 dim         Si         -36 dim           Si         -36 dim         Si         -35 dim           Si         -35 dim         Si         -35 dim           Si         -35 dim         Si         -35 dim           Si         -35 dim         Si         -35 dim           Si         -47 dim         Si         -47 dim	d bd rrote mport: Su-20, rus, ring	> Frame 11: 46 bytes on wire (TAB bits), 46 bytes captured (TAB bits) on interface Unvice/byt_(DAST888-2898-4468-453)-CM3166434888), > Itterent Trotocol werlion 4, 5rc: 393.1461.155, Dat: 183.2467.1588 (BB:18:07:07:08) > Discretarger Potocol, 5rc cort: 5555, Dit Tab.1461.151 > Unvice/Barger Potocol, 5rc cort: 5555, Dit Tab.1461.151 > Base: Tab.2587 (Potocol, 5767 (Potocol, 5777 (Potocol, 5777 (Potocol, 5777 (Potocol, 5777 (Potocol, 57
(elan. basd == 00 . Tre 2 e. 492157 1 e. 102257 2 e. 102257 2 e. 102257 2 e. 102257 2 e. 102257 2 e. 102567 2 e.	Defi idado 7d:30) && ( 0.00000 Intel Co 0.00000 Intel Co 0.0000	n.add == 28:60:35: Destrution 8:151: (150.61) 15 192.164.1 15 192.164.1	B:58:57) or vi Protocol 1022.11 1. 1022.11 1. 1022	lan f; type_su Length Ot 168 96 76 284 76 275 76 221 76 221 76 221 76 293 76 293 76 293 76 293 76	bbype         ==         0x00           annel         Signal sty           S1         -142         dilla           S2         -56         dilla           S3         -56         dilla           S4         -53         -53           S5         -53         dilla           S3         -56         dilla           S3         -56         dilla           S4         -57         dilla           S5         -57         dilla           S4         -57         dilla           S5         -57         dil	d info Probe Report, Swa20, Flud, FlagsC, SSID-wildcard (Broadcast) Atthetication, Swa24, Flud, FlagsC Attobulgement, FlagsC Association Report, Swa25, FlagsC Association Report, Swa25, FlagsC Association Report, Swa25, FlagsC Association Report, Swa25, FlagsC Association Report, FlagsC Machine Report, FlagsC Machine Report, FlagsC Key (Dessage 1 of 4) Astonaldgement, FlagsC Key (Dessage 1 of 4) Astonaldgement, FlagsC	> Frame 11: 46 bytes on wire (TAB bits), Ho bytes (aphored (TAB bits) on interface Unvice/byt_(DAT2085-2008-AASE-4C3)-CA0166ALMAG), > Itherent Trobocol werlaw (A, Src: 392.166.1.55, Dat: 392.166.1.51) > Interent Trobocol werlaw (A, Src: 392.166.1.55, Dat: 392.166.1.51) > User Datagram Protocol, Src Cort: SSM, Of the Tori SBMD > Marchenk/Mmilterk respuisited IEEE B02.11 > B02.1 Engementer() (A) DatagramC > Werlaw (A) Amander (A) DatagramC > Werlaw (A) Amander (A) DatagramC > Werlaw (A) Datagram
Color. bass         Tme           2         0.4015           3         0.4016           3         0.4016           3         0.4016           3         0.4016           3         0.4016           3         0.4016           3         0.4016           3         0.4016           3         0.4016           3         0.4017777           3         0.40176           3	Definition         Telestory         Telestory           0         Delas         Source           0         0.00000         TeleIco           0         0.000000         TeleIco           0         0.000000         TeleIco           0.0000000         TeleIco         0.000000           0.00000000         Te	n.adv = 23:60:13:1 Destination 9:51:1 9:51:1 15:19:11:1 15:19	8:58:00) or w Protocol 802.11 d. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 1. 802.11 8. 802.11	Ann. Sc. hypesu Length On 168 96 76 284 275 76 284 275 76 221 76 221 76 221 76 221 76 221 76 221 76 225 76 225 76 225 76 225 76 225 76 235 76 235 21 255 76 21 255 76 21 27 26 22 21 27 26 22 26 22 26 22 27 26 22 27 26 22 27 26 22 26 22 26 22 27 26 22 27 26 22 26 22 26 22 27 26 22 21 27 26 22 21 27 26 22 21 27 26 22 21 27 26 22 21 27 26 22 21 27 22 21 27 26 22 21 27 26 22 21 27 26 22 21 27 26 22 21 27 26 22 27 26 26 26 26 26 26 26 26 26 26 26 26 26	bbype         ==         0x001           annel         Soyal st           3         3.4         dill           53         -3.4         dill           53         -3.6         dill           53         -3.5         dill           53         -3.5         dill           53         -3.5         dill           53         -3.5         dill           53         -4.7         dill           53         -4.5         dill           54         dill         3.45	d Sofo Proce Reports, Society, Fuely, FlagsC, SSIDwalldcard (Broadcast) Arbonidgment, FlagsC Arbonidgment, FlagsC Kay (Harbar 10, Harbonic) Kay (Harbar 10, Harbar 10, Harba	> Frame 11: 46 bytes on wire (TAB bits), Ho bytes (aphored (TAB bits) on interface Unvice/byt_(DAT2085-2008-AASE-4C3)-CA0166ALMAG), > Itherent Trobocol werlaw (A, Src: 392.166.1.55, Dat: 392.166.1.51) > Interent Trobocol werlaw (A, Src: 392.166.1.55, Dat: 392.166.1.51) > User Datagram Protocol, Src Cort: SSM, Of the Tori SBMD > Marchenk/Mmilterk respuisited IEEE B02.11 > B02.1 Engementer() (A) DatagramC > Werlaw (A) Amander (A) DatagramC > Werlaw (A) Amander (A) DatagramC > Werlaw (A) Datagram
Columbos         Time           0         1         1         0         1 <td< td=""><td>Definition         Control         Control         Source           0.0000         IntelCont         Source           0.00000         IntelCont         Source           0.000000         IntelCont         Source</td><td>n.add         =         28:60:35:           Destination           98:54:         Cisco_dd:           15:15:         152:161.           16:15:12:161.         152:161.           16:15:13:17:161.         151:161.           16:15:13:17:161.         151:161.           16:15:13:17:161.         152:161.           17:18:17:161.         152:161.           15:19:161.         152:161.           15:19:161.         152:161.           15:19:161.         152:161.           15:19:161.         152:161.           15:19:161.         151:161.           15:19:161.         151:161.           16:19:161.         151:161.           16:19:161.         151:161.</td><td>B-SB:Sf) or w Protocol 802.11 d. 902.11 1. 902.11 1. 902.11 1. 902.11 1. 902.11 1. 902.11 1. 902.11 d. 902.11 d. 902.11 d. 802.11 1. 902.11 d. 802.11 1. 902.11 d. 802.11 1. 802.11</td><td>An f. type pu Length On 168 76 76 284 76 284 76 275 76 221 76 221 76 221 76 221 76 227 76 227 76 227 76 237 76 76 237 76 76 76 76 76 76 76 76 76 76 76 76 76</td><td>bbype         ==         0x000           arrel         Signal str           51         -136 dills           51         -166 dills           51         -166 dills           51         -166 dills           51         -156 dills           51         -55 dills           52         -55 dills           51         -55 dills           51         -72 dills           51         -74 dills           51         -74 dills           53         -74 dills           51         -74 dills           51&lt;-747 dills</td>           51&lt;-747 dillls</td<>	Definition         Control         Control         Source           0.0000         IntelCont         Source           0.00000         IntelCont         Source           0.000000         IntelCont         Source	n.add         =         28:60:35:           Destination           98:54:         Cisco_dd:           15:15:         152:161.           16:15:12:161.         152:161.           16:15:13:17:161.         151:161.           16:15:13:17:161.         151:161.           16:15:13:17:161.         152:161.           17:18:17:161.         152:161.           15:19:161.         152:161.           15:19:161.         152:161.           15:19:161.         152:161.           15:19:161.         152:161.           15:19:161.         151:161.           15:19:161.         151:161.           16:19:161.         151:161.           16:19:161.         151:161.	B-SB:Sf) or w Protocol 802.11 d. 902.11 1. 902.11 1. 902.11 1. 902.11 1. 902.11 1. 902.11 1. 902.11 d. 902.11 d. 902.11 d. 802.11 1. 902.11 d. 802.11 1. 902.11 d. 802.11 1. 802.11	An f. type pu Length On 168 76 76 284 76 284 76 275 76 221 76 221 76 221 76 221 76 227 76 227 76 227 76 237 76 76 237 76 76 76 76 76 76 76 76 76 76 76 76 76	bbype         ==         0x000           arrel         Signal str           51         -136 dills           51         -166 dills           51         -166 dills           51         -166 dills           51         -156 dills           51         -55 dills           52         -55 dills           51         -55 dills           51         -72 dills           51         -74 dills           51         -74 dills           53         -74 dills           51         -74 dills           51<-747 dills	<pre>d     to     rob Request, Sun209, Flueb, FlagsC, SSID=Nildcard (Breadcast)     Actonicagement, FlagsC     Actonicagement, FlagsC     Acconicagement, FlagsC     Association Reports, Sun29, FlagsC     Association Reports, Sun29, FlagsC     Association Reports, Sun29, FlagsC     Association Report, FlagsC     Association Report, FlagsC     Association Report, FlagsC     Association Report, Sun29, FlagsC     Association Report, FlagsC     Association Report, FlagsC     Association Report, FlagsC     Action.jossed, Flagse, Flags</pre>	> Frame 11: 46 bytes on wire (TAB bits), Ho bytes (aphored (TAB bits) on interface Unvice/byt_(DAT2085-2008-AASE-4C3)-CA0166ALMAG), > Itherent Trobocol werlaw (A, Src: 392.166.1.55, Dat: 392.166.1.51) > Interent Trobocol werlaw (A, Src: 392.166.1.55, Dat: 392.166.1.51) > User Datagram Protocol, Src Cort: SSM, Of the Tori SBMD > Marchenk/Mmilterk respuisited IEEE B02.11 > B02.1 Engementers() (B) (B)(1) > B02.1 Authoritication (B)(1) > B02.1 Authoritication (B)(1) > Horizon (B
[class.basd == 0.0         Tene           2         -0.49135         -0.49135           3         0.10016         -0.1016           1         0.10016         -0.1016           1         0.10016         -0.1016           1         0.10075         -0.1016           1         0.10076         -0.1016           1         0.10076         -0.10096           2         0.10076         -0.10096           2         0.10076         -0.10096           2         0.10016         -0.10096           2         0.10016         -0.10097           2         0.10016         -0.10097           2         0.10016         -0.10097           2         0.10016         -0.10097           2         0.10016         -0.10097           2         0.10016         -0.10097           2         0.10016         -0.10097           2         0.10016         -0.10097           2         0.10016         -0.10097           2         0.10016         -0.10097           2         0.10016         -0.10097           2         0.10016         -0.10097	Definition         Telestory         Telestory           0         Delas         Source           0         0.00000         TeleIco           0         0.000000         TeleIco           0         0.000000         TeleIco           0.0000000         TeleIco         0.000000           0.00000000         Te	n. add * * 28:00.35: Dethnason 98:58: medicat 99:59: medica	8:53:07) or w Protocol 802.11 0:02.1	An fc type au Length On 168 96 76 76 76 76 76 76 93 76 93 76 221 76 227 76 227 76 227 76 76 199 76 183 76 183 76	bbppe         == 0x00;           armel         Soyal st           53         -34 dim           53         -34 dim           53         -36 dim           53         -35 dim           53         -35 dim           53         -35 dim           53         -42 dim           53         -35 dim           53         -47 dim           54         -47 dim           55         -47 dim           54         -47 dim           54         -47 dim           54         -47 dim <td>d Sofo Proce Reports, Society, Fuely, FlagsC, SSIDwalldcard (Broadcast) Arbonidgment, FlagsC Arbonidgment, FlagsC Kay (Harbar 10, Harbonic) Kay (Harbar 10, Harbar 10, Harba</td> <td>&gt; Frame 11: 46 bytes on wire (TAB bits), M bytes cabined (TAB bits) on interface Unrice/wr_(DeXTMBS-2988-AAGE-GC3-CA4146A1A8E), &gt; Itterret Trobock write (TAB bits), M bytes cabined (TAB bits) on interface Unrice/wr_(DeXTMBS-2988-AAGE-GC3-CA4146A1A8E), &gt; Interret Trobock write (TAB bits), A bit 192.161.151 &gt; Unre Datamar Protock, Src 197.161.153, Dit1 192.161.151 &gt; Unre Datamar Protock, Src 197.161.153, Dit1 192.161.151 &gt; Unre Datamar Datamar Datamar (TAB bits), A bit 192.161.151 &gt; Unre Datamar (Datamar Datamar Datamar</td>	d Sofo Proce Reports, Society, Fuely, FlagsC, SSIDwalldcard (Broadcast) Arbonidgment, FlagsC Arbonidgment, FlagsC Kay (Harbar 10, Harbonic) Kay (Harbar 10, Harbar 10, Harba	> Frame 11: 46 bytes on wire (TAB bits), M bytes cabined (TAB bits) on interface Unrice/wr_(DeXTMBS-2988-AAGE-GC3-CA4146A1A8E), > Itterret Trobock write (TAB bits), M bytes cabined (TAB bits) on interface Unrice/wr_(DeXTMBS-2988-AAGE-GC3-CA4146A1A8E), > Interret Trobock write (TAB bits), A bit 192.161.151 > Unre Datamar Protock, Src 197.161.153, Dit1 192.161.151 > Unre Datamar Protock, Src 197.161.153, Dit1 192.161.151 > Unre Datamar Datamar Datamar (TAB bits), A bit 192.161.151 > Unre Datamar (Datamar Datamar

Then, a 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:

Cisco Cataly	yst 9800	0-CL Wireless (	òn	troller			Welcome a	admin	* * 4		0 0 0 0	Search APs and Cl	onts Q	edback 🖌
Q. Search Menu Items	Monitoring * > Wireless * > Clients													×
	Clients Sleeping Clients Excluded Clients							General	QOS Statis	tics	ATF Statistics	Mobility History	Call Statistics	
Dashboard								ies Al	P Properties	Securi	ity Information	Client Statistics	QOS Properties	EoGRE
Monitoring >	× Delete						Client State S	Servers			None			
Configuration	Selected 0 out of 12 Clients						Client ACLs Client Entry C	Create Time			None 43 seconds			
	Ο	Client MAC Address	Ŧ	IPv4 Address	IPv6 Address	AP Name	Policy Type	JIEGUE TIIN			WPA3			
Administration	0	286b.3598.580f	×	192.168.1.159	fe80::ac5b:e1e1:67ba:c353	AP6849.9253.CA50	Encryption Ci				CCMP (AES)			
C Licensing	0	60fb.008b.0e66	×	N/A	N/A	AP01_RC_9136_F80C	Authentication EAP Type	in Key Man	agement		OWE Not Applicable			
	Ο	34ea.e702.6240	۶	192.168.1.70	N/A	AP6849.9253.CA50	Session Time	nout.			Not Applicable 86400			

### NetGear A8000

Connection OTA with focus on the RSN information from client:

No.         Tech         Outo         Source         Prime LBM 1: Constraints         P	
93       2019       0.00002       1019       10	
131       2013       2014       121       2014       2014 </td <td>68.1.121</td>	68.1.121
01       02	
30       30 <td< td=""><td></td></td<>	
0.000       0.00000       0.00000       0.00000	
1844 827.4-12 14-8194-84.818       0.00000 192.141.13       192.141.13 <td></td>	
1015       2013-01.1       1013-01.01	
1013       2013	
1393       2019	
1928       2019-02.1 1401016.049475       0.000000 1521.01.1.1       192.181.1.12 <td></td>	
1041 2021-0-12 1400100,71001 0, 0.31000 bttgstg-starter       96       5.1.0 dtt Athenticities(s), 5.0.0 (start, start, s	
1915 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 000000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 00000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 00000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 00000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 00000 1012, 01110:11       1912 201-4:11 (1010):71401 4, 00000 1014, 01110:11       1912 201-4:11 (1010):71401 4, 00000 1014, 01110:11       1912 201-4:11 (1010):71401 4, 00000 1014, 01110:11       1912 201-4:11 (1010):71401 4, 00000 1014, 01110:11       1912 201-11:11       1912 201-11:11       1912 201-11:11       1912 201-11:11       1912 201-11:11       1912 201-11:11       1912 201-11:11       1912 201-11:11       1912 201-11:11       1912 201-11:11       1912 201-11:11       1912 201-11:11       1912 201-11:11       1912 201-11:11	48, 54, [Mbit/sec]
104       2014	
1917 2017-012 1010100.72441 0.00000 1912(0-113)       1913.101.112 102.11       76       5 -80 dB       Achonoleggeent f, fags	
1993 201-0-12 14981887.20144 6.00073 NETAger_417-929 Cisc_1189.1       200       5 -14 GM ANDROLOGING TABLES, Non-C         1994 201-0-12 14981887.20144 6.00073 NETAger_417-919 Cisc_1189.1       201       5 -14 GM ANDROLOGING TABLES, Non-C         1994 201-0-12 14981887.20144 6.00073 NETAger_417-919 Cisc_1189.1       215       5 -14 GM ANDROLOGING TABLES, Non-C         1994 201-0-12 14981887.20145 6.00073 NETAGER_417.1       215       5 -14 GM ANDROLOGING TABLES, Non-C       191         1994 201-0-12 14981887.20145 6.00073 NETAGER_417.1       215       5 -14 GM ANDROLOGING TABLES, Non-C       191 <td></td>	
1040       201-04-121       10-081087.20144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.000000       12-08108.7.12144       0.0000000       12-08108.7.12144       0.0000000       12-08108.7.12144       0.0000000       12-08108.7.12144       0.000000000000       12-08108.7.12144       0.00000000000000000000000000000000000	
1944       221-46-11       14103106.773039       0.00236       theraper_stress 0.042 bits (2010)       114       5 -16 dim       114       5 -16 dim       114       5 -16 dim       114 <td>rmation Element</td>	rmation Element
1845 2201-40:11 14001067,73318 4, 000000 512:16:1.13       291 5 -3 6 008 Association Response, Such, Fine, Filags	
144       201-44       21.481/281       21.281/1.21       102.146	
1847 2021-0-12 140101067,79484         6.000001         114         536 dim K r (Distage 167 4)         114	
1000 3201-0-12 14031001,77339 0.00795 0.00795 0.00795 0.00795 0.00795 0.00795 0.0075 0.00110.0011 0.001100000000	
1968       2010-01       1961       2010-01	(H)
1951 2021-0-12 1401808_1741242 0.000000 bttgstgs_417:PS (155,11081, L405), 222 5 5.3 GBM (Eq. (Postage 2 of 4).       > Palroist (120er Soilt List 00:017240, Langest List 00:01744,	
1842 2023-4-12 1482188,74842 8,00000 102,1161,13       122,181,132       120,111,13       121,111,138,,       144 2023,141,1344       144 2023,141,134       144 20	AES (CCH)
1953       2013-0-12       1910/1917.11314       6.000000       (1000)       295       560       67 (Descing)       67 41       ) Act Kay Management (ANO)       ) Act Kay Management (ANO)         1965       2013-0-12       1910/1917.11314       6.000000       (1000)       295       560       67 (Descing)       67 41       ) Act Kay Management (ANO)       ) Act Kay Manageme	
066         0253-04-12         04140128-013324         0.00000         025         0.0000         025         0.000000         025         0.0000000	2.11) Opportunistic Wireless Encryption
1995 8220-612 14921087/3314 0.000000 Https://stars.in.c.         95 300 M.AndRetzgeney/, right	
Dist         Dist         S - 40 dis         Acconsidegrater, Trages	
1000 32100012 (100100017)1141 (N000000 321:11113 (10011111) 100:111 (1001111) 100       100 32100012(100101111) 100       1001 3210012(100101111) 100       1001 3210012(100101111) 100       1001 3210012(100101111) 100       1001 3210012(100101111) 100       1001 3210012(100101111) 100       1001 3210012(100101111) 100       1001 3210012(1001011111) 100       1001 3210012(100101111) 100       1001 3210011111111       1001 32100111111111111111111111111111111	
165 201-0-12 101081/17141 8.00000 122.101.13 102.141.121 80.11 12 5 5 -0 08 47000000000000 (1000000000000000000000000	
1002 2021-00-12 14(0):00:770-01 0.000000 12:100.11.13 10:101.11.11 00:11.1 10 5 -3 -3000 ACCMINGTOR (10):000000 12:100.11.10 00:11 10:00000 12:100.11.11 00:0000 12:10000 12:10000 12:10000 12:10000 12:10000 12:10000 12:10000 12:10000 12:10000 12:10000 12:10000 12:10000 12:10000 12:10000 12:10000 12:100000 12:100000 12:1000000 12:1000000 12:10000000 12:10000000000	
1057 2023-00-12 141031001737401 VIOD0000 17210011115 17210011112 002111 117 5 40 000 112ggr 00110 31003 NEDVIL 1011 (0597); Fidgs+1111114	
1101 2023-06-12 14:03:00.00000 0.001495 NETGRO_GRIVE195 1PV0RCB1_16 LLC 227 5 -61 000 1, N(X)+49, N(3)+75, USAP PROMAT (14C955) ACTIVE STBLIDT LLST MAINTENB	
1202 2023-06-12 14:03:00.00000 192.160.1.12 002.11 /6 5 -43 000 ACKNOWLOOGDENT, Figgs	
1104 2023-06-12 14:03:00.00000 192.100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (1222100.1.121 002.11 119 5 -42 000 (122200.11 119 5 -42 000 (12200.11 119 5 -42 000) (12200.11 119 5 -42 000) (12200.11 119 5 -42 000) (12200.11 119 5 -42 000) (12200.11 119 5 -42 000) (12200.11 119 5 -42 000) (12200.11 119 5 -42 0000) (12	
1126 2023-06-12 14:03:00.809249 0.000806 192.168.1.15 192.168.1.15 192.168.1.12 002.11 76 5 -42 08m Acknowledgement; FlagsC	
1130 2022-06-12 14:03:00.809249 0.000000 Netgear_48:70:95 Broadcast LLC 444 5 -56 dBm U P, funcFRM: DSAP 0x16 Command	
1131 2022-06-12 14:03:08.89249 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -42 dBm Acknowledgement; FlagsC	
1132 2023-06-12 14:03:08.889249 0.000000 Netgear_48:70:95 IPvGecast_01_ LLC 195 5 -37 dBm I, N(8)+115, N(5)+49; DSAP 0x24 Response	
1135 2023-06-12 14:03:00.090025 0.001576 Netger 40:70:95 Broadcest LLC 442 5 -36 dBm I P, N(8)+118, N(5)+104; DSAP 0x04 Response 0 = Beacon Heasurement Reporting Con	Ations: Disabled
1143 2023-06-12 14/03/08.917921 0.027096 Netgear 48:70:95 IPvGncast 01. LLC 305 5 -61 dBm U F, func-Unknown; DSAP 0xcc Individual, SSAP 0xcc Individual, S	
1144 2023-06-12 14:03:08.917921 0.000000 192.168.1.15 192.168.1.121 802.11 76 5.41 dBm Acknowledgement, FlagsC	
1146 2023-06-12 14:01:08.017921 0.000000 Netrear 48:70:05 IPvincast 01 LLC 268 5 -17 dBm I. N(8)+66. N(5)+58: DSAP ETA 85-511 Hanufacturing Message Service Ind > RM Capabilities: 0x00 (octet 4)	
1148 2023-06-12 14-03:00.921977 0.004056 (isco_11:00:e7 Netgeer_40:7_002.11 118 5 -36 00m Action, SN=1, FN=0, Flagis.pC	
1149 2021-06-12 14:03:01.021977 0.000000 192.100.1.15 192.100.1.121 002.11 76 5-51 dlm Acknowledgement, FlatsC	

### Client details in WLC:

Cisco Catal	lyst 9800	0-CL Wireless (	Con	troller			Welcome admin   # 🖘 🏝 🖹 🏟 🔞 🗭 🎜 Isearch APs and Clients 🔍   ( EFeedback) 🖉 G				
Q. Search Menu Items	Monitori	ing • > Wireless •	> (	Clients			Client				
Dashboard	Clients	Sleeping Client	s	Excluded Client	s		360 View General QOS Statistics ATF Statistics Mobility History Call Statistics				
Monitoring >	×	Delete C					Client Properties         AP Properties         Security Information         Client Statistics         QOS Properties         EoGRE           Client State Servers         None         Other Servers         None         <				
Configuration	Select	ed 0 out of 11 Clients					Client ACLs None Client Entry Create Time 25 seconds				
0	0	Client MAC Address	Ŧ	IPv4 Address	IPv6 Address	AP Name	Policy Type WPA3				
O Administration	0	9418.6548.7095	×	192.168.1.163	fe80::ce19:6f16:279d:515f	AP6849.9253.CA50	Encryption Cipher CCMP (AES)				
C Licensing	0	60fb.008b.0e66	×	192.168.1.155	N/A	AP04_OutdoorF_3DC8	Authentication Key Management OWE EAP Type Not Applicable				
-	0	34ea.e702.6240	×	192.168.1.70	N/A	AP6849.9253.CA50	Session Timeout 86400				
X Troubleshooting	0	a810.87bb.b833	×	192.168.1.94	fe80::aa10:87ff:febb:b833	AP03_Sotao_9548	Session Manager				

### Pixel 6a

Connection OTA with focus on the RSN information from client:

((peekremote) && (wlan.addr == 24	95:2f:72:8a:66) )    (vlan.fc.type_s	ubtype == 0x001d)					X 🗆 🔹 +
Time	Delta Source	Destination	Protocol L	engti Channel	Signal stre	Info	> Frame 589: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\WFF_(04578905-2998-4
574 2023-06-12 15:53:27.5858	5 1.319752 Google 72:8a:66	Broadcast	802.11	204	5 -40 d8m	Probe Request, SN+1696, FN+0, Flags+C, SSID+"wif166_test"	Ethernet II, Src: Cisco_dd:7d:37 (00:df:1d:dd:7d:37), Dst: Universa_b7:cf:06 (00:3a:00:b7:cf:06)
583 2023-06-12 15:53:27.6939		Cisco 13:80:	802.11			Authentication, SN+1697, FN+0, Flags+C	> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
584 2023-06-12 15:53:27,6939		192.168.1.121	882.11			Acknowledgement, Flags+C	> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
587 2023-06-12 15:53:27.7256		Google_72:88.				Authentication, SN+116, FN+0, Flags+C	> AiroPeek/OmniPeek encapsulated IEEE 802.11
588 2023-06-12 15:53:27.7256		192,168,1,121				Acknowledgement, flagsC	> 802.11 radio information
589 2023-06-12 15:53:27,7265		Cisco_13:80:				Association Request, SN=1698, FN=0, Flags=C, SSID="wifi6E_test"	> IEEE 002.11 Association Request, Flags:C
590 2023-06-12 15:53:27.7265		192.168.1.121				Acknowledgement, FlagsC	✓ IEEE 802.11 wireless Hanagement
598 2023-06-12 15:53:27.7919		Google_72:8a_				Association Response, SNu0, FNu0, FlagsC	> fixed parameters (4 bytes)
599 2023-06-12 15:53:27.7919		192.168.1.121				Acknowledgement, FlagsC	✓ Tagged parameters (199 bytes)
600 2023-06-12 15:53:27.7941		Google_72:8a_				Key (Message 1 of 4)	> Tag: SSID parameter set: "wifi6E_test"
601 2023-06-12 15:53:27.7941		192.168.1.121				Acknowledgement, flags	> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Whit/sec]
604 2023-06-12 15:53:27.8321		Cisco_13:80:				Key (Message 2 of 4)	> Tag: Power Capability Min: -7, Max: 19
605 2023-06-12 15:53:27.8321		192.168.1.121				Acknowledgement, Flags=C	> Tag: Supported Channels
606 2023-06-12 15:53:27.8344		Google_72:8a.				Key (Message 3 of 4)	<ul> <li>Tag: RSN Information</li> </ul>
607 2023-06-12 15:53:27.8344		192.168.1.121				Acknowledgement, Flags+C	Tag Number: R5N Information (48)
							Tag length: 26
688 2023-06-12 15:53:27.8407		C15C0_13:80:_				Key (Message 4 of 4)	RSN Version: 1
689 2023-06-12 15:53:27.8407		192.168.1.121				Acknowledgement, flags+C	> Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CON)
	4 0.020191 CiscoHer_53:ca:50					I P, N(R)+17, N(S)+3; DSAP excc Group, SSAP exce Command	Pairwise Cipher Suite Count: 1
612 2023-06-12 15:53:27.8609		192.168.1.121				Acknowledgement, FlagsC	> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) ASS (CCH)
613 2023-06-12 15:53:27.8609		192.168.1.121				Acknowledgement, FlagsC	At they Hangement (Ad) Saite Court: 1
614 2023-06-12 15:53:27.8641		192.168.1.121				Acknowledgement, flagsC	Auth Key Management (A00) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption
616 2023-06-12 15:53:27.8756		192.168.1.121				Acknowledgement, Flags=C	> Not carbinities: evene
617 2023-06-12 15:53:27.8821		192.168.1.121				Acknowledgement, Flags=C	Picit Countil 0
618 2023-06-12 15:53:27.8841		Cisco_13:80:_				Action, SN=1703, FN=0, Flags=.pC	PHED COUNCI @
619 2023-06-12 15:53:27.0041	3 0.000000 192.168.1.15	192.168.1.121	802.11			Acknowledgement, Flags+C	
623 2023-06-12 15:53:27.9334		Google_72:88.				Action, SN+1, FN+0, Flags+.pC[Malformed Packet]	> Group Hanagement Cipher Suite: 00:0f:ac (Ieee 802.11) 8IP (128)
624 2023-06-12 15:53:27.9334	1 0.000000 192.168.1.15	192.168.1.121	802.11			Acknowledgement, Flags+C	<ul> <li>Tag: RH Enabled Capabilities (5 octets)</li> </ul>
629 2023-06-12 15:53:28.0186	6 0.005205 Google_72:88:66	Cisco_13:80:_	802.11	115	5 -48 d8m	Action, SN=1704, FN=0, Flags=.pC	Tag Number: RH Enabled Capabilities (70)
630 2023-06-12 15:53:28.0186	6 0.000000 192.168.1.15	192.168.1.121	802.11	76	5 -36 dên	Acknowledgement, Flags=C	Tag length: 5
631 2023-06-12 15:53:28.0187	@ 0.000054 Google_72:88:66	IPv6mcast_ff	LLC	227	5 -55 dem	I, N(R)+37, N(S)+11; DSAP exec Individual, SSAP ex4a Command	<ul> <li>RH Capabilities: 0x73 (octet 1)</li> </ul>
632 2023-06-12 15:53:28.0188	4 0.000114 192.168.1.15	192.168.1.121	802.11	76	5 -46 dbm	Acknowledgement, Flags+C	1 = Link Heasurement: Enabled
634 2023-06-12 15:53:28.0209	7 0.002003 Cisco_13:00:e7	Google_72:88_	802.11	115	5 -37 dbm	Action, SN+2, FN+0, Flags+.pC	
635 2023-06-12 15:53:28.0209	7 0.000000 192.168.1.15	192.168.1.121	802.11	76	5 -48 d8m	Acknowledgement, Flags+C	
636 2023-06-12 15:53:28.0215	4 0.000627 192.168.1.15	192.168.1.121	802.11	86	5 -48 d8m	802.11 Block Ack Reg, Flags+C	0 = Repeated Measurements: Disabled
637 2023-06-12 15:53:28.0215	4 0.000000 192.168.1.15	192.168.1.121	802.11	94	5 -37 d8m	802.11 Block Ack, Flags+C	Beacon Passive Measurement: Enabled
638 2023-06-12 15:53:28.0266	6 0.005042 192.168.1.15	192.168.1.121	802.11	82	5 -55 dbm	Request-to-send, FlagsC	1 = Beacon Active Measurement: Enabled
639 2023-06-12 15:53:28.0266	6 0.000000 192.168.1.15	192.168.1.121	882.11	76	5 -46 dbm	Clear-to-send, FlagsC	.1 = Beacon Table Heasurement: Supported
640 2023-06-12 15:53:28.0266		192.168.1.121				802.11 Block Ack, Flags+C	e = Beacon Measurement Reporting Conditions: Disabled
652 2023-06-12 15:53:28.2066		Broadcast				I, N(R)=122, N(S)=124; DSAP @xSc Individual, SSAP @x9e Command	> RM Capabilities: 0x00 (octet 2)
653 2023-06-12 15:53:28.2066		192.168.1.121				Acknowledgement, FlagsC	MM Capabilities: 0x01 (octet 3)
657 2023-06-12 15:53:28.2416		Google_72:88.				Action, SN+3, FN+0, Flags+.pC	= AP Channel Report capability: Enabled
658 2023-06-12 15:53:28.2416		192.168.1.121				Acknowledgement, FlagsC	
659 2023-06-12 15:53:28.2419		Cisco_13:801				Action, SN+1705, FN+0, Flags+.pC[Malformed Packet]	0 00 = Operating Channel Max Measurement Duration: 0
660 2023-06-12 15:53:28.2419		192.168.1.121				Acknowledgement, FlagsC	000 = Nonoperating Channel Max Measurement Duration: 0
	2 0.001766 AlticeLa_9e:59:af					S, func+RNR, N(R)+85; DSAP 0x96 Individual, SSAP 0x9a Command	> RM Capabilities: 0x00 (octet 4)
662 2023-06-12 15:53:28.2437		192.168.1.121				502.11 Block Ack, FlagsC	> RM Capabilities: 0x00 (octet 5)
667 2023-06-12 15:53:28.3282		Cisco 13:00:				Action, SN+1706, FN+0, Flags+.pC[Malformed Packet: length of contained iter	> Tag: Supported Operating Classes
668 2023-06-12 15:53:28.3282		192.168.1.121				Action, Smalleb, Field, FlagsC	> Tag: Extended Capabilities (10 octets)
		Broadcast					> Ext Tes: HE Capabilities
669 2023-06-12 15:53:28.3282						I P, N(R)=19, N(S)=114; DSAP exce Individual, SSAP ex48 Command Acknowledgement, Flags=C	> Ext Tag: HE 6 GHZ Band Capabilities
670 2023-06-12 15:53:28.3283		192.168.1.121					> Ext Tag: OwE Diffle-Wellman Parameter
672 2023-06-12 15:53:28.3306		Google_72:8a_				Action, SN=4, FN=0, Flags=.pC[Malformed Packet]	> Tag: vendor Specific: Broadcom
673 2023-06-12 15:53:28.3306		192.168.1.121				Acknowledgement, Flags+C	> Tag: Vendor Specific: Hicrosoft Corp.: WHV/WHE: Information Element
674 2023-06-12 15:53:28.3309	7 0.000279 192.168.1.15	192.168.1.121	802.11	86	5 -49 dbm	802.11 Block Ack Reg, Flags+C	- test server operation compare compare and and and and and and

Client details in WLC:

Cisco Cat	alyst 9800	0-CL Wireless C	Conti	roller			Welcome admin   # 🕫 🛕 🖹 🏟 🔞 🗭 🕄 Search APs and Clients Q
Q. Search Menu Items	Monitori	ing • > Wireless • :	c	lients			Client
	Clients	Sleeping Clients		Excluded Client	s		360 View General QOS Statistics ATF Statistics Mobility History Call Statistics
Dashboard							Client Properties AP Properties Security Information Client Statistics QOS Properties EoGRE
Monitoring >		Deleto					Client State Servers None
N) Configuration	Select	ted 0 out of 13 Clients					Client ACLs None
Configuration	-		_	_			Client Entry Create Time 135 seconds
	0	Client MAC Address	Ŧ	IPv4 Address	IPv6 Address	AP Name	Policy Type WPA3
(c) Administration	0	2495.2172.8a66	×	192.168.1.162	fe80::b13:f107:7c5f:a7e0	AP6849.9253.CA50	Encryption Cipher CCMP (AES)
C Licensing	0	0429.2ec9.e371	×	192.168.1.160	fe80::6a20:34e8:ab1b:6332	AP6849.9253.CA50	Authentication Key Management OWE
Croning	ō	60fb.008b.0e66	×	N/A	N/A	AP01_RC_9136_F800	EAP Type Not Applicable
Y Troubleshooting	ō	34ea.e702.6240	×	192.168.1.70	N/A	AP6849.9253.CA50	Session Timeout 88400 Session Manager

### Samsung S23

la:

Connection OTA with focus on the RSN information from client:

peek	mote) && ((wian.addr == 04:29:	2e:c9:e3:71	)    (wian.fc.type_subt	ype == 0x001d))						2
¥0.	line	Delta	Source	Destination	Protocol	Lengt Channel	Sonal stre	Info		> Frame 2387: 388 bytes on wire (3184 bits), 388 bytes captured (3184 bits) on interface \Device\NFF_(D4578985-2998-446
2383	023-06-12 15:38:49.930966	0.419828	Sansunel c9:e3:71	Cisco 13:80:		96		Authentication, SN+2164, FN+0, Flags+C		Ethernet II, Srci Cisco_ddi7di37 (00:df:1d:ddi7di37), Osti Universa_b7:cf:06 (00:3a:00:07:cf:06)
	023-06-12 15:38:49,930966			192.168.1.121		76		Acknowledgement, Flags,C		> Internet Protocol Version 4, Src: 192.168.1.15, 0st: 192.168.1.121
	023-06-12 15:38:49,937354			Samsungt c91.		96		Authentication, SN+110, FN+0, Flags+C		> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
	023-06-12 15:38:49,937354			192,168,1,121		76		Acknowledgement, flagsC		> AiroPeek/OmniPeek encapsulated IEEE 802.11
	023-06-12 15:38:49.941841							Association Request, SN=2165, FN=0, Flags=C, SSID="wif166_test"		> 802.11 radio information
	023-06-12 15:38:49.941841			192.168.1.121		76		Acknowledgement, FlagsC		> IEEE 002.11 Association Request, Flags:C
	023-06-12 15:38:49.956542			SamsungE_c9:				Association Response, SN+0, FN+0, Flags+C		✓ IEEE 002.11 Wireless Management
	023-06-12 15:38:49.956542			192.168.1.121		76		Acknowledgement, Flags+C		> Fixed parameters (4 bytes)
	023-06-12 15:38:49.958831			SansungE_C91		221		Key (Nessage 1 of 4)		<ul> <li>Tagged parameters (294 bytes)</li> </ul>
	023-06-12 15:38:49.958831			192.168.1.121		76		Acknowledgement, Flags=C	1.1	> Tag: SSID parameter set: "wifies test"
	023-06-12 15:38:49.984449					227		Key (Nessage 2 of 4)		> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Mbit/Sec]
	023-06-12 15:38:49.984821			192.168.1.121		76		Acknowledgement, FlagsC		> Tag: Power Capability Min: 8, Max: 16
										> Tag: Supported Channels
	2023-06-12 15:38:49.985981			SamsungE_c91_		295		Key (Message 3 of 4)		<ul> <li>Tag: RSN Information</li> </ul>
	1023-06-12 15:38:49.985981			192.168.1.121		76		Acknowledgement, flags+C		Tag Number: RSN Information (48)
	1023-06-12 15:38:50.007376					199		Key (Message 4 of 4)		Tag length: 26
	1023-06-12 15:38:50.007376			192.168.1.121		76		Acknowledgement, Flags+C		Kin version: 1
	023-06-12 15:38:50.093619							Action, SNw2, FNw0, Flags+.pC[Halformed Packet: length of contained if		> Group Cipher Suite: 00:0f:ac (leee 002.11) AES (CCN)
	023-06-12 15:38:50.093619			192.168.1.121		76		Acknowledgement, Flags+C		Paire ciper Suite out: 1
	023-06-12 15:38:50.096046			Samsungt_c91_				Action, SN+1, FN+0, Flags+.pC		> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCH)
	1023-06-12 15:38:50.096046			192.168.1.121		76		Acknowledgement, flags=C		
	1023-06-12 15:38:50.101726					227		I, N(R)=54, N(S)=52; DSAP @xce Group, SSAP SNA Command		Auth Key Management (AKM) Suite Count: 1
2415	023-06-12 15:38:50.101726	0.000000	SamsungE_c9:e3:71	IPv6mcast_16	LLC	251	5 -59 d8m	I, N(R)=47, N(S)=43; DSAP @x6e Group, SSAP @xc0 Response		> Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Hireless Encryption
2416	023-06-12 15:38:50.101726	0.000000	192.168.1.15	192.168.1.121	802.11	110	5 -46 d8m	802.11 Block Ack, Flags+C		> KSN Capabilities: 0x00c0
2419	023-06-12 15:38:50.100529	0.006503	Sansungt_c9:e3:71	Broadcast	LLC	450	5 -46 dbm	U P, func+UI; DSAP ex3a Individual, SSAP exbe Command		PHKID Count: 0
2420	023-06-12 15:38:50.100529	0.000000	192.168.1.15	192.168.1.121	882.11	76	5 -37 d8m	Acknowledgement, #lags+C		PHKID List
2429	023-06-12 15:38:50.182652	0.074123	Cisco_13:80:e7	SansungE_c91	882.11	118	5 -37 d8m	Action, SN=2, FN=0, Flags=.pC[Halformed Packet]		> Group Hanagement Cipher Suite: 00:0f:ac (Ieee S02.11) SIP (128)
2430	023-06-12 15:38:50.182652	0.000000	192.168.1.15	192.168.1.121	802.11	76	5 -45 d8m	Acknowledgement, FlagsC		✓ Tag: RM Enabled Capabilities (5 octets)
2431	023-06-12 15:38:50.188281	0.005629	SamsungE c9:e3:71	Cisco 13:00:_	002.11	118	5 -46 d8m	Action, SN=2166, FN=0, Flags=.pC[Malformed Packet: length of contained		Tag Number: RM Enabled Capabilities (70)
2432	023-06-12 15:38:50.188586	0.000305	192.168.1.15	192.168.1.121	002.11	76	5 -37 dbm	Acknowledgement, Flags+C		Tag length: 5
2433	023-06-12 15:38:50.189704	0.001115	AlticeLa 9e:59:af	Sansungt (91	LLC	429	5 -47 d8m	U P, func-RESET; DSAP 0x46 Group, SSAP 0x6e Command		RH Capabilities: 0x73 (octet 1)
	023-06-12 15:38:50.189704			192.168.1.121		118		882.11 Block Ack, Flags+C		1 = Link Measurement: Enabled
	023-06-12 15:38:50.197365					446		S P. funcwRR, N(R)+17; DSAP PROWAY (IEC955) Active Station List Maintenance		
	023-06-12 15:38:50.197365			192.168.1.121		76	5 -37 d8m	Acknowledgement, Flagi+C		0 = Parallel Measurements: Oisabled
2441	023-06-12 15:38:50.239457	0.042092	AlticeLa Se:59:af	Samsungt co:-	LLC	459	5 -47 dbm	I. N(R)+54, N(S)+28; DSAP @x50 Group, SSAP @x84 Response		0 = Repeated Measurements: Disabled
	023-06-12 15:38:50.239457			192.168.1.121		118		802.11 Block Ack, Flags+C		
	023-06-12 15:38:50.248619					456		I P, N(R)=75, N(S)=42; DSAP Ungermann-Bass Group, SSAP PROMAY (IEC955) Netwo		* Beacon Active Measurement: Enabled
	023-06-12 15:38:50.248619			192.168.1.121		76		Acknowledgement, FlagsC		.1 = Beacon Table Measurement: Supported
	023-06-12 15:38:50.307062					459		S P, func+SRE3, N(R)+0; DSAP exce Group, SSAP exc2 Command		0 = Beacon Heasurement Reporting Conditions: Disabled
	023-06-12 15:38:50.307062			192.168.1.121		110		802.11 Block Ack, Flag1+C		> RH Capabilities: 0x10 (octet 2)
	023-06-12 15:38:50.344977					144		I, N(R)+9, N(S)+42; DSAP 0x46 Individual, SSAP 0x36 Response		✓ RH Capabilities: 0x91 (octet 3)
	023-06-12 15:38:50.344977			192.168.1.121		76		Acknowledgement, flagsC		1 = AP Channel Report capability: Enabled
	023-06-12 15:38:50.340061					197		I, N(R)=10, N(S)=37; DSAP @xie Individual, SSAP @x4a Response		
	023-06-12 15:38:50.340061			192.168.1.121		118		802.11 Block Ack, FlagtsC		1 00 = Operating Channel Max Measurement Duration: 4
	023-06-12 15:38:50.358349					219		I, N(R)+68, N(S)+77; DSAP @x1e Group, SSAP @xca Response		100 = Nonoperating Channel Max Measurement Duration: 4
				192.168.1.121						> RM Capabilities: 0x00 (octet 4)
	1023-06-12 15:38:50.350349					110		802.11 Block Ack, Flags+C		> RM Capabilities: 0x04 (octet 5)
	1023-06-12 15:38:50.358338							I, N(R)=67, N(S)=94; DSAP @x4a Group, SSAP @x6a Response		> Tag: Supported Operating Classes
	1023-06-12 15:38:50.358569			192.168.1.121		118		882.11 Block Ack, Flags+C		> Tag: Extended Cacabilities (11 octets)
	1023-06-12 15:38:50.374150					230		I P, N(R)+97, N(S)+23; DSAP PROMAY (IEC955) Active Station List Maintenance		> Ext Tag: wE Capabilities
	023-06-12 15:38:50.374150			192.168.1.121				802.11 Block Ack, Flags+C		> Ext Tag: HE 6 GH: Band Capabilities
	023-06-12 15:38:50.391157					242		S, func+SREJ, N(R)+12; DSAP exce Group, SSAP exde Command		> Ext Tag: OwE Diffie-Hellman Parameter
	023-06-12 15:38:50.391157			192.168.1.121		118		802.11 Block Ack, Flags+C		> tag: Vendor Specific: Qualcomm Inc.
	023-06-12 15:38:50.391157					215		U, func+XID; DSAP @x40 Group, SSAP @x1e Response		
	023-06-12 15:38:50.391157			192.168.1.121				882.11 Block Ack, Flags=C		> Tag: Vendor Specific: Samsung Electronics Co.,Ltd
	023-06-12 15:38:50.391157	0.000000	SansungE c9:e3:71	AlticeLa Se:_	LLC	217	5 -58 d8m	U, func+Unknown; DSAP exic Group, SSAP exi2 Response		> Tag: Vendor Specific: Samsung Electronics Co.,Ltd
	023-06-12 15:38:50.391157			192.168.1.121		110		802.11 Block Ack, FlagsC		

### Client details in WLC:

Cisco Cat	alyst 9800-CL Wireless Controller	Welcome admin   🔗 🎨 🏝 🖹 🏟 🔞 🕢 🌫 Search APs and Clients 🔍   (#Feedback) 🖍 🕪
Q. Search Menu Items	Monitoring * > Wireless * > Clients	Client *
Dashboard	Clients Sleeping Clients Excluded Clients	360 View General QOS Statistics ATF Statistics Mobility History Call Statistics
Dashooard		Client Properties AP Properties Security Information Client Statistics QOS Properties EoGRE
Monitoring >	× Decess O	Client State Servers None
ے کر Configuration	Selected 0 out of 13 Clients	Client ACLs None
S coninguration		
(O) Administration		Energine Coher COND (AES)
~~	0 0012.17e1.dd57 / 192.168.1.33 fe80::212:17ff:fee1:dd57 AP03_Sotao_9548	
C Licensing	0 0012.17e2.4856 / 192.168.1.37 fe80::212:17ff.fee2:4856 AP05_Outdoor8_2	20
	0012.17e2.4b40 🖌 192.168.1.31 fe80::212:17ff:fee2:4b40 AP04_OutdoorF_3	
X Troubleshooting	O 0429.2ec9.e371 ≠ 192.168.1.160 fe80::6a20:34e8:ab1b:6332 AP6849.9253.CA5	
	Clients       Clients       Clients       Clients       Clients       Clients       Clients       APP roperties       APT ropertroperties       APT roperties	

### WPA3 - AES(CCPM128) + OWE with Transition Mode

Detailed configuration and troubleshooting of OWE Transition Mode available in this document: <u>Configure</u> <u>Enhanced Open SSID with Transition Mode - OWE</u>.

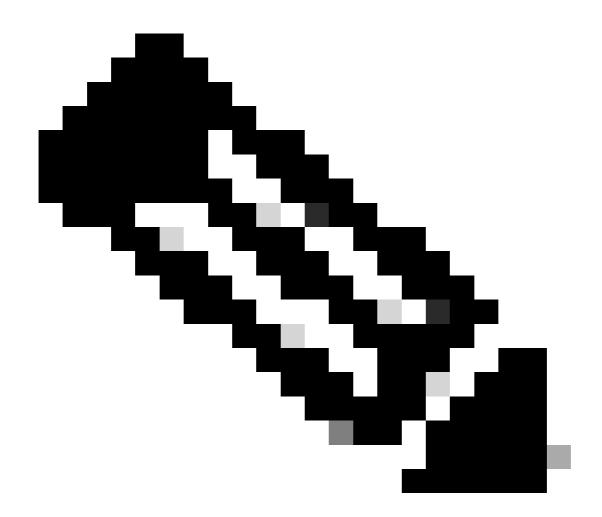
### WPA3-Personal - AES(CCMP128) + SAE

WLAN Security configuration:

### Edit WLAN

eral Security	Advanced Add To	Policy Tags		
er2 Layer3	АЛА			
O WPA + WPA2	O WPA2 + WPA3	WPA3	O Static WEP	O None
MAC Filtering	0			
Lobby Admin Acce	ss O			
NPA Parameters		Fast	Transition	
WPA O	WPA2 O	Stat	US .	Disabled •
GTX O	WPA3	Ove	r the DS	0
Randomize Transition	Policy	Data	speciation Timeout *	20
Disable				
MPAZ/WPA3 Encr	yption	Auth	Key Mont	
AES(CCMP128)	CCMP256		Key Mgmt	FT + SAE 0
	CCMP256	5		FT + SAE 0 FT + 802.1x 0
AES(CCMP128) GCMP128	CCMP256 C	S	AC 🖸	
AES(CCMP128) GCMP128	CCMP256 C GCMP256 C GCMP25	S S	AE 0 WE 0	
AES(CCMP128) GCMP128	CCMP256 C	• A	AE O WE O 12.1x* O HA256 nti Clogging Threshold*	FT - 802.1x 0
AES(CCMP128) GCMP128	CCMP256 C GCMP256 C	• A	AE 0 WE 0 12.1x- 0 HA256	FT - 802.1x 0
AES(CCMP128) C GCMP128 C Protected Manage PMF Association Comeb	CCMP256 C GCMP256 C	• A	AE O WE O 12.1x* O HA256 nti Clogging Threshold*	FT - 802.1x 0
AES(CCMP128) C GCMP128 C Protected Manage PMF Association Comeb	CCMP256 C GCMP256 C ment Frame Required ack Timer* 1	• A	AE O WE O 02.1x* HA255 nti Clogging Threshold* iax Retries*	FT - 802.1x 0
AES(CCMP128) C GCMP128 C Protected Manage PMF Association Comeb	CCMP256 C GCMP256 C ment Frame Required ack Timer* 1	- A - A - A - A - A - A - A - A	AE O WE O 02.1x- O HA256 nti Clogging Threshold* iax Retries* stransmit Timeout*	FT - 802.1x 0
GCMP128 C Protected Manage PMF	CCMP256 C GCMP256 C ment Frame Required ack Timer* 1	• N • N • N • N • N • N • N • N	AE O WE O 12:1x* O HA256 nti Clogging Threshold* lax Retries* stransmit Timeout*	FT - 802.1x 0

WPA3 SAE Configuration



**Note**: 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.

wifi6E\_test

[WPA3][SAE][AES]

View on WLC GUI of the WLAN Security settings:

5

O O wifi6E\_test

Verification of beacons OTA:

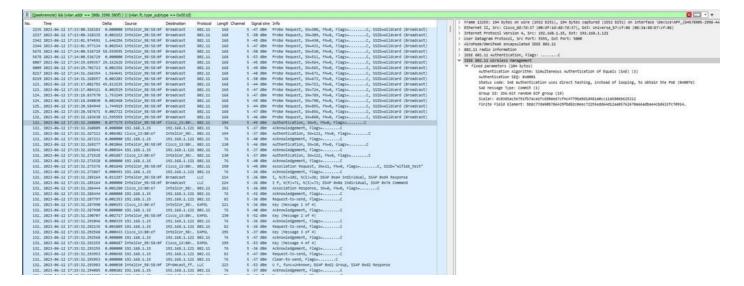
					> Frame 6: 500 bytes on wire (4064 bits), 500 bytes captured (4064 bits) on interface \Device\NFF (D4578905-2998-4456-
No. Time Delta Source			ingti Channel Signal stre		> Frame a: Sea bytes on wire (weaw bits), Sea bytes captured (weaw bits) on interface (device(wes_lows/seas-interface)) athermet II, Sec: Clsco.dd(7d(37) (00)df(1d(dd(7d(37), Dst) universa.b7)cf(00) (00)3a(0):b7(cf(00)))
2 2023-06-12 17:12:24.650110 0.000000 Cisco_13:80:ed				Probe Response, SN+717, FN+0, Flags+C, BI+100, SSID+"Wif160_test_02", SS	2 Internet Protocol version 4, Src 132,166,1,15, Ost 132,166,1,121
4 2023-06-12 17:12:24.670646 0.020536 Cisco_13:00:ed				Probe Response, SN=718, FN=0, Flags=C, #1=100, SSID="wif166_test_02", SS	) user Datagram Protocol, Src Port: 5555, Dst Port: 5000
\$ 2023-06-12 17:12:24.691121 0.020475 Cisco_13:80:ed				Probe Response, SN+719, FN+0, Flags+C, #I+100, SSID+"wif16E_test_02", SS	> VSEr Untegrem Protocus, Src Parti SSSS, USC Parti Seve > AiroPeek/OmniPeek encapsulated IEEE 802.11
6 2023-06-12 17:12:24.711672 0.020551 Cisco_13:80:ed				Beacon frame, SN+720, FN+0, Flags+C, HI+100, SSID+"wif168_test_02", SSID	> Abroneek. Unipresk encapsulated least sec.11 > 882.11 radio information
7 2023-06-12 17:12:24.732106 0.020434 Clsco_13:00:ed				Probe Response, SN#721, FN#0, Flags*C, BI+100, SSID="wifi68_test_02", SS	
10 2023-06-12 17:12:24.752541 0.020435 Cisco_13:00:ed				Probe Response, SN+722, FN+0, Flags+C, 81+100, SSID+"wif168_test_02", SS	> IEEE 802-11 Beacon frame, Flags:C
11 2023-06-12 17:12:24.773081 0.020540 Cisco_13:80:ed				Probe Response, SN+723, FN+0, Flags+C, B1+100, SSID+"wifi68_test_02", SS	V IEE D02.11 Mireless Management
13 2023-06-12 17:12:24.793509 0.020428 Cisco_13:00:ed	Broadcast 4	102.11	461 5 -37 dêm	Probe Response, SN=724, FN=0, Flags=C, 81=100, SSID="wifi66_test_02", SS	> Fixed parameters (12 bytes)
14 2023-06-12 17:12:24.814002 0.020493 Clsco_13:80:ed	Broadcast 1	102.11	500 5 -36 d8m	Beacon frame, SN+725, FN+0, Flags+C, 82+500, SSID+"Hifi6E_test_02", SSID	<ul> <li>Tagged parameters (406 bytes)</li> </ul>
15 2023-06-12 17:12:24.034577 0.020575 Cisco_13:80:ed	Broadcast 1	102.11	461 5 -36 d0m	Probe Response, SN=726, FN=0, Flags=C, B1=100, SSID="wifi66_test_02", SS	> Tag: SSID parameter set: "wifiet_test_02"
16 2023-06-12 17:12:24.055069 0.020492 Clico_13:00:ed	Broadcast B	102.11	461 5 -36 dBm	Probe Response, SN=727, FN=0, Flags=C, 81=100, SSID="wifi60_test_02", 55	> Tag: Supported Rates 6(0), 9, 12(0), 10, 24(0), 36, 40, 54, [MDit/sec]
17 2023-06-12 17:12:24.875470 0.020401 Cisco_13:80:ed	Broadcast I	102.11	461 5 -36 dbm	Probe Response, SN+728, FN+8, Flags+C, 81+100, SSID+"wifi68_test_02", SS	> Tag: Traffic Indication Map (TIM): OTIM 2 of 3 bitmap
18 2023-06-12 17:12:24.895829 0.020359 Cisco_13:80:ed	Broadcast 1	102.33		Probe Response, SN+729, FN+0, Flags+C, 81+100, SSID+"wif16E_test_02", SS	> Tag: Country Information: Country Code na, Environment Global operating classes
19 2023-06-12 17:12:24.916558 0.020729 Cisco_13:80:ed	Broadcast 1	102.11	588 5 -36 d8m	Beacon frame, SN+730, FN+0, Flags+C, 81+300, SSID+"x1F16E_test_02", SSID	> Tag: Power Constraint: 6
20 2023-06-12 17:12:24.937923 0.021365 Cisco_13:00:ed	Broadcast 8	102.11		Probe Response, SN#731, FN#0, Flags#C, 81+100, SSID#"wif166_test_02", SS	> Tag: TPC Report Transmit Power: 17, Link Hargin: 0
21 2023-06-12 17:12:24.969625 0.001702 Cisco_13:00:ed	Broadcast 1	102.11		Probe Response, SN#732, FN#0, Flags=C, BI=100, SSID="wifi6E_test_02", SS	✓ Tag: RSN Information
22 2023-06-12 17:12:24.998372 0.028747 Cisco_13:80:ed				Probe Response, SN+734, FN+0, Flags+C, #I+100, SSID+"wifi68_test_02", SS	Tag Number: RSN Information (48)
23 2023-06-12 17:12:25.018811 0.020439 Cisco_13:80:ed				Beacon frame, SN#735, FN#0, Flags*C, BI#100, SSID#"wifi68_test_02", SSID	Tag length: 26
24 2023-06-12 17:12:25.039348 0.020537 Cisco 13:80:ed				Probe Response, SN+736, FN+0, Flags+C, BI+100, SSID+"wifi6E_test_02", 55	RSN Version: 1
25 2023-06-12 17:12:25.059012 0.020464 Cisco_13:00:ed				Probe Response, SN=737, FN=0, Flags=C, 81=100, SSID="wif160_test_02", SS	> Group Cipher Suite: 00:0fiac (Ieee 802.11) A45 (CDM)
26 2023-86-12 17:12:25.008400 0.020588 Cisco_13:80:ed				Probe Response, SN=730, FN=0, Flags=C, 8I=100, SSID="wifi6E_test_02", SS	Pairwise Cipher Suite Count: 1
27 2023-06-12 17:12:25.100854 0.020484 Cisco 13:80:ed				Probe Response, Sha739, Flags	> Pairwise Cipher Suite List 00:0fiac (leve 802.11) A65 (CCN)
28 2823-66-12 17:12:25.121559 0.020675 Cisco_13:00:ed				Bescon frame, SN+740, FN+0, Flags+C, BI+100, SSID+"xifi6E_test_02", SSID	Auth Key Management (AKH) Suite Count: 1
31 2023-06-12 17:12:25.141678 0.020119 Clisco 13:00:ed				Probe Response, SNo741, Fineb, Flags+C. BI+100, SSID+"wifi6E test 02", SS	> Auth Key Management (AUH) List 00:0f:ac (Zeee 802.11) SAE (SHA256)
				Probe Response, SNx742, FNx0, FlagsC, B1x100, SSIDx "HT164_CEST_02", SS Probe Response, SNx742, FNx0, FlagsC, B1x100, SSIDx"Hif166_test_02", SS	> RSN Capabilities: dw00ed
34 2023-06-12 17:12:25.162724 0.021046 Cisco_13:00:ed 35 2023-06-12 17:12:25.182664 0.019940 Cisco_13:80:ed				Probe Response, SN=743, FN=0, Flags=	PHOD Count: 0
				Probe Response, Shu744, Phu8, Flagsw	PKID List
37 2023-06-12 17:12:25.203081 0.020417 Cisco_13:80:ed					> Group Management Cipter Suite: 00:0fiac (Ieee 802.11) 82P (128)
38 2023-06-12 17:12:25.223702 0.020621 Cisco_13:80:ed				Beacon frame, SN+745, FN+0, Flags+C, HI+100, SSID+"W1f16E_test_02", SSID	> Tag: QBSS Load Element 882.11e CCA Version
39 2023-06-12 17:12:25.244147 0.020445 Cisco_13:00:ed				Probe Response, SNx746, FNx0, FlagsC, BIx100, SSIDx"wifi6E_test_02", SS	> Tag: Multiple #SSID
40 2023-06-12 17:12:25.264534 0.020307 Cisco_13:00:ed				Probe Response, SN+747, FN+0, Flags+C, BI+100, SSID+"wifi68_test_02", SS	> Tag: RH Erabled Capabilities (5 octets)
41 2023-06-12 17:12:25.205014 0.020400 Cisco_13:00:ed				Probe Response, SN+740, FN+0, Flags+C, 01+100, SSID+"wifi60_test_02", SS	> Tag: Extended Capabilities (11 octets)
42 2023-06-12 17:12:25.305513 0.020499 Cisco_13:00:0d				Probe Response, 5%x749, F%x8, FlagsxC, 81x100, 551Dx*wif166_test_02*, 55	> Ter: Tx Power Envelope
44 2023-06-12 17:12:25.326072 0.020559 Cisco_13:00:ed				Beacon frame, SN=750, FN=0, Flags=C, Bl=100, SSID="Hifi6E_test_02", SSID	> Teal TX Power Envelope
45 2023-06-12 17:12:25.346502 0.020430 Clsco_13:00:ed				Probe Response, SN=751, FN=0, Flags=C, 81=100, SSID="wif166_test_02", SS	> Ext Tag: Aultiple BSSID Configuration
46 2023-06-12 17:12:25.367033 0.020531 Cisco_13:00:ed				Probe Response, SN=752, FN=0, Flags=C, HI=100, SSID="wifi6E_test_02", SS	> Ext Tag: Hel Capabilities
47 2023-06-12 17:12:25.387452 0.020419 Cisco_13:80:ed				Probe Response, Shu753, FNu0, Flags+C, #I+100, SSID+"wifi6E_test_02", SS	> Ext Tag: re conversion
48 2023-06-12 17:12:25.407950 0.020498 Cisco_13:80:ed				Probe Response, SN+754, FN+0, Flags+C, 81+100, SSID+"wifi66_test_02", SS	> Ext Tag: To Spatial Route Parameter Set
49 2023-06-12 17:12:25.428554 0.020604 Clsco_13:00:ed				Beacon frame, SN+755, FN+0, Flags+C, BI+100, SSID+"Hifi6E_test_02", SSID	> Ext Tag: NU EDCA Parameter Set
50 2023-06-12 17:12:25.449029 0.020475 Cisco_13:00:ed				Probe Response, SN+756, FN+0, Flags+C, 81+100, SSID+"wif166_test_02", SS	> Ext Tag: HE 6 GK1 Band Capabilities
51 2023-06-12 17:12:25.469415 0.020306 Clsco_13:00:ed				Probe Response, SN+757, FN+0, Flags+C, #I+100, SSID+"wifi6E_test_02", SS	v Tagi RSV extension (1 octet)
52 2023-06-12 17:12:25.489890 0.020475 Clsco_13:80:ed				Probe Response, SNx758, FNx0, Flags+C, 81+100, SSID+"wif166_test_02", SS	
53 2023-06-12 17:12:25.510333 0.020443 Cisco_13:00:ed				Probe Response, SNx759, FNx0, Flags+C, 81x100, SSID+"wifi66_test_02", SS	Teg Number: Kin extension (244)
54 2023-06-12 17:12:25.530937 0.020604 Cisco_13:00:ed				Beacon frame, SN+760, FN+0, Flags+C, BI+100, SSID+"wifi6E_test_02", SSID	Teg length: 1
55 2023-06-12 17:12:25.551260 0.020323 Cisco_13:80:ed	Broadcast I	102.11	461 5 -36 d8m	Probe Response, SN=761, FN=0, Flags=C, HI=100, SSID="wifi68_test_02", SS	<ul> <li>RSNX: 8x20 (octet 1)</li> </ul>
56 2023-06-12 17/12/25.571762 0.020502 Cisco_13:80:ed	Broadcast 1	102.11	461 5 -36 dBm	Probe Response, SNx762, FNx0, Flags+C, #1+100, SSID+"wifi6E_test_02", SS	0000 = RSNX Length: 0
57 2023-06-12 17:12:25.592295 0.020533 Clsco_13:00:ed	Broadcast 1	102.11	461 5 -36 dBm	Probe Response, SN+763, FN+0, Flags+C, #1+100, SSID+"wif166_test_02", SS	0 + Protected TwT Operations Support: 0
58 2023-06-12 17:12:25.612775 0.020400 Cisco_13:00:ed	Broadcast I	102.33	461 5 -36 d8m	Probe Response, SN+764, FN+0, Flags+C, BI+100, SSID+"wifi66_test_02", SS	= SAE wash to element: 1
59 2023-06-12 17:12:25.633372 0.020597 Cisco_13:80:ed	Broadcast I	102.11	548 5 -36 den	Beacon frame, SN+765, FN+0, Flags+C, 81+100, SSID+"wifi68_test_02", SSID	00., + Reserved: 0x0
62 2023-06-12 17:12:25.653036 0.020464 Cisco_13:00:ed	Broadcast I	102.11		Probe Response, SN#766, FN#8, Flags=C, #I=100, SSID="wifi66_test_02", SS	> Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
63 2023-06-12 17:12:25.674190 0.020362 Cisco_13:00:ed	proadcast 1	102.11		Probe Response, SN#767, FN#0, Flags#C, 81+100, SSID#"wifi68_test_02", SS	> Tag: Vendor Specific: Hicrosoft Corp.: WHVWHE: Parameter Element
64 2023-06-12 17:12:25.694585 0.020390 Cisco_13:00:ed	proadcast 1	102.11		Probe Response, SN+768, FN+8, Flags+C, 82+100, SSID+"wifi68_test_02", SS	> Tag: Vendor Specific: Cisco Systems, Inc: Aironet unknown (44)
65 2023-06-12 17:12:25.715057 0.020469 Cisco 13:00:ed			461 5 -36 d8m	Probe Response, 5%+769, F%+0, Flags+C, 81+100, 551D+"wifi60_test_02", 55	> Tag: Vendor Specific: Cisco Systems, Inc: Aironet unknown (11) (11)
66 2023-06-12 17:12:25.736219 0.021162 Clsco_13:80:ed				Beacon frame, SN=778, FN=0, Flags=C, 81=100, SSID="wif166_test_02", SSID	> Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client NUP Disabled
67 2023-06-12 17:12:25.756092 0.019073 Cisco_13:80:ed				Probe Response, SN=771, FN=0, Flags=C, BI=100, SSID="wifi66_test_02", SS	> Tag: vendor Specific: Cisco Systems, Inc: Aironet CCK version = 5
the second				the second	

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:

Cisco Catal	yst 9800-CL Wireless Controlle	r	Welcome admin 🛛 😤 🐨	A 🗈 🌣 🕅 🕢 🎜 Search APs and Clients Q
Q. Search Menu Items	Monitoring * > Wireless * > Clients		Client	
	Clients Sleeping Clients Excl	uded Clients	360 View General QOS Sta	tistics ATF Statistics Mobility History Call Statistics
Dashboard	× Delete C		Client Properties AP Properties Client State Servers	Security Information Client Statistics QOS Properties EoGRE None
Configuration	Selected 0 out of 12 Clients		Client ACLs Client Entry Create Time	None 339 seconds
~~~	Client MAC Address T IPv4	Address T IPv6 Address AP	Name Policy Type	WPA3
Administration	O 0012.17e1.dd57 ≯ 192.1	68.1.33 fe80::212:17ff:fee1:dd57 AP0	3_Sotao_9548 Encryption Cipher	CCMP (AES)
C Licensing	O 0012.17e2.4856	68.1.37 fe80::212:17ff:fee2:4856 APC	5_OutdoorB_2200 Authentication Key Management	SAE
•	O 0012.17e2.4b40	68.1.31 fe80::212:17ff:fee2:4b40 AP0	4_OutdoorF_3DCI Session Timeout	Not Applicable 86400
X Troubleshooting	O 0c8b.9509.3518    ▲ 192.1	68.1.129 N/A APO	3_Sotao_9548 Session Manager	0000
	☐ 286b.3598.580f	68.1.159 fe80::ac5b:e1e1:67ba:c353 AP6	849.9253.CA50	
	O 34ea.e702.6240  ≠ 192.1	68.1.70 N/A AP	Point of Attachment	capwap_90000010
	O 60fb.008b.0e66 ≯ N/A	N/A APO	11_RC_9136_F800 IF ID	0x90000010
	■ 84d8.1b0f.294f	68.1.91 N/A AP	3_Sotao_9548 Authorized	TRUE
Walk Me Through >	O 9669.5a28.a115	68.1.138 fe80::9469:5aff:fe28:a115 AP0	Common Session ID 12_Suite_1084	0000000000FACB09B2189
	a810.87bb.b833 / 192.1	68.1.94 fe80:::aa10:87ff:febb:b833 AP(	Acct Session ID 3_Soteo_9548 Auth Method Status List	0x0000000
	H 4 1 2 M 10	•	Method	SAE
			Local Policies	

### NetGear A8000

1

Connection OTA with focus on the RSN information from client:

	sekremote)) && ((wlan.addr == 941)	8.6548.7095) )    (wlan.fc.type_sul	btype == 0x001d)							S 🗆 • +
No.	Time	Delta Source	Destination	Protocol	Lengt Channe	Signal stre	Info			Frame 757: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF_(D4578905-2998-4456
3	22 2023-06-12 17:22:13.919260	0,000000 Netgear 48170195	Broadcast	802.11	166	5 -48 dbm	Probe Request, SN+1739, FN+0, Flags+C. SSID+"blizzard"			Ethernet II, Src: Cisco_dd:7d:37 (00:df:1d:dd:7d:37), Dst: Universa_b7:cf:06 (00:3a:80:b7:cf:06)
	23 2023-06-12 17:22:13.920174			802.11	166	5 -48 d8m	Probe Request, SN+1740, FN+0, Flags+C, SSID+"blizzard"			Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
3	24 2023-06-12 17:22:13.921093	0.000919 Netgear 48:70:95	Broadcast	802.11	166	5 -48 d8m	Probe Request, SN+1741, FN+0, Flags+C, SSID+"blizzard"			User Datagram Protocol, Src Port: 5555, Ost Port: 5000
3	26 2023-06-12 17:22:13.921977	0.000004 Netgear 40:70:95	Broadcast	802.11	166	5 -48 d8m	Probe Request, SN+1742, FN+0, Flags+C, SSID+"blizzard"			AiroPeek/OmniPeek encapsulated IEEE 802.11
7	3 2023-06-12 17:22:21.416940	7,494963 Netgear 48:70:95	Cisco 13:00:	802.11	360	5 -49 dbm	Probe Request, SNe4, FNe0, FlagsC, SSIDe"wifi6E_test"			802.11 radio information
7	4 2023-06-12 17:22:21.416940	0.000000 192.168.1.15	192.168.1.121	802.11	76	5 -36 dbm	Acknowledgement, flags+C			IEEE 802.11 Association Request, Flags:C
7	16 2023-06-12 17:22:21.419412	0.002472 Netgear_48:70:95	C15C0_13:80:	802.11	360	5 -49 d8m	Probe Request, SN+5, FN+0, Flags+C, SSID+"wif16E_test"		× ا	IEEE 802.11 Wireless Management
7	7 2023-06-12 17:22:21.419412	0.000000 192.168.1.15	192.168.1.121	802.11	76	5 -37 d8m	Acknowledgement, Flags=C			> Fixed parameters (4 bytes)
7	40 2023-06-12 17:22:21.444035	0.024623 Netgear_48:70:95	Cisco_13:00:	802.11	360	5 -49 dbm	Probe Request, SN+6, FN+0, Flags+C, SSID+"wifieE_test"			<ul> <li>Tagged parameters (122 bytes)</li> </ul>
7	41 2023-06-12 17:22:21.444035	0.000000 192.168.1.15	192.168.1.121	802.11	76	5 -37 dbm	Acknowledgement, Flags+C			> Tag: SSID parameter set: "wifi6E_test"
2	46 2023-06-12 17:22:21.498056	0.054021 Netgear 48:70:95	Cisco 13:80:	802.11	194	5 -50 dbm	Authentication, SN+2, FN+0, Flags+C			> Tag: Supported Rates 6(0), 9, 12(0), 10, 24(0), 36, 40, 54, [Hbit/sec]
	47 2023-06-12 17:22:21.498056		192.168.1.121		76		Acknowledgement, Flags+C			> Ext Tag: HE Capabilities
7	50 2023-06-12 17:22:21.546544	0.048488 Cisco 13:80:e7	Netgear_48:7.	802.11	294	5 -37 d8m	Authentication, SN+123, FN+0, Flags+C			Ext Tag: HE 6 GHz Band Capabilities
	51 2023-06-12 17:22:21.546544		192.168.1.121		76		Acknowledgement, Flags+C			> Tag: vendor Specific: Ralink Technology, Corp.
7	53 2023-06-12 17:22:21.550097	0.004353 Netgear 48:70:95	Cisco 13:00:	892.11	130		Authentication, SN+3, FN+0, Flags+C			> Tag: Extended Capabilities (10 octets)
	54 2023-06-12 17:22:21.550097		192,168,1,121		76	5 -37 dbm	Acknowledgement, flags+C			> Tag: Vendor Specific: Hicrosoft Corp.: WHYVHE: Information Element
7	55 2023-06-12 17:22:21.553602	0.002705 Cisco 13:80:e7	Netgear_48:7.	802.11	130	5 -37 d8m	Authentication, SN=124, FN=0, Flags=C			Tag: RSN Information
7	56 2023-06-12 17:22:21.553602	0.000000 192.168.1.15	192.168.1.121	802.11	76	5 -49 d8m	Acknowledgement, Flags+C			Tag Number: RSN Information (48)
c 7	57 2023-06-12 17:22:21.557006	0.003404 Netgear_48:70:95	Cisco_13:80:	802.11	216	5 -49 d8m	Association Request, SN=4, FN=0, Flags=C, SSID="wifi6E_test"			Tag length: 22
- 7	58 2023-06-12 17:22:21.557006	0.000000 192.168.1.15	192.168.1.121	802.11	76	5 -37 dbm	Acknowledgement, Flags+C			RSN Version: 1
2	60 2023-06-12 17:22:21.560605	0.003599 Netgear_48:70:95	Broadcast	LLC	114	5 -37 dbm	U, funcwUnknown; DSAP excc Group, SSAP SNAP Command			> Group Cipher Suite: 00:0f:ac (Ieee 002.11) AES (COM)
2	63 2023-06-12 17:22:21.567111	0.006506 Cisco_13:80:e7	Netgear_48:7_	802.11	262	5 -37 d8m	Association Response, SN=0, FN=0, Flags=C			Pairwise Cipher Suite Count: 1
7	64 2023-06-12 17:22:21.567111	0.000000 192.168.1.15	192.168.1.121	802.11	76	5 -49 d8m	Acknowledgement, Flags+C			> Pairwise Cipher Suite List 00:0fiac (Ieee 802.11) AES (CCH)
7	65 2023-06-12 17:22:21.567160	0.000049 Netgear_48:70:95	Broadcast	LLC	114	5 -37 d8m	I P, N(R)+63, N(S)+9; DSAP ex9c Group, SSAP ex56 Response			Auth Key Management (AAH) Suite Count: 1
7	66 2023-06-12 17:22:21.568723	0.001563 Cisco_13:00:e7	Netgear_48:7_	EAPOL	221	5 -37 dbm	Key (Message 1 of 4)			> Auth Key Hanagement (AKH) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
7	67 2023-06-12 17:22:21.568723	0.000000 192.168.1.15	192.168.1.121	802.11	76	5 -48 d8m	Acknowledgement, #lags+C			> RSN Capabilities: 0x00c0
7	12 2023-06-12 17:22:21.742256	0.173533 Netgear_48:70:95	Cisco_13:00:	EAPOL	226	5 -55 d8m	Key (Message 2 of 4)			PHID Count: 0
7	13 2023-06-12 17:22:21.742256	0.000000 192.168.1.15	192.168.1.121	802.11	76	5 -44 d8m	Acknowledgement, Flags+C			PikID List
7	15 2023-06-12 17:22:21.743972	0.001716 Cisco_13:80:e7	Netgear_48:7.	EAPOL	295		Key (Message 3 of 4)			Y Tag: #SN extension (1 octet)
7	06 2023-06-12 17:22:21.743972	0.000000 192.168.1.15	192.168.1.121	802.11	76		Acknowledgement, Flags+C			Tag Number: RSN extension (244)
L 7	17 2023-06-12 17:22:21.744676	0.000704 Netgear_48170195	Cisco_13:00:	EAPOL	199		Key (Message 4 of 4)			Tag length: 1
7	88 2023-06-12 17:22:21.744676	0.000000 192.168.1.15	192.168.1.121	802.11	76		Acknowledgement, Flags=C			✓ RSNX: ex2e (octet 1)
7	09 2023-06-12 17:22:21.752542	0.007866 CiscoHer_53:ca:50			187		U, func-Unknown; DSAP exc6 Group, SSAP ex30 Response			0000 = RSAX Length: 0
7	00 2023-06-12 17:22:21.752542	0.000000 192.168.1.15	192.168.1.121	802.11	76		Acknowledgement, Flags+C			0 = Protected TwT Operations Support: 0
	91 2023-06-12 17:22:21.754271		192.168.1.121		119		Trigger Buffer Status Report Poll (BSRP), Flags+C			-1 SAE Hash to element: 1
7	93 2023-06-12 17:22:21.754647	0.000376 Netgear_48:70:95	Broadcast	LLC	144	5 -55 dbm	I P, N(R)+81, N(S)+32; DSAP Banyan Vines Group, SSAP LLC Sub-Layer Manageme	ei		00 # Reserved: 0x0
7	94 2023-06-12 17:22:21.754647	0.000000 192.168.1.15	192.168.1.121	802.11	76	5 -44 d8m	Acknowledgement, Flags+C			> Tag: RH Enabled Capabilities (\$ octets)

### Client details in WLC:

Cisco Ca	alyst 9800-CL Wireless Controller	Welcome admin   🐐 🎨 🛕 🖹 🏟 🔞 🥥 🎜 Search APs and Clients 🔍   🖀 Feedback) 🖉 🕪
Q. Search Menu Items	Monitoring * > Wireless * > Clients	Client ×
	Clients Sleeping Clients Excluded Clients	360 View General QOS Statistics ATF Statistics Mobility History Call Statistics
Dashboard		Client Properties AP Properties Security Information Client Statistics QOS Properties EoGRE
Monitoring >	× Delete	Client State Servers None
2	Selected 0 out of 12 Clients	Client ACLs None
Configuration		Client Entry Create Time 24 seconds
Administration	Client MAC Address T IPv4 Address T IPv6 Address AP Name	Policy Type WPA3
	O 0012.17e1.dd57	Encryption Cipher CCMP (AES) Authentication Key Management SAE
C Licensing	0012.17e2.4856 / 192.168.1.37 fe80::212:17ff.fee2:4856 AP05_Outdoor8_2	200 EAP Type Not Applicable
	O 0012.17e2.4b40	CCI Session Timeout 86400
Y Troubleshooting	O 0c8b.9509.3518 ≯ 192.168.1.129 N/A AP03_Sotao_9548	
	O 34ea.e702.6240 ≠ 192.168.1.70 N/A AP6849.9253.CA5	
	0 60tb.008b.0e66 ≯ N/A N/A AP01_RC_9136_F/	80C Point of Attachment capwap_90000010
	84d8.1b0f.294f / 192.168.1.91 N/A AP03_Sotao_9548	IIF ID 0x9000010
	■ 9418.6548.7095  ¥ 192.168.1.163 fe80::ce19:6f16:279d:515f AP6849.9253.CA5	Authorized TRUE
Walk Me Through >	O 9669.5a28.a115  ≠ 192.168.1.138 fe80::9469:5aff:fe28:a115 AP02_Suite_1084	Common Session ID 00000000000000000000000000000000000
	-	Acct Session ID 0x0000000
	0	Auth Method Status List
	H 4 1 2 F H 10 F	Method SAE

### Pixel 6a

Connection OTA with focus on the RSN information from client:

((peek	remote) 88 (viar	1.800r == 24:95	:21:72:8a:66	))    (wlan.fc.type_su	ibtype == 0x001d	9				S 🗠 🔹
λ.	Time		Delta	Source	Destination	Protoco	i Lengti Channel	Signal stre	Info	> Frame 1255: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits) on interface \Device\NFF_(D4578905-2998
1235	2023-06-12 17	:37:02.730333	0.000000	Google_72:88:66	Broadcast	802.11	343	5 -42 d8m	Probe Request, SN+2096, FN+0, Flags+C, SSID+"wifi66_test"	Sthernet II, Src: Cisco_dd:7d:37 (00:df:1d:dd:7d:37), Dst: Universa_b7:cf:06 (00:3a:80:b7:cf:06)
1243	2023-06-12 17	:37:02.851631	0.121298	Google_72:88:66	Cisco_13:00:_	802.11	194	5 -42 d8m	Authentication, SN+2097, FN+0, Flags+C	> Internet Protocol Version 4, Src: 192.168.1.15, Ost: 192.168.1.121
1244	2023-06-12 17	:37:02.051631	0.000000	192,168,1,15	192.168.1.121	002.11	76	5 -37 dbm	Acknowledgement, Flags+C	> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
				Cisco 13:80:e7	Google_72:88.	802.11			Authentication, SN+141, FN+0, Flags+C	> AiroPeek/OmniPeek encapsulated IEEE 802.11
1247	2023-06-12 17	137102.858984	0.000000	192.168.1.15	192.168.1.121			5 -43 dbm	Acknowledgement, Flags+C	> 802.11 radio information
				Google_72:88:66	Cisco_13:80:	802.11			Authentication, SN+2098, FN+0, Flags+C	> IEEE 802.11 Association Request, Flags:C
		:37:02.868831			192.168.1.121			5 -37 dila	Acknowledgement, Flags+C	✓ IEEE 802.11 Wireless Management
				Cisco_13:80:e7	Google_72:8a				Authentication, SN+142, FN+0, Flag1+C	> Fixed parameters (4 bytes)
		:37:02.904326			192.168.1.121				Acknowledgement, Flags+C	✓ Tapped parameters (168 bytes)
					Cisco_13:80:				Association Request, SN+2099, FN+0, Flags+C, SSID+"wifi6E_test"	> Tag: SSID parameter set: "wifi66_test"
		:37:02.920933			192.168.1.121				Acknowledgement, Flags+C	 > Tag: Supported Rates 6(0), 9, 12(0), 18, 24(0), 36, 48, 54, [Hbit/sec]
				Google_72:88:66	Broadcast		114		I P, N(R)=52, N(S)=7; DSAP ex16 Individual, SSAP ex66 Command	> Tag: Extended Supported Rates SAE Hash to Element Only, [Mbit/sec]
				Cisco_13:80:e7	Google_72:8a.				Association Response, SN=0, FN=0, Flags=C	> Tag: Power Capability Min: -7, Max: 19
		:37:02.934129			192,168,1,121				Acknowledgement, FlagsC	> Tag: Supported Channels
				Google_72:88:66	Broadcast		114		5 F, func+RNR, N(R)+82: DSAP 0x8e Group, SSAP 0x74 Response	Tag: RSN Information
				Cisco_13:80:e7	Google_72:8a.				Key (Message 1 of 4)	Tag Number: RSN Information (48)
		:37:02.941092			192.168.1.121				Acknowledgement, Flags+C	Tag length: 26
									Key (Hessage 2 of 4)	RSN Version: 1
				Google_72:8a:66	Cisco_13:80:_		230		Key (Message 2 of 4) Acknowledgement, Flags+C	> Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCH)
		:37:02.992247			192.168.1.121					Paintie Cipher Suite Count: 1
				Cisco_13:80:e7	Google_72:88.		295		Key (Message 3 of 4)	> Pairwise Cipher Suite List 00:0fiac (Ieee 802.11) AES (CCM)
		137102.995369			192.168.1.121				Acknowledgement, Flags+C	Auth Key Hanagement (AON) Suite Count: 1
				Google_72:88:66	Cisco_13:80:				Key (Message 4 of 4)	> Auth Key Management (AKM) List 00:0f1ac (Ieee 802.11) SAE (SMA256)
		:37:03.000159			192.168.1.121				Acknowledgement, Flags=C	> Main Key Hanagement (MAN) List Weierleit (Leee Weilit) SAE (SMAIN) > MSN Keyenings
		:37:03.023390			192.168.1.121				Acknowledgement, Flags+C	PokiD Count: 0
1282	2023-06-12 17	:37:03.025924	0.002534	Google_72:88:66	Cisco_13:00:	. 802.11			Action, SN+2101, FN+0, Flags+.pC[Halformed Packet]	
1283	2023-06-12 17	:37:03.025924	0.000000	192.168.1.15	192.168.1.121	802.11			Acknowledgement, #lags+C	PWKID List
1285	2023-06-12 17	:37:03.043013	0.017009	192.168.1.15	192.168.1.121	802.11			Acknowledgement, #lags+C	> Group Hanagement Cipher Suite: 00:0f:ac (Ieee 802.11) 8IP (128)
1286	2023-06-12 17	:37:03.050766	0.007753	192.168.1.15	192.168.1.121	802.11	76	5 -37 d8m	Acknowledgement, Flags+C	> Tag: RM Enabled Capabilities (5 octets)
1290	2023-06-12 17	:37:03.078167	0.027401	Cisco_13:80:e7	Google_72:88.	802.11	124	5 -37 dên	Action, SN+1, FN+0, Flags+.pC	> Tag: Supported Operating Classes
1291	2023-06-12 17	:37:03.078167	0.000000	192,168,1,15	192,168,1,121	002.11	76	5 -49 dbm	Acknowledgement, Flags+C	> Tag: Extended Capabilities (10 octets)
1297	2023-06-12 17	17:03.166223	0.055056	Google_72:88:66	Cisco_13:00:	882.11	115	5 .45 (04	Action, SN+2104, FN+0, Flags+.pC	> Ext Tag: HE Capabilities
		137103.166223			192.168.1.121				Acknowledgement, FlagsC	Tag: RSN extension (1 octet)
				Google_72:8a:66	IPv6mcast_ff.				U P, func+XID; DSAP 0x32 Group, SSAP 0x6c Command	Tag Number: RSN extension (244)
		:37:03.166299			192.168.1.121				Acknowledgement, FlagsC	Tag length: 1
				Cisco_13:80:e7	Google_72:8a.				Action, SN+2, FN+0, Flags+.pC[Halformed Packet]	✓ #SNX: 8x28 (octet 1)
		:37:03.167999			192.168.1.121				Acknowledgement, FlagsC	0000 = RSAX Length: 0
		137:03.168296			192.168.1.121				802.11 Block Ack Reg. FlagsC	
									802.11 Block Ack, Flags+C 802.11 Block Ack, Flags+C	SAE Wath to element: 1
		:37:03.168396			192.168.1.121					00 = Reserved: 0x0
				Google_72:88:66	IPv6mcast_ff.				I P, N(R)=5, N(S)=45; DSAP exc0 Individual, SSAP ex4a Response	> Ext Tag: HE 6 GHz Band Capabilities
		:37:03.177442			192.168.1.121				Request-to-send, Flags+C	> Tag: Vendor Specific: Broadcom
		:37:03.177442			192.168.1.121				Clear-to-send, Flags+C	> Tag: Vendor Specific: Hicrosoft Corp.: W00/WNE: Information Element
1309	2023-06-12 17	:37:03.177515	0.000073	Google_72:88:66	IPv6mcast_16	LLC	271	5 -56 dbn	I, N(R)=7, N(S)=34; DSAP 0xb6 Group, SSAP 0xe6 Response	> tag: vendor spectrus: Hicrosoft Corp.: avvine: Information Element

### Client details in WLC:

	Monito	oring • > Wireless •	> (	Clients			Client					
Q Search Menu Items	Client	s Sleeping Clier	rts	Excluded Clien	ts		360 View General QOS Statistics	s ATF Statistics	Mobility History	Call Statistics		
Dashboard ) Monitoring		C Delete					Client Properties AP Properties Client State Servers Client ACLs	Security Information Client Statistics QOS Properties EoGRE None None				
Configuration >	Sele	cted 0 out of 12 Clients					Client Entry Create Time	83 seconds				
Administration >	0	Client MAC Address	T	IPv4 Address	IPv6 Address	AP Name	Policy Type	WPA3				
Auministration	0	2495.2f72.8a66	×	192.168.1.162	fe80::b13:f107:7c5f:a7e0	AP6849.9253.CA50	Encryption Cipher	CCMP (AES)				
Licensing	0	60fb.008b.0e66	×	N/A	N/A	AP01_RC_9136_F80C	Authentication Key Management	SAE				
	0	34ea.e702.6240	1	192.168.1.70	N/A	AP6849.9253.CA50	EAP Type Session Timeout	Not Applicable 86400				
Troubleshooting	0	a810.87bb.b833	×	192.168.1.94	fe80::aa10:87ff:febb:b833	AP03_Sotao_9548	Session Manager	86400				
	o	9669.5a28.a115		192.168.1.138	fe80::9469:5aff;fe28;a115	AP02_Suite_1084	Session manager					
	0	84d8.1b0f.294f		192.168.1.91	N/A	AP03_Sotao_9548	Point of Attachment	capwap_90000	010			
	0	0c8b.9509.3518		192.168.1.129	N/A	AP03_Sotao_9548	IIF ID	0x90000010				
	0	0012.17e2.4b40		192.168.1.31	fe80::212:17ff:fee2:4b40	AP04 OutdoorF 3DC8	Authorized	TRUE				
Walk Me Through >	0	0012.17e2.4856		192,168,1,37	fe80::212:17ff:fee2:4856	AP05_Outdoor8_2200	Common Session ID	000000000000000000000000000000000000000	FB5B0AED363			
	_						Acct Session ID	0x00000000				
	0	0012.17e1.dd57	1	192.168.1.33	fe80::212:17ff:fee1:dd57	AP03_Sota0_9548	Auth Method Status List					

### Samsung S23

Connection OTA with focus on the RSN information from client:

77       2021-66.12       1721515       5.490000       5.490000       Activation press, heads       Activation		(peekremote) && ((wlan.addr == 04:29	:2e:c9:e3:71)    (vian.fc.type_sub	stype == 0x001d))					🛛 📼 💌 +
79         2021-06-11         21/25/35/70229         0.000000         22/25/35/70219         0.00000         ACONDUCTIONERS         21/25/35/70219         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000         0.00000	_	The           71         822-86-12         173-855         572218           72         822-86-12         173-855         72218           73         822-86-12         173-855         72218           74         822-86-12         173-855         72218           74         822-86-12         173-855         72218           74         822-86-12         173-855         72218           74         822-86-12         173-855         72218           74         822-86-12         173-855         72218           74         822-86-12         173-855         72218           74         822-86-12         173-855         72218           74         822-86-12         173-855         72218           74         822-86-12         173-855         72218           74         822-86-12         173-855         73218           742         822-86-12         173-855         73218           743         822-86-12         173-855         73218           744         822-86-12         173-855         73218           745         822-86-12         173-855         73218           746         822-86-12	Other         Source           0.00000         Support           0.000000         Sip.(cl, 1, 1)           0.000000         Sip.(cl, 1, 1)	Destnation Clisco_313087 192.164.1.21 Sastungt_09 192.164.1.21 Clisco_313087 192.164.1.21 Clisco_313087 192.164.1.21 Proadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadca	Protocol 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11	194 76 194 76 100 76 130 76 154 114 114 114 226 76 220 76 230 76	5         -45         clin           5         -32         clin           5         -37         clin           5         -45         clin           5         -45         clin           5         -36         clin           5         -36         clin           5         -36         clin           5         -37         clin           5         -36         clin           5         -37         clin	Athentication, SNAIDS, Fade, FlagsC Antonalegneent, FlagsC Athentication, SNAIDS, FlagsC Athentication, SNAIDS, FlagsC Athentication, SNAIDS, FlagsC Athentication, SNAIDS, FlagsC Athentication, SNAIDS, FlagsC Athentications, SNAID, FlagsC	) From T21: SAK bytes on usrc (1552 bith), IAN bytes captured (1552 bith) on interface locica/mr_(putrome.rspsasse ) Between t1, sc: (1562,6471-271 (ModelField/AFC207), St (UMAYER_2)/SF(F46 (MellasEE/27)/off-66 (Me

Client details in WLC:

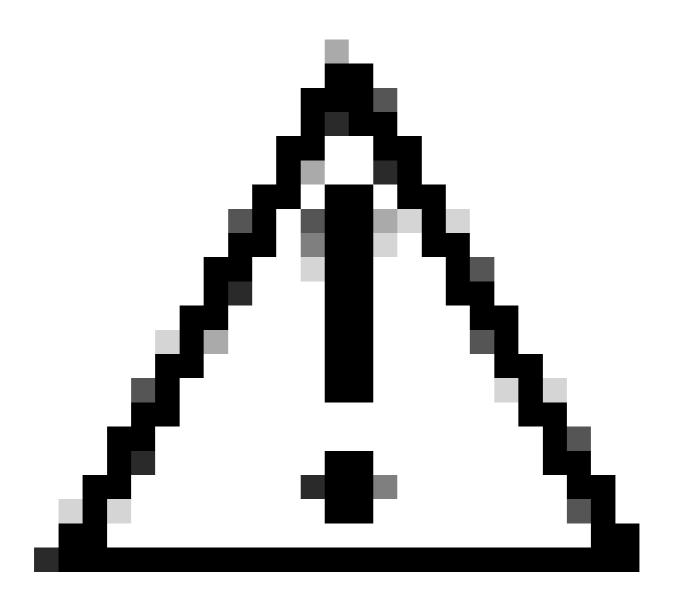
Cisco Cata	lyst 9800-CL Wireless	Controller			Welcome admin 🛛 🚓 🕏 🛔	Search APs and Search APs and G	Clients Q
Q. Search Menu Items	Monitoring * > Wireless	-> Clients			Client		×
	Clients Sleeping Clie	nts Excluded Client	s		360 View General QOS Statistics	ATF Statistics Mobility History	Call Statistics
Dashboard	× Delete 2				Client Properties AP Properties Se Client State Servers	Client Statistics	QOS Properties EoGRE
Configuration	Selected 0 out of 12 Clients	s			Client ACLs Client Entry Create Time	None 78 seconds	
~	Client MAC Addres	ss 🝸 IPv4 Address 🍸	IPv6 Address	AP Name	Policy Type	WPA3	
(i) Administration	0 0012.17e1.dd57	▶ 192.168.1.33	fe80::212:17ff:fee1:dd57	AP03_Sotao_9548	Encryption Cipher	CCMP (AES)	
C Licensing	0012.17e2.4856	▶ 192.168.1.37	fe80::212:17ff:fee2:4856	AP05_Outdoor8_220		SAE	
	0 0012.17e2.4b40	▶ 192.168.1.31	fe80::212:17ff:fee2:4b40	AP04_OutdoorF_3D0	EAP Type Session Timeout	Not Applicable 86400	
Y Troubleshooting	0429.2ec9.e371	▶ 192.168.1.160	fe80::6a20:34e8:ab1b:6332	AP6849.9253.CA50	Session Manager	86400	
	O 0c8b.9509.3518	▶ 192.168.1.129	N/A	AP03_Sotao_9548	oussion manager		
	<b>34ea.e702.6240</b>	▶ 192.168.1.70	N/A	AP6849.9253.CA50	Point of Attachment	capwap_90000010	
	60fb.008b.0e66	🔎 N/A	N/A	AP01_RC_9136_F80	IIF ID	0x90000010	
	B4d8.1b0f.294f	▶ 192.168.1.91	N/A	AP03_Sotao_9548	Authorized	TRUE	
Walk Me Through >	9669.5a28.a115	▶ 192.168.1.138	fe80::9469:5aff:fe28:a115	AP02_Suite_1084	Common Session ID Acct Session ID	00000000000000FB1B0A58F78 0x00000000	
	a810.87bb.b833	ا 192.168.1.94 ≯	fe80::aa10:87ff:febb:b833	AP03_Sotao_9548	Auth Method Status List	00000000	
	∺ 4 1 2 ▶	H 10 V			Method	SAE	

### WPA3-Personal - AES(CCMP128) + SAE + FT

WLAN Security configuration:

### Edit WLAN

Changing WLAN parameters while it is enabled will represent the second secon	result in loss of connectivity for clients con	mected to it.
eneral Security Advanced Add To Policy Tag	15	
ayer2 Layer3 AAA		
○ WPA + WPA2 ○ WPA2 + WPA3 ● W	PA3 O Static WEP	O None
MAC Filtering		
Lobby Admin Access 0		
WPA Parameters	- Fast Transition	
WPA O WPA2 O	Status	Enabled •
GTK O WPA3 O Randomize Policy	Over the DS	0
Transition O Disable	Reassociation Timeout *	20
WPA2/WPA3 Encryption	- Auth Key Mgmt	
AES(CCMP128) O CCMP256	S46 🖸	FT + SAE
GCMP128 O GCMP256 O	OWE O	FT + 802.1x 0
Protected Management Frame	802.1x- SHA256	
PMI Required •	Arti Clogging Threshold*	1500
Association Comeback Timer*	Max Retries*	5
SA Query Time* 200	Retransmit Timeout*	400
	PSK Format	ASCI •
	PSK Type	Unencrypted •
	Pre-Shared Key*	
	SAE Password Element 0	Hash to Element O.T



**Caution**: 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.

wifi6E\_test

[WPA3][SAE][FT + SAE][AES].[FT Enabled]

View on WLC GUI of the WLAN Security settings:

6

Verification of beacons OTA:

wif6E\_test

Ο

0

	Time	Delta	Source	Destination	Output	Lengt Channel	Constate	14	> Frame 1: 508 bytes on wire (4064 bits), 508 bytes captured (4064 bits) on interface \Device\WFF_(D4578305-2398-4456-BC33-C3431664
140.	1 2023-06-12 10:34:49.305337			Broadcast	802.11	Sea		Beacon frame, SN+422, FN+0, Flags+C, BI+100, SSID+"wifi68_	> Ethernet II, Src: Cisco_dd:7d:37 (00:df:1d:dd:7d:37), Dst: Universa_b7:cf:06 (00:3a:88:b7:cf:06)
_	2 2023-06-12 18:34:49.487544			Broadcast	802.11			Beacon frame, SN+427, FN+0, Flags+C, BI+100, SSID+"wifi68	> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
	3 2023-06-12 18:34:49.589867			Broadcast	802.11			Beacon frame, SN+432, FN+0, Flags+C, BI+100, SSID+"wifi68	> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
	4 2023-06-12 18:34:49.692332				802.11			Beacon frame, SN=437, FN=0, Flags=C, BI=100, SSID="wifi68	> AiroPeek/OmniPeek encapsulated IEEE 002.11
	5 2023-06-12 18:34:49.791004			Cisco_13:80:_		360		Probe Request, SN=10, FN=0, Flags=C, SSID="wifi6E_test"	> B02.11 radio information
	6 2023-06-12 18:34:49.791004			192.168.1.121		76		Acknowledgement, Flags+C	> IEEE 802.11 Beacon frame, flags:C
	7 2023-06-12 18:34:49.791356	0.000352	Netgear_48:70:95	Cisco_13:80:_	802.11	360	5 -49 dom	Probe Request, SN+11, FN+0, Flags+C, SSID+"wifi68_test"	✓ IEEE 002.11 Wireless Management
	8 2023-06-12 18:34:49.791427	0.000071	192.168.1.15	192.168.1.121	802.11	76	5 -37 dbm	Acknowledgement, Flags+C	> Fixed parameters (12 bytes)
	9 2823-06-12 18:34:49.794493	0.003066	Cisco_13:80:ed	Broadcast	802.11	505	5 -37 dbm	Beacon frame, SN+442, FN+0, Flags+C, BI+100, SSID+"wifi68	<ul> <li>Tagged parameters (406 bytes)</li> </ul>
	10 2023-06-12 18:34:49.810282	0.015789	Netgear_48:70:95	Cisco_13:80:	802.11	368	5 -49 d8m	Probe Request, SN+12, FN+0, Flags+C, SSID+"wifi6E_test"	> Tag: SSID parameter set: "wifi6E_test_02"
	11 2023-06-12 18:34:49.810282	0.000000	192.168.1.15	192.168.1.121	802.11	76	5 -37 d8m	Acknowledgement, Flags+C	> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Mbit/sec]
	12 2023-06-12 18:34:49.874951			Cisco_13:80:_	802.11	194		Authentication, SN=4, FN=0, Flags=C	> Tag: Traffic Indication Map (TIM): DTIM @ of 3 bitmap
	13 2023-06-12 10:34:49.074951			192.168.1.121		76		Acknowledgement, Flags+C	> Tag: Country Information: Country Code na, Environment Global operating classes
	14 2023-06-12 18:34:49.896563			Netgear_4817_		194		Authentication, SN+146, FN+0, Flags+C	> Tag: Power Constraint: 6 > Tag: TPC Report Transmit Power: 17, Link Margin: 0
	15 2023-06-12 18:34:49.896563			192.168.1.121		76		Acknowledgement, flags+C	y rag: the appendix framme power 17, the margin: o y rag: the information
	16 2023-06-12 18:34:49.904966			Broadcast		588		Beacon frame, SN+447, FN+0, Flags+C, BI+100, SSID+"wifi6E_	Tag number: RSN Information (48)
	17 2023-06-12 18:34:49.904966			Cisco_13:80:				Authentication, SN+5, FN+0, Flags+C	Tag length: 24
	18 2023-06-12 18:34:49.904966			192.168.1.121		76		Acknowledgement, Flags+C	RSN Version: 3
	19 2023-06-12 18:34:49.904966			Netgear_48:7.				Authentication, SN+147, FN+0, Flags+C	> Group Cipher Suite: 00:0f:sc (Ieee 802.11) AES (CCH)
	20 2023-06-12 18:34:49.904966			192.168.1.121		76		Acknowledgement, Flags+C	
	21 2023-06-12 18:34:49.904966			Cisco_13:801.		216		Association Request, SN+6, FN+0, Flags+C, SSID+"wifi6E_tes	> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
	22 2023-06-12 18:34:49.904966			192.168.1.121				Acknowledgement, FlagsC	Auth Key Management (AKH) Suite Count: 1
	23 2023-06-12 18:34:49.911474 24 2023-06-12 18:34:49.911474			Netgear_48:7. 192.168.1.121		262		Association Response, SN=0, FN=0, Flags=C Acknowledgement, Flags=C	> Auth Key Management (ADV) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
	25 2023-06-12 10:34:49.911719			Broadcast		114		U, funcwUP; DSAP ex32 Individual, SSAP ex62 Command	> RSN Capabilities: 0x00e8
	26 2023-06-12 10:34:49.911719			Broadcast		114		U, funceunknown; DSAP exiz Individual, SSAP exiz Committe U, funceUnknown; DSAP exiz Individual, SSAP exiz Committe	PHKID Count: 0
	27 2023-06-12 10:34:49.922346			Netgear_48:7.		221		Key (Nessage 1 of 4)	PHOLD List
	28 2023-06-12 18:34:49.922346			192.168.1.121		76		Acknowledgement, Flags+C	> Group Hanagement Cipher Suite: 00:0fiac (Icee 802.11) 8IP (128)
	29 2023-06-12 18:34:49.999581			Broadcast		588		Beacon frame, SN=452, FN=0, Flags=C, BI=100, SSID="wifi6E_	> Tag: QBSS Load Element 802.11e CCA version
	30 2023-06-12 18:34:50.104510				802.11			Beacon frame, SNo457, FNo0, FlagtoC, BIo100, SSIDo"wifi68	> Tag: Multiple 8551D
	31 2023-06-12 18:34:50.204600			Broadcast				Beacon frame, SN+462, FN+0, Flags+C, BI+100, SSID+"wifi68	> Tag: RH Enabled Capabilities (5 octets)
	32 2023-06-12 18:34:50.211615			Cisco_13:80:_		226		Key (Message 2 of 4)	> Tag: Extended Capabilities (11 octets)
	33 2023-06-12 18:34:50.211615			192.168.1.121		76		Acknowledgement, Flags+C	> Tag: Tx Power Envelope
	34 2023-06-12 18:34:50.213376			Netgear 48:7.		295		Key (Hessage 3 of 4)	> Tag: Tx Power Envelope
	35 2023-06-12 18:34:50.213376	0.000000	192.168.1.15	192.168.1.121	802.11	76	5 -50 d8m	Acknowledgement, Flags+C	> Ext Tag: Multiple BSSID Configuration
	36 2023-06-12 18:34:50.214354			Cisco_13:00:_	EAPOL	199		Key (Hessage 4 of 4)	> Ext Tag: HE Capabilities
	37 2023-06-12 18:34:50.214354	0.000000	192.168.1.15	192.168.1.121	802.11	76	5 -42 dom	Acknowledgement, Flags+C	> Ext Tag: HE Operation
	38 2023-06-12 18:34:50.220721	0.006367	192.168.1.15	192.168.1.121	802.11	76	5 -42 dbm	Acknowledgement, #lags+C	> Ext Tag: Spatial Reuse Parameter Set
	39 2023-06-12 18:34:50.224049	0.003328	192.168.1.15	192.168.1.121	802.11	119	5 -44 d8m	Trigger Buffer Status Report Poll (85RP), Flags=C	> Ext Tag: HU EDCA Parameter Set
	40 2023-06-12 18:34:50.224049	0.000000	AlticeLa_9e:59:af	Netgear_48:7.	LLC	223		U, func-Unknown; DSAP @xb6 Group, SSAP @xd8 Response	> Ext Tag: HE 6 GHZ Band Capabilities
	41 2023-06-12 18:34:50.224049	0.000000	192.168.1.15	192.168.1.121	802.11	76	5 -54 d8m	Acknowledgement, Flags+C	<ul> <li>Tag: HSW extension (1 octet)</li> </ul>
									Tag Number: #SN extension (244)
									Tag length: 1
									✓ R5NX: 8x20 (ottet 1) 0000 = R5NX Length: 0
									00
									> Tag: Vendor Specific: Atheros Communications, Inc.: Umknown
									> Tag: vendor Specific: Microsoft Corp.: WWIAWE Parameter Element
									) Tag: vendor Specific: Cisco Systems, Inc: Aircost Unknown (44)
									) reg: vendor Specific: Clsco systems, Inc: Alropet Unknown (H1) (11)
									> Tagi vendor Specifici Cisco Systems, Inci Aironet Client WP Oisabled
									> Tag: vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5
1									
1									

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:

	ekremote) && (vilan.addr == 286b	3598.580f)	)    (wlan.fc.type_subl	type == 0x001d) (	or wlan, fc.1	type_subtype ==	0x0008)		2
No.	Time	Delta	Source	Destination	Protocol	Lengt Channel	Signal stre	Info	> Frame 1019: 250 bytes on wire (2000 bits), 250 bytes captured (2000 bits) on interface \Device\NPF_{D4578905-2998-4
101	2023-06-12 18:51:35.249793	0.017337	IntelCor se:se:ef	Cisco 13:00:-	882.11	194	5 -42 dbn	Authentication, SNw0, FNw0, Flags+C	Ethernet II, Src: Cisco_dd:7d:37 (00:df:id:dd:7d:37), Dst: Universa_b7:cf:06 (00:3a:80:b7:cf:06)
	2023-06-12 18:51:35.249793			192.168.1.121				Acknowledgement, Flags+C	 > Internet Protocol Version 4, Src: 192.168.1.15, Ost: 192.168.1.121
	2023-06-12 18:51:35.256827			IntelCor 981.				Authentication, SN+159, FN+0, Flags+C	> User Datagram Protocol, Src Port: 5555, Ost Port: 5000
	2023-06-12 18:51:35.256827			192.168.1.121		76	5 -42 d8m	Acknowledgement, Flags+C	> AiroPeek/OmniPeek encapsulated IEEE 802.11
	2023-06-12 18:51:35.259394					130		Authentication, SN=1, FN=0, Flags=C	> 802.11 radio information
	2023-06-12 18:51:35.259394			192.168.1.121		76		Acknowledgement, FlagsC	> IEEE 802.11 Association Request, Flags:C
	2023-06-12 18:51:35.263679			IntelCor_98:_		130		Authentication, SN+160, FN+0, Flags+C	✓ IEEE 802.11 wireless Hanagement
101	2023-06-12 18:51:35.263679	0.000000		192.168.1.121		76	5 -42 dbm	Acknowledgement, Flags+C	> Fixed parameters (4 bytes)
- 101	2023-06-12 18:51:35,263679	0.000000	IntelCor_98:58:0f	Cisco 13:00:	882.11	250	5 -46 dbm	Association Request, SN+2, FN+0, Flags+C, SSID+"wifi6E test"	<ul> <li>Tagged parameters (156 bytes)</li> </ul>
102	2023-06-12 18:51:35.263679	0.000000	192.168.1.15	192.168.1.121	882.11	76	5 -36 dbm	Acknowledgement, Flags+C	> Tag: SSID parameter set: "wifi66_test"
102	2023-06-12 18:51:35.274142	0.010463	IntelCor_98:58:0f	Broadcast	LLC	114	5 -36 d8m	I, N(R)=98, N(S)=63; DSAP @x84 Group, SSAP @x88 Response	> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [HBit/sec]
102	2023-06-12 18:51:35.274142	0.000000	IntelCor_98:58:0f	Broadcast	LLC	114	5 -36 d8m	I, N(R)=67, N(S)=122; DSAP ex50 Group, SSAP Spanning Tree BPDU Response	> Tag: Power Capability Min: 0, Max: 9
	2023-06-12 18:51:35.277402			IntelCor_98:_		262		Association Response, SN+0, FN+0, Flags+C	✓ Tag: RSN Information
	2023-06-12 18:51:35.277402			192.168.1.121		76		Acknowledgement, Flags+C	Tag Number: RSN Information (48)
	2023-06-12 18:51:35.286107			Broadcast	882.11	517		Beacon frame, SN+371, FN+0, Flags+C, BI+100, SSID+"wifi6E test 02",	Tag length: 26
103	2023-06-12 18:51:35.311349	0.025242	192.168.1.15	192.168.1.121	882.11	76	5 -36 dbm	Acknowledgement, flags+C	RSN Version: 1
103	2023-06-12 18:51:35.316198	0.004545	192.168.1.15	192.168.1.121	882.11	76	5 -52 dbm	Clear-to-send, FlagsC	> Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCH)
103	2023-06-12 18:51:35.333425	0.017227	192.168.1.15	192.168.1.121	882.11	76	5 -36 d8m	Acknowledgement, Flags=C	Pairwise Cipher Suite Count: 1
104	2023-06-12 18:51:35.388460	0.055035	Cisco_13:00:ed	Broadcast	882.11	517	5 -37 d8m	Beacon frame, SN=376, FN=0, Flags=C, BI=100, SSID="wifi6E_test_02",	> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
104	2023-06-12 18:51:35.389808	0.001340	192.168.1.15	192.168.1.121	802.11	76	5 -53 d8m	Clear-to-send, Flags+C	Auth Key Management (AKM) Suite Count: 1
104	2023-06-12 18:51:35.397943	0.000135	192.168.1.15	192.168.1.121	802.11	82	5 -38 d8m	Request-to-send, Flags+C	> Auth Key Hanagement (AOH) List 00:0f:ac (Ieee 002.11) SAE (SHA256)
104	2023-06-12 10:51:35.390902	0.001035	192.168.1.15	192.168.1.121	882.11	82	5 -36 dbm	Request-to-send, Flags+C	> RSN Capabilities: 0x00fc
104	2023-06-12 18:51:35.399012	0.000530	192.168.1.15	192.168.1.121	882.11	82	5 -36 dbm	Request-to-send, Flags+C	PHKID Count: 0
104	2023-06-12 18:51:35.400524	0.000712	192.168.1.15	192.168.1.121	882.11	82	5 -36 dbm	Request-to-send, Flags+C	PHKID List
104	2023-06-12 18:51:35.401191	0.000663	192.168.1.15	192.168.1.121	882.11	82	5 -36 d8m	Request-to-send, Flags=C	> Group Management Cipher Suite: 00:0fiac (Ieee 802.11) 8IP (128)
104	2023-06-12 18:51:35.402035	0.000544	192.168.1.15	192.168.1.121	802.11	82	5 -36 d8m	Request-to-send, Flags+C	> Tag: Supported Operating Classes
105	2023-06-12 18:51:35.402617	0.000583	192.168.1.15	192.168.1.121	802.11	82	5 -36 d8m	Request-to-send, Flags+C	> Tag: RH Enabled Capabilities (5 octets)
105	2023-06-12 18:51:35.403253	0.000630	192.168.1.15	192.168.1.121	802.11	82	5 -36 dbm	Request-to-send, Flags+C	> Tag: Extended Capabilities (10 octets)
105	2023-06-12 18:51:35.404574	0.001321	192.168.1.15	192.168.1.121	882.11	82	5 -36 dbm	Request-to-send, Flags+C	> Tag: Vendor Specific: Hicrosoft Corp.: WHW/WHE: Information Element
105	2023-06-12 18:51:35.405306	0.000732	192.168.1.15	192.168.1.121	882.11	82	5 -36 dbm	Request-to-send, Flags+C	> Tag: Vendor Specific: Intel Wireless Network Group
105	2023-06-12 18:51:35.405877	0.000571	192.168.1.15	192.168.1.121	882.11	82	5 -36 dbm	Request-to-send, Flags+C	Tag: RSN extension (1 octet)
105	2023-06-12 18:51:35.406637	0.000760	192.168.1.15	192.168.1.121	882.11	82	5 -36 d8m	Request-to-send, Flags=C	Tag Number: RSN extension (244)
105	2023-06-12 18:51:35.406681	0.000044	192.168.1.15	192.168.1.121	882.11	76	5 -36 d8m	Acknowledgement, Flags+C	Tag length: 1
105	2023-06-12 18:51:35.407244	0.000563	192.168.1.15	192.168.1.121	882.11	82	5 -36 d8m	Request-to-send, Flags+C	✓ RSNX: 0x20 (octet 1)
105	2023-06-12 18:51:35.407527	0.000283	Cisco_13:00:e7	IntelCor_98:_	EAPOL	221	5 -36 dbm	Key (Hessage 1 of 4)	0000 = RSAX Length: 0
100	2023-06-12 18:51:35.407527	0.000000	192.168.1.15	192.168.1.121	802.11	76	5 -48 dbm	Acknowledgement, Flags+C	e = Protected TwT Operations Support: 0
106	2023-06-12 18:51:35.410712	0.003185	IntelCor_98:58:0f	Cisco_13:80:	EAPOL	230	5 -52 dbm	Key (Message 2 of 4)	= SAE Hash to element: 1
105	2023-06-12 18:51:35.410712	0.000000	192.168.1.15	192.168.1.121	882.11	76	5 -37 d8m	Acknowledgement, Flags+C	ee # Reserved: exe
106	2023-06-12 18:51:35.412220	0.001500	192.168.1.15	192.168.1.121	882.11	82	5 -37 d8m	Request-to-send, Flags=C	> Ext Tag: HE Capabilities
106	2023-06-12 18:51:35.412651	0.000433	Cisco_13:00:e7	IntelCor_98:_	EAPOL	343	5 -37 d8m	Key (Hessage 3 of 4)	> Ext Tag: HE 6 GHZ Band Capabilities
106	2023-06-12 18:51:35.412651	0.000000	192.168.1.15	192.168.1.121	882.11	76	5 -48 d8m	Acknowledgement, FlagiC	
- 106	2023-06-12 18:51:35.413651	0.001000	IntelCor_98:58:ef	Cisco_13:00:	EAPOL	199		Key (Message 4 of 4)	
100	2023-06-12 18:51:35.413651	0.000000	192.168.1.15	192.168.1.121	802.11	76	5 -37 dbm	Acknowledgement, #lags+C	

Roaming event where you can see the PMKID:

((peekremote) && (wlan.addr == 286b.3598.580f) )    (wlan.fc.type_subtype == 0x001d) or	<pre>r wlan.fc.type_subtype == 0x00</pre>	008	+ 🗉 🗖
No. Time Delta Source Destination	Protocol Lengt Channel	Signal stre Info	> Frame 22065: 272 bytes on wire (2176 bits), 272 bytes captured (2176 bits) on interface \Device\NFF_(D4578905-2998-4
220. 2023-06-12 18:53:11.488635 0.000129 IntelCor_98:58:0f IntelCor_98:.	LLC 325 5	-75 dBm S, Func+RR, N(R)+0: DSAP NULL LSAP Individual, SSAP NULL LSAP Command	Ethernet II, Src: Cisco_6d:7d:37 (00:df:1d:dd:7d:37), Dst: Universa_b7:cf:06 (00:3a:00:b7:cf:06)
220. 2023-06-12 10:53:11.400601 0.000046 IntelCor_90:50:0f IntelCor_90:.		-75 dBm S, func=RR, N(R)=0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command	> Internet Protocol Version 4, Src: 192.168.1.15, Ost: 192.168.1.121
220. 2023-06-12 10:53:11.409310 0.000629 IntelCor_90:58:0f IntelCor_90:.		-75 dBm S, func+RR, N(R)+0: DSAP NULL LSAP Individual, SSAP NULL LSAP Command	> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
220. 2023-06-12 18:53:11.409310 0.000000 IntelCor_98:58:0f IntelCor_98:.		-69 dBm S, func+RR, N(R)+0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command	> AiroPeek/OmiPeek encapsulated IEEE 002.11
220. 2023-06-12 18:53:11.409359 0.000049 IntelCor_98:58:0f IntelCor_98:.		-74 dBm S, func+RR, N(R)+0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command	> B02.11 radio information
220. 2023-06-12 18:53:11.489462 0.000103 IntelCor_98:58:0f IntelCor_98:.		-74 dBm 5, func+RR, N(R)+0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command	> IEEE D02.11 Reassociation Request, Flags:C
220. 2023-06-12 18:53:11.489504 0.000042 IntelCor_98:58:0f IntelCor_98:.		-74 dBm S, func+RR, N(R)=0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command	✓ IEEE D02.11 Wireless Hanagement
220. 2023-06-12 18:53:11.409639 0.000135 IntelCor 98:58:0f IntelCor 98:		-74 dBm S, func+RR, N(R)+0: DSAP NULL LSAP Individual, SSAP NULL LSAP Command	> fixed parameters (10 bytes)
220. 2023-06-12 18:53:11.490161 0.000522 IntelCor_98:58:0f IntelCor_98:.		-74 dBm S, func+RR, N(R)+0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command	✓ Tagged parameters (172 bytes)
220. 2023-06-12 18:53:11.490363 0.000202 IntelCor_98:58:0f IntelCor_98:.		-D0 dBm S, func+RR, N(R)+0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command	> Tag: SSID parameter set: "wifi66_test"
220, 2023-06-12 10:53:11,491197 0.000034 IntelCor 90:50:0f IntelCor 90:		-77 dbm 5, func+RR, N(R)+0: DSAP NULL LSAP Individual, SSAP NULL LSAP Command	> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Hbit/sec]
220. 2023-06-12 18:53:11.491197 0.000000 IntelCor_98:58:0f IntelCor_98:.		-76 dBm 5, func+RR, N(R)=0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command	> Tag: Power Capability Hin: 0, Hax: 9
220. 2023-06-12 18:53:11.491242 0.000045 IntelCor_98:58:0f IntelCor_98:.		-77 dBm S, func+RR, N(R)+0: DSAP NULL LSAP Individual, SSAP NULL LSAP Command	Tag: RSN Information
220. 2023-06-12 18:53:11.491353 0.000111 IntelCor_98:58:0f IntelCor_98:.		-77 dBm S, func+RR, N(R)=0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command	Tag Number: RSN Information (48)
220. 2023-06-12 18:53:11.491399 0.000046 IntelCor_98:58:0f IntelCor_98:.		-76 dBm S, func+RR, N(R)+0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command	Tag length: 42
220, 2023-06-12 18:53:11.491965 0.000566 IntelCor 98:58:0f IntelCor 98:.		-77 dBm S, func+RR, N(R)+0: DSAP NULL LSAP Individual, SSAP NULL LSAP Command	RSN Version: 1
220. 2023-06-12 10:53:11.500563 0.016590 IntelCor_90:50:0f Cisco_13:00:		-63 dem Authentication, SN+16, FN+0, Flags+C	> Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCH)
220. 2023-06-12 18:53:11.508632 0.000009 192.168.1.15 192.168.1.121		-36 dBm Acknowledgement, Flags+C	Pairwise Cipher Suite Count: 1
220. 2023-06-12 18:53:11.513546 0.004914 Cisco_13:00:e7 IntelCor_90:		-36 dBm Authentication, SN=161, FN=0, Flags=C	> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCH)
220. 2023-06-12 18:53:11.513546 0.000000 192.168.1.15 192.168.1.121		-62 d8m Acknowledgement, Flags+C	Auth Key Management (ARM) Suite Count: 1
- 220. 2023-06-12 18:53:11.514178 0.000632 IntelCor_98:58:0f Cisco_13:00:		-66 dBm Reassociation Request, SN+17, FN+0, Flags+C, SSID+"wifi6E_test"	> Auth Key Management (AUN) List 00:0f:ac (Ieee 802.11) SAE (SMA256)
220. 2023-06-12 18:53:11.514178 0.000000 192.168.1.15 192.168.1.121		-36 dBm Acknowledgement, Flags+C	> RSN Capabilities: #x00fc
220. 2023-06-12 18:53:11.527665 0.013487 Cisco_13:00:e7 IntelCor_98:		-36 dBm Reassociation Response, SN+0, FN+0, Flags+C	PHKID Count: 1
220, 2023-06-12 10:53:11,527665 0.000000 192,160.1.15 192,160.1.121		-62 dBm Acknowledgement, Flags+C	V PHOLD List
		-36 dBm I P, N(R)+54, N(S)+122; DSAP XNS Group, SSAP Netware Response	PVKID: 666273181996e329c292171380276e25
220. 2023-06-12 18:53:11.528445 0.000040 IntelCor_98:58:0f Broadcast		-36 dBm I, N(R)=77, N(S)=27; DSAP 0x1e Individual, SSAP XNS Command	> Group Hanagement Cipher Suite: 00:0fiac (Ieee 802.11) 8IP (128)
220. 2023-06-12 18:53:11.530430 0.001905 192.168.1.15 192.168.1.121		-36 dBm Request-to-send, Flags+C	> Tag: Supported Operating Classes
220. 2023-06-12 18:53:11.530638 0.000208 Cisco_13:80:e7 IntelCor_98:		-36 dBm Key (Hessage 1 of 4)	> Tag: RM Enabled Capabilities (5 octets)
220. 2023-06-12 18:53:11.530638 0.000000 192.168.1.15 192.168.1.121		-67 dBm Acknowledgement, Flags+C	> Tag: Extended Capabilities (10 octets)
220, 2023-06-12 10:53:11.533160 0.002530 IntelCor 90:50:0f Cisco 13:00:		-67 dBm Key (Nessage 2 of 4)	> Tag: Vendor Specific: Hicrosoft Corp.: WHM/WHE: Information Element
220. 2023-06-12 10:53:11.533168 0.000000 192.168.1.15 192.168.1.121		-36 dbm Acknowledgement, Flags+C	> Tag: Vendor Specific: Intel Wireless Network Group
220, 2023-06-12 10:53:11.534769 0.001601 192.168.1.15 192.168.1.121		-36 dBm Request-to-send, Flags+C	Tag: RSN extension (1 octet)
220. 2023-06-12 10:53:11.535072 0.000303 Cisco_13:00:e7 IntelCor_90:		-36 dBm Key (Nessage 3 of 4)	Tag Number: RSN extension (244)
220, 2023-06-12 10:55:11.555072 0.000000 192.168.1.15 192.168.1.121		-Jo dom Key (Hessage 5 of 4) -70 dom Acknowledgement, Flags+C	Tag length: 1
220, 2023-06-12 10:55:11.535907 0.000000 192:100:1115 192:100:11124		-70 dim Key (Hessage 4 of 4)	✓ R5NX: 0×20 (octet 1)
220. 2023-06-12 18:53:11.535907 0.000000 192.168.1.15 192.168.1.121		-36 dBm Acknowledgement, Flags+C	0000 = KSXX Length: 0
220, 2023-06-12 18:53:11.545206 0.009299 Cisco 13:80:ed Broadcast		-36 dBm Beacon frame, SN+974, FN+0, Flags+C. BI+100, SSID+"wifi6E test 02".	
220, 2023-06-12 10:53:11.545206 0.000000 192.168.1.15 192.168.1.121		-46 dom Request-to-send, FlagsC	= SAE wash to element: 1
220. 2023-06-12 18:53:11.545206 0.000000 Ciscover_53:ca:50 IntelCor_98:		-46 dBm I, N(R)=16, N(S)=21 DSAP NULL LSAP Group, SSAP 0x6e Command	00 = Reserved: 0x0
220, 2023-06-12 18:53:11.545206 0.000000 192.168.1.15 192.168.1.121		-72 dBm Acknowledgement, FlagsC	Ext Tag: HE Capabilities
220, 2023-06-12 10:55:11.556775 0.011569 192.160.1.15 192.160.1.121		-72 dim Request-to-send, Flags+C	Ext Tag: HE 6 GHZ Band Capabilities
220. 2023-06-12 10:53:11.556775 0.0011509 192.160.1.15 192.160.1.121 220. 2023-06-12 10:53:11.556775 0.000000 192.160.1.15 192.160.1.121		-36 dBm Clear-to-send, Flags+C	
220. 2023-06-12 18:53:11.556977 0.000000 192.168.1.15 192.168.1.121 220. 2023-06-12 18:53:11.556977 0.000202 IntelCor_98:58:0f Broadcast		-76 dBm I P, N(R)+67, N(S)+77; DSAP @x48 Individual, SSAP Banyan Vines Command	
220_2023-06-12 10:53:11.556977 0.000000 192.168.1.15 192.168.1.121		-75 dem 1 P, N(K)+67, N(5)+77; USAP exke individual, SSAP earlyen vines commend -36 dem Acknowledgement, Flags+C	
	76 9		

WPA3 SAE + FT Reassociation Request

#### Client details in WLC:

Search Menu Items	Monitor	ring • > Wireless •	> (	Clients			Client	
	Clients	Sleeping Clien	ts	Excluded Client	ts		360 View General QOS Statistics ATF Statistics Mobility History Call Statistics	
Dashboard Monitoring	×	Delete Ø					Client Properties AP Properties Security Information Client Statistics QOS Properties EoGRE Client State Servers None	
Configuration	Selec	ted 0 out of 12 Clients					Client ACLs None Client Entry Create Time 380 seconds	
	0	Client MAC Address	Ŧ	IPv4 Address	IPv6 Address	AP Name	Policy Type WPA3	
Administration	0	286b.3598.580f	×	192.168.1.159	fe80::ac5b:e1e1:67ba:c353	AP6849.9253.CA50	Encryption Cipher CCMP (AES)	
Licensing	0	60fb.008b.0e66	×	N/A	N/A	AP01_RC_9136_F800		
,	Ο	34ea.e702.6240	×	192.168.1.70	N/A	AP6849.9253.CA50	EAP Type Not Applicable Session Timeout 86400	
Troubleshooting	0	a810.87bb.b833	×	192.168.1.94	fe80::aa10:87ff:febb:b833	AP03_Sotao_9548	Session Manager	
	Ο	9669.5a28.a115	×	192.168.1.138	fe80::9469:5aff:fe28:a115	AP01_RC_9136_F800		
	0	84d8.1b0f.294f	×	192.168.1.91	N/A	AP03_Sotao_9548	Point of Attachment capwap_90000010	
	0	0c8b.9509.3518	×	192.168.1.129	N/A	AP03_Sotao_9548	IIF ID 0x9000010	
Walk Me Through >	0	0012.17e2.4b40	×	192.168.1.31	fe80::212:17ff:fee2:4b40	AP04_OutdoorF_3DC8	8 Authorized TRUE Common Session ID 00000000000FC9B0F311A6	
	0	0012.17e2.4856	×	192.168.1.37	fe80::212:17ff:fee2:4856	AP05_Outdoor8_2200		
	0	0012.17e1.dd57	×	192.168.1.33	fe80::212:17ff:fee1:dd57	AP03_Sotao_9548	Auth Method Status List	

### NetGear A8000

Connection OTA with focus on the RSN information from client. Initial connection:

ko.	Time	Delta	Source	Destination	Protocol	Length	Channe	Signal strength	BSS Id	Info	> Frame 21: 256 bytes on wire (1728 bits), 236 bytes captured (1728 bits) on interface \Device\WPF_{00578995-2008-60
	1 18:54:49.385337		0 Cisco_17:00:ed	Broadcast	892.11	508		5 -36 dBm	38:91:37:13:80:ed	Beacon frame, S0+422, F0+0, flags+C, 82+100, SSID="wified_test_02", SSID="wif	<ul> <li>Ethernet II, Seci Claco_dd:7d:37 (00:0f11d:dd:7d:37), Dxt: Universa_D7:cf:06 (00:1a:00:07:cf:06)</li> <li>Internet Protocol Version 4, Sec: 102.108.1.15, Dxt: 102.108.1.125</li> </ul>
	2 18:34:49.487544	0.58228	07 Cisco_13:00:ed	Broadcast	862.11	5496		5 -36 (00)	38:91:57(13)801ed	Beacon Frame, 58+427, F8+0, Flags+C, 82+100, 5525-"xdF166_test_82", 5525+"xdF	
	3 18:34:49.589867	0.38232	S Cisco 11:80:ed	Broadcast	882.11	500		5 -37 die	38:91:57:13:80:ed	Beacon Frame, SN+632, Hiele, Flags+C, 82+100, 55320-"hd/fi62_test_42", 5520+"hdf	> User Detagram Protocol, Src Port: 5555, Dat Port: 5000
	4 18:34:49.892332	8.38246	6 Cisco 13:80 ed	Broadcast	882.11	548		5 -32 day	061951071531001ed	Beacon frame, Studi7, Hues, FlagssC, 81+100, SSID-"ud-Fist_test_80", SSID-"ud-F	> AiroPeek/OmriPeek encapsulated IEEE 802.11
	5 18:34:49.793804	0.20867	2 Netpear 48:70:95	Cisco 13:88:e7	802.11	368		5 -49 dim	38:01:b7:13:80:e7	Probe Request, SWoD4, Flw4, Flags+C, SSED+"wdfist test"	) BR0.11 radio information
	6 18:34:49.793884		0 102.168.1.15	192.168.1.121	862.11	- N		5 -17 dlm		Arian-Jatamant Bana /	> IOE H02.11 Association Request, Flags:C
	7 18:34:49.795356		2 Setgear 48:79:95	Cisco 13:80:#7	882.52	168		5 -49 dBs	10-01-02-11-00-42	Probe Request, SHvil, FN+0, FlagssC. SSIDs"wifist test"	✓ IEEE 802.11 Wireless Management
	8 18(34)49,795427		1 192.368.1.15	192.168.1.121	882.11	26		5 -37 dla		Acknowledgement, FlagsC	<ul> <li>Fixed parameters (4 bytes)</li> </ul>
	9 18:14:49,794493		6 Cisco 17:80:ed	Broadcast	882.11	528		5 -37 dBm	18:11:57:11:80:ed	Beacon frame, Sk-642, Fis-B, Flags+	) Capabilities Information: 0x1511
	10 18:34:49.838282		0 Netgear_48(29)95	Cisco_130800#7	882.11	368		5 -49 (04	18:01:57(11:88)e7	Probe Request, SH-12, FM-0, FlagsC, SSID-"wif16E_test"	Listen interval: 0x0000
	11 18:14:49.454290		0 192.368.1.15	192.368.1.321	882.11			5 -17 dbs	Second Construction	Acknowledgement, Flags	<ul> <li>Tagged parameters (122 bytes)</li> </ul>
	12 18:34:49.874951		0 Netgear 48:20:25	Cisco 10:80:e7	942.11	194		5 -42 day	18:11:17:13:80:e7	Authentication, Sol, Ned, FlagsC	) fag: SSID parameter set: "wifiel_test"
	13 18:34-49.474951		0 192.158.1.15	192.368.3.121	802.11	26		5 -17 dbs	Decarder recenter	Acknowledgement, FlagssC	> Tag: Supported Rates 6(8), 9, 12(8), 18, 26(8), 36, 48, 54, [Mbit/sec]
					862.11	194		5 -37 dla		Activation, Shida, Nee, FlagsC	> Det Tag: HE Capabilities
	14 18:34:49.898563 15 18:34:49.898563		2 Cisco_13:80:e7 0 192.168.1.15	Netgear_48179:55 192,368,1,323	882.11	254		5 -49 dlm	38:93:07(13):80;67		5 Ext Tar: HE 6 GHz Band Capabilities
										Acknowledgement, Flags+C	) fag: Wender Specific: Ralink Technology, Corp.
	16 18:34:49,994966		S Cisco_13:80:ed	Broadcast	842.11	546		5 -37 d8e	38:91:57:15:80:ed	Beacon frame, SN-647, Hu-0, FlagsC, 81+100, 5512+"wd-Fi86_test_82", 5512+"wd-f	> Tag: Extended Capabilities (20 octets)
	17 18:34:49.904966		0 Netpear_48:70:95	Cisco_13:80:#7	802.11	138		5 -49 dBt	38:91:57:13:80:e7	Authentication, SN-5, FN-8, FlagsC	1 Tag: Wender Specific: Microsoft Corp.; WHY/WE: Deformation (Lenert
	18 18:34:49.984966		0 152,168.1.15	192.168.1.121	942.11	- 76		5 -37 dBm		Acknowledgement, Flags+C	V Tag: KN Information
	19 18:34:49.904966		0 Cisco_13:80:e7	Netgear_48:70:95	862.11	238		5 -37 die	38:91:57:11:88:47	Authentication, SN-547, FN-0, FlagsC	Tag Number: HSA Information (48)
	20 18:34:49.984966		0 192.168.1.15	192.188.1.121	882.11	75		5 -48 dBt		Acknowledgement, Flags+C	Tag length: 22
	21 18:34:49.004966		0 Netgear_AB179195	Cisco_10:80:e7	802.11	235		5 -49 454	38:91:57:13:80)47	Association Request, SN+6, FlagssC, SSID="addisk_text"	RSV Version: 1
	22 18:34:49.984966		0 192.168.1.15	192.168.1.121	882.33	- 76		5 -36 dBr		Acknowledgement, FlagseC	> Group Cipher Sulte: 00:0f:ac (leve NU2.11) ALS (CDM)
	23 18:34:49.915474	0.00058	H Cisco_11:80:e7	Netgear_48:79:95	882.11	362		5 -36 dbt	38:91:57:13:80:47	Association Response, Sk-0, Hk-0, Flags+C	Patrolice Clother Solite County 1
	24 18:34:49.915474	0.00000	0 192.168.1.15	192.168.1.121	862.11	- 76		5 -49 dbn		Acknowledgement, Flags+C	> Paindise Cipher Suite List 00:07:ac (Seee M0.31) ALS (CON)
	25 18:14:49.911719	0.00024	is Netgear_48:70:95	Broadcast	LLC	114		5 -37 dbs	38/91/67/13:80:47	U, Func-KP) DSAP BKI2 Individual, SSAP BK62 Command	
	25 18:34:49.911719	0.00000	0 Netgear_48:70:05	Broadcast	LLC	134		5 -36 d8n	58:91:b7:13:80:e7	U, func-vinknown; DSAP Bx7s Individual, SSAP Bx6H Response	Auth Key Ranagement (ARR) Subte Count: 1
	27 18:34:49.922346	0.05042	7 Cisco 13:80:47	Netgeor 48:20:05	EXPOS.	225		5 -36 dla	38:91:b7:13:80:e7	Key (Message 1 of 4)	✓ Auth Key Management (AUM) List 00:00f:ac (Leve BR2.11) SAE (S96256)
	28 18:34:49.922348	0.00000	0 192.168.1.15	192.168.1.121	882.11	75		5 -49 dlm		Acknodedgement, FlagsC	✓ Auth Key Management (ARM) Suite: 00:0Fisc (Lees 802.11) SAE (SHA256)
	29 18:34:49.999581	8.87721	5 Cisco 11:Mont	Broadcast	882.11	501		5 -36 dbs	18:91:07:13:80:ed	Beacon frame, 50-452, 80-0, FlagsC, 82-100, 5535-"ud-finit text 82", 5535-"ud-f	Auth Key Management (AMM) CUI: 00:04:ac (leve 802.11)
	30 18:34:58.104518		9 Cisco 13:80:ed	Broadcast	882.11	505		5 -35 dbr	38:91:57:13:80:ed	Beacon frame, SN-457, FN-0, FlagsC, 81-100, SSID-"hdf560_test_82", SSID-"hdf	Auth Key Hanagement (ARM) type: SAE (SHR256) (8)
	11 18:14:58.284608		0 Cisco 11:00red	Broadcast	882.11	500		5 -17 day	18:91(b7:11:80:ed	beacon frame, Studio2, Hu-0, FlagsC, 82-100, 55325-"ud-Finit test 82", 55225-"ud-F	<ul> <li>RSW Capabilities: Booker</li> </ul>
	12-18-14-18-212615		5 Setgear 48:79:55	Cisco 13:80:e7	EAPOL	228		5 -55 dlin	38:91:57:12:80:e7	Key (Ressage 2 of 4)	
	13 18:34:50.211615		0 192,168.1.15	192.168.1.121	882.11	25		5 -42 dis		Acknowledgement, FlagsC	
	34 18:34:38.213376		1 Cisco_13080:#7	Netgear_48170195	LAPEL	295		5 -35 dBt	10-01-h7-11-00-e7	Key (Nessage 3 of 4)	00., = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STG
	35 18:34:58.213376		0 192.168.1.15	192.168.1.121	882.11	26		5 -50 dan	an-reason station of	Acknowledgenett, Flags	
	36 18:34:58.214354		% Netgear_48:70:95	Cisco_13:80:#7	EAPOL	199		5 -56 dbr	14:75:57:13:80:47	Key (Pethods 4 of 4)	
	17 18:14:59.214354		0 192.168.1.15	192.168.1.121	582.11	200		5 -42 dla	10.712.0112.0100.007	Acknowledgement, Flags	+ Management Frame Protection Capable: True
	IN 18114-18-228721		7 152.158.1.15	192.168.1.121	802.11	- 2		5 -42 dim		Acknowledgement, FlagsC	
	10 18:14:14.10.220721		8 192.188.1.15		882.11	110		5 -42 dat			
				192.168.1.121						trigger Buffer Status Report Poll (HERP), FlagsC	
	#0 18:34:50.224849		0 AlticeLa_0e:59:af	Netgeor_48:20:55	LLC .	223		5 -44 dbt	38:91:57:13:80:47	U, Func-Unknown; DSAP Ibdel Group, SSAP Ibdel Response	MAXID Count: 0
	45 18(34)58.224849	0.00000	0 152.158.1.15	192.368.1.121	882.13	- 76		5 -54 dbs		Acknowledgement, Flags+	PMKID List
											5 Tag: KN extends (1 octet)
											> Tag: WM Enabled Capabilities (5 octets)

SSSS

Client details in WLC:

Cisco Cataly	yst 9800-CL Wireless	Controller			Welcome admin 🛛 🕷 📽 🖺	Search APs and	Clients Q
Q. Search Menu Items	Monitoring • > Wireless •	> Clients			Client		×
	Clients Sleeping Clier	nts Excluded Clier	ts		360 View General QOS Statistics	ATF Statistics Mobility History	Call Statistics
Dashboard	_				Client Properties AP Properties Secu	rity Information Client Statistics	QOS Properties EoGRE
Monitoring >	× Delete				Client State Servers	None	
Configuration	Selected 0 out of 13 Clients	)			Client ACLs Client Entry Create Time	None 11 seconds	
0	Client MAC Address	s T IPv4 Address T	IPv6 Address	AP Name	Policy Type	WPA3	
(O) Administration	9418.6548.7095	ا 192.168.1.163 ا	fe80::ce19:6f16:279d:515f	AP6849.9253.CA50	Encryption Cipher	CCMP (AES)	
C Licensing	286b.3598.580f	ا 192.168.1.159	fe80::ac5b:e1e1:67ba:c353	AP6849.9253.CA50	Authentication Key Management	SAE	
	60fb.008b.0e66		N/A	AP01_RC_9136_F80C	EAP Type Session Timeout	Not Applicable 86400	
Y Troubleshooting	<b>3</b> 4ea.e702.6240	ا 192.168.1.70	N/A	AP6849.9253.CA50	Session Manager	00400	
	<b>9669.5a28.a115</b>	ا 192.168.1.138 ا	fe80::9469:5aff:fe28:a115	AP01_RC_9136_F80C			
	84d8.1b0f.294f	ا 192.168.1.91	N/A	AP03_Sotao_9548	Point of Attachment	capwap_90000010	
	Oc8b.9509.3518	192.168.1.129	N/A	AP03_Sotao_9548	IF ID	0x90000010	
Walk Me Through >	0012.17e2.4b40	/ 192.168.1.31	fe80::212:17ff:fee2:4b40	AP04_OutdoorF_3DC8	Authorized Common Session ID	TRUE 000000000000000000000000000000000000	
and the standard by a	O 0012.17e2.4856	192.168.1.37	fe80::212:17ff:fee2:4856	AP05_Outdoor8_2200		0x000000000000000000000000000000000000	
	0012.17e1.dd57	192.168.1.33	fe80::212:17ff:fee1:dd57	AP03_Sotao_9548	Auth Method Status List	*********	
	∺ 4 1 2 ▶	H 10 ¥			Method	SAE	

### Pixel 6a

Device was not able to roam when FT is enabled.

### Samsung S23

Device was not able to roam when FT is enabled.

### WPA3-Enterprise + AES(CCMP128) + 802.1x-SHA256 + FT

### WLAN Security configuration:

Configuration * > Tags & Profiles * > WLAN	s	Edit WLAN	
	Enable WLAN	Changing WLAN parameters while it is enabled will result in ions of connectivity for cliness connected to it.	
Monitoring > Selected WLANs : 0		General Security Advanced Add To Policy Tags	
Configuration > Configuration > Name	T D	Layer2 Layer3 AAA	
Administration , O O dot1x	2	O WPA + WPA2 O WPA2 + WPA3 O Static WEP O	None
Joursting OWL, Transform	× 4 × 6	MAG Fitering O Lobby Admin Access O WPA Parameters WA O WPA2 O Policy GTK O WPA2 O Cover the DS O Policy Transition O Reassociation Timeout * 20	a
		Disable         WPA2/WPA3 Encryption           A55(0CMP128)         CCMP256           GCMP128         GCMP256           Protected Management Frame         SN2 50	× 0
		PME Recurred  Association Comeback Time* SA Query Time* 200	

WPA3 Enterprise 802.1x-SHA256 + FTWLAN Security Configuration

### View on WLC GUI of the WLAN Security settings:



Here we can see the ISE Live logs showing the authentications coming from each device:

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint Profile	Authenticat	Authorizati	Authorizati	IP Address		Network Device
<				Identity	Endpoint ID	Endpoint Profile	Authentication	Authorization	Authorization	IP Address	~	Network Device
Jun 27, 2023 01:52:38.130 PM	•	a	0	tantunes	04:29:2E:C9:E3:71		WirelessDot	WirelessDot	PermitAccess			
Jun 27, 2023 01:52:38 130 PM		a		tantunes	04:29:2E C9:E3:71		WirelessDot	WirelessDot	PermitAccess			eWLC-9800-01
Jun 27, 2023 01:51:53.850 PM	•	a	0	tantunes	24:95:2F:72:8A:66	Unknown	WirelessDot	WirelessDot	PermitAccess			
Jun 27, 2023 01:51:53.850 PM		.0		tantunes	24:95:2F:72:8A:66	Unknown	WirelessDot	WirelessDot	PermitAccess			eWLC-9800-01
Jun 27, 2023 01:50:58.679 PM	•	a	0	tantunes	94:18:65:48:70.95	Netgear-Device	WirelessDot	WirelessDot	PermitAccess			
Jun 27, 2023 01:50:58.679 PM				tantunes	94.18:65:48:70:95	Netgear-Device	WirelessDot	WirelessDot	PermitAccess			eWLC-9800-01
Jun 27, 2023 01:50:43.883 PM		0		tantunes	94:18:65:48:70.95	Netgear-Device	WirelessDot	WirelessDot	PermitAccess			eWLC-9800-01
Jun 27, 2023 01:50:42.877 PM	0	Q	0	tantunes	28.68:35.98:58.0F	Intel-Device	WirelessDot	WirelessDot	PermitAccess			
Jun 27, 2023 01:50:42.877 PM		0		tantunes	28.6B:35.98.58.0F	Intel-Device	WirelessDot	WirelessDot	PermitAccess			eWLC-9800-01

ISE Live Logs

### Beacons OTA look like this:

Time	Delta	Source	Destination	Protocol	Length Ch	annel Signalist		> frame 327: 428 bytes on vdrw (3424 bits), 428 bytes captured (3424 bits) on interface 'Decics/WW(D4378085-2018-4466-8C33-C34116643408), ) (therwet IL, Src: Clace d2:07:47 (36:11:32:42:97:47), Det: Universa 57:c7:68 (38:137:c7:08))
124 3.4098421	0.011949	IntalCor_98:58:64	Broadcast	802.11	268	51 -40 dbs	Probe Request, SH-2664, Ph-0, FlagsC, SSID-Gildcard (Broadcast)	<ul> <li>Dervet Potteol Weiter A. Sci 101 164.15. Det 101 164.111</li> </ul>
125 3.105402		£1400_MI:7/F:38	Broadcast	882.53	374	55 -32 dile	Probe Response, Study, Fluely, FlagsC, 81-280, SSID-"schiet_text", SSID-sclidcart (Broadcast)	5 Internet revision (writing is, b): and an internet set (b): and an internet set (b): an other bit and the revision (b): and an internet set (b): an int
326 3.713368	0.053868	£1sco_dd:78:38	Broadcast	892.11	374	53 -35 dile	Probe Response, Sp.2005, Phys. Flags. C. 82-200, SSID-"sidiat test", SSID-Wildcard (Broadcan.	> view unagree restored, set port: 500, ust rent: 5000 > Attrobust (Denis) and the exception of the BU(1)
327 3.727583		Cisco_dd:7d:38	<b>Broadcast</b>	882.11	428	55 -35 dat	Beacon Frane, Sho3006, He-R, FlagsC, 81-500, 5510-"wifing_test", SiD-Mildcard (Broadcast)	> Altower(unitive: ecopialitie) list mc.11 > MC.11 ratio information
128 3.734811	8,007308	202.268.1.25	292.168.1.121	882.11	26	5.3 -40 108	Clear-Ni-Sent, Flagis	) DE NG 11 PARTY FINE FLEET
178 3.747806	#. #52995	CLoco_dd:7d:38	Broadcast.	882.13	3274	53 -33 dBr	Probe Response, SN-2007, HW-9, FlagsC, 80-000, SSID-"wdFint_test", SSID-Mildcard (Broadcas.	
179.3.759204	0.811798	IntelCor_98:58:00	Cisco_dd:7d:88	882.11	96	51 -40 dbs	Authentication, SW-01, HH-0, FlagsC	V IIIE BE: 11 Kirsless Recapsed
181 3.763938	8.004712	E1400_MIT/6:38	IntelCor_98:58:HF	882.55	96	53 -33 dBe	Authentication, Sted, FNed, FlagsC	> Sixed parameters (12 bytes)
183 3,764858	0.000142	IntelCor_98:58:00	Cisco_dd:7d:38	882.53	274	53 -42 dim	Ressociation Report, SHVR, Flags	<ul> <li>Tagpid parameters (IOS hytes)</li> </ul>
185 3.258913	0.004875	£1sco_dd:7d:38	Broadcasit	802.53	374	53 -13 dile	Probe Response, SN-2008, NN-8, FlagsC, 82-000, SSID-'sdfild_test', SSID-wildcard (Broakcas.	> Tag: SSID parameter set: "withR_test"
386 3.772296	0.001173	148#1Cor 98:58:84	Broadcast	LLC	154	53 -34 dile	U.P., Func-Onknown; DSAP Bude Group, SSAP Birls Command	> Tag: Supported Mates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [MGT/Sec]
367 3,776363	0.004255	CLSco_dd:70:38	IntelCor_38:58:ef	882.33	313	53 -33 dile	Ressociation Response, Ski0, Field, FlagsC	> Tag: Traffic Indication Rep (TIR): 0104 0 of I bitmap
389 3.777572	0.001211	292.368.1.35	192.168.1.121	882.51	82	51 -33 dile	Request-to-send, Flags+C	> Tag: Country Information: Country Code na, Environment Global operating claimes
303 3.777572	8.000000	£1500 dd:70:18	IntelCor_HEISENH	1.02	109	53 -33 dite	Request, Identity	> Tag: Power Constraint: 6
393 3,788848	0.051276	Claco MI:70:38	Broadcast	892.11	374	53 -33 dBs	Probe Response, Sk-2009, Hive, FlagsC, 82-500, SSID="sifiet, test", SSID-sildcard (Broadcas,	> Tag: TDC Report Translet Power; 56, LSAR Margin; 8
394 3.889467	0.020125	Eisco dd:7d:3M	Broadcast	862.11	324	55 -35 dile	Probe Response, Sh-2018, Filed, FlagsC, 81-500, SSIN-"wif160 test", SSID-wildcard (Broadcas.	V Tag: RM Information
395 3.824287	0.054820	intelior_08:5810f	£1400_dd:7d:38	644	117	53 -41 (89)	Response, Identity	Tag Number: HSN Information (48)
397 3.829933	0.005646	\$55co.dd;70:38	Broadcast.	882.33	428	53 -33 dBe	Bascon frame, Shoull, Field, FlagsC, 81-500, SSID-"hdfist test", SSID-bdldard (Broadcast)	Tag Length: 30
398 3.871248	0.001215	192.168.1.15	192.168.1.121	892.11	82	55 -33 dile	Request-to-send, Flags	Ris Werston: 1
400 1.811548	8,00000	CLaco 48:76:38	Intelline 10:58:04	1.02	118	53 -13 dbs	Request, Protected GP (LBP-PERP)	<ul> <li>Group Cipher Subte: 00:247:ac (Leee 882.11) ALS (CDV)</li> </ul>
482 3.829355	0.004807	292.168.1.15	192.168.1.121	882.11	28	53 -45 dile	Clear-to-sent, Flags	Group Clyber Suite OLD: 00:0Flac (lees 802.11)
403 3,850236	0.054283	Cisco dd:7d:38	Broadcast	882.11	374	53 -33 dile	Probe Response, Se-2012, Fe-B, FlagsC, 80-500, SSID-"sdfine test", SSID-sdldcard (Broadcas,	Group Clipher Subte type: AES (CDR) (4)
405 3.851118			Claco dd:7d:38	TL5v5.2	365	\$3 -42 dite	cliert mulo	Paindise Lipher Suite Count: 1
407 3.868558		192.168.1.15	192.168.1.121	842.11	67	55 -35 dire	Nequest-to-send, Flagss	✓ Paindise Cipher Solte List 00:0fiac (Ieee 802.21) AIS (COM)
400 3.862958		Cisco dd:7d:38	1ntelCor_98:58:04	1.64	1116	53 -33 dBe	Request, Protected LAP (LAP-PEAP)	<ul> <li>Painsise Cipher Suite: 00:0f:ac (Lees 000.11) Al5 (CON)</li> </ul>
411 3.963808		istalior bartared	Cisco dd:7d:18	6.62	138	51 -41 day	Response, Protected LAP (LAP-PLAP)	Pairwise Cipher Suite DUI: 00:0ficc (leee 802.11)
413 3.866585		192.168.1.15	192.168.1.121	882.11	82	53 -15 dile	Repet-to-sed, Flags	Pairwise Cipher Suite type: ALS (COP) (4)
415 3.866778		Claco dd:7d:38	IntelCor 98:58:84	71.5v1.2	374	53 - 13 dBe	Latored Unknow Record	Auth Key Management (ABM) Subte Count: 2
417 3.879928		Elsco_dd:76:18	Broadcast	862.11	174	53 -13 dis	Probe Response, Skidstl, Huie, FlagsC. Birdde, SSID-"wifibit test", SSID-adidcard (Broadcas.	Auth Key Management (AMM) List 00:001ac (lees B02.11) FT over LLLE B02.13 00:001ac (lees B02.11) WM (S90256)
418 3.877396		IntelCor 98:58:84	CLINER, 64178138	TL5v2.2	240	53 -42 dile	Client Key Exchange, Dange Cipher Spec, Encrypted Handshake Ressage	<ul> <li>This can be address (read parts) relation (read and real and r</li></ul>
420 3,880938		292.168.1.15	192,168,1,121	842.11	80	53 -13 dBr	Request-to-send, Flags	Auth Key Management (AMM) OLC: M0:0fiac (Leve M02.11)
422 3.888935		Elsco_dd:7/f:38	IntelCor_98:58:04	71.5x5.2	263	51 -11 dbr	Charge Cloher Spec, Encrypted Handshake Ressage	Auth Key Management (ARM) type: FT over IEEE 882.1X (3)
424 3,885572		IntelCor Stitline	C3A(0, 01/20138	1.62	110	53 -43 -884	Response, Protected (AP ((AP-P(AP)	<ul> <li>Auth nay Hanagement (AMM) Sulte: 0010F1ac (Lees 802.11) MHA (SH4256)</li> </ul>
425.3.887787		292, 168, 1, 15	192.568.1.121	862.11	82	\$1 -11 die	Request-to-send, Flags	Auth Key Management (ARM) 001: 00:001ac (Leve M02.11)
425 3.887889		Clace dd:7d:38	IntelCor 98:58:04	TLSv5.2	140	53 -33 dBe	Application Data	Auth Key Ranagament (AMR) type: WR (SM256) (5)
438 3.896392		1vts1cor_98(58)84	Cisco_48(28)18	TLSv5.2	148	53 -43 dbs	Application Data	✓ KSN Capabilities: 0x00e8
412 3.891177		Cisco dd:70:38	Broadcast	882.11	376	55 -35 dile	Probe Response, SN-2814, Heek, FlagsC. 80-000, SSID-"wif166 test", SSID-wildcard (Broadcas,	
413 3.891289		232.368.3.35	192.569.1.121	842.23	82	53 -13 day	Request-to-send, Flags	
435 3.893343		CLoco dd:70:58	LitalCor 98:58:04	TLSv9.2	367	53 -11 dile	Application Outa	
437 3.500079		IntelCor_98:58:00	Cisco dd:7d:38	TLSv2.2	282	53 -43 dBe	Acolication Outs	10
417 3,986079		210.168.1.15	182.348.1.121	HS2.11	282	53 -45 day	Application on a Clear-to-seed, Flags	
443 3.954054		CLaco 40:74:38	Inc. Sec. 1. Lts	862.11	111	53 -45 dla	Probe Response, SH-2015, FM-R, FlagsC, 85-000, SSID-"v(FDR_test", SSID-Mildcard (Broadcas.	
443 3,925584		292.168.1.15	192,168,1,121	892.11	104	53 - 33 dile	Proce Response, Secards, reve, FlagsC. Birdee, SSLD-Wirldigtest', SSLD-Mildigter' (Broadcas, Recust-to-send, FlagsC	- JOSAT ROLLING RANGE RANGE RANGE FALSE
				71592.2	100	53 -35 dile	Application Data	
445 3.925584		Elsco_dd:7d:38	IntelCor_S0:S0:M					
447 3,990023		148x1Cor_98:58:84	C2400_6578138	TLSv1.2	343	53 -43 dBt	Application Data	INCO COURT 0
449 3.932392		Claco_dd:7d:38	Broadcast	882.11	428	53 -33 dbt	Bescon frame, SW-2016, FM-0, FlagsC, 81-100, SSID-"wifisf_test", SSID-Wildcard (Broadcast)	PMCID List
458 3.532998		292.168.1.15	192.568.1.121	882.33	82	53 -33 dBe	Request-to-send, Flags	) Known Menamener ( Knewn Sectors and Car ( Knewn Mill 11) MIP ( 118)
452 3.903074		£1500_00170138	InteScor_9815810H	TL3v2.2	150	53 -34 iller	Application duta	> Tag: Rebility Domain
454 3.905511		141#1Cor_98:58:04	Cinco_dd:7d:38	TLSv1.2	150	55 -42 dbr	Application Owta	> Tax: 0055 Load Element NR2 lie CCA Version

WPA3 Enterprise 802.1x +FT Beacon

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

### Intel AX211

Connection OTA with focus on the RSN information from client on a roaming event:

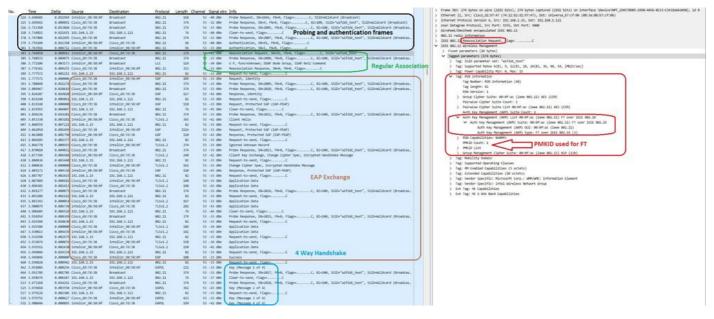
Vo.	Tim	ne	Delta Source	Destination	Protocol	Length (	Channel	Signal stre	Info	> Frame S7: 235 bytes on wire (1888 bits), 235 bytes captured (1888 bits) on interface \Device\WFF_(D4578085-2998-4456-8C33-C143)
	1 0.0	00000	0.000000 Cisco_dd:a0:18	Broadcast	892.11	428	69	-36 dbs	Beacon Frame, SN+220, FN+0, Flags+C, BI+300, SSID+"wiF16E_test"	Ethernet II, Src: Cisco_d2:97:47 (74:11:82:d2:97:47), Dst: Universa_b7:cf:06 (08:3a:88:87:cf:06)
	2 0.1	102260	0.182260 Cisco_dd:a0:18	Broadcast	882.11	428	69	-37 dBm	Beacon frame, SN+221, FN+0, Flags+C, BI+100, SSID+"wdfi66_test"	> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
	3 0.2	204689	0.102429 Cisco_dd:a0:18	Broadcast	882.11	428	69	-36 dBm	Seacon Frame, SN+222, FN+0, Flags+C, BI+100, SSID+"wifi66_test"	> User Datagrae Protocol, Src Port: 5555, Ost Port: 5000
	4 0.2	280665	0.075976 192.168.1.15	192.168.1.121	802.11	76	69		Clear-to-send, Flags+C	AiroPeek/OmiPeek encapsulated IEEE 802.11     802.11 radio information
	57 0.3	994987	0.024322 IntelCor_98:58:8f	Cisto_dd:s0:18	892.11	235	69		Authentication, SW423, HW+0, Flags+C	> BE2.11 Facto Information > IEEE 882.11 Authentication, Flags:C
	58 0.3	105271	0.000284 192.168.1.15	192.168.1.121	802.11	75	69		Acknowledgement, Flags+C	✓ IEEE NR2.11 Wireless Management
	59 0.3		0.001855 Cisco_dd:a0:18	Broadcast	882.11	428			Beacon frame, SN+223, FN+0, Flags+C, BI+100, SSID+"wifi66_test"	<ul> <li>Fixed parameters (6 bytes)</li> </ul>
	58 0.3		0.001697 Elsco_dd:a0:18	IntelCor_98:58:0f	892.11	247			Authentication, SN+12, FN+0, Flags+C	✓ Tagged parameters (100 bytes)
	61 0.3		0.000000 192.168.1.15	192.168.1.121	882.11	76			Acknowledgement, Flags+C	✓ Tag: RN Information
	62.0.3		0.001540 IntelCor_98:58:04	Cisco_dd:a0:18	802.11	372			Reassociation Request, SN+24, FN+0, Flags+C, SSID+"wifi6E_test"	Tag Number: RSN Information (48)
	63 0.3		0.000000 192.168.1.15	192.168.1.121	882.11	75			Acknowledgement, Flags=C	Tag length: 42
	66 0.3		0.028914 Cisco_dd:a0:18	IntelCor_98:58:0f	882.11	433			Reassociation Response, SN+0, FN+0, Flags+C	RSN Vention: 1
	67 0.3		0.000000 192.168.1.15	192.168.1.121	802.11	76			Acknowledgement, Flags+C	> Group Cipher Suite: 00:0f:ac (leee 802.11) AIS (COM)
	68 0.3	346279	0.007002 192.168.1.15	192.168.1.121	892.11	82	69	-68 dbm	Request-to-send, Flags+C	Painwise Cipher Suite Count: 1
										<pre>PHED Cont: 1 PHED CONT PHED CON</pre>

WPA3 Enterprise 802.1x + FT Roaming event

An interesting behavior happens if you manually delete the client from the WLAN (from WLC GUI for example). The client receives a disassociation frame but tries to reconnect to the same AP and uses a re-

association frame followed by a complete EAP exchange because the client details were deleted from the AP/WLC.

This is basically the same frame exchange as in a new Association process. Here you can see the frame exchange:



WPA3 Enterprise 802.1x + FT Ax211 Connection flow

### Client details in WLC:

lonitorin	g* > Wireless* >	Clien	ts						Client							*
lients	Sleeping Clients		cluded Clients						360 View Gene	eral	QOS Statist	ATF Statistics	Mobility History	Call Statistics		
_		2.000							<b>Client Properties</b>	AP	Properties	Security Information	<b>Client Statistics</b>	QOS Properties	EoGRE	
× 0	C								Re-Authentication	Timec	out	1800 sec (Rema)	ning time: 462 sec)			-
-									Client State Server	ris		None				
Selected	d 0 out of 1 Clients								Client ACLs			None				
0	Client MAC Address	٣	IPv4 Address	Ŧ	IPv6 Address	AP Name	۲	SSID	Client Entry Create	Time		1338 seconds				
0	286b.3598.580f	×	192,168,1,159		2001-8a0-fb91:1c00:c07a:1190:8069:7398	AP9136_5C.F524	1	wihte	Policy Type			WPA3				
farmer.								AND DESCRIPTION OF	Encryption Cipher			OCMP (AES)				
1.1	1 1	• 0							Authentication Key	Mana	gement	FT-802.1x				
									EAP Type			PEAP				
									Session Timeout			1800				

WPA3 Enterprise 802.1x + FT Client details

This client was also tested using FT over the DS and was able to roam using 802.11r:

No.	Time	Delta	Source	Destination	Protocol	Length (	Channel	Signal stre	Info		Frame 3084: 372 bytes on wire (2976 bits), 372 bytes captured (2976 bits) on interface 1
	3028 16.491589	0.102243	Cisco_dd:aW:18	Broadcast	882.11	364	62	-36 dBn	Beacon frame, SN+387, FN+0, Flags+C, 81+100, SSID+"xd#		Ethernet II, Src: Cisco_d2:97:47 (74:11:b2:d2:97:47), Ost: Universa_b7:cf:86 (88:3a:88:b
	3829 16.594273	0.102684	Cisco_dd:a0:18	Broadcast	882.11	364	69	-36 dBm	Beacon frame, SN=388, FN=0, Flags=C, BI=100, SSID="wif		Internet Protocol Version 4, Src: 192.168.1.15, Ost: 192.168.1.121
	3838 16.644794	0.050521	IntelCor_98:58:0f	Broadcast	892.11	268	62	-45 d8e	Probe Request, SN+527, FN+0, Flags+C, SSID+Wildcard (B		User Datagnam Protocol, Src Port: 5555, Dst Port: 5000
	3831 16.644794	0.000000	Cisco_dd:a0:18	Broadcast	882.11	312	69	-38 dbt	Probe Response, SN-460, FN+0, Flags+C, BI+100, SSID+"w		AiroPeek/OmniPeek encapsulated IEEE 802.11
	3879 16,696429	0.051635	Cisco_dd:a0:18	Broadcast	802.11	364	69	-38 dBm	Beacon frame, SN+390, FN+0, Flags+C, 81+100, SSID+"wdf		802.11 radio information
	3898 15.701455	0.005826	IntelCor_98:58:0f	Cisco_dd:a0:18	882.11	235	69	-46 dbt	Authentication, S0x31, FNx0, Flags+C		IEEE 802.11 Reassociation Request, Flags:C
	3081 16,701542	0.000087	192.168.1.15	192.168.1.121	892.11	76	69	-39 dBe	Acknowledgement, Flags+C	v	IEEE 882.11 Wireless Management
	3882 16.706278	0.004736	Cisco_dd:a0:18	IntelCor_98:58:0f	882.11	247	60	-35 dbt	Authentication, SN+119, FN+0, Flags+C		> Fixed parameters (S0 bytes)
	3083 16.706278	0.000000	192,168.1.15	192.168.1.121	882.11	-76	69	-39 (58	Acknowledgement, Flags+C		✓ Tagged parameters (272 bytes)
	3084 16.708297	0.002019	IntelCor_98:58:84	Cisco_dd:a0:18	802.11	372	60	-48 dbs	Reassociation Request, SN+32, FN+0, Flags+C, SSID+"wdf		> Tag: SSID parameter set: "wifi66_test"
	3085 16.708297	0.000000	192,168.1.15	192.168.1.121	892.11	76	69	-38 dBH	Acknowledgement, FlagswC		> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Mbit/sec]
	3067 16.718126	0.009829	Cisco_dd:a0:18	IntelCor_98:58:0f	882.11	433	60	-39 d8m	Reassociation Response, SN+0, FN+0, Flags+C		> Tag: Power Capability Min: 0, Max: 9 V Tag: RDN Information
	3088 16.718126	0.000000	192.168.1.15	192.168.1.121	892.11	26	69	-41 dbe	Acknowledgement, Flags+C		
	3091 16.727349	0.009223	IntelCor_98:58:0f	IPv6ecast_FF19e1591aF	LLC	223	60	-59 d8n	1 P, N(R)+90, N(S)+182; DSAP SMAP Group, SSAP 0xde Response		Tag Number: RSN Information (48)
	3892 16.727457	0.000108	192.168.1.15	192.168.1.121	882.11	76	69	-47 dbm	Acknowledgement, Flags+C		Tag length: 42
	3895 16.748833	0.013376	IntelCor_98:58:0F	Broadcast	LLC	515	69	-59 dBt	U P, Func-Unknown; DSAP exi6 Individual, SSAP exi62 Command		RSN Version: 1
	3096 16.740833	0.000000	192.168.1.15	192.168.1.121	882.11	76	60	-48 d8e	Acknowledgement, #lags=C		> Group Cipher Suite: 00:0f:ac (Ieee 802.13) ALS (CCM)
	3899 16.742984	0.002071	Cisco_5c:f8:0c	IntelCor_98:58:0F	LLC	183	69	-58 d8m	I P, N(R)=113, N(S)=72; DSAP Ungermann-Bass Individual, SSAP 8		
	1100 16.742904	0.000000	192.168.1.15	192.168.1.121	892.11	76	62	-53 dbs	Acknowledgement, Flags+C		> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (COM)
	3101 16.742904	0.000000	Cisco_Scif8:0c	IntelCor_98:58:0f	LLC	283	69	-50 dae	I, N(R)=16, N(S)=75; DSAP SMAP Individual, SSAP Bx7c Command		Auth Key Management (ARM) Suite Count: 1
	1102 16.742984	0.000030	192.168.1.15	192.168.1.121	802.11	76	60	-53 dBt	Acknowledgement, Flags+C		> Auth Key Management (A0M) List 00:0f:ac (Leee S02.11) FT over LEEE 802.1X
	3106 16.768589	0.025525	IntelCor_98:58:8f	Diviscast_ff:9e:59:af	LLC	223	69	-59 dbm	I P, N(R)=16, N(S)=31; DSAP 0x48 Individual, SSAP 0x64 Respons		> KON Capabilities: BANDYC
	3107 16.768633	0.000124	192.168.1.15	192.168.1.121	992.11	76	69	-45 (01)	Acknowledgement, Flags+C		PMKID Count: 1
	3109 16.772475	0.003842	Cisco_dd:a0:18	IntelCor_98:58:0f	802.11	118	69	-40 dbs	Action, Skil, Field, Flagss.pC		V PMKID List
	3110 16.772475	0.000000	192.168.1.15	192.168.1.121	882.11	76	69	-52 dBe	Acknowledgement, Flags+C		PMKID: 642cf85b40c421b56e585c13d78f0F77
	3113 16.773542	0.000667	IntelCor_98:58:0f	Broadcast	LLC	179	60	-59 d8m	I P, N(R)+59, N(S)+33; DSAP SHAP Group, SSAP 150 Network Layer		) Groun Management Clober Suite: AB:Afiar (Lees 882 11) 802 (128)
	3114 16.773142	0.000000	192,168.1.15	192.168.1.121	882.11	76	69	-48 dbn	Acknowledgement, Flags+C		V Tag: Mobility Domain
	3115 16.773436	0.000294	intelCor_98:58:04	Cisco_dd:a0:18	802.11	118	60	-48 din	Action, SW+33, FN+0, Flags+.pC[Malformed Packet]		Tag Number: Hobility Domain (54)
	3116 16.773436	0.000000	192.168.1.15	192.168.1.121	882.11	76	69	-41 d8m	Acknowledgement, Flags+C		Tag length: 3
	3120 16.775112	0.001676	AlticeLa_Sec59:af	IntelCor_98:58:0f	LLC	223	69	-49 dBs	U, Func-Unknown; DSAP exil2 Group, SSAP exila Command		Mobility Dowain Identifier: 0xeF27
	3122 16.776545	0.001433	Cisco_dd:a0:18	IntelCor_98:58:0f	802.11	118	69	98 d8m	Action, SN+2, FN+0, Flags+.pC		✓ FT Capability and Policy: 0x01
	1123 16.776545	0.000000	192.168.1.15	192.168.1.121	882.11	- 76	69	-52 dilt	Acknowledgement, Flags+C		1 = Fast 855 Transition over 05: 0d
	1124 16.778399	0.001854	IntelCor_98:58:0f	Cisco_dd:a0:18	892.11	118	62	-48 d8m	Action, 5N+34, FN+0, Flags+.pC[Malformed Packet: length		0. * Resource Request Protocol Capability: 0x0
	3125 16.778399	0.000000	192.168.1.15	192.168.1.121	882.11	76	69.	-40 dim	Acknowledgement, Flags+C		
	3128 15.781449	0.003050	AlticeLa_Sec59:af	IntelCor_98:58:0f	LLC	197	69	-49 dbs	U P, funceSNOPE; DSAP Backe Individual, SSAP Back Command		✓ Tag: Fast BSS Transition
	3132 16.781449	0.000000	IntelCor_98:58:8F	AlticeLa 9e:59:af	LLC	222	69	-58 dBm	U, Func-Unknown; DSAP Bace Group, SSAP Bx64 Command		Tag Number: Fast BSS Transition (55)
	1133 16.781449	0.000000	192.168.1.15	192.168.1.121	882.11	26	62	-47 din	Acknowledgement, FlagssC		Tag length: 96
	3136 16.798815	0.009366	IntelCor_98:58:ef	AlticeLa 9e:59:af	LLC	292	69	-58 dBt	I P, N(R)=84, N(S)=36; DSAP 0x96 Group, SSAP ISO Network Layer		> MIC Control: 0x0300
	3137 16,790815	0.000000	192.168.1.15	292.168.1.121	802.11	76	60	-47 dbs	Acknowledgement, Flags+C		MLC: 491289737c15a2675185Fdc68cc16caf
	3140 16.793414	0.082599	IntelCor_98:58:0f	Broadcast	LLC	515	60	-58 dBs	1, N(R)=68, N(S)=22; DSAP HP Extended LLC Group, SSAP NetWare		Mionce: d514fb17ab7fa885b7fd75e5b6d6a9e882cf4ec50fbd1f492e13089fb1a869cb
	3143 16.793477	0.000063	192.168.1.15	192.168.1.121	882.11	26	60	-47 dbm	Acknowledgement, Flags+C		SNonce: 65c3778b523b83d717c8c897bb28b8ec678edfc365743f3dfb8ae6c7483554fc
	1144 16.793774	0.000297	IntelCor_98:58:0f	Broadcast	LLC	179	69	-58 dbt	S, func+SPEJ, N(R)+12; DSAP 0x70 Individual, SSAP 0x30 Respons		> Subelement: PMK-R1 key holder identifier (R104-10)
	3145 16,793849	0.000075	192,168,1,15	192.168.1.121	882.11	76	69	-48 dBn	Acknowledgement, Flags+C		> Subelement: #MK-M0 key holder identifier (M0MIS-ID)
	3149 16.794563	0.000714	IntelCor_98:58:04	DPvincast_fb	LLC	183	69	-58 dbm	1 P, N(R)=12, N(S)=113; DSAP Exelc Group, SSAP Ex/R Response		> Tag: Supported Operating Classes
	3158 16.794626		192,168.1.15	192.168.1.121	892.11	76	69	-48 dBe	Acknowledgement, Flags=C		> Tag: MM Enabled Capabilities (5 octets)
	1154 16.794926		IntelCor_98:58:04	IPvincast_74:ff:fa	LLC	283		-58 d8e	5 F, Func+SRE3, N(R)+6; 05AP 8x9a Group, SSAP 8x96 Response		> Tag: Extended Capabilities (10 octets)
	3155 16.794998		192.168.1.15	292.168.1.121	882.11	76		-48 dBm	Acknowledgement, Flags=C		> Tag: Vendor Specific: Microsoft Corp.: WMV/WE: Information Element
	1158 16.795654		IntelCor_98:58:04	IPvincast_ff:ba:c3:53	LLC	215		-58 dlm	U F, Func-Unknown; DSAP NULL LSAP Individual, SSAP Banyan Vine		> Tag: Vendor Specific: Intel Wireless Network Group
	3159 16,795699		192.168.1.15	192.168.1.121	882.11	76		-48 dbs	Acknowledgement, Flags+C		> Ext Tag: HE Capabilities
	1168 16.795785		IntelCor_98:58:04	IPv9ecast_ff:79:c5:30	LLC	215		-58 dbs	S, Func+RR, N(R)+SR; DSAP 8x38 Group, SSAP 8xF2 Response		Ext Tag: HE 6 GH2 Band Capabilities
	3161 16,795852		192,168,1.15	192.168.1.121	882.11	76		-45 dbs	Acknowledgement, flagsC		

AX211 roaming with FT over DS

### We can also see the FT roaming events:

Aonitoring	-> Wireless -> Client	s											Clie	ent										
Clients	Sleeping Clients Ex	lude	d Clients										360	View General		QOS Statist	tics	ATF Statistics	1	Mobility H	istory	Call Statistics		
×De	loto 2													Recent associati	ion ł	nistory:								
Selected	0 out of 1 Clients													AP Name	BS	sid T	AP Slot	Assoc Time	Ŧ	Instance	Nobility Note	Run Latency (ms)	Roam Type	٣
0	Client MAC Address	Ŧ	IPv4 Address	٣	IPv6 Address	AP Name	Ŧ	SSID	Ŧ	WLAN ID	Ŧ	Client Type		AP01_RC_9136_F80C	00	df.1ddd.a018	з	08/04/2023 14:24:27		0	Local	15	802.11	R
-	286b.3598.580f	×	192.168.1.159		N/A	AP01_RC_9136_F80C		wifi6E_test		5		WLAN		AP9136_5C.F524	00	df.1ddd.7d38	3	08/04/2023 14:22:59		0	Local	6	802.11	R
	· · · · · · · · · · · · · · · · · · ·																	000040000						

WPA3 Enterprise with FT

### And client ra trace from wlc:

	(QRT) for Hostname: [eMLC-9800-01], Model: [C9800-CL-K9], Version: [17.09.03], SN: [9RY35HS18059] MD_SN: [9RY35HS18059]
	[client-orch-sm] [16210]: (note): MAC: 284b.3590.600f Re-Association received. BSSID 00df.1ddd.7d30, WLAN wifi4K_rest, Slot 3 AP 00df.1ddd.7d30, AP9134_SC.F524, old BSSID 00df.1ddd.a010
	[dot11] [15210]: (note): MAC: 204b.3590.500f Association success. AID 33, Roaming = True, WGB = False, 11r = True, 11w = True Fast roam = True
	(client-orch-sm) (15210): (note): NAC: 20(b.3590.500f Delete mobile payload sent for BSSID: 00df.1ddd.a010 MTP mac: 00df.1ddd.a010 slot id: 3
	(client-orch-state) (15210): (note): MAC: 206b.3598.500f Client state transition: S_CO_RUM -> S_CO_L2_AUTH_IN_PROGRESS
	[client-wuth] [15218]: (note): MAC: 206D.3598.580f ADD MOBILE sent. Client state flags: 0x71 BSSID: HAC: Oldf.1ddd.7d38 capwap IFID: 0x9000000d, Add mobiles sent: 1
	[client=orch=sm] [15210]: (note): NAC: 20%b.3590.500f Mobility discovery triggered. Client mode: Local
	<pre>(client=orch=state) (15210): (note): NAC: 200b.3590.500f Client state transition: S_CO_L2_AUTH_IM_PROGRESS -&gt; S_CO_MOBILITY_DISCOVERY_IM_PROGRESS</pre>
2023/08/04 14:22:59.321064980 (wned_x_R0=0){1}: (	(mm-client) (15218): (note): MAC: 206b.3550.500f Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_INTRA_INSTANCE, Previous BSSID MAC: 00df.1ddd.a010 Client IFID: 0xa0000003, Client Role:
Local PoA: 0x9000000d PoP: 0x0	
2023/08/04 14:22:59.321213982 (wnod x R0-0)(1); (	[client=wuth] [15210]: (note): MAC: 206b.3590.500f ADD MOBILE sent. Client state flags: 0x76 BSSID: MAC: 00df.1ddd.7d30 capwap IFID: 0x9000000d, Add mobiles sent: 1
2023/00/04 14:22:59.321256052 (wned x R0=0){1}: (	[client=orch=state] [15210]: (note): MAC: 20%b.3590.500f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS => S_CO_DPATH_PLUMB_IN_PROGRESS
	(client-orch-state) (15210): (note): MAC: 20(b.3590.500f Client state transition: 5 CO DPAIN FLUME IN FROGRESS ->> 5 CO IP LEARM IN FROGRESS
2023/08/04 14:22:59.321666600 (wned x R0-0)(1): (	(client-orch-state) (15210): (note): MAC: 206b.3598.500f Client state transition: S CO IP LEARN IN PROGRESS -> S CO RUN
2023/08/04 14:24:27.918855521 (wned x R0-0)(1): (	(client-orch-sm) [15210]: (note): HAC: 28(b.3598.580f Re-Association received. BSSID 00df.iddd.a010, WLAH wifi(8_test, Slot 3 AP 00df.iddd.a010, AP01 RC_9136_F80C, old BSSID 00df.iddd.7d38
	(dot11] [15210]: (note): NAC: 286b.3590.580f Association success, AID 33, Roaming = True, NGB = False, 11r = True, 11w = True Fast roam = True
	[client-orch-sm] [15210]: (note): MAC: 20%b.3590.500f Delete mobile psyload sent for BSSID: 00df.1ddd.7d30 WIP mac: 00df.1ddd.7d30 slot id: 3
	(client-orch-state) (15210): (note): MAC: 2040-3550.500f Client state transition: S_CO_RUN => S_CO_L2_AUTH_IN_ERCORRES
	(client-auth) (15210): (note): MAC: 2065.3550.550f ADD HOBILE sent. Client state flags: 0x71 BESID: MAC: 004f.1ddd.s010 capwap IFID: 0x5000000e, Add mobiles sent: 1
2023/08/04 14:24:27.531505871 (whed x 20-0)(1): (	[client-orch-sm] [15218]: (note): NAC: 2840-3858.580f Mobility discovery triggered. Client mode: Local
	[client-orch-state] [16218]: (note): MAC: 286b.8598.580f Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
	mm-client) [15210]: (note): MAC: 2060.3590.600f Mobility Successful. Roam Type Mone, Sub Roam Type MM SUB ROAM TYPE INTRA INSTANCE, Frevious BSSID MAC: 00df.1ddd.7d30 Client IFID: 0xa00000003, Client Role:
Local PoA: 0x5000000e PoP: 0x0	
	(client-auth) (15218): (note): MAC: 206b.3558.580f ADD MOBILE sent. Client state flags: 0x76 BSSID: MAC: 00df.1ddd.a018 capwap IFID: 0x5000000e, Add mobiles sent: 1
	[client-orch-state] [15218]: (note): NAC: 286D.3559.580f Client state transition: S CO MOBILITY DISCOVERY IN PROGRESS
	Client-orch-state) [18210]: [note): MAC: 28cb.3590.800f Client state transition: S CO DPATE FLUME IN PRODESS -> S CO IP LEARN IN PRODESS
	[client=orch=state] [15110]: [note]: MAC: 28cb.3590.500f Client state transition: S CO IP LIABH IN FROMESS → S CO SUM
seed of a strate the sector failed & wo-oldal.	ferene orth start [ firstil [ mark] ; must start start start start start a start of a first start a start of a first start a start of a first

#### NetGear A8000

WPA3-Enterprise is not supported on this client.

### Pixel 6a

Connection OTA with focus on the RSN information from client:

No	2 1	Time	Delta Source	Destnation	Protocol	Length (	Channel Signal stre	Infe	> Frame 925: 261 bytes on wire (2008 bits), 261 bytes captured (2008 bits) on interface (Device/WPF_(D4578905-2908-4456-8C3)-C3431
		1,468897	0.102322 Cisco dd:#0:18	Broadcast	802.11	428	69 -37 dBn	Beacon frame, 5N+3682, FN+0, Flags+C, 81+100, SS1D+"vd	Ethernet II, Src: Cisco_62:97:47 (74:11:b2:62:97:47), Dst: Universa_b7:cf:06 (08:3a:08:b7:cf:06)
		1.562867	0.101970 Google_72:8a:66	Broadcast	892.11	204	69 -29 dlin	Probe Request, SN+1830, FN+0, Flags+C, SSID+"sdfi66_te	) Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
		1,563362	0.000405 Cisco dd:a0:18	Broadcast	892.11	428	69 - 17 dBe	Beacon frame, SN+3683, FN+8, Flags+C, 81+100, SSID+"will	> User Datagram Protocol, Src Port: 5555, Ost Port: 5000
		1.564878	0.000716 Cisco dd:a0:18	Broadcast	802.11	374	69 -37 dlm	Probe Response, SN×108, FN+0, Flags+C, B1×100, SSID+"M	> AiroPeek/OmiPeek encapsulated IEEE 882.11
		1.675576	0.111498 Cisco dd:a0:18	Broadcast	892.11	428	60 - 37 dBs	Beacon frame, SN+3685, FN+8, Flags+C, 81+100, SSID+"xd	> B02.11 radio information
		1.675809	0.000233 Google_72:8a:66	Cisco_dd:a0:18	802.11	208	60 -34 dim	Authentication, SW1031, FM+0, FlagsC	> IEEE 802.11 Association Request, Flags:C
			0.000000 192.168.1.15	192.168.1.121	882.11	75	69 - 37 dbm	Acknowledgement, FlagsC	✓ IEEE 802.11 Mireless Management
		1.675809							> Fixed parameters (4 bytes)
		1.679651	0.003842 Cisco_dd:a0:18	Google_72:8a:66	802.11	208	69 -37 dim	Authentication, SN=14, FN=0, Flags=C	<ul> <li>Tagged parameters (167 bytes)</li> </ul>
		1.679651	0.000000 192.158.1.15	192.168.1.121	882.11	75	69 -34 dBH	Acknowledgement, Flags+C	1 ) Tag: SSID parameter set: "wdfide_test"
10		1.681281	0.001630 Google_72:8a:66	Cixco_dd:a0:18	882.11	261	69 -34 dBe	Association Request, SN+1812, FM+0, Flags+C, SSID+"wif	> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Hbit/sec]
- 181		1.681281	0.000000 192.168.1.15	192.168.1.121	892.11	76	69 - 37 dBm	Acknowledgement, Flags+C	> Tag: Power Capability Min: -7, Max: 19
- 18		1.705251	0.023970 Cisco_dd:a0:18	Google_72:8a:66	882.11	313	69 -37 dBm	Association Response, SN+0, FN+0, Flags+C	> Tag: Supported Channels
		1.705251	0.000000 192.168.1.15	192.168.1.121	882.11	75	69 -31 dBH	Acknowledgement, Flags+C	V Tag: KNL Enconation
		1.718288	0.005029 Cisco_dd:a0:18	Google_72:8a:66	EAP	209	69 -37 dBm	Request, Identity	Tag Number; ISN Information (48)
		1.710298	0.000000 192.168.1.15	192.168.1.121	802.11	76	60 -31 dBm	Acknowledgement, Flags+C	
- 12	939 1	1,747377	0.037097 Google_7218a166	Cisco_dd:a0:28	EAP	337	69 -33 (88)	Response, Identity	Tag Length: 28 RSN Version: 1
	948.3	1.747377	0.000000 192.168.1.15	192.168.1.121	882.11	76	69 -37 dBn	Acknowledgement, FlagsvC	
- 12	942 1	1.758424	0.011047 Cisco_dd:a0:18	Google_7218a066	EAP	110	69 -37 dBm	Request, Protected EAP (EAP-PEAP)	> Group Cipher Suite: 00:0f:sc (leee 802.11) ALS (COV)
- 83	943 3	1.758424	0.000000 192.168.1.15	192.168.1.121	802.11	76	69 -31 dile	Acknowledgement, FlagsvC	Pairwise Cipher Suite Count: 1
		1.768896	0.009672 Cisco dd:a0:18	Broadcast	882.11	428	60 -37 dBH	Beacon frame, SN+3686, FN+8, Flags+C, 81+188, SSID+"vd	> Paindise Cipher Suite List 90:00fiat (Leee NH2.11) AES (COM)
		1.768484	0.000388 Google_72:8a:66	Broadcast	LLC	114	60 -37 dim	1, N(R)=26, N(S)=7; DSAP Ex68 Individual, SSAP Netware Respons	Auth Key Management (AMM) Suite Count: 1
18		1.779457	8.010973 Google_72:8a:66	Cisco_dd:a0:18	TLSv1.Z	241	62 -48 dBm	Client mello	Auth Key Management (AGM) List 00:0f:ac (Leee BR2.11) FT over List BR2.1X
- 18		1.779457	0.000000 192,168,1.15	192.168.1.121	802.11	76	69 -37 dila	Acknowledgement, Flags+C	<ul> <li>Auth Key Management (ARM) Suite: 00:0fiac (Leee 802.11) FT over IEEE 802.1X</li> </ul>
- 32		1.794520	0.015063 Cisco_dd:a0:18	Google_72:8a:66	EAP	1116	69 -37 dBm	Request, Protected EAP (EAP-PEAP)	Auth Key Management (AMM) OLI: 00:09f:ac (leve 802.11)
- 11		1.794520	0.000000 292.168.1.15	192.168.1.121	882.11	76	60 -60 dbs	Acknowledgement, FlagsC	Auth Key Management (APP) type: FT over IEEE 882.1X (3)
- 83		1.797858	0.002538 Google 72:8a:66	Cisco dd:a0:18	EAP	110	60 -30 dan	Response, Protected EAP (EAP-PEAP)	✓ RSW Expabilities: 0x00x0
- 11		1.797058	0.000000 192.168.1.15	192.168.1.121	802.11	76	69 -37 dBe	Acknowledgement, Flags+C	
1		1.801714	0.004656 Cisco_dd:a0:18	Google_72:8a:66	TLSv1.2	382	69 -37 dBm	Ignored Unknown Record	
- 181		1.801714	0.000000 192.168.1.15	192.168.1.121	882.11	76	69 -39 dBe	Acknowledgement, Flags+C	
- 18		1.820673	0.018959 Google_72:8a:66	Cisco_dd:a0:18	TLSv1.2	236	60 -39 dðin	Client Key Exchange, Change Cipher Spec, Encrypted Handshake M	
- 12		1.820673	0.000000 192.168.1.15	192.168.1.121	882.11	76	69 -37 dBm	Acknowledgement, Flags+C	and a standard stand Standard standard stan
	965 1	1.824990	0.004317 Cisco_dd:a0:18	Google_72:8a:66	TLSv1.2	361	69 -37 d8m	Change Cipher Spec, Encrypted Handshake Message	
- 12	966 3	1.824998	0.000000 192.168.1.15	192.168.1.121	882.11	76	60 -39 dBe	Acknowledgement, Flags+C	
- 83	968 3	1.829289	0.004219 Google_72:8a:66	Cisco_dd:a0:18	EAP	338	69 -39 dilt	Response, Protected EAP (EAP-PEAP)	
- 12	969 1	1.829209	0.000000 192.168.1.15	192.168.1.121	802.11	76	60 -37 dBH	Acknowledgement, Flags+C	= Extended Key ID for Individually Addressed Frames: Not supported
- 12	971 1	1.833178	0.001969 Cisco_dd:a0:18	Google_72:8a:66	fLSv1.2	364	69 -37 dim	Application Data	PMCD Count1 0
- 1	972.1	1.833178	0.000000 192.168.1.15	192,168,1,121	882.11	75	69 - 39 dBm	Acknowledgement, Flags+C	PHUD List
1.2	073 1	1.817328	0.004150 Google_72:8a:66	Cisco_dd:a0:18	TLSv1.2	152	69 -19 dlin	Application Data	) Group Ranagement Cipher Suite: 00:0f:ac (Lees 802.11) BIP (128)
- 18	974 1	1.837406	0.000078 192,168.1.15	192.168.1.121	882.11	76	69 - 37 dim	Acknowledgement, Flags+C	> Tag: RM Enabled Capabilities (5 octets)
- 18		1.840705	0.003299 Cisco_dd:a0:18	Google_72:8a:66	TLSv1.2	373	69 -37 dbs	Application Data	> Tag: Mobility Domain
- 18		1.848785	0.000000 192.168.1.15	192.168.1.121	892.11	76	69 - 39 dBm	Acknowledgement, Flags+C	> Tag: Supported Operating Classes
1		1.845522	0.004817 Google 72:8a:66	Cisco dd:a0:18	TLSV1.2	206	60 - 30 dbm	Application Data	) Tag: Extended Capabilities (10 octets)
		1.845522	0.000000 192.168.1.15	192.168.1.121	882.11	200	69 - 37 dbm	Acknowledgement, FlagsvC	> Ext Tag: HE Capabilities
			0.0000000 192.168.1.15 0.019872 Cisco dd:a0:18	Google 72:83:66					> Ext Tag: HE 6 GHz Band Capabilities
- 88		1.864594			TLSv1.2	290	69 -37 dBe	Application Data	<ul> <li>Tag: Vendor Specific: Broadcon</li> </ul>
		1.864752	0.000158 192.168.1.15	192.168.1.121	882.11	76	60 -39 dBm	Acknowledgement, FlagsC	Tag Number: Vendor Specific (221)
1		1.866887	0.002135 Google_72:8a:66	Cisco_dd:a0:38	n.sv1.2	145	69 -48 dBe	Application Data	Tag length: 10
		1.856897	0.000000 192,168.1.15	192.168.1.121	802.11	76	69 -37 dilm	Acknowledgement, Flags+C	OUI: 00:20:18 (Broadcom)
		1.870658	0.003771 Eisco_dd:a0:18	Broadcast	882.11	428	69 -37 088	Beacon frame, SN+3687, FN+8, Flags+C, 81+188, SSID+"wd	Vendor Specific OII Type 2
		2.870658	0.000000 Cisco_dd:a0:18	Google_72:8a:66	TLSv1.2	343	69 -37 dBm	Application Data	Vendor Specific Data (0000010000000)
		1.870658	0.000000 192.168.1.15	192.168.1.121	802.11	76	69 -39 dBH	Acknowledgement, Flags+C	Tag: Vendor Specific: Microsoft Corp.: WMVAME: Information Element
- 18	992 1	1.877128	0.006470 Google_72:8a:66	Cisco_dd:a0:18	EAP	150	69 -38 dim	Response, Protected EAP (EAP-PEAP)	<ul> <li>rig: Hinter apecaraci recovers corp.: HTVHEL antoniation Element</li> </ul>
	. 993 1	1.877128	0.000000 192.168.1.15	192.168.1.121	882.11	76	69 -37 dBm	Acknowledgement, Flags+C	
- 88	096 1	1.920065	0.042937 Cisco_dd:a0:18	Google_72:8a:66	EAP	208	60 -37 dim	Success	
- 83		1.920065	0.000000 102.168.1.15	192.168.1.121	882.11	76	69 - 39 dBm	Acknowledgement, Flags+C	
	998.1	1.920065	0.000000 Cisco dd:a0:18	Google 72:8a:66	EAPOL	221	60 -37 dBm	Key (Message 1 of 4)	
18		1.928865	0.000000 192.168.1.15	192.168.1.121	882.11	76	69 - 39 dBm	Acknowledgement, Flags+C	
- 19		1.925255	0.005190 Google 72:8a:66	Cisco.dd:a0:18	LAPOL	346	60 -40 dim	Key (Message 2 of 4)	
		1.925255	0.000000 192.168.1.15	192.168.1.121	802.11	76	69 -37 dBm	Acknowledgement, FlagivC	
		1.926677	0.001422 Cisco dd:a0:18	Google 72:8a:66	EAPOL	423	69 -37 dbs	Key (Message 3 of 4)	
		1.926677	0.000000 192.168.1.15	900g1#_72188186 192.168.1.121	B02.11	425	69 -37 dbs	key (Message 3 of 4) Acknowledgement, Flags=C	
		1.928885	0.002209 Google_72:8a:66	Cisco_dd:a0:38	EAPOL	199	69 -39 dBe	Key (Message 4 of 4)	
		1.928886	0.000000 192.168.1.15	192.168.1.121	882.11	76	60 -37 dlin	Acknowledgement, FlagsvC	

WPA3 Enterprise 802.1x + FT Pixel6a Association

### Client details in WLC:

Q. Search Menu Nerro	Monitoring * > Wireless * > Clients		Client		
	Clients Sleeping Clients Excluded Clients		360 View General QOS Statist	tics ATF Statistics	Mobility History Call Statistics
Dashboard	Contraction of the second s		Client Properties AP Properties	Security Information	Client Statistics QOS Properties EoGRE
Monitoring	C Deletter C		Re-Authentication Timeout	1800 sec (Remainin	ng time: 267 sec)
			Client State Servers	None	
Configuration	Selected 0 out of 2 Clients		Client ACLs	None	
	Client MAC Address T IPv4 Address T IPv6 Address	AP Name T	Client Entry Greate Time	1536 seconds	
C Administration	0429.2ec9.e371 / 192.168.1.160 /re80::6a20:34e8.ab1b:6332	AP01_RC_9136_F80C	Policy Type	WPA3	
C Licensing	O 2495.2172.8a66	AP01_RC_9136_F80C	Encryption Clipher	CCMP (AES)	
			Authentication Key Management	FT-802.1x	
X Troubleshooting		EAP Type Session Timeout	PEAP 1800		

WPA3 Enterprise 802.1x + FT Pixel6a Client details

Focus on the roam type Over the Air where we can see the roam type 802.11R:

Carrier and the second second second second	Monitor	ing >> Wireless >>	Clie	ents				Cli	ient									
Q. Search Manu Items	Clients			Excluded Clients				36	i0 View General	QOS Statist	cs /	ATF Statistics	M	obility H	istory C	all Statistics		
Dashboard Monitoring Configuration	·	ted 0 out of 2 Clients							Recent association		AP Y	Assoc Time	T in	stance	Mobility <b>T</b> Role	Run Latency Im	Y Roam Type	Ŧ
Sconinguration	, o	Client MAC Address	٣	IPv4 Address	Ŧ	IPv6 Address	AP Name T		AP01_RC_9136_F80C	00dl.1ddd.a018	3	07/12/2023	0		Local	7	802.118	
	0																	
Administration	· 0	0429.2ec9.e371	×	192,168.1.160		fe80::6a20:34e8:ab1b;6332	AP01_RC_9136_F80C		AP9136_5C.F524	00df.1ddd.7d38	3	07/12/2023 11:43:48	0		Local	3161	N/A	_

### Samsung S23

Connection OTA with focus on the RSN information from client:

No. Time	Profess.	Par and	Desta Non	Buchevel	Recently Mars	and Read at	- 1-6		> Frame 5136: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface \Device\WP_{04578005-2998-4656-8C33-C34.
	Delta	Source	Destination	Protocol		nnel Signal str			> ithernet II, Src: Cisco d2:97:47 (74:11:b2:d2:97:47), Dst: Universa b7:cf:06 (00:3a:88:b7:cf:06)
5874 9.739729		9 Cisco_dd:a0:18	Broadcast	892.11	428	69 -35 dBm	Beacon frame, SN+3280, FN+0, Flags+C, BI+100, SSID+"vd		> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
5120 9.830173		4 SansungE_c9te3t71	Cisco_dd:a0:18	882.11	211	69 -39 dBm	Probe Request, SN+2476, FN+0, Flags+C, SSID="wdF16L_te		> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
5121 9.830173		0 192.168.1.15	192.168.1.121	802.11	76 374	69 -35 dBm 69 -36 dBm	Acknowledgement, FlagswC		> AiroPeek/OmiPeek encapsulated IEE 882.11
5122 9.830955 5123 9.830955		2 Cisco_dd:a0:18 0 192.168.1.15	SansungE_c9:e3:71 192.168.1.121	802.11 802.11	76	69 -36 clas	Probe Response, SN-207, FN-0, Flags=C, 81×100, SSID="w Acknowledgement, Flags=C		> MR2.11 radio information
									> IEEE 882.11 Association Request, Flag:C
5128 9.838052		7 SamsungE_c91e3171	C1sco_dd:a0:18	882.11	96 75	69 -40 dBm	Authentication, SN=2477, FN=0, Flags=C		V IEEE 882.11 kireless Hanagement
5129 9.K38852		0 192.168.1.15	192.168.1.121	882.11		69 -36 d8m	Acknowledgement, Flags=C		) fixed parameters (4 bytes)
5132 9.842012		@ Cisco_dd:a@:18	Broadcast	882.11	428	69 -35 dBm	Beacon frame, SN+3282, FN+0, Flags+C, 81+100, SSID+"wd		<ul> <li>Tagged parameters (263 bytes)</li> </ul>
5133 9.842237		5 Cisco_dd:a0:18	Sansungt_c9:e3:71	802.11	96	69 -35 dBm	Authentication, SN+55, FN+0, Flags+C		> Tag: SSID parameter set: "wdfi5E_test"
5134 9.842237		0 192.168.1.15	192.168.1.121	882.11	76	69 -48 dBm	Acknowledgement, Flags+C		> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Mbit/sec]
- 5136 9.845838			Cisco_dd:a0:18	802.11	357	69 -41 cBm	Association Request, SH-2478, FNH0, FlagtsC, SSID="wif		> Tag: Power Capability Min: 8, Max: 16
5137 9,845838		0 192.168.1.15	192.168.1.121	892.11	76	69 -36 dBm	Acknowledgement, Flags+C		> Tar: Supported Channels
5143 9,870722		A Cisco_dd:a0:18	Samsungl_c9:e3:71	802.11	313	69 -36 dBm	Association Response, SN+0, FN+0, Flags+C		v Iag: RN Information
5144 9.878722		0 192.168.1.15	192.168.1.121	892.11	76	69 -41 dBm	Acknowledgement, Flags+C		Tag Number: RSW Information (48)
5145 9.878538		6 Cisco_dd:a0:18	Samsungt_c9:e3:75	EAP .	109	69 -36 dim	Request, Identity		Tag length: 26
5146 9.878538		0 192.168.1.15	192.168.1.121	882.11	76	69 -41 dBm	Acknowledgement, FlagsC		PSN Version: 1
5150 9.897013		5 SansungE_clice3:71		UP .	337	69 -42 dBm	Response, Identity		> Group Cipher Suite: 00:0F:ac (Leee B02.11) ALS (CCM)
5151 9,897013		8 192.168.1.15	192.168.1.121	892.11	76	69 -36 dBm	Acknowledgement, Flags+C		Painsise Cipher Suite Count: 1
5157 9.903463		@ Cisco_dd:a0:38	SamsungE_c9:e3:71	EAP	118	69 -36 d8m	Request, Protected EAP (EAP-PEAP)		> Pairwise Cipher Suite List 00:0f:ac (leee 802.11) AES (CDM)
5158 9.983774		1 192.168.1.15	192.168.1.121	882.11	- 76	69 -43 d8m	Acknowledgement, Flags+C	13	Auth Key Management (AMM) Suite Count: 1
5166 9.926800		6 SamsungE_clite3:71	Cisco_dd:a0:18	TLSv1.2	273	69 -43 dBm	Encrypted Handshake Message		Auth Key Management (ADM) List 00:00fisc (leve 502.11) FT over IEEE 502.1X
5367 9.926800		0 192.168.1.15	192.168.1.121	802.11	76	69 -36 d8m	Acknowledgement, Flags=C		<ul> <li>✓ Auth Key Ranagement (A00) Suite: 00:0f:ac (Leee 802.11) FT over 1EEE 802.1X</li> </ul>
5173 9.930440		W Cisco_dd:a0:18	SansungE_c9:e3:71	EAP	1116	69 -36 d8m	Request, Protected EAP (EAP-PEAP)		Auth Key Management (ADM) OUL: 00:0fiat (Leee 882.11)
5174 9.938448		0 192.168.1.15	192.168.1.121	802.11	76	69 -63 dBm	Acknowledgement, Flags+C		Auth Key Ranagement (A00) type: FT over IEEE 882.1X (3)
5175 9.934701		1 SamsungE_c9:e3:71		EAP	110	69 -42 dBm	Response, Protected EAP (EAP-PEAP)		<ul> <li>ISN Caubilities: 0.0000</li> </ul>
5176 9.934701		0 192.168.1.15	192.168.1.121	802.11	76	69 -36 dBm	Acknowledgement, Flags+C		
5181 9.938770	0,00406	0 Cisco_dd:a0:18	Samsungt_c9:e3:71	TL5v1.2	382	69 -36 d8m	Encrypted Handshake Message, Encrypted Handshake Message, Encr		
5182 9.938770	0.00000	0 192.168.1.15	192.168.1.121	882.11	26	69 -42 dlin	Acknowledgement, Flags+C		
5187 9.944434	0.00566	4 Cisco_dd:a0:18	Broadcast	882.11	428	69 -36 dBm	Beacon frame, SN+3283, FN+0, Flags+C, BI+100, SSID+"wd		
5188 9.944704		0 Sansungl_c9:e3:71	Cisco_dd:a0:18	TLSv1.2	236	69 -43 dim	Encrypted Handshake Message, Change Clpher Spec, Encrypted Han		
5189 9.944704	0.00000	0 192.168.1.15	192.168.1.121	892.11	76	69 -36 dBm	Acknowledgement, Flags+C		
5290 9,944850	0.00014	6 SamsungE_c0:e3:71	Broadcast	uc	114	69 -36 dBm	I, N(R)+7, N(S)+87; DSAP 0xF2 Individual, SSAP Banyan Vines Co		
5193 9.948782	0.00323	2 Cisco_dd:a0:18	Sansungt_c9:e3:71	TL5v1.2	161	69 -36 d8m	Change Cipher Spec, Encrypted Handshake Message		
5194 9.948864	0.00008	2 192.168.1.15	192.168.1.121	882.11	76	69 -44 d8m	Acknowledgement, Flags+C		
\$195 9.952821	0.00315	7 Samungt_clice3:71	Cisco_dd:a0:18	EAP	118	69 -64 d8m	Response, Protected EAP (EAP-PEAP)		Period Count: 8
5196 9.952255	0.00023	4 192.168.1.15	292.168.1.121	882.11	76	69 -36 dBm	Acknowledgement, Flags+C		PHID LOURT 0
5199 9.956895	0.00355	0 Cisco_dd:a0:18	Samsungt_c9:e3:71	TL5v1.2	144	69 -36 d8m	Application Data		
5200 9.956895	0.00000	0 192.168.1.15	192.168.1.121	882.11	76	69 -43 d8m	Acknowledgement, Flags+C		> Group Management Cipher Suite: 00:00fisc (leve N02.11) BIP (128)
\$282 9.950476	0.00338	1 Samungt_c9:e3:71	Cisco_dd:a0:18	TL5v1.2	152	69 -43 dBm	Application Data		> Tag: RM Enabled Capabilities (5 octets) > Tag: Nobility Domain
5283 9.959476	0.00000	0 192.168.1.15	192.168.1.121	882.11	76	69 -36 dBm	Acknowledgement, Flags+C		
5204 9.962667	0.00319	1 Cisco_dd:a0:18	SansungE_c9:e3:71	TLSv1.2	171	69 -36 dBm	Application Data		> Tag: Supported Operating Classes
5285 9.962667	0.00000	0 192.168.1.15	192.168.1.121	882.11	76	69 -43 d8m	Acknowledgement, FlagswC		> Tag: Extended Capabilities (3 octets)
\$287 9.966228	0.00355	& Sansungl_clicel:71	Cisco_dd:a0:18	TLSv1.2	205	69 -43 dBm	Application Data		) Ext Tag: HE Capabilities ) Ext Tag: HE 6 GHz Hand Capabilities
5288 9.966228	0.00000	0 192.168.1.15	192.168.1.121	882.11	76	69 -36 dBm	Acknowledgement, Flags+C		<ul> <li>Ext rag: ML &amp; Grd Band Lapadilities</li> <li>Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element</li> </ul>
\$211 9.974391		8 Cisco_dd:a0:18	SamsungE_c9:e3:75	TLSv1-2	199	69 -36 dân	Application Data		<ul> <li>Tag: Vendor Specific: Qualcom Inc.</li> </ul>
5212 9.974391		0 192.168.1.15	192.168.1.121	802.11	76	69 -43 dBm	Acknowledgement, Flags+C		Tag Number: Vendor Specific: Quilcom Inc.
5235 9,986936		5 SamurgE_cRie3:71		TLSv1.2	345	69 -43 dBm	Application Data		
5216 9.986916		0 192.168.1.15	192.168.1.121	892.11	76	69 -36 d8m	Acknowledgement, Flags+C		Tag length: 11 OUI: Sc:fd:Fd (Qualcomm Inc.)
5217 9.986916		@ Cisco_dd:a0:18	SatsungE_c9:e3:71	TLSv1.2	143	69 -36 d8m	Application Data		Vendor Specific OUI Type: 1
\$218 9.986916		0 192.168.1.15	192.168.1.121	802.11	76	69 -64 d8m	Acknowledgement, Flags=C		Vendor Specific Outa: 0101020100020101
5221 9.986916	0.00000	@ Samsungl_crite3:71	Cisco_dd:a0:18	EAP	110	69 -44 dBm	Response, Protected EAP (EAP-PEAP)		
5222 9.996916	0.00000	0 192.168.1.15	192.168.1.121	802.11	76	69 -35 d8m	Acknowledgement, Flags+C		<ul> <li>Tag: Vendor Specific: Samsung Electronics Co., Ltd Tag Number: Vendor Specific (221)</li> </ul>
5227 9.997886	0.01089	@ Cisco_dd:a0:18	SansungE_c91e3171	EAP	108	69 -36 d8m	Success		
5228 9.997886	0.00000	0 192.168.1.15	192.168.1.121	802.11	76	69 -43 dBm	Acknowledgement, Flags+C		Tag length: 11
5229 9.998664	0.00085	8 Cisco_6d:a0:18	SamsungE_c9:e3:71	EAPOL	221	69 -36 dBm	Key (Message 1 of 4)		OUI: 00:00:f0 (Samsing Electronics C
5230 9.998664	0.00000	0 192.168.1.15	192.168.1.121	802.11	76	69 -43 dBm	Acknowledgement, Flags+C		Vendor Specific OUL Type: 34
5234 18.007005	0.00834	1 SamungE_ckte3:71	Cisco_dd:a0:18	EAPOL	346	69 -43 dBm	Key (Message 2 of 4)		Vendor Specific Outa: 220001040000000f
5215 10.007005		0 192.168.1.15	192.168.1.121	802.11	76	69 -36 dBm	Acknowledgement, Flags+C		> Tag: Vendor Specific: Samsung Electronics Co., Ltd
5236 18.009443	0.00243	8 Cisco_dd:a0:18	Samsungt_c9:e3:71	EAPOL	423	69 -36 dBm	Key (Message 3 of 4)		
\$237 10.009443	0.00000	0 192.168.1.15	192.168.1.121	802.11	76	69 -43 dim	Acknowledgement, Flags+C		
5239 18.815678	0.00523	5 SamsungE_citie3:71	Cisco_dd:a0:18	EAPOL	199	60 -44 dBm	Key (Message 4 of 4)		
		0 192.168.1.15	192.168.1.121	802.11	76	69 -36 dBm	Acknowledgement, Flags+C		

S23 FToTA Roaming event

### Client details in WLC:

Cisco Cisco Ca			Last loge 02113/0523 10 58-47			
Q Search Menu Itents	Monitoring * > Wireless * > Clients		Client			*
New Street Stree	Clients Sleeping Clients Excluded Clients		360 View General QOS Statist	ics ATF Statistics Mobility History	Call Statistics	
Dashboard			Client Properties AP Properties	Security Information Client Statistics	QOS Properties EoGRE	
Monitoring	× Deleter C		Re-Authentication Timeout Client State Servers	1800 sec (Remaining time: 798 sec) None		•
Configuration :	Selected 0 out of 2 Clients		Client ACLs	None		- 1
	Client MAC Address T IPv4 Address T IPv6 Address	AP Name T	Client Entry Create Time	1003 seconds		- 8
Administration	O 0429.2ec9.e371 → 192.168.1.160 fe80:;6e20:34e8:ab1b:6332	AP01_RC_9136_F80C	Policy Type	WPA3		- 8
Licensing	O 2495.2172.8a66  ✔ 192.168.1.162  1e80::b13.1107:7c5fa7e0	AP01_RC_9136_F80C	Encryption Clipher Authentication Key Management	CCMP (AES) FT-802.1x		- 8
	····· 1 ···· 10 ··		EAP Type	PEAP		- 8
Troubleshooting			Session Timeout	1800		- 8

S23 Client Properties

### Focus on the roam type Over the Air where we can see the roam type 802.11R:

	Monitoring * > Wireless	· > Clients				Clie	nt							
Q. Switch Many Items	Clients Sleeping Clie		Sients			360	View General	QOS Statist	cs /	ATF Statistics	Mobility	History	Call Statistics	
Monitoring >	X Database D						Recent associati	on history:						Roam ¥
Configuration	Selected 0 out of 2 Clients					4	AP Name 🛛 🕇	BSSID T	AP Y Sibt	Assoc Time	T Instance	<ul> <li>Mobility T Role</li> </ul>	Latency (ma)	
	Client MAC Addre	ss 🝸 IPv4 Add	055 <b>T</b>	Pv6 Address	AP Name T		AP01_RC_9136_FROC	00at.1aad.a018	3	07/12/2023	0	Local	12	802.11R
		▶ 192,168.	160	fe80::6a20:34e8:ab1b:6332	AP01_RC_9136_F80C		AP9136_5C.F524	00dt 1ddd.7d38	3	07/12/2023	0	Local	4536	N/A
Administration	O 0429.2ec9.e371	122.100.												

S23 Roaming type 802.11R

This client was also tested using FT over the DS and was able to roam using 802.11r:

No.	Time	Delta	Source	Destination	Protocol	Length Chann	el Signal stro	Info		> Frame 1265: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface \Device\MPF_[D4578005-2
1246	8.299585	0.102333	Cisco_dd:a0:18	Broadcast	882.11		69 - 39 dBm	Beacon Frame, SN+305, FN+0, Flags+C, 81+100, SSID+">	44	> Ethernet II, Src: Cisco_d2:97:47 (74:11:b2:d2:97:47), Dst: Universa_b7:cf:06 (08:3a:88:b7:cf:06)
	8.481955		Cisco_dd:a0:18	Broadcast	802.11		69 -40 dBm	Beacon frame, SN#306, FN#0, Flags+C, BI+100, SSID=">		> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
1248	8,504375		Cisco dd:a0:18	Broadcast	882.11	364	69 - 39 dBm	Beacon frame, SN+307, FN+0, Flags+C, 81+100, SSID=">		> User Datagram Protocol, Src Port: 5555, Ost Port: 5800
1249	8,686814	0.102439	Cisco dd:a0:18	Broadcast	882.11	364	69 -48 dBm	Beacon frame, SN=388, FN=0, Flags=C, BI+100, SSID=">	df	> AiroPeek/OmiPeek encapsulated IEEE 802.11
	8.612759		Cisco_dd:a0:18	Broadcast	882.11	312	69 -40 dBm	Probe Response, SN=459, FN=0, Flags=C, BI=100, SSID-		> 882.11 radio information
	8,709133		Cisco_dd:a0:18	Broadcast	882.11		69 - 39 dBm	Beacon frame, 99+310, FN+0, Flags+C, 81+100, 551D+"		> IEEE 802.11 Reassociation Request, Flags:C
	8.786412			Cisco dd:a0:18	882.11		69 -48 dBm	Authentication, SN-99, FN-0, Flags=C	30.	✓ IEEE 882.11 Wireless Management
	8.786412		192.168.1.15	192,168,1,121	882.11		69 -39 dBm	Acknowledgement, Flags=C		> Fixed parameters (10 bytes)
	8,798571		Cisco_dd:a0:18	SansungE_c9:e3:71	882.11		69 -39 dBn	Authentication, SN+118, FN+0, Flags+C		✓ Tagged parameters (385 bytes)
	8.798571		192.168.1.15	192.168.1.121	802.11		69 -47 dbs	Acknowledowneot, flagsC		> Tag: SSID parameter set: "wifi66_test"
	8.796439			Ciaco_dd:a0:18	882.11		69 -48 dile	Reassociation Request, SN+100, FlagsC, SSID+	GR .	> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Pbit/sec]
	8.796439		192.168.1.15	192.168.1.121	802.11		69 - 39 dBm	Acknowledgement, FlagtsC		> Tag: Power Capability Min: 8, Max: 16
	8.806878		Sansungt_c9:e3:71	Broadcast	LLC		69 - 39 dBm	S, Func-REJ, N(R)+57; DSAP 8x3a Group, SSAP 8xa6 Command		> Tag: Supported Channels
	8.887948		Cisco_dd:a0:18	Sansungl_c9:e3:71	802.11		63 - 19 dBm	Reassociation Response, SN+0, FN+0, Flags+C		> Tag: RM Enabled Capabilities (5 octets)
	8.807940		192.168.1.15	192.168.1.121	802.11		69 -48 dBn	Acknowledgement, Flags=C		> Tag: RSM Information
	8,887948		Samsungl_c9:e3:71	Broadcast	LLC		69 -39 dBn	<pre>I P, N(R)=11, N(S)=19; DSAP 0x58 Individual, SSAP 0x5a Resp.</pre>	_	V Tag: Robility Domain
	8.811521		Cisco_dd:a0:18	Broadcast	802.11		69 - 39 dBm	Beacon frame, SN×311, FN×0, Flags+C, BI×100, SSID+'S		Tag Number: Mobility Domain (54)
	8.832754		Cisco Scif8:0c	SansungE_c9:e3:71	LLC		69 - 49 dBm	U, Func-DISC: DSAP (hola Group, SSAP (her2 Contand	a1	Tag length: 3
	8.832754		192.168.1.15	192.168.1.121	882.11		69 -58 dBs	Acknowledgement, Flags+C		Mobility Dowain Identifier: 0xef27
					LLC			U, Func-Unknown: 05AP Texas Instruments Group, SSAP 0x28 Re:		<ul> <li>FT Capability and Policy: exel</li> </ul>
	8.832754		Cisco_Scif8:0c	SansungE_c9:e3:71	882.11		69 -49 dBm		(po	
	8,832817		192.168.1.15	192.168.1.121			69 -58 dBm	Acknowledgement, Flags+C	4.	
	8,988548			Broadcast	LLC		69 -46 dBH	5 F, func=REJ, N(R)=32; DSAP Bx26 Individual, SSAP Bxd4 Resp	on	0000 00 = Reserved: 0x00
	8.999549		192.168.1.15	192.168.1.121	882.11		69 -48 dBn	Acknowledgement, Flags=C		Y Tag: Fast 855 Transition
	8.984143		Cisco_dd:a0:18	SansungE_c9:e3:71	882.11		69 -48 dBn	Action, SN+1, FN+0, Flags+.pC		Tag Number: Fast BSS Transition (SS)
	8.984143		192.168.1.15	192.168.1.121	882.11		69 -47 dBm	Acknowledgement, Flags+C		Tag Length: 96
	8.984883			Cisco_dd:a0:18	882.11		69 -47 dBm	Action, SN+0, FN+0, Flags+.pC		> MEC Control: dxdixb0
	8.984883		192.168.1.15	192.168.1.121	802.11		69 -48 dBn	Acknowledgement, Flags*C	1.2	MIC: 0/814df7fe156ad6e4cf650aa53a4aca
	8.906878		AlticeLa_9e:59:af	Samsungt_c9:e3:71	LLC		69 -50 dBm	1 P, N(R)=25, N(5)=40; DSAP 0x3e Individual, SSAP 0x8a Comm		Wence: d514fb17ab7fa885b7fd75e5bfdka9e882cf4ec58fbd3f492e13889fb1a869ca
	8.913912		Cisco_dd:a0:18	Broadcast	882.11		69 -41 dBm	Beacon frame, SN+313, FN+0, Flags+C, 81+100, SSID+")	41	Skince: 00172e455c738aa1b8cfe6fd142b425070879eb5cce3fa11283f566d849bb2c9
	8.958493		192.168.1.15	192.168.1.121	882.11		69 - 39 dBm	Acknowledgement, Flags=C		Subelement: PMK-R1 key holder identifier (R101-ID)
	8,975553		192.168.1.15	192.168.1.121	802.11		69 - 39 dBn	Acknowledgement, Flags=C		Subelement ID: PMK-R1 key holder identifier (R1804-ID) (1)
	9.016519		Cisco_dd:a0:18	Broadcast	882.11		69 -38 dBs	Beacon frame, SN+314, FN+0, Flags+C, BI+100, SSID+"		Length: 6
	9.118683		Cisco_dd:a0:18	Broadcast	802.11		69 - 39 dBm	Beacon frame, SN+315, FN+0, Flags+C, 81+100, SS1D+5	df	PMK-R1 key holder identifier (R1KH-ID): d4887b497a4b
	9.176814		192.168.1.15	192.168.1.121	882.11		69 -48 dBn	Acknowledgement, Flags=C		✓ Subelement: PMK-R0 key holder identifier (R0KH-ID)
	9,221145		Cisco_dd:a0:18	Broadcast	882.11		69 - 39 dBm	Beacon frame, SN=316, FN=0, Flags=C, BI=100, SSID="		Subelement ID: MMK-M0 key holder identifier (M00H-ID) (3)
	9.324107		Cisco_dd:a0:18	Broadcast	882.11		69 - 39 dBm	Beacon Frame, SN+317, FN+0, Flags+C, BI+100, SSID+"		Length: 4
	9.425938		Cisco_dd:a0:18	Broadcast	882.11		69 -48 dBm	Beacon frame, SN+318, FN+8, Flags+C, 81+108, SSID+"		PMK-RB key holder identifier (RBRH-ID): 082055a2
	9.528463		Cisco_dd:a0:18	Broadcast	882.11		69 -38 dBn	Beacon frame, SN=319, FN=8, Flags=C, BI=100, SSID="		> Tag: Supported Operating Classes
	9.631028		Cisco_dd:a0:18	Broadcast	882.11		69 -38 dBe	Beacon frame, SN+320, FN+0, Flags+C, BI+100, SSID+"		> Tag: Extended Capabilities (11 octets)
	9.733295		Cisco_dd:a0:18	Broadcast	882.11		69 -39 dBm	Beacon frame, SN+321, FN+8, Flags+C, BI+108, SS1D+"		> Tag: Vendor Specific: Microsoft Corp.: WMV/WE: Information Element
	9,835864		Cisco_dd:a0:18	Broadcast	882.11		69 -48 dBn	Beacon frame, SN+322, FN+0, Flags+C, 8I+100, SSID+"	df	> Ext Tag: ME Carabilities
	9.925936			Cisco_dd:a0:18	882.11		69 -45 dBm	Action, SN=4, FN=0, Flags=.pTC		bit Tag: HE 6 GHz Band Capabilities
	9.925936		192.168.1.15	192.168.1.121	882.11		69 -48 dBs	Acknowledgement, Flags=C		) Tag: Vendor Specific: Qualcom Inc.
	9.926893		192.168.1.15	192.168.1.121	882.11		69 -48 dBn	Acknowledgement, Flags=C	100	<ul> <li>) Tag: Vendor Specific: Qualcom Inc.</li> <li>) Tag: Vendor Specific: Samung Electronics Co.,Ltd</li> </ul>
1954	9.937895	0.011002	Cisco_dd:a0:18	Broadcast	882.11		69 -48 dBm	Beacon frame, SN=323, FN=0, Flags=C, BI=300, 55ID=3	44	> Tag: Vendor Specific: Samsung Electronics Co., Ltd > Tag: Vendor Specific: Samsung Electronics Co., Ltd
1955	9.942343	0.004448	192.168.1.15	192.168.1.121	882.11	76	69 -48 dBn	Acknowledgement, Flags#C		A refer to one observate: sense a sectorize reference.
		-		tragements and second to be					14	

S23 Roaming FToDS packets

### WPA3-Enterprise + GCMP128 cipher + SUITEB-1X

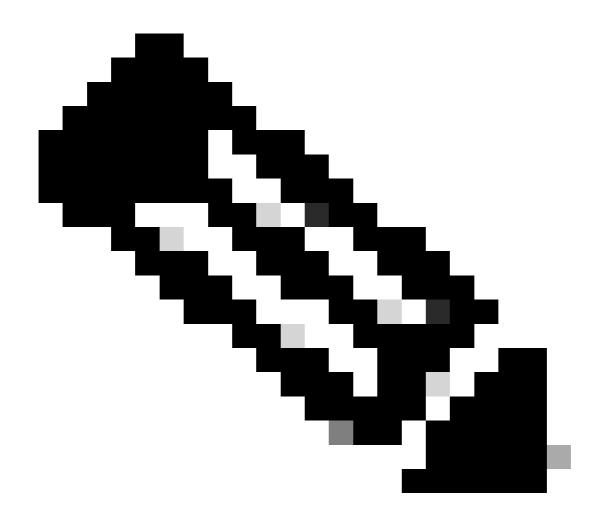
### WLAN Security configuration:

### Edit WLAN

ayer2 Layer3 AAA	A			
O WPA + WPA2	O WPA2 + WPA3	• WPA3	O Static WEP	O None
MAC Filtering	כ			
Lobby Admin Access	כ		7- <b></b>	1944 C
WPA Parameters		Fast	Transition	10 <u></u>
WPA <b>D</b> Policy	WPA2 O Policy	Sta	tus	Disabled 🔻
GTK <b>O</b> Randomize	WPA3 O Policy	Ov	er the DS	0
Transition <b>D</b> isable	2	Rea	association Timeout *	20
WPA2/WPA3 Encryption				
AES(CCMP128)	ССМР256		h Key Mgmt	
GCMP128	GCMP256 O		Joined TX	
Protected Management F	Frame			
PMF	Required			
Association Comeback Tim	ier* 1			
SA Query Time*	200			

×

WPA3 Enterprise SuiteB-1X Security Configuration



Note: FT is not suported in SUITEB-1X

View on WLC GUI of the WLAN Security settings:

**\$**5

O O wih6E\_test

Verification of beacons OTA:

wih6E\_test

[WPA3][SUITEB-1X][GCMP128]

No. Tim	e i	Delta Source	Destination	Protocol	Length	Channel Signal st	e Info	> Frame 37626: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface \Device\WF(04578905-2998-4456-8C33-C
37376 59.	169776	0.020402 Cisco dd:a0:18	Broadcast	882.11	312	67 -40 CM	Probe Response, SN-2002, FN+0, Flags+C, BI+100, SSID+"	> Ethernet II, Src: Cisco_d2:97:47 (74:11:b2:d2:97:47), Dst: Universa_b7:cf:06 (08:3a:08:b7:cf:06)
17385 59.	290316	0.020540 Cisco_dd:a0:18	Broadcast	882.11	322	60 -17 dile	Probe Response, SN=2003, FN=0, Flags=C, 81=100, SSID="	) Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
37396 59.	238799	0.020483 Cisco dd:a0:18	Broadcast	882.11	355	60 -37 d8m	Beacon frame, SN+2004, FN+0, FLags+C. 81+100, 551D+"wd	> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
37414 59.	233263	0.820452 Cisco dd:a0:18	Broadcast	882.11	332	69 -38 dBs	Probe Response, 59+2005, FN+0, Flags+C, 81+100, 5510+"	> AiroPeek/OmiPeek encapsulated IEEE 802.11
37424 59.	251733	0.020472 Cisco dd:a0:18	Broadcast	892.11	332	69 -48 dbs	Probe Response, Ste2886, Flee, Flags+C., 81+100, SSID+"	> 882.11 radio information
37437 59.	272258	0.020517 Cisco dd:a0:18	Broadcast	882.11	322	69 -35 dbs	Probe Response, SN=2007, FN=0, Flags=C, 81=100, 5520="	ELLE 802.11 Beacon Frame, Flags:C
37447 59.	292792	0.020542 Cisco dd:a0:18	Broadcast	802.11	312	60 - 37 dBm	Probe Response, SN+2888, FN+0, Flags+C, BI+100, SSID+*	✓ IIIE 802.11 kireless Paragement
37459 59.	333334	0.020522 Cisco dd:a0:18	Broadcast	882.11	355	60 -38 dBm	Beacon frame, SN-2009, FN-0, FlagsC, 81-100, 5510+"wd	> Fixed parameters (12 bytes)
37470 59.	133619	0.020305 Cisco dd:a0:18	Broadcast	802.11	312	60 - 39 dBr	Probe Response, SN+2010, FN+0, Flags+C, BI+100, SSID+"	<ul> <li>Fagged parameters (253 bytes)</li> </ul>
37488 59.	354345	0.020526 Cisco dd:a0:18	Broadcast	882.11	312	69 - 37 dbs	Probe Response, SW-2011, FM+0, Flags+C, BI+100, SSID+*	> Tag: SSID parameter set: "wdf166_test"
37489 59.	375487	0.021342 Cisco dd:a0:18	Broadcast	902.11	352	69 -38 dBm	Probe Response, SN+2012, FN+0, Flags+C, 81+100, SSID="	> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Mbit/sec]
37499 59.	395116	0.019629 Cisco dd:a0:18	Broadcast	882.11	312	69 - 37 dBe	Probe Response, SN+2813, FN+0, Flags+C, BI+100, SSID+*	> Tag: Traffic Indication Map (TIM): OTIM 0 of 1 bitmap
37520 39.	415733	0.020617 Cisco dd:a0:18	Broadcast	882.11	355	60 -37 dbs.	Beacon Frame, SN+2014, FN+0, Flags+C, BI+100, SSID+"vd	> Tag: Country Information: Country Code na, Environment Global operating classes
37519 59.	436898	0.020347 Cisco dd:a0:18	Broadcast	882.11	332	69 - 37 dön	Probe Response, SN+2815, FN+0, Flags+C, B1+100, SSID+1	) Tag: Power Constraint: 6
37532 59.	457236	0.021156 Cisco dd:a0:18	Broadcast	882.11	332	69 - 37 dbs	Probe Response, Stiv2016, Fli+0, Flags+C, 81+100, SSID+*	) Tar: IPC Report Transmit Power: 15. Link Marrin: 0
37539 59.	476989	0.019753 Cisco_dd:a0:18	Broadcast	882.11	332	69 -37 dBe	Probe Response, SNx2017, FNx0, Flags+C, 81x100, SSID+"	V Tag: RN Information
37552 59.	497448	0.020459 Cisco dd:a0:18	Broadcast	882.11	312	60 -37 dBs	Probe Response, 59+2018, FN+0, Flags+C, 81+100, SSID+1	Tag Number: SSN Information (48)
17565 59.	537993	0.020545 Cisco_dd:a0:18	Broadcast	882.11	355	69 -37 dlm	Beacon frame, Stiv2019, File0, FlagssC, BI×100, SSIDw"sd	Tag length: 26
37574 59.		0.020430 Cisco_65:a0:18	Broadcast	882.11	312	60 -37 (88)	Probe Response, SN-2820, FN+0, FlagsC, BI-100, SSID-"	PSN Version: 1
37585 59.	558965	0.020542 Cisco_dd:a0:18	Broadcast	802.11	352	69 -17 dlm	Probe Response, SW-2021, FN+0, Flags+C, 81+100, SSID+*	> Group Cipher Suite: 00:0fiac (Leee 802.11) GOP (128)
37596 59.		0.020474 Cisco dd:a0:18	Broadcast	882.11	312	69 -37 dbm	Probe Response, 5N+2822, FN+0, Flags+C. 81+100, 553D+1	Paindse Cipher Suite Count: 1
37616 59.	599940	0.820501 Cisco_dd:a0:18	Broadcast	882.11	352	60 -37 dim	Probe Response, SN-2023, FN-0, Flags+C, 81-100, SSID-1	<ul> <li>Pairwise Cipher Suite List 00:0fiac (leee 802.11) GOP (128)</li> </ul>
37626 59.	628421	0.020481 Cisco dd:a0:18	Broadcast	882.11	355	69 -38 c0m	Beacon frame, SN+2824, FN+8, Flags+C, 81+109, SSID+"wd	Auth Key Management (AMM) Suite Count: 1
37641 59.	640964	0.020563 Cisco dd:a0:18	Broadcast	882.11	332	69 -38 dBe	Probe Response, SN-2825, FN+0, FlagsC, 81-100, SSID="	<ul> <li>Auth Key Management (A0M) List 00:0fiac (Ieee 882.11) WWA (SHA256-SuiteB)</li> </ul>
37652 59.	661337	0.020353 Cisco dd:a0:18	Broadcast	882.11	312	69 - 38 dBe	Probe Response, 59+2826, Ph+0, Flags+C, 81+100, 5520+1	<ul> <li>Auth Key Management (A00) Suite: 00:0f:ac (Leee 802.11) MPA (SM4256-Suite0)</li> </ul>
37668 59.	681765	0.020428 Cisco dd:a0:18	Broadcast	882.11	332	60 - 38 dBm	Probe Response, SN-2827, FN+0, Flags+C, 81-100, 5520-7	Auth Key Management (ADM) OU[: 00:0f:ac (Leee 802.11)
37687 59.	782467	0.020702 Cisco dd:a0:18	Broadcast	882.11	332	69 -38 dbs	Probe Response, SN+2828, FN+0, Flags+C, BI+100, SSID+*	Auth Key Management (AKH) type: WPA (SHA256-SuiteB) (11)
37696 59.	722867	0.020400 Cisco dd:a0:18	Broadcast	882.11	355	60 -38 dbm	Beacon frame, 99+2829, FN+0, Flags+C, 81+100, SS10+"wd	> RiN Capabilities: 4x000e8
37704 59.	743477	0.020610 Cisco dd:a0:18	Broadcast	802.11	312	60 -38 dim	Probe Response, SN+2030, FN+0, Flags+C, BI+100, SSID+"	PMCID Count: 0
37719 59.	763721	0.020244 Cisco dd:a0:18	Broadcast	882.11	332	69 -38 dBm	Probe Response, SN+2831, FN+0, Flags+C, 81+100, SSID+*	PekiD List
87733 59.	784549	0.020828 Cisco_dd:a0:18	Broadcast	882.11	332	69 -38 dBs	Probe Response, 50x2012, FN+0, Flags+C, 81+100, 5510+1	> Group Hanagement Cipher Suite: 00:0f:ac (Lees 802.11) BIP (GMXC-128)
37738 59.	884659	0.020110 Cisco_dd:a0:18	Broadcast	882.11	312	60 - 38 dBH	Probe Response, SN=2033, FN=0, Flags=C, 81=100, SSID="	> Tag: QBOS LOAD Element MB2.11e CCA Verision
37749 59.	825260	0.020601 Cisco_dd:a0:18	Broadcast	882.11	355	69 -38 dlm	Beacon frame, SN-2834, FN+0, Flags+C, BI+100, SSID+"sd	> Tag: RM Enabled Capabilities (5 octets)
37773 59.	845621	0.020351 Cisco_dd:a0:18	Broadcast	882.11	312	69 -37 dBm	Probe Response, SN+2035, FN+0, Flags+C, 81+100, SSID+"	> Tag: Extended Capabilities (11 octets)
37792 59.	866121	0.020500 Cisco dd:a0:18	Broadcast	882.11	332	69 -37 dbs	Probe Response, SN=2006, FN=0, Flags=C, 81=100, SSID="	> Tag: Tx Power Envelope
17889 59.	887802	0.021681 Cisco_dd:a0:18	Broadcast	882.11	312	69 -38 dbs	Probe Response, SN+2017, FN+0, Flags+C, 81+100, SSID+"	> Tag: Tx Power Envelope
37814 59.	987313	0.019511 Cisco_dd:a0:18	Broadcast	882.11	312	69 - 37 dile	Probe Response, SN-2038, FN-0, Flags+C, BL-100, SSID+"	> Ext Tag: Multiple BSSID Configuration
37822 59.	927668	0.020347 Cisco_dd:a0:18	Broadcast	882.11	355	60 -38 dBe	Beacon frame, SN+2019, FN+0, Flags+C, BI+100, SSID+"vd	> Ext Tag: HE Capabilities
37833 59.	948858	0.020390 Cisco_dd:a0:18	Broadcast	882.11	312	69 - 38 (594	Probe Response, SN+2040, FN+0, Flags+C, BI+100, SSID+1	> Ext Tag: HE Operation
37841 59.	968540	0.020090 Cisco_dd:a0:18	Broadcast	802.11	332	60 -38 dBm	Probe Response, SN=2041, FN=0, Flags=C, B1=100, SSID="	I > Ext Tag: Spatial Reuse Parameter Set
37857 59.	969696	0.020550 Cisco_dd:a0:18	Broadcast	882.11	312	69 -38 dBe	Probe Response, SN+2042, FN+0, Flags+C, BI+100, SSID+1	> Ext Tag: MJ EDGA Parameter Set
37864 60.	013692	0.824582 Cisco_dd:a8:18	Broadcast	802.11	312	60 -37 dBs	Probe Response, SN+2043, FN+0, Flags+C, 81+100, SSID+7	> Ext Tag: HE 6 GHz Band Capabilities
37868 60.	030192	0.016500 Cisco_dd:a0:18	Broadcast	882.11	355	60 -38 dBm	Beacon frame, 59x2844, FNx0, Flags+C, 81x100, 5510x"xd	> Tag: Vendor Specific: Atheros Comunications, Inc.: Unknown
37881 60.	058489	0.020297 Cisco_dd:a0:18	Broadcast	882.11	352	69 -38 dbs	Probe Response, SN=2045, FN=0, Flags=C, 81=100, SSID="	> Tag: Vendor Specific: Microsoft Corp.: WMV/WE: Parameter Element
37887 68.	071057	0.020568 Cisco_dd:a0:18	Broadcast	892.11	332	69 -38 dBr	Probe Response, SN+2846, FN+0, Flags+C, BI+100, SSID+1	> Tag: Vendor Specific: Cisco Systems, Inc: Advonet Client MPP Disabled
37897 60.	091896	0.020839 Cisco_dd:a0:18	Broadcast	882.11	392	69 -38 dBe	Probe Response, SN+2047, FN+0, Flags+C, 81+100, SSID+"	) Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5
17988 58.	111976	0.020080 Cisco_dd:a0:18	Broadcast	882.11	312	60 -38 dBe	Probe Response, SN+2048, FN+0, Flags+C, 81+100, SSID+*	> Tag: Vendor Specific: Cisco Systems, Inc: Adronet Unknown (44)
37917 68.	133414	0.020438 Cisco_60:a0:18	Broadcast	882.11	355	69 -37 dBm	Beacon frame, SN+2049, FN+8, Flags+C, BI+100, SSID+"wd	> fag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)
37928 60.	153047	0.020633 Cisco_dd:a0:18	Broadcast	882.11	312	60 -17 dilm	Probe Response, 59+2050, F8+0, Flags+C, 81+100, 5510+"	
37936 60.	173314	0.020267 Cisco_dd:a0:18	Broadcast	882.11	352	69 -38 dBm	Probe Response, SN-2051, FN-0, FlagsC, 81-100, SSID-1	
17943 60.	293778	0.020464 Cisco_dd:a0:18	Broadcast	882.11	312	69 -37 dim	Probe Response, 596-2052, F8+0, Flags+C, 81+100, 552D+*	
37949 60.	214369	0.020501 Cisco_dd:a0:18	Broadcast	882.11	312	69 -37 dBH	Probe Response, 59-2053, FN+0, Flags=C, 81=100, 552D="	
17961 60.	234873	0.020504 Cisco_dd:a0:18	Broadcast	882.11	355	60 -37 dbs	Beacon frame, SN+2054, FN+0, Flags+C, BI+100, SSID+"wd	

WPA3 Enterprise SuiteB-1X Beacon

None of the tested clients were able to connect to the WLAN using SuiteB-1X confirming that none supports this security method.

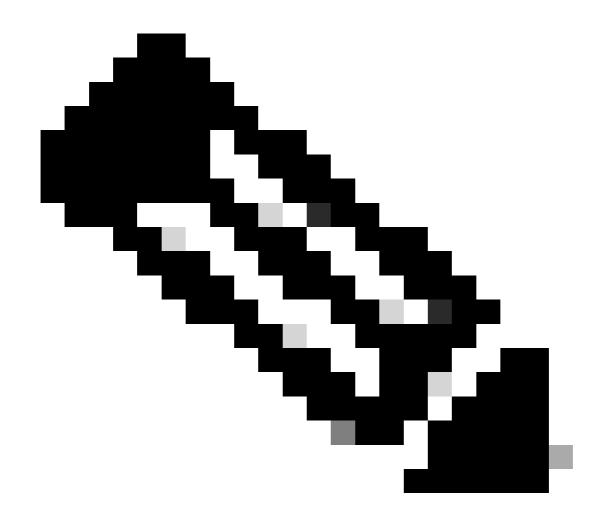
### WPA3-Enterprise + GCMP256 cipher + SUITEB192-1X

WLAN Security configuration:

### Edit WLAN

neral	Security	Advanced Add To	Policy Tags		
yer2	Layer3	ААА			
O WF	PA + WPA2	O WPA2 + WPA3	• WPA3	O Static WEP	O None
MAC F	Filtering	0			
Lobby	Admin Access	0			
WPA P	arameters		Fast	Transition	
WPA Policy	D	WPA2 C	) Stat	us	Disabled
GTK	O	WPA3	Ove	r the DS	0
Rando Transit	-	Policy	·		
Disabl			Kea	ssociation Timeout *	20
	WPA3 Encrypt		Auth	Key Mgmt	
AES(C GCMP	CMP128)	CCMP256	2	UITEB192- 🖸 Х	
GOMP	120	GOMP200		<u> </u>	
Protect	ted Manageme	ent Frame			
PMF		Required	•		
Associ	ation Comeback	Timer* 1			

WPA3 Enterprise SUITEB192-1x security settings



**Note**: FT is not supported with GCMP256+SUITEB192-1X.

### WLAN on WLC GUI WLANs list:



. Tin	ne	Delta Source	Destination	Protocol	Length Cha	nnel Signal stre	Info	> Frame 8: 355 bytes on wire (2640 bits), 355 bytes captured (2640 bits) on interface 'Device/WF_(DAS30065-2008-AdS6-BC33-CAS166AAD08), 55 0
2 8.8	013335	0.000000 Cisco_dd:a0:18	Broadcast	\$92.11	312	60 -60 dBs	Probe Response, SH-242, FN+0, Flags+	> Ethernet II, Sec: Chon.gC:97:47 (Mc11:52:82:97:47), Det: Universa.h7:cf:06 (00:36:08:57:cf:06)
3.0.4	833784	0.020360 Ciscs_6d:a0:18	Broadcast	882.11	51.2	10 -40 dbs	Probe Response, 59-243, F0-0, Flags+C, 81-300, 5532+"vdfist_test"	Sterver Protocol Werston 4, Src: 202.368.3.15, 0st: 202.368.3.123
5.0.1	054144	0.000460 Cisco_6d:a0:18	Broadcast	802.11	332	60 -40 dbs	Probe Response, Sh-244, FM-0, Flags+C, 82+300, 5520+"wdFi66_test"	> User Datagram Protocol, Src Port: 5555, Ost Port: 5860
7 0.4	474543	0.020399 Ciscs_6d:a0:18	Broadcast	992.11	312	80 -40 dbs	Probe Response, 59+245, F8+0, Flags+C, 81+180, 5510+"vd/166_test"	> AiroPeek/Omi/Peek encapsulated IEEE 882.11
8.0.0	birisece	0.000517 Claco.00:00:18	Broadcast	802.11	155	10 -40 (54	Beacon frame, SN-246, FN-0, FlagsC, BI-100, SSID-"wifield_test"	> 802.11 radio information
30 0.1	115495	0.020435 Cisco_dd:a0:18	Broadcast	802.11	112	10 -40 dbs	Probe Response, 99-267, F9-0, Flags+C, 81-300, 5535+"sdf166_test"	> 1812 802.11 Beacon frame, flags:C
11 0.1	1. Incidente	0.000545 Cisco dd:s0:18	Broadcast	892.11	312	80 -40 dbs	Probe Response, SH-248, FM-9, Flags+C, SL-109, SSID-"xdfist test"	V 100 80.11 Wireless Nangement
12 0.1		0.020634 C1sto_60:00:18	Broadcast	802.11	112	80 -60 dbs	Probe Response, S0x289, Fb-0, Flags+	> Fixed parameters (12 bytes)
11 9.1	170348	0.020204 Cisco_dd:a0:18	Broadcast	892.11	212	40 - 39 dBe	Probe Response, 59+250, FM+0, Flags+C, 82+100, 5512+"wdf16E_test"	<ul> <li>Tagged parameters (253 bytes)</li> </ul>
14 0.1		0.020687 C1sco.dla8118	Broadcast	892.11	155	10 -39 dbs	Beacon frame, SN-251, HW-P, FlagsC, 81-109, SSID-"wifi6E test"	> fag: SSDD parameter set: "hdfb86_test"
15 0.3		0.620287 Cisco_dd:a0:18	Broadcast	892.11	112	40 -30 dis	Probe Response, S0+252, FN+0, Flags+C, 82+300, 5532+"sdF16E_text"	> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Mbit/sec]
16 0.3		0.020547 Claco dd:a0:18	Broadcast	892.11	322	10 - 39 dbr	Probe Response, SH-253, FM-0, FlagsC, 81-100, 5522-"offict test"	) Tag: Traffic Indication Map (TIM): DTIM # of 1 bitmap
17 0.3		0.020405 Cisco_df(a0)18	Broadcast	897.11	112	40 -39 dbs	Probe Response, Sh-254, FM-0, FlagsC, 82-100, SSID-"x6FINE test"	> fag: Country Information: Country Code na, Environment Global operating classes
18 9.3		0.020468 Cisco_dd:a0:18	Broadcast	802.11	112	49 - 19 die	Probe Response, Sik-255, Filed, FlagsC, H2+100, SSIDe'wdfisit test"	> Tag: Power Constraint: 6
19 4.3		0.029222 Cisco_0d:x0:10	Broadcast	992.11	355	10 - 39 das	Beacon frame, SN-256, FN-0, Flags+C, 81-100, SSID+"wifi68_test"	3 Tag: TPC Report Translit Power: 16, Link Margin: #
								V Tag: RW Information
28.0.3		0.011681 Cisco_dd:a0:18	Broadcast	802.11	312	89 -39 dBe	Probe Response, SH-257, FH+0, Flags+C, H1+100, SSID+"wifiH_test"	Tag Number: HSN Information (AB)
23 0.3		0.020455 Cisco_6d:a0:18	Broadcast	802.11	312	80 -39 dBm	Probe Response, 50+258, F0+0, Flags+	Tag Length: 26
22 4.3		0.820645 Cisco_6d:a0:18	Broadcast	882.11	312	82 -40 (88	Probe Response, S0+250, FN+0, Flags+C, 81+100, SSID+"wdF166_test"	SN Westor: 1
23 0.3		0.020357 Cisco_dd:a0:18	Broadcast	802.11	112	80 -60 dbs	Probe Response, S0+200, FM+0, Flags+C, 81+300, SSID+"wdfi66_test"	> Group Cloher Subter WHOF(ac (leee 802.11) GOP (256)
24 0,4		0.820663 Clscs_6d:a0:18	Broadcast	802.11	255	80 -40 dBe	Beacon frame, SN-261, FN+0, Flags+C, 81+100, SSID+"wif166_test"	Raindae Capter Suite Court: 1
28.0.4		0.620249 Clsco_6f:88:18	Broadcast	802.13	312	80 -40 dbe	Probe Response, SN+262, FN+0, Flags+C, H1+100, SS12+"xdF166_test"	> Paintise Cipher Softe List 00:01:ac (less 882.11) 609 (256)
29 0.4		0.020622 Cisco_dd:a0:18	Broadcast	802.11	312	80 -40 dbs	Probe Response, SH4263, FM+0, Flags+C, B1+300, SS3D+"xdF16E_test"	Arth key Augement (ANO Suite Court: 1
32.0.4		0.020486 Cisco_65:00:18	Broadcast	882.11	33.2	80 -40 dbs	Probe Response, SN-264, FN+0, Flags+C, 81+300, SSID+"xdfiel_test"	<ul> <li>Arth. Gov. Research (1990). 1141 40: First Res. 8(0, 11) 302. (Spilling Softwill).</li> </ul>
33.9.4		0.020672 Cisco_df:a0:18	Broadcast	802.11	312	80 -40 dbs	Probe Response, SN+265, FN+0, Flags+C, 81+100, SS10+"w1F16E_test"	Auth Key Management (AON) Softe: (0):0f(ac (Leee NR,33) MA (94388-5x(tel))
34 0.5	584028	0.020456 Cinco_6d:a0:18	Broadcest	892.11	355	69 -41 d84	Beacon frame, SN-266, FN+0, Flags+C, Bl+100, SSID+"wif162_test"	Author May Management (Author) Satter World's (Laws MacLan) was (Process-Satters) Author May Management (Author) (Satter (Laws MacLan))
35 0.5	525123	0.020139 Clsco_65;00128	Broadcast	802.11	332	80 -41 (58	Probe Response, SH-267, HH-0, Flags+C, EI+300, SS35+"vEFISE_test"	Acts May Amagement (AMA) Social Microsoft (Communication (Communication) (Communication (Communication) (Commu
36 9.3	545728	0.020687 Cisco_6d:a0:18	Broadcast	802.33	332	80 -40 dbs	Probe Response, SB4268, FN+0, Flags+C, 82+380, 5530+"xdf168_test"	
37.0.5	566216	0.000488 Cisco_66:00:18	Broadcast	882.23	31.2	80 -40 dbs	Probe Response, 59+260, FN+0, Flags+C, 82+100, SSID="wdflift_test"	✓ HSN Capabilities: HoRMe8 
38 0.5	586754	0.020538 Cisco_60:00:18	Broadcast	802.11	332	80 -40 dbs	Probe Response, SNx270, FN+0, Flags+C, 81+100, SS3D+"w1F16E_test"	
20 0.4	687115	0.020361 Cisco_6f:a0:18	Broadcast	892.11	255	80 -40 dbs	Beacon frame, 59+271, F8+0, Flags+C, 81+100, 5510+"wifit6_test"	
40 0.0	627613	0.808496 Cisco_651#0:18	Broadcast	892.11	312	80 - 30 dbit	Probe Response, 59+272, FN+0, Flags+C, 82+380, 5532+"wiffiel test"	10 + RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAGaySA (8x2)
41 0.4	642908	0.829387 Ciscs_6d:a0:18	Broadcast	802.11	222	80 -40 dbs	Probe Response, 59x27), FN+0, Flags+C, 81x300, 5530+"wdFi64_text"	
43 6.8	666633	0.020633 Cisco dd:x0:18	Broadcast	892.13	312	10 -40 dbs	Probe Response, SN-274, FM-0, Flags	1
44 0.4	688017	0.020126 C1sco_66:a0:18	Broadcast	802.33	112	40 - 39 dbs	Probe Sesponse, 99-275, Flod, FlagsC, EL-200, SS25-"ud-Fise text"	1
45 8.3	789471	0.020534 Cisco_dd:a0:18	Broadcast	892.11	255	40 -39 dBe	Beacon frame, SNe276, Pile0, Flags+C, BI+100, SSID+"wif15E_test"	
45.0.1		0.020625 C1603.00130118	Broadcast	802.11	312	10 -30 dila	Probe Response, SH-277, FM-0, Flags	
47.9.3		0.028367 Cisco dd:a0:18	Broadcast	802.11	112	80 - 30 day	Probe Response, SH-278, Hi-0, FlagsC. 82-100, SSED-"uffind test"	
48.0.3		0.020436 Cisco_dd:a0:18	Broadcast	892.11	312	10 -30 dbs	Probe Response, 99-279, Ple9, Flags	PMCDD Count1 @
43 0.1		0.020534 Cisco_60:a0:18	Broadcast	802.11	112	40 - 39 das	Probe Response, 99-280, Filed, FlagsC, 82-200, 5522+"scFild test"	99K20 L1st
50 0.5		0.400539 Cisco_dd:a0:18	Broadcast	802.33	255	80 -40 dbr	Beacon frame, SN-281, FN-0, FlagsC, 81+100, SSID+"wdf16E_test"	> Group Management Cipher Suite: 00:0f:ac (leee 302.11) 81P (GMG-256)
51 0.0		0.400350 Claco_65:00:18	Broadcast	892.11	312	80 -30 das	Probe Response, Sh-282, Field, FlagsC, 81-100, SSID-"wifild test"	1 Fag: (803 Call Editor), 842-127 Col Version
51 0.0		0.000634 Cisco dd:a0:18	Broadcast	892.11	112	82 - 32 day	Probe Response, Sb-283, Ph-0, Flags	> Tag: HM Enabled Capabilities (5 octuts)
54 8.8			Broadcast	802.11	312			> Tag: Extended Capabilities (11 octets)
		0.020600 Cisco_dd:a0:18 0.020411 Cisco_dd:a0:18		802.11	312		Probe Response, SH-204, FM-0, FlagsC, 82-100, SS20*Adfide_test* Probe Response, SH-205, FM-0, FlagsC, 82-100, SS20*Adfide_test*	> Tag: Tx Power Envelope
55 @.8			broadcast			40 -40 dbs		> Tag: Tx Power Envelope
56 0.5		0.000587 Cisco_dd:a0:18	Broadcast	802.11	355	69 -68 dbs	Beacon frame, S0-286, FN+0, Flags+C, 82+200, SSID+"w1F16E_text"	but fag: Multiple BSSD Configuration
57-0.5		0.020401 C1sto_6d:a0:18	Broadcast	802.11	312	60 -40 dBr	Probe Response, SH-287, FN=0, Flags+C, 81+100, SSID="wif166_test"	> Ext Tag: W Capabilities
58.9.5		0.020200 Cisco_65:a0:18	Broadcast	802.11	322	80 -40 dbs	Probe Response, S9x288, F8x0, Flags+	<ul> <li>bit rag: is operation</li> </ul>
68 9.5		0.020473 Cisco_dd:a0:18	Broadcast	802.11	322	80 -68 dbs	Probe Response, SH-280, FM+8, Flags+	<ul> <li>bit ing. Solid Rune Parameter Set</li> </ul>
65 0.3		0.020404 Cisto_65:00:18	Broadcast	882.11	312	80 -40 dbs	Probe Response, SN+290, FN+0, Flags+	> bit for a particular from the set
62 3,6	817136	0.020543 Cisco_dd:a0:10	Broadcast	802.11	255	80 -40 dbe	Beacon Frame, Ste292, HowB, Flags+C, B1+100, SSID+"wifildC_test"	<ul> <li>bit rag: H6 6 Mer Band Cashillities</li> </ul>

WPA3 Enterprise SUITEB192-1x beacons

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

### Intel AX211

Connection OTA with focus on the RSN information from client:

No	Time	Delta Source	Destination	Protocol	Length Chann	el Signal strength	BSS Id	lofo	> Frame 17873: 1116 bytes on wire (8028 bits), 1116 bytes captured (8028 bits) on interface 'Device's
	17760 13:51:17.057043	0.015572 IntelCor 98:58:04	Broadcast	802.11		64 -39 dlin	11:11:11:11:11:11	Probe Request, SH+352, FM+0, Flags+C, SSIDw"hdf16E_test"	1 > Ethernet II, Src: Cisco_d2:97:47 (74:11:b2:d2:97:47), Dat: Universa_b7:cf:06 (00:5a:80:b7:cf:06)
	17790 11:51:17, 312635	0.275592 192.168.1.15	192.168.1.121	892.11	26	69 -44 dlm		Clear-to-send, flags,C	I > Internet Protocol Version 4, Src: 292.168.1.15, Ost: 292.168.1.121
	17831 13:51:37,355711	0.023876 IntelCor 98:58:04	Cisco dd:a0:18	882.11		60 -44 dBm	00:df:1d:dd:a0:10	Authentication, SNv7, FNv8, FlagssC	> User Dutagram Protocol, Src Port: 5555, Dst Port: 5000
	17632 13:51:37, 355711	0.000000 192.158.1.15	192.168.1.121	882.11		69 -37 dBe		Acknowledgement, Flags+C	> AiroPeek/OmiPeek encapsulated IEEE 882.11
	17833 13:51:37,359876	0.004165 Cisco dd:a0:18	IntelCor_98:58:0f	882.11		69 - 37 dBm	00:df:1d:dd:a0:18	Authentication, SN+20, FN+0, Flags+C	> 882.11 radio information
	17635 13:51:37.368682	0.000806 IntelCor 98:58:0f	Cisco dd:a0:28	882.11		69 -45 dBn	WestFradsdraft18	Association Request, SH+8, FN+0, Flags+C, SSID+"wifing test"	1111 912.11 Qo5 Data, Flags:F.C
	17636 13:51:37.360682	0.000000 192,168,1,15	292.168.1.121	802.11		60 +37 dbn	66.001.200.001.001.00	Acknowledgement, Flags	Type/Subtype: QoS Data (8x8028)
	17638 13:51:37.369329	0.008647 IntelCor 38158:04	Broadcast	LLC		69 - 37 d8e	0010F(5d)dd(a0158	I P, N(R)=48, N(S)=21; DSAP 0x36 Group, SSAP 0x52 Response	> Frame Control Field: 0x8002
	17839 13:51:37.372564	0.002215 Cisco dd:a0:18	IntelCor_98158:0F	802.13		69 - 17 dBs	Weidf (1d) dd all 18	Association Response, Skiel, Place, FlagsC	.000 0000 0100 1100 - Duration: 76 microseconds
	17841 13:51:17.102564	0.000000 192.158.1.15	292.168.1.121	802.13		69 -17 dBs	00/04/140/00/00/00/00	Request-to-send, FlagsC	Receiver address: IntelCor_98:58:0f (28:6b:35:98:58:0f)
	17843 13:51:17.102564	0.000000 Cisco dd:a0:18	intelCor_98:58:04	LAP		69 -17 dBm	00:df:5d:dd:a0:15	Request, Identity	Transmitter address: Cisco_dd:a0:18 (40:df:ld:dd:a0:18)
	17847 13:51:17.406678	0.035114 IntelCor 30:58:04	Cisco_dd:a0:18	LAPOL		69 -46 dla	00-dF:1d-dd:a0-18	Start	Destination address: IntelCor_98:58:0F (28:08:35:98:58:0F)
	17868 13:51:37,406678	0.000000 107.148.1.15	192.168.1.121	802.11		69 - 37 clim	10.07.20.00.20.20		Source address: Clscs.dd:a0:18 (40:df:1d:dd:a0:18)
	17849 13:51:37.409431	0.000000 102.108.1.15	192.168.1.121	802.11		69 -37 dile		Acknowledgement, Flags+C Request-to-send, Flags+C	855 Idi (15co.ddia0:18 (00:dfild:dd:a0:18)
	17851 13:51:37.408572		192.100.1.111 IntelCor_98:58:0f	1002.111 LAP		69 -37 dile	00:df:1d:dd:a0:18	Request-to-serg, Flags	STA address; intelCor.98(58)8f (28(66:35)98(58)8f)
	17851 13:51:37.408572 17855 13:51:37.425798	0.000141 Cisco_dd:a0:18		EAP		69 -49 dBm	00:df:1d:dd:a0:18		
	17855 13:51:37.425798	0.017226 IntelCor_90:58:0/ 0.000000 192.168.1.15	Cisco_68:a0:18 192.168.1.121	882.11		69 -49 clas 69 -37 dBe	00007130000180138	Response, Identity	0000 0000 0011 = Sequence number: 3
							20202220222	Acknowledgement, Flags+C	Frame check sequence: 0x00000000 [unverified]
	17858 13:51:37,425952	0.000154 IntelCor_90:58:04	Cisco_65:a0:18	EAP		69 -48 dBm	00:df:1d:dd:a0:18	Response, Identity	[FCS Status: Unverified]
	17859 13151137,425952	0.000000 192.168.1.15	192,168.1.121	882.11		69 -37 dBe		Acknowledgement, Flags+C	> Qos Control: 6x60007
	17861 13151137,458271	0.032319 192.168.1.15	192.368.1.123	802.11		69 -37 dbm	020222000000000	Request-to-send, Flags+C	✓ Logical-Link Control
	17863 13151137,458271	0.000000 Cisco_dd:a0:18	IntelCor_98:58:0F	EAP-		69 -37 dbs	00105134104128	Request, TLS EAP (EAP-TLS)	v (Sar: Sar (haa)
	17866 13:51:37.469889	0.011618 192.168.1.15	192.168.1.121	882.11		69 -48 dbn		Clear-to-send, Flags+C	1010-101. = SAP: SNAP
	17868 11:51:37.486723	0.016832 192.168.1.15	192.168.1.121	802.11		69 -37 dBm		Acknowledgement, FlagsC	0 = 15 Bit: Individual
	17869 13:51:37.487783	0.001062 IntelCor_90:58:04	Cisco_dd:a0:10	TL5v1.2		69 -48 d8s	00:df:1d:dd:a0:18	Client Wello	> SSAP: SNAP (Boas)
	17870 13:51:37.487783	0.000000 192.168.1.15	192.168.1.121	802.11		69 -17 dim		Acknowledgement, Flags+C	✓ Control field: U, func-UI (0x03)
	17871 13:51:37.497138	0.009355 192.168.1.15	192.168.1.121	892.13		69 -17 d8m		Request-to-send, Flags+C	000. 00 = Command: Unnumbered Information (0x00)
	17073 13:51:37.498652	0.001514 Cisco_dd:#0:18	IntelCor_98:58:0f	ENP		69 -17 dBn	00:df:1d:dd:a0:18	Repurst, TLS EAP (EAP-TLS)	
	17875 13:51:37.502459	0.003807 IntelCor_96158:04	CLisco_dd:a0:18	LAP		69 -48 dBm	00:df:1d:dd:a0:18	Response, TLS EAP (EAP-TLS)	Organization Code: 00:00:00 (Officially Xerox, but
	17876 13:51:37.582459	0.000000 192.158.1.15	292.168.1.121	882.11		69 -17 dBm		Acknowledgement, Flags+C	Type: B02.1X Authentication (0x888e)
	17877 13:51:37.584792	0.002333 192.168.1.15	192.168.1.121	882.11		69 -17 dBs		Request-to-send, Flags+C	✓ W2.1X Authentication
	17879 13151:37.505493	0.000701 Cisco_dd:a0:18	1stelCor_98:58:0f	TLSv1.2		69 -17 dbs	001dF13d1dd1a0138	Ignored Unknown Record	Version: 882.18-2010 (3)
	17883 13:51:37,518581	0.013088 IntelCor_98:58:0f	Cisco_dd:a0:28	EAP		69 -48 dBm	00:dF:1d:dd:a0:18	Response, TLS EAP (EAP-TLS)	Type: LAP Packet (0)
	17884 13:51:37.518581	0.000000 192.168.1.15	292.368.5.321	892.33		69 -37 d8n		Acknowledgement, Flags+C	Length: 3812
	17885 13:51:37.522955	0.003374 192.168.1.15	192.168.1.121	802.11		69 -38 dBn		Request-to-send, Flags+C	V Extensible Authentication Protocol
	17887 13:51:37.521955	0.000000 Cisco_dd:a0:18	lstelCor_98:58:0f	LAP		69 -37 dBn	00:df:1d:dd:a0:18	Request, TLS LAP (EAP-TLS)	Code: Request (1)
	17889 13:51:37.523974	0.000019 IntelCor_96:58:04	Cisco_dd:a0:18	TL5v1.2		62 -48 dBn	00:df:1d:dd:a0:18	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, En	10:98
	17990 13:51:37.523974	0.000000 192.158.1.15	192.168.1.121	882.11		69 -37 dBt		Acknowledgement, Flags+C	Length: 3012
	17993 13:51:37,528839	0.000056 192.158.1.15	192.168.1.121	882.11		69 -37 dBm		Request-to-send, Flags+C	Type: TLS (AP ((AP-TLS) (13)
	17995 13:51:37.528355	0.000325 Cisco_dd:a0:18	IntelCor_98:58:0f	TL5v1.2		60 -37 dBm	00:df:1d:dd:a0:18	Change Cloher Spec, Encrypted Handshake Message	<ul> <li>(g)e: (is be (bends) (a)</li> <li>✓ (bP-fLS Flag: 0x0</li> </ul>
	17998 13:51:37.534810	0.006455 192.168.1.15	192.168.1.121	882.11		60 -38 dBH		Acknowledgement, Flags+C	1 + Length Included: True
	17899 13:51:37.539457	0.064647 192.168.1.15	192.168.1.121	882.11		69 -48 dbs		Clear-to-send, Flags=C	.1
	17941 13151137.556537	0.017088 192.158.1.15	192.168.1.121	882.11		69 -38 dBe		Acknowledgement, Flags+C	
	17982 13151:37,556624	0.000087 IntelCor_98:58:0f	£1500_65180128	EAP		69 -49 dBs	000dF13d0dd1a0138	Response, TLS EAP (EAP-TLS)	
	17983 13:51:37.556624	0.000000 192.168.1.15	192.168.1.121	80.11	76	69 -38 dBn		Acknowledgement, Flags+C	EAP-TLS Length: 1381
	17906 13:51:37.586732	0.030108 192.148.1.15	192.168.1.121	802.11		69 -35 dlm		Acknowledgement, FlagseC	
	17908 13:51:37.592524	0.004792 192,168.1.15	192.168.1.121	882.11		60 -38 din		Clear-to-send, FlaguxC	
	17965 13:51:37.688659	0.017135 192.168.1.15	192.168.1.121	802.11	76	69 -38 dlin		Acknowledgement, Flags+C	
	17967 11:51:17.618408	0.001749 192.168.1.15	192.168.1.121	802.11	82	69 -38 dlin		Request-to-send, FlagsC	
	17969 13:51:37,638472	0.000064 Cisco_dd:s0:18	IntelCor_98:58:0f	EAP	288	69 -38 dBe	00:df:1d:dd:a0:18	Success	
	17971 13:51:37,611308	0.000836 192.168.1.15	192.168.1.123	882.13	82	69 -37 dBm		Request-to-send, FlagsC	
	17973 13:51:37.611446	0.000138 Cisco_dd:a0:18	1#telCor_98:58:0f	EAPOL	221	69 -37 d8m	00:df:1d:dd:a0:18	Key (Message 1 of 4)	
	17975 13:51:37.621381	0.000035 IntelCor_90158:04	Cisco_6d:a0:18	EAVOL	346	69 -49 d9m	00:df:1d:dd:a0:18	Key (Message 2 of 4)	
	17976 13:51:37.621381	0.000000 192.158.1.15	292.168.1.121	802.11	76	69 -38 dBm		Acknowledgement, Flags+C	
	17980 13:51:37.630913	0.009532 192.168.1.15	192.168.1.121	802.11	82	69 -17 d8m		Request-to-send, Flags+C	
	17982 13:51:37.631510	0.000507 Cisco_dd:a0:18	1=telCor_98:58:0f	EAPOL	423	69 -17 dBs	00:df:1d:dd:a0:18	Key (Hessage 1 of 4)	
	17984 13:51:37.632421	0.000911 IntelCor_99:58:04	C1sco_dd:a0:38	EAPOL	299	69 -42 dbs	WeidF:1didd:a0:18	Key (Hessage 4 of 4)	
	17985 13:51:37.632421	0.000000 192.158.1.15	292.168.1.121	802.11	76	69 -37 dBs		Acknowledgement, FlagueC	

WPA3 Enterprise with EAP-TLS Association with Intel AX211 client and RSN Info

### And the EAP-TLS exchange:

No, Time	Delta Source	Destination	Protocol	Leonth Cha	nnel Signal strength	BCC 14	Info	> Frame 17875: 110 bytes on wire (800 bits), 110 bytes captured (800 bits) on interface 'Device'APP_
17760 11:51:17.05700		Broadcast	882.11	236	64 - 10 dis	**:**:**:**:**	Probe Request, SN-352, PN-0, FlagsC, SSID-"ulfine_test"	) Ethernet II, Src: Cisco_d2:97:47 (74:11:82:d1:97:47), Ost: Universa_b7:cf:06 (08:3a:88:b7:cf:06)
17780 11:51:17.33263		292.168.1.121	882.11	26	69 -44 dis		Clear-to-send, FlagsC	I > Internet Protocol Version 4, Src: 192.168.1.15, Dit: 292.168.1.121
17831 13:51:37.35571		Cisco_dd:a0:18	802.11	56	40 -44 dim	00:0013d:00130	Authentication, SHo7, Flore, FlagssC	> User Datagram Protocol, Src Port: 5555, Ost Port: 5980
17812 13:51:37.35571		192.168.1.121	882.11	26	69 -37 dBm		Acknowledgement, FlagsC	3 AbroPeek/OmriPeek encapsulated IEEE 882.11
17853 13:51:37,35987		intelCor SH:58:0f	882.11	96	69 -37 dBm	00:00:10:00:00	Authentication, SN+20, FN+0, Flags+C	> 882.11 radio information
17835 11:51:37.36868		Cisco_dd:a0:18	882.11	252	69 -45 d8e	001-0111d-011a0-18	Association Request, SN+8, FN+8, Flags+C, SSID="wifi6E_test"	> IEEE 882.33 QoS Data, Flags:TC
17836 13:51:37,36869		192.168.1.121	872.11	26	69 -37 dBe		Acknowledgement, Flags	✓ Logical-Link Control
17838 13:51:37,36933	9 0.008647 IntelCor 98:58:0F	broadcast	LLC	114	69 -37 dbs	00107134145140138	1 P, N(R)=48, N(S)=21; DSAP BiO6 Group, SSAP BirF2 Response	✓ 054F: SMP (Boa)
17839 13:51:37.37156	4 0.002235 CLsos_dd:a0:18	1stelCor_98:58:0F	882.11	32.5	60 -37 dBs	001dF11d1df1a0118	Association Response, SNe0, FNe0, FlagsC	1819 181. × SMP: SMP
17841 11:51:17.17154		192.168.1.121	882.11	82	60 -37 dim		Request-to-send, FlagsC	
17843 13:51:37.37154		DetelCor_SH:SH:04	LIP	109	60 -37 clim	00:df:1d:dd:a0:18	Request, Identity	> SS#: SWP (Bus)
17847 13:51:17.40667		Cinco_dd:a0:18	LAPOL	385	60 -46 dim	00:df:1d:dd:a0:18	start	<ul> <li>Control flaid: U, funcial (BuRI)</li> </ul>
17548 13:51:37,48667		192.168.1.121	882.11	76	69 -37 dlm		Acknowledgement, FlagsC	000. 00., - Command: Unruebered Information (0x00)
17940 13:51:37.40843		192,168,1,121	882.11	112	69 -37 dbm		Request-to-send, FlagsC	
17851 13:51:37,40857		IntelCor_98:58:0f	LAP	189	69 -37 dBm	80:07:10:00:18	Request, Identity	Organization Code: 00:00:00 (Officially Xerox, but
17855 13:51:37.4257		Cisco_dd:a0:18	640	132	60 -40 dBm	0010F130100100138	Response, Identity	Type: 802.1X Authentication (bx888e)
17856 13:51:37.4257		292.168.1.121	882.11	26	60 -37 dile		Acknowledgement, Flags+C	V B02.1X Authentication
17858 13:51:37.4259		Cisco_Ad:a0:18	64P	117	40 -48 dbs	00:0F12d:dd:a0:15	Response, Identity	Version: 802.DR-2005 (1)
17859 13:51:37.42595		292.168.1.121	802.11	28	49 -37 dla		Acknowledgement, Flags+C	Type: LAP Packet (0)
17861 13:51:37.45827		292.168.1.121	802.11	82	69 -37 dim		Request-to-send, Flags+C	Longth: 6
17863 13:51:37.45827		IntelCor_98:58:04	LAP	118	69 -37 dlm	00100110100100110		✓ Extensible Arthentication Protocol
17866 13:51:37.46988		192.168.1.121	892.11	25	69 -46 die	CONTRACTOR CONTRACTOR	Clear-to-setd, FlagsC	Code: Response (2)
17868 13:51:37.48672		192.168.1.121	882.11	25	69 -37 dBs		Acknowledgement, flagsC	16: 98
- 17869 13:51:37.48779		Cisco dd:a0:18	1LSv1.2	365	69 -48 dBs	00107124148128	Clievt Hello	Leight: 6
17870 13:51:37,48779		192.168.1.121	882.11	26	49 -37 dBs	00.007.200.000.000.00	Acknowledgement, Flags+C	Type: TLS EAP (EAP-TLS) (23)
17871 13:51:37.4971		192.368.1.121	882.11	82	69 -37 dim		Request-to-send, Flags+C	✓ LAP-TUS #lags: 0x00
17873 13:51:37.49865		IntelCor_98:58:84	6AP	1116	69 -37 dim	00:07:14:00:18	Request, TLS EAP (EAP-TLS)	0 = Length Included: False
17875 11:51:17.50345		CLISCO_dd:a0:18	WP	128	69 -48 dbs	00107110100100-10		.0., + More fragments: false
17876 13:51:37.50245		192.168.1.121	802.11	25	60 -37 dim	denses resconsidentes	Acknowledgement, FlagsC	Start: False
17877 13:51:37.50475		292.168.1.121	882.13	82	60 -37 das		Request-to-send, FlagsC	
17879 13:51:37.50540		IntelCor_98:58:0f	TL5v1.2	489	69 -37 688	00:07:10:07:18		
17883 13:51:37.51858		Cisco dd:a0:18	UP	116	60 -48 008	00:df:1d:dd:a0:18	Response, TLS EAP (EAP-TLS)	
17884 13:51:37.51858		292.168.1.121	882.11	28	69 -37 686	00107120200100120	Actional edgement, FlagsC	
17885 13:51:37.5239		292.168.1.121	882.13	12	60 -35 dla		Request-to-send, FlagsC	
17887 13:51:37.5239		IntelCor_98:58:00	LAP	118	60 - 17 dille	00107124144148128	Request, TLS EAP (EAP-TLS)	
17889 13:51:37.5239		Cisco_ddtail:18	TLSv1.2	938	60 -48 dist	001dF11d1dd1a0118	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, En	
17890 13:51:37.52397		192.168.1.121	802.15	75	69 -17 dim	decise recompanyaer se	Actualedgenent, flags	
17893 13:51:37.52880		592.368.3.321	892.11	82	69 -17 dla		Request-to-send, Flags=C	
17895 13:51:37.52835		IntelCor_98:58:07	R62.13	161	69 -37 dim	00:df:1d:dd:a0:18		
17898 13:51:37.55485		192.168.1.121	882.13	75	69 -38 dBm	00000120000000018	Acknowledgement, Flags+C	
17899 13:51:37.53945		292.168.1.121	882.11	28	60 - 58 dile		Clear-to-send, FlagsC	
17009 13:51:37.55653		292.168.1.121	882.33	28	40 - 38 dBm		Acknowledgement, Flags	
17902 13:51:17.55662		Cisco ddia0:18	UAP	138	40 -40 dbs	00107134105100138	Response, TLS (AP ((AP-7LS)	
17902 13:51:37.55662		192.168.1.121	882.13	26	60 - 18 dim		Acknowledgement, FlagsC	
17905 13:51:37.5867		292.168.1.121	802.13	2	60 - 18 dan		Acknowledgement, Flags	
17908 11:51:17.50152		192.368.3.321	882.33	24	69 - 38 dan		Clear-to-send, FlagsC	
17965 13:51:37.60855		192.168.1.121	882.33	75	69 - 38 dBm		Acknowledgement, FlagssC	
17965 13:51:37.60000		192.168.1.121	882.13	10	60 - 36 dBm		Request-to-send, FlagsC	
17967 13:51:37.61042		1/12.100.1.111 1/101Cor_96:58:0f	642	106	60 - 35 dBH	00:07120:00:00:18	Success	
17971 13:51:37.8118		292.168.1.121	892.33	100	69 - 37 dbs	A6744 (\$5000)96(18	Request-to-send, Flags+C	
17973 13:51:37.6114		IntelCor_98:58:04	EAPOL	223	60 -37 dila	0010712410100128		
17975 13:51:37.6213		CEsco_6d1a8/18	EAPOL	346	60 -40 (88	0010F110100100108	Key (Message 2 of 4)	
17976 13:51:37.6213		192.368.1.323	882.13	75	49 -38 dila	00/07 1 20/00 1 20/1 28	Acknowledgement, FlagseC	
17990 13:51:37.62630		292.368.1.321	802.13	42	69 - 17 dim		Request-to-send, Flags+	
17982 13:51:37.63153		intelCor_98:58:04	EAPOL	423	69 - 17 dan	00:07:10:00:08:18		
17984 13:51:37.6316		Cisco_dd:a0:18	EAPOL	199	69 -49 dlm	00:07:10:00:00:18	Key (Ressage 4 of 4)	
17984 13:51:37.6324		Cisco_dd:a0:18 192.168.1.121	B82.13	199	40 -40 dan 40 -37 dan	ee.0011000018018	Key (Hessage 4 of 4) Acknowledgement, Flagt=C	
			882.11	12	60 -47 dbs			
17986 13:51:37.64017		192.168.1.121 IntelCor_98:58:0f		183	69 -48 (88)	00107120100100158	Repuest-to-send, Flags=C 5, func=RE3, NCR3=83; DSAP 19M Net Management Group, SSAP Wx00 Response	
17988 13:51:37.6401 17998 13:51:37.6402		IntelCor_98:58:64	LLC	183	60 -45 dile	0010F1101001a0118	5, Func-IRL2, N(R)+63; VSWP Jah Wet hanagement unoup, SSWP wide hesponse 5 F, func-IRM, N(R)+52; USAP Netkane Group, SSAP Wide Response	
17994 13:51:37.6462		192.168.1.121	882.11	283	60 -17 dila	00101140000180028	S.F., functione, scholars, cour network uroup, sour ease response Actinouladgement, FlagssC	
		192.168.1.121 392.168.1.121		100	69 - 17 das 69 - 49 das			
17995 13:51:37.67629	6 0.001725 192.168.1.15	392.368.1.321	882.13		69 - 49 das		Clear-to-send, Flags*C	

WPA3 Enterprise with EAP-TLS Association with Intel AX211 client and EAP-TLS Focus

### Client details in WLC:

Image: Instrume       Montoring *> Wireless *> Clients       300 Vew General QOS Statistics ATF Statistics Mobility History Cult         Image: Instrume       Image: Instrume       Image:	Cisco Cisco Cata	yst 9800-CL Wireless Controller	Welcome admin 👘 🕷 🛕	Search APs and Clients
Cients Stepping Cients Excluded Cients   Configuration Cient Statistics Cient Statistics   Cients Stepping Cients Funded Cients   Cients Stepping Cients Funded Cients   Cients Stepping Cients Funded Cients   Cients Funded Cients Funded Cients   Cients Stepping Cients Funded Cients   Cients Funded Cients Funded Cients   Funded Cients Funded Cients   Funded Cients Funded Cients   Funded Cients Funded Cients   Funded Cients Funded Cients   Funded Cients Funded Cients   Funded Cients Funded Cients   Funded Cients Funded Cients   Funded Cients Funded Cients   Funded Cients Funded Cients   Funded Cients Funded Cients   Funded Cients Fund	Q Search Menu Items	Monitoring * > Wireless * > Clients	Client	
Image: Configuration		Clients Sleeping Clients Excluded Clients	360 View General QOS Statisti	cs ATF Statistics Mobility History Call
	Dashboard		Client Properties AP Properties	Security Information Client Statistics QO
Sector double should in T Clearts       Sector double should in T Clearts <ul> <li></li></ul>	Monitoring >	× Delete C	Re-Authentication Timeout	1800 sec (Remaining time: 1172 sec)
		Selected 0 cut of 1 Clients		
	U U			
Image: Control of Attachment       Encryption Cipher       COMP (AES)         Image: Control of Attachment       Encryption Cipher       COMP (AES)         Image: Control of Attachment       Encryption Cipher       Encryption Cipher         Image: Control of Attachment       Common Session Timour       1800         Image: Control of Attachment       Common Session ID       0x00000000         Image: Control of Contr	Administration		Policy Type	WPA3
EAP Troubleshooting     EAP Trype     EAP-TLS       Session Timout     1800       Session Timout     1800       Session Timout     0x9000000       If ID     0x9000000       If ID     0x9000000       Authorized     TRUE       Common Session ID     0x00000001BC0080064       Acth Method Status List     Valide Status List       Method     Status     Det ix       SM Bend State     AUTHENTICATED       SM Bend State     DLE		-		
Session Timeout         Session Timeout         1800           Session Manager         Session Manager         Point of Attachment         capwap_900000e           IF (D         0x000000E         IF (D         0x000000E           Authorized         TRUE         Common Session ID         0F01ABC0000001BC008064           Actt Session ID         0x0000000E         Authorized         AuthORIZED           Memod         Det1x         Session ID         Det1x           SM Bend State         AUTHENTICATED         SM Bend State         DE	Ū			
Point of Attachment         capwap_9000000e           BF (p         0x4000000E           Authorized         TRUE           Common Session ID         0x00000001BC0D80064           Acthorized         0x0000000           Authorized         0x000000000           Authorized         0x00000000           Authorized         0x000000000           Authorized         0x000000000           Authorized         Deltix           Method         Deltix           SM Bend State         ULE	X Troubleshooting			
IF ID         0x900000E           Authorized         TRUE           Common Session ID         0F01A8C0000001BC0080064           Acct Session ID         0x000000           Auth Method Status List         Herhod           Method         Dot1x           SM Bend Status         AUTHENTICATED           SM Bend Status         DUE			Session Manager	
Authorized         TRUE           Common Session ID         0F01A8C0000001BC0D80D64           Acct: Session ID         0x0000000           Authorized         Authorized           Auth Method Status List         Herbod           Method         De11x           SM Bend State         DUE			Point of Attachment	capwap_9000000e
Common Session ID         OF01A8C0000001BC0080064           Acct: Session ID         0x0000001           Auth: Method         Status List           Method         Dot1 x           SM State         Dot1 x           SM Bend State         DuE			IIF ID	
Acct Session ID 0x0000000 Auth Method Status List Method Dot 1x SM Bend State AL/THENTICATED SM Bend State IDLE				TRUE
Auth Method Status List Method Dot1x SM State AUTHENTICATED SM Bend State DLE			Common Session ID	0F01A8C0000001BC0D80D64
Method Dot1x SM State AUTHENTICATED SM Bend State IDLE				0x00000000
SM State AUTHENTICATED SM Bend State IDLE				
SM Bend State DLE				

WPA3 Enterprise with EAP-TLS client details

### NetGear A8000

WPA3-Enterprise is not supported on this client.

### Pixel 6a

At the date of writing this document, this client was not able to connect to WPA3 Enterprise using EAP-TLS.

This was a client side issue that is being worked on and as soon its resolved, this document shall be updated.

### Samsung S23

At the date of writing this document, this client was not able to connect to WPA3 Enterprise using EAP-TLS.

This was a client side issue that is being worked on and as soon its resolved, this document shall be updated.

### **Security Conclusions**

After all the previous tests, this is the resultant conclusions:

Protocol	Encryption	AKM	AKM Cipher	EAP Method	FT- OverTA		Intel AX211	Samsung/Google Android	Net A8(
( ) ) ) [ ]	AES- CCMP128	OWE	NA.	NA.	NA	NA	Supported	Supported	Sup
S A F	AES- CCMP128	SAE (H2E Only)	SHA256	NA.	Supported	Supported	Supported: H2E Only and FT- oTA	Supported: H2E Only. FT Failed. FT- oDS Failed.	Sup H2I and oTA FT- Fail
Enterprise		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 SHL and oTA Not Sup EA FAS
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

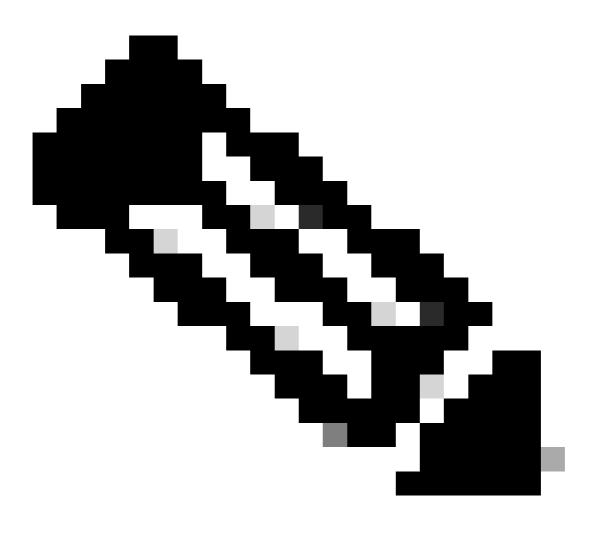
The troubleshooting used in this document was based on the online document:

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 Commands before 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