Collect Packet Captures Over the Air on a MacBook

Contents

Introduction Prerequisites Requirements Components Used Background Information Configure Option A. Configure PCAP with Wireless Diagnostics Option B. Configure PCAP with Airtool Option C. Configure PCAP with Wireshark Verify Troubleshoot Related Information

Introduction

This document describes how to collect Packet Captures (PCAPs) Over the Air (OTA) with the native tool Wireless Diagnostics and third-party applications such as Airtool and Wireshark on a MacBook in order to troubleshoot and analyze wireless behaviors.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Wireless LAN Controllers (WLCs) AireOS or Cisco IOS®-XE
- Basic knowledge in the 802.11 Standard

Components Used

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

- Apple MacBook with macOS version 10.14.X or higher
- Apple Wireless Diagnostics tool
- Airtool 1.9 or higher
- Wireshark 3.X or higher
- Cisco Access Point (AP) 2802

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

Things to consider:

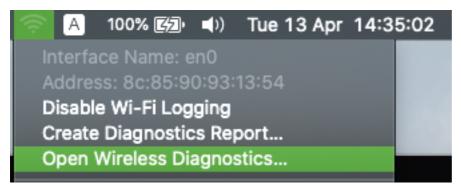
- It is recommended to have the Macbook acting as a Wireless Sniffer close to the AP and target device.
- Ensure you know which 802.11 Channel and Width, the client device, and the AP use.
- The Channel and Width can be found on: Cisco IOS®-XE Web Graphical User Interface (GUI) under Configuration > Wireless > 5GHz or 2.4GHz > Select an AP > Channel and WidthAireOS Web GUI under Wireless > Access Points > 802.11a/n/ac (5GHz) or 802.11
 b/g/n (2.4GHz) > Select an AP > Channel and Width

Configure

Option A. Configure PCAP with Wireless Diagnostics

Step 1. Launch the Wireless Diagnostics Tool.

Press and hold the **ALT/Option** Key from the keyboard and click on the top-right **Wi-Fi icon**, as shown in the image.



Step 2. Open the Sniffer Tool.

Select the **Window** menu from the Wireless Diagnostic Tool on the menu bar and select **Sniffer** or use the keyboard shortcut, press at the same time **ALT + Command + 6** Keys, as shown in the image.

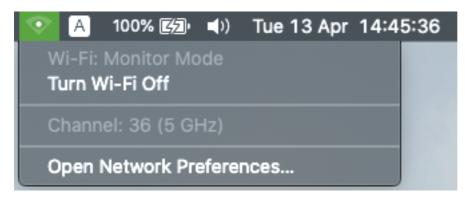
Wireless Diagnostics	File	Edit	Window		
			Minimize	жм	 Wireless Diagnostics
	**	100			Introduction Wireless Diagnostics is an application that detects common
		5		ж1 ж2	problems with your wireless connection. It can also monitor your wireless connection for intermittent connectivity failures. <u>More</u>
			Scan Y	жз ж4	Upon completing this assistant, a diagnostics report will be created in /var/tmp. By sending a copy of the report to Apple, you
Teppe		Aurica		.₩5 .₩6	are consenting to Apple's use of the content of such report. More
			Sidecar T	% 7	Wireless Diagnostics may temporarily change your network settings when running diagnostics tests.
A CONTRACTOR	14		✓ Wireless Diagnostics		Click "Continue" to begin diagnosing your wireless environment and configuration.
7					
	Ser and				Start Over Continue

Step 3. Choose the **Channel** and **Width** that the target device and AP use, as shown in the image.

	Sniffer					
Use your Mac as a dedicated sniffer to capture Wi-Fi traffic. Choose a channel and channel width, then click 'Start' to begin.						
Click 'Stop' when you a created in /var/tmp.	Click 'Stop' when you are finished and a wireless capture file will be created in /var/tmp.					
Channel:	36	0				
Width:	20 MHz	0				
	Start					

Step 4. Click Start.

This action places the Wireless adapter in Monitor Mode and it cannot be used to connect the device to a Wireless LAN (WLAN), as shown in the image.



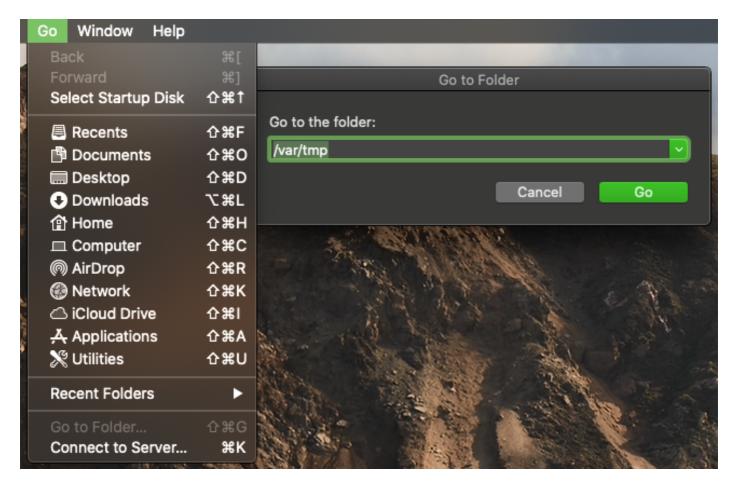
Step 5. Wait for some time to collect the information required and click Stop.

	Sniffer				
Use your Mac as a dedicated sniffer to capture Wi-Fi traffic. Choose a channel and channel width, then click 'Start' to begin. Click 'Stop' when you are finished and a wireless capture file will be					
created in /var/tmp.	re ministreu anu a wireless capit				
Channel:	36	\$			
Width:	20 MHz	\$			
		ن الله الله المعام المحمد ا محمد المحمد ا			

Tip: If the WLAN uses encryption such as Pre-shared Key (PSK), ensure the capture catches the four-way handshake between the AP and the desired client. This can be done if the OTA PCAP starts before the device is associated with the WLAN or if the client is deauthenticated and reauthenticated while the capture runs.

Step 6. The file is located in the Desktop folder or at the path **/var/tmp/** (It may vary on the macOS version the MacBook runs).

- 1. Launch the Finder application on the MacBook, as shown in the image.
- 2. Select the **Go** Menu from Finder.
- 3. Choose **Desktop** Folder or **Go to Folder** and type the destination path.



The destination folder is displayed.

🚞 tmp			
		C	Search
Name	^ Date Modified	Size	Kind
🔚 CARCERVA-M-V7L5_ch36_2021-04-13_14.44.18.924.pcap	Today, 14:44	123 KB	Pcap Napture
📠 CARCERVA-M-V7L5_ch36_2021-04-13_14.45.17.755.pcap	Today, 14:45	1.1 MB	Pcap Napture

Option B. Configure PCAP with Airtool

Step 1. Install the third-party <u>Airtool</u> application.

Step 2. Launch the tool.

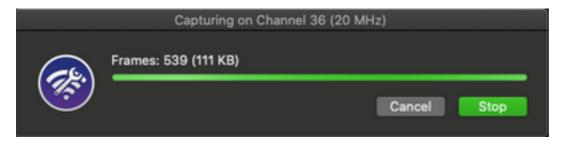
Once launched, the Airtool can be located at the top-right from the macOS menu bar, as shown in the image.

ę	🧟 🦳 1	100% 😰	(۱	Tue	13 Apr	16:50
	Status: Not a	ssociated				
	Channel: 1 (2 Channel Wid		z			•
	Link-Layer H	eader: 802	2.11 R	adiot	tap	►
	Single Chanr Capture Capture Othe Capture Othe	er 2.4 GHz				* *
	Multiple Char Capture All Capture All 2 Capture All 5 Capture Cust	.4 GHz GHz	ıre			
	Upload Capt	ure				•
	Preferences. Help					
	Check for Up Launch at Lo About Airtoo	gin				
	Quit					жQ

Step 3. Select the **Channel** and **Width** that the target device and AP use (this action starts the PCAP), as shown in the image.



Step 4. Wait some time to collect the information required and click **Stop**, as shown in the image.



Tip: If the WLAN uses encryption such as Pre-shared Key (PSK), ensure the capture catches the four-way handshake between the AP and the desired client. This can be done if the OTA PCAP starts before the device is associated with the WLAN or if the client is deauthenticated and reauthenticated while the capture runs.

Step 5. The file is located in the Desktop folder.

Option C. Configure PCAP with Wireshark

- Step 1. Install Wireshark.
- Step 2. Launch the application, as shown in the image.

• • •	The Wireshark Network Analyzer		
🖪 🔳 🗟 🎯 🖿	🗎 🔯 ସ୍ 🗢 🔿 🥶 🖉 🛃 📕 ସ୍ ର୍ ସ୍ 🎟		
Apply a display filter <%/>			+
	Welcome to Wireshark		
	Open		
	/Users/carcerva/Desktop/airtool_2021-04-13_16.28.04_pcap (106 KB)		
	/Users/carcerva/Downloads/FH WLC.pcapng (33 MB)		
	/Users/carcerva/Downloads/tac complete 9800 macbook.pcaping (72 MB)		
	/Users/carcerva/Downloads/C9800 client roaming issue/tac complete 9800 macbook.pcapng (72 M8)		
	/Users/carcerva/Downloads/TACAP (1)-1.pcap (90 MB)		
	/Users/carcerva/Downloads/AP-MC-28-OTA/ailing.pcapng (6098 KB)		
	/Users/carcerva/Downloads/TAC.pcap (21 MB)		
	/Users/carcerva/Downloads/TAC2.pcap (46 MB)		
	Capture		
		 All interfaces shown 	
		All interfaces shown	
	stun6		
	USB 10/100/1000 LAN: en10		
	Loopback 100 non-to-state when the state of		
	Wirks end Thunderbolt Bridge: bridge0		
	Thunderbolt 1: en1		
	Thunderbolt 2: en2		
	Thunderbolt 3: en3 Thunderbolt 4: en4		
	gilo		

	Learn		
	User's Guide · Wiki · Questions and Answers · Mailing Lists		
	You are running Wireshark 3.4.4 (v3.4.4-0-gc33f6306cbb2). You receive automatic updates.		
Ready to load or capture	No Packets		 Profile: Default

Step 3. Select the **Capture** menu from the menu bar and select **Options**, as shown in the image.



This action opens a pop-up window, as shown in the image.

Interface	Traffic	Link-layer Header	Promiscı	Snaplen (B)	Buffer (MB)	Monito
▶ utun4		BSD loopback	Image: A start and a start	default	2	
▶ utun5		BSD loopback	S	default	2	
▶ utun6	Lunn	BSD loopback	S	default	2	
USB 10/100/1000 LAN: en10	Lunn	Ethernet	S	default	2	
Loopback: Io0	1h.m.h.m.h.	BSD loopback	<u></u>	default	2	—
Wi-Fi: en0		Ethernet	✓	default	2	
Thunderbolt Bridge: bridge0		Ethernet	S	default	2	
Thunderbolt 1: en1		Ethernet	S	default	2	
Thunderbolt 2: en2		Ethernet	S	default	2	
Thunderbolt 3: en3		Ethernet	S	default	2	
Enable promiscuous mode on all interfaces Manage Interfaces Capture filter for selected interfaces: Enter a capture filter Compile BPFs						

Step 4. Select the Wi-Fi: en0 (Wireless adapter) and tick the Monitor option that is to the right of

the interface as shown in the image.

Inte	erface	Traffic	Link-layer Header	Promisci	Snaplen (B)	Buffer (MB)	Monito
►	utun4		BSD loopback	V	default	2	
►	utun5		BSD loopback	V	default	2	
►	utun6	MMMmmmm	BSD loopback	V	default	2	
►	USB 10/100/1000 LAN: en10	white many marked and the second seco	Ethernet	V	default	2	—
►	Loopback: lo0	human	BSD loopback	V	default	2	—
	Wi-Fi: en0		802.11 plus radiotap header		default	2	
	Thunderbolt Bridge: bridge0		Ethernet	N	default	2	
	Thunderbolt 1: en1		Ethernet	V	default	2	
	Thunderbolt 2: en2		Ethernet	N	default	2	
	Thunderbolt 3: en3		Ethernet	N	default	2	
	Enable promiscuous mode on all interface			-		ige Interface Compile Bl	

Note: In this method, Wireshark is unable to select the desired Channel and Width to scan. The Channel and Width are assigned with the Sniffer tool explained in this document. Refer to Option A. Step 3 in order to change them.

Step 5. Select Start.

Step 6. Wait for some time to collect the information required and select the **Stop** button from Wireshark, as shown in the image.

			Capturing from Wi-Fit en0
⊿ 🗖 👖 🔘 🔘 🔍 🔍	🗢 🔿 🖆 🔆 👲	🛄 🔳 લ્લ્	, e, 🔛
ay filter <%/>			
No. Time	Protocol Signal	strength SSID	Time delta from previous < Info Calling-Station-Id
28250 2021-04-14 12:19:25.875678	802.11 -77	dBm	0.000064000 Acknowledgement, Flags=C
28251 2021-04-14 12:19:25.883050	802.11 -71	dBm Cervantes	0.007372000 Beacon frame, SN=2263, FN=0, Flags=C, BI=100, SS
28252 2021-04-14 12:19:25.897228	802.11 -41	dBm	0.014178000 QoS Data, SN=247, FN=0, Flags=.pF.C
28253 2021-04-14 12:19:25.897293	802.11 -76	dBm	0.000065000 Acknowledgement, Flags=C
28254 2021-04-14 12:19:25.897520	802.11 -41	dBm	0.000227000 QoS Data, SN=248, FN=0, Flags=.pF.C
28255 2021-04-14 12:19:25.897588	802.11 -77		0.000068000 Acknowledgement, Flags=C
28256 2021-04-14 12:19:25.898400	802.11 -76		0.000812000 Request-to-send, Flags=C
28257 2021-04-14 12:19:25.898443	802.11 -43	dBm	0.000043000 Clear-to-send, Flags=C
28258 2021-04-14 12:19:25.899216	802.11 -77	dBm	0.000773000 Request-to-send, Flags=C
28259 2021-04-14 12:19:25.899259	802.11 -43		0.000043000 Clear-to-send, Flags=C
28260 2021-04-14 12:19:25.899301	802.11 -43	dBm	0.000042000 802.11 Block Ack, Flags=C
28261 2021-04-14 12:19:25.905274	802.11 -62	dBm Cervantes	0.005973000 Beacon frame, SN=2945, FN=0, Flags=C, BI=100, SS
28262 2021-04-14 12:19:25.905918	802.11 -43	dBm	0.000644000 Null function (No data), SN=3891, FN=0, Flags=PTC
28263 2021-04-14 12:19:25.905961	802.11 -43		0.000043000 Acknowledgement, Flags=C
28264 2021-04-14 12:19:25.909433	802.11 -62	dBm	0.003472000 Beacon frame, SN=2946, FN=0, Flags=C, BI=100, SS

Tip: If the WLAN uses encryption such as Pre-shared Key (PSK), ensure the capture catches the four-way handshake between the AP and the desired client. This can be done if the OTA PCAP starts before the device is associated with the WLAN or if the client is deauthenticated and reauthenticated while the capture runs.

Step 7. Save the PCAP file. Click on the **Save** button from Wireshark, as shown in the image.

		Wi-Fi: en0	
	🗢 🗢 🗟 春 👲 🔳 🔳 @ @ @ 🎟		
Apply a display filter < 10 Save his capture file			🛋 🔹 +
No. Time	Destination	Protocol	Signal strength Time delta from previous c Info
78 2021-04-14 12:44:44.884666	Broadcast	802.11	-74 dBm 0.000118000 Data, SN=1889, FN=0, Flags=.pF.C
79 2021-04-14 12:44:44.946877	Broadcast	802.11	-39 dBm 0.062211000 Beacon frame, SN=1054, FN=0, Flags=
80 2021-04-14 12:44:44.946950	Broadcast	802.11	-39 dBm 0.000073000 Data, SN=2795, FN=0, Flags=.pF.C
81 2021-04-14 12:44:44.986948	Broadcast	802.11	-74 dBm 0.039998000 Beacon frame, SN=2324, FN=0, Flags=
82 2021-04-14 12:44:45.049283	Broadcast	802.11	-41 dBm 0.062335000 Beacon frame, SN=1055, FN=0, Flags=
83 2021-04-14 12:44:45.089391	Broadcast	802.11	-74 dBm 0.040108000 Beacon frame, SN=2325, FN=0, Flags=C, B

Select the destination folder, as shown in the image.

	Wireshark	· Save Capture File As	
Look in:]/Users	0	• • • • =
I Computer	Name		Kind Date Modified Folder 13/04/2114:33 Folder 25/02/2119:25
File name:			Save
Save as: W	ireshark/ pcapng ith gzip		Help

Verify

Use this section in order to confirm that your configuration works properly.

Open the capture with Wireshark and verify that 802.11 frames are visible, as shown in the image.

			<u> </u>
📶 🔳 🗟 🎯 🖿 🗎 🖹 🙆 🤇	승 💩 🔯 🚡 🖖		
Apply a display filter <¥t/>			
No. Time	Destination Protocol	Signal strength SSID	Time delta from info info in the second seco
12 2021-04-13 16:28:05.813108	Broadcast 802.11	-75 dBm Cervantes	0.012434 Beacon frame, SN=448, FN=0, Flags=C, BI=100, SSI
13 2021-04-13 16:28:05.871204	Broadcast 802.11	-38 dBm Cervantes	0.058096 Beacon frame, SN=1755, FN=0, Flags=C, BI=100, SS
14 2021-04-13 16:28:05.920690	Broadcast 802.11	-75 dBm Cervantes	0.049486 Beacon frame, SN=449, FN=0, Flags=C, BI=100, SSI
15 2021-04-13 16:28:05.973624	Broadcast 802.11	-38 dBm Cervantes	0.052934 Beacon frame, SN=1757, FN=0, Flags=C, BI=100, SS
16 2021-04-13 16:28:06.017899	Broadcast 802.11	-75 dBm Cervantes	0.044275 Beacon frame, SN=451, FN=0, Flags=C, BI=100, SSI
17 2021-04-13 16:28:06.07601	Broadcast 802.11	-37 dBm Cervantes	0.058116 Beacon frame, SN=1758, FN=0, Flags=C, BI=100, SS
18 2021-04-13 16:28:06.07644	Broadcast 802.11	-38 dBm	0.000432 Data, SN=3801, FN=0, Flags=.pF.C
19 2021-04-13 16:28:06.12032	Broadcast 802.11	-75 dBm Cervantes	0.043875 Beacon frame, SN=452, FN=0, Flags=C, BI=100, SSI
20 2021-04-13 16:28:06.12069	Broadcast 802.11	-75 dBm	0.000369 Data, SN=150, FN=0, Flags=.pF.C
21 2021-04-13 16:28:06.178412	2 Broadcast 802.11	-37 dBm Cervantes	0.057721 Beacon frame, SN=1761, FN=0, Flags=C, BI=100, SS
22 2021-04-13 16:28:06.222688	Broadcast 802.11	-75 dBm Cervantes	0.044276 Beacon frame, SN=455, FN=0, Flags=C, BI=100, SSI
23 2021-04-13 16:28:06.28097	Broadcast 802.11	-37 dBm Cervantes	0.058289 Beacon frame, SN=1762, FN=0, Flags=C, BI=100, SS
24 2021-04-13 16:28:06.28124	Broadcast 802.11	-37 dBm	0.000263 Data, SN=3802, FN=0, Flags=.pmF.C
25 2021-04-13 16:28:06.28269	7 IPv4mcas 802.11	-37 dBm	0.001457 Data, SN=3803, FN=0, Flags=.pF.C
26 2021-04-13 16:28:06.32508	5 Broadcast 802.11	-75 dBm Cervantes	0.042388 Beacon frame, SN=456, FN=0, Flags=C, BI=100, SSI
27 2021-04-13 16:28:06.325444	Broadcast 802.11	-76 dBm	0.000359 Data, SN=151, FN=0, Flags=.pmF.C
28 2021-04-13 16:28:06.327019	9 IPv4mcas 802.11	-76 dBm	0.001575 Data, SN=152, FN=0, Flags=.pF.C
29 2021-04-13 16:28:06.383259	Broadcast 802.11	-37 dBm Cervantes	0.056240 Beacon frame, SN=1763, FN=0, Flags=C, BI=100, SS
30 2021-04-13 16:28:06.431298	Broadcast 802.11	-75 dBm Cervantes	0.048039 Beacon frame, SN=458, FN=0, Flags=C, BI=100, SSI
31 2021-04-13 16:28:06.491274	Broadcast 802.11	-37 dBm Cervantes	0.059976 Beacon frame, SN=1765, FN=0, Flags=C, BI=100, SS

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- Fundamentals of 802.11 Wireless Sniffing
- <u>Technical Support & Documentation Cisco Systems</u>