# 在MacBook上通过空中收集数据包捕获

### 目录

简介 <u>先决条件</u> 要求 <u>使用的组件</u> <u>背景信息</u> 配置 <u>选项A.使用无线诊断配置PCAP</u> <u>选项B.使用Airtool配置PCAP</u> <u>选项C.使用Wireshark配置PCAP</u> <u>验证</u> <u>故障排除</u> <u>相关信息</u>

### 简介

本文档介绍如何在MacBook上使用本机工具无线诊断和第三方应用(如Airtool和Wireshark)收集空中数据包捕获(PCAP),以排除和分析无线行为。

### 先决条件

#### 要求

Cisco 建议您了解以下主题:

- •思科无线局域网控制器(WLC)AireOS或Cisco IOS®-XE
- •802.11标准中的基本知识

#### 使用的组件

本文档中的信息基于以下软件和硬件版本:

- Apple MacBook,带MacOS版本10.14.X或更高版本
- Apple无线诊断工具
- Airtool 1.9或更高版本
- Wireshark 3.X或更高版本
- 思科接入点(AP)2802

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

## 背景信息

注意事项:

- 建议将Macbook用作无线嗅探器,使其靠近AP和目标设备。
- 确保您知道使用哪个802.11通道和宽度、客户端设备和AP。
- 信道和宽度可在以下位置找到: Cisco IOS®-XE Web图形用户界面(GUI)在Configuration > Wireless > 5GHz or 2.4GHz > Select an AP > Channel and Width下AireOS Web GUI在 Wireless > Access Points > 802.11a/n/ac(5GHz)或802.11 b/g/n(2.4GHz)> Select an AP > Channel and Width

### 配置

#### 选项A.使用无线诊断配置PCAP

步骤1.启动无线**诊断**工具。

按住键盘上的ALT/Option键,然后单击右上角的Wi-Fi图标,如图所示。



步骤2.打开嗅探器工具。

从菜单栏的**Wireless Diagnostic Tool中选**择"Window"菜单,然后选择**Sniffer**或使用键盘快捷键,同 时按**ALT + Command + 6** Keys,如图所示。



步骤3.选择目标设备和AP使用的通道和宽度,如图所示。

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

步骤4.单击"开**始"。** 

此操作将无线适配器置于监控模式,且无法将设备连接到无线局域网(WLAN),如图所示。



步骤5.等待一段时间以收集所需信息,然后单击"停止"。

	Sniffer	
Use your Mac as a dedi channel and channel wi Click 'Stop' when you ar	cated sniffer to capture Wi-Fi traffic dth, then click 'Start' to begin. re finished and a wireless capture fil	:. Choose a le will be
created in /var/tmp.		
Channel:	36	
Width:	20 MHz	
	, rt	Stop

**提示:**如果WLAN使用加密(如预共享密钥(PSK)),请确保捕获捕获AP与所需客户端之间的四 次握手。如果OTA PCAP在设备与WLAN关联之前启动,或者如果客户端在捕获运行期间取消 身份验证并重新进行身份验证,则可以执行此操作。

步骤6.该文件位于Desktop(桌面)文件夹或路径/**var/tmp/**(MacBook运行的macOS版本可能不同 )。

1.在MacBook上启动Finder应用程序,如图所示。

2.从Finder中选择"开始"菜单。

3.选择"桌面文件夹"或"转到文件夹"并键入目标路径。

	Go Window Help		
	Back	¥[	
	Forward	¥]	Go to Folder
	Select Startup Disk	<b>ዮ</b> ដ†	
2	Recents	ት¥F	Go to the folder:
a,	Documents	<b>企業O</b>	/var/tmp
199	🔜 Desktop	企業D	
	Downloads	٦ж٦	Cancel Go
	😭 Home	<del></del>	
	Computer	<del>ሰ</del> <mark>ස</mark> C	
	ด AirDrop	<del></del>	
	Wetwork	<del></del>	
1.14	iCloud Drive	ዕዝበ	
	🕂 Applications	<mark>ዮ</mark> සA	
	💥 Utilities	<mark>ት</mark>	
1000	Recent Folders	►	
	Go to Folder	企ℋG	
	Connect to Server	жк	
	TO A DESCRIPTION OF THE OWNER OF THE OWNER	THE OWNER OF	

显示目标文件夹。



#### 选项B.使用Airtool配置PCAP

步骤1.安装第三方Airtool应<u>用程</u>序。

步骤2.启动工具。

启动后,Airtool可位于macOS菜单栏的右上角,如图所示。



步骤3.选择目标设备和AP使用的通道和宽度(此操作将启动PCAP),如图所示。

🍄 🛜 🗚 100% 🖾 📣 Tue 13 Apr	16:28:01	। ୦ 🔇
Status: Not associated		
Channel: 1 (2.4 GHz) Channel Width: 20 MHz		
Link-Layer Header: 802.11 Radiotap		20 MHz
Single Channel Capture Capture Capture Other 2.4 GHz	•	36 40 44 48
Capture Other 5 GHz		52

步骤4.等待一段时间收集所需信息,然后单击"停止",如图所示。



**提示:**如果WLAN使用加密(如预共享密钥(PSK)),请确保捕获捕获AP与所需客户端之间的四 次握手。如果OTA PCAP在设备与WLAN关联之前启动,或者如果客户端在捕获运行期间取消 身份验证并重新进行身份验证,则可以执行此操作。

步骤5.该文件位于Desktop(桌面)文件夹中。

#### 选项C.使用Wireshark配置PCAP

步骤1.安装Wireshark。

步骤2.启动应用程序,如图所示。

• • •		The Wireshark Network Analyzer	
🚄 🔳 🔬 🎯 🖿	🗎 🗋 🔇 🗢 🔿 🕋 春 💆 📒 🔍 🔍 🔍 🛄		
Apply a display filter <%/>			- +
n (nppy z unpoy z unpoy	Welcome to Wireshark Open Merkiarcena/Deviladdi/140 (2021-04-13,36.28.04.pcap (105.K8) Merkiarcena/Dowiladdi/140 (2003) Merkiarcena/Dowiladdi/140 (2004) Merkiarcena/Dowiladdi/140 (2004) Merkiarcena/Dowila		
Ready to load or capture	Capture		At interfaces shown

#### 步骤3.从菜单栏中选择"捕获"菜单,然后选择"选项",如图所示。



#### 此操作将打开一个弹出窗口,如图所示。

Inte	erface	Traffic	Link-layer Header	Promiscı	Snaplen (B)	Buffer (MB)	Monit				
►	utun4		BSD loopback	<b>S</b>	default	2					
►	utun5		BSD loopback	<b>S</b>	default	2					
►	utun6	hamman	BSD loopback	Sec.	default	2					
►	USB 10/100/1000 LAN: en10	rmmmmm	Ethernet	Solution	default	2					
►	Loopback: Io0	A.M. Markan	BSD loopback	<b>S</b>	default	2					
	Wi-Fi: en0		Ethernet	<ul> <li>✓</li> </ul>	default	2					
	Thunderbolt Bridge: bridge0		Ethernet	Sec.	default	2					
	Thunderbolt 1: en1		Ethernet	Image: A state of the state	default	2					
	Thunderbolt 2: en2		Ethernet	<b>S</b>	default	2					
	Thunderbolt 3: en3		Ethernet	Image: A state of the state	default	2					
Enable promiscuous mode on all interfaces											

#### 步骤4.选择Wi-Fi:en0(无线适配器),并勾选接口右侧的"Monitor(监控)"选项,如图所示。

	ITallic 			actual		Monito					
▶ utun4		BSD loopback		default	2						
▶ utun5		BSD loopback		default	2						
	NWWWWWWW	BSD loopback		default	2						
USB 10/100/1000 LAN: en10	NWWWWWWWWWWWW			default	2	_					
	human human	BSD loopback		default	2	_					
WI-FI: enu Thursdorthalt Dridges, heider 0		802.11 plus radiotap neader		detault	2						
Thunderbolt Bridge: bridge0		Ethernet		default	2						
Thunderbolt 1: en1		Ethernet		default	2						
Thunderbolt 3: en3		Ethernet		default	2						
<ul> <li>✓ Enable promiscuous mode on all interfaces</li> <li>Manage Interfaces</li> <li>Capture filter for selected interfaces: Letter a capture filter</li> <li>✓ Compile BPFs</li> </ul>											

**注意:**在此方法中,Wireshark无法选择要扫描的所需通道和宽度。"通道"和"宽度"是使用本文档中介绍的嗅探器工具分配的。请参阅选项A。步骤3以更改它们。

步骤5.选择"**开始"。** 

步骤6.等待一段时间收集所需信息,然后从Wireshark中选择"停止"按钮,如图所示。

•	••														Capt	uring from Wi-Fi: en0	
4					🙆 ବ୍	🔶 🔿	· 💼 1	🗛 👲			e,	e,		•••			
		ay filter <															+
No.		Time				Proto	ol lo	Signal	strengti	SSID			Time o	delta from	n previous c	: Info   Calling-Station-Id	
	28250	2021-04	-14 1	2:19:25	.875678	802.	11	-77	dBm					0.00	0064000	Acknowledgement, Flags=C	
	28251	2021-04	-14 1	2:19:25	.883050	802.	11	-71	dBm	Cerv	ante	5		0.00	7372000	Beacon frame, SN=2263, FN=0, Flags=C, BI=100, SS	
	28252	2021-04	-14 1	2:19:25	. 897228	802.	11	-41	dBm					0.01	4178000	QoS Data, SN=247, FN=0, Flags=.pF.C	
	28253	2021-04	-14 1	2:19:25	.897293	802.	11	-76	dBm					0.00	0065000	Acknowledgement, Flags=C	
	28254	2021-04	-14 1	2:19:25	.897520	802.	11	-41	dBm					0.00	0227000	QoS Data, SN=248, FN=0, Flags=.pF.C	
	28255	2021-04	-14 1	2:19:25	.897588	802.	11	-77	dBm					0.00	0068000	Acknowledgement, Flags=C	
	28256	2021-04	-14 1	2:19:25	.898400	802.	11	-76	dBm					0.00	0812000	Request-to-send, Flags=C	
	28257	2021-04	-14 1	2:19:25	.898443	802.	11	-43	dBm					0.00	0043000	Clear-to-send, Flags=C	
	28258	2021-04	-14 1	2:19:25	.899216	802.	11	-77	dBm					0.00	0773000	Request-to-send, Flags=C	
	28259	2021-04	-14 1	2:19:25	.899259	802.	11	-43	dBm					0.00	0043000	Clear-to-send, Flags=C	
	28260	2021-04	-14 1	2:19:25	.899301	802.	11	-43	dBm					0.00	0042000	802.11 Block Ack, Flags=C	
	28261	2021-04	-14 1	2:19:25	.905274	802.	11	-62	dBm	Cerv	ante	5		0.00	5973000	Beacon frame, SN=2945, FN=0, Flags=C, BI=100, SS	
Γ	28262	2021-04	-14 1	2:19:25	.905918	802.	11	-43	dBm					0.00	0644000	Null function (No data), SN=3891, FN=0, Flags=PTC	
Γ	28263	2021-04	-14 1	2:19:25	.905961	802.	11	-43	dBm					0.00	0043000	Acknowledgement, Flags=C	
_	28264	2021-04	-14_1	2:19:25	.989433	802.	11	-62	dBm					0.00	3472000	Beacon frame, SN=2946, FN=0, Flags=C, BI=100, SS	

**提示:**如果WLAN使用加密(如预共享密钥(PSK)),请确保捕获捕获AP与所需客户端之间的四 次握手。如果OTA PCAP在设备与WLAN关联之前启动,或者如果客户端在捕获运行期间取消 身份验证并重新进行身份验证,则可以执行此操作。

步骤7.保存PCAP文件。单击Wireshark中**的Save**按钮,如图所示。

WITH BID	
⊿ 🗖 🖉 📓 🚺 🖉 🗢 ⇔ 🗟 🗟 📕 🔳 🔍   🎟	
📕 Apply a display filter < xt Seaton and the company of the c	+
No.   Time   Destination   Protocol   Signal strength   Time delta from previous ( Info	
78 2021-04-14 12:44:48.884666 Broadcast 802.11 -74 dBm 0.000118000 Data, SN=1889, FN=0, Flags=.p	F.C
79 2021-04-14 12:44:44.946877 Broadcast 802.11 -39 dBm 0.062211000 Beacon frame, SN=1054, FN=0, FN	ags=
80 2021-04-14 12:44:44.946950 Broadcast 802.11 -39 dBm 0.000073000 Data, SN=2795, FN=0, Flags=.p	F.C
81 2021-04-14 12:44:44.986948 Broadcast 802.11 -74 dBm 0.039998000 Beacon frame, SN=2324, FN=0, FU	ags=
82 2021-04-14 12:44:45.049283 Broadcast 802.11 -41 dBm 0.062335000 Beacon frame, SN=1055, FN=0, FU	ags=
83 2021-04-14 12:44:45.089391 Broadcast 802.11 -74 dBm 0.040108000 Beacon frame, SN=2325, FN=0, FU	ags= в

选择目标文件夹,如图所示。

	Wireshark - Save Capture File As		
Look in: 🛄 /Users		C • • • Ø	88
Computer Carcerva Carcerva Shared	^  Size	Kind Date Modifie Folder 13/04/2114 Folder 25/02/2119	d   4:33 9:25
File name:	na		iave Incel
Compress with gzip		<u> </u>	lelp

### 验证

使用本部分可确认配置能否正常运行。

使用Wireshark打开捕获并验证802.11帧是否可见,如图所示。

••	•																💋 airtool_2021-04-
		<u>s</u> (	)		$\mathbf{X}$	3	্	(= 🔿	· 🕋	<u>.</u>	<u>↓</u>		. (	€ (	a, e		
An	olv a dis	olav filte	۲<۲/														
		1						1 Decel		Dester		10'		and the second			197 and date descel to fa
NO.			1-04-13	- 10	. 20. 0.			Destin	ation	Proto		Sign	al strer	ngtn∣s '	SID		lime della from   into   U-uouuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
	1	2 202	1-04-13	16	:28:05	.813	108	Broa	dcast	802	.11	-75	5 dBm	1 (	Cerva	ntes	0.012434 Beacon frame, SN=448, FN=0, Flags=C, BI=100, SSI
	1	3 202	1-04-13	16	:28:05	.871	204	Broa	dcast	802	.11	-38	3 dBm	n (	Cerva	ntes	0.058096 Beacon frame, SN=1755, FN=0, Flags=C, BI=100, SS
	1	4 202	1-04-13	16	:28:05	.920	690	Broa	adcast	802	. 11	-75	5 dBm	i (	Cerva	ntes	0.049486 Beacon frame, SN=449, FN=0, Flags=C, BI=100, SSI
	1	5 202	1-04-13	16	:28:05	.973	624	Broa	adcast	802	.11	-38	3 dBm	ı (	Cerva	ntes	0.052934 Beacon frame, SN=1757, FN=0, Flags=C, BI=100, SS
	1	6 202	1-04-13	16	:28:06	.017	899	Broa	dcast	802	. 11	-75	5 dBm	. (	Cerva	ntes	0.044275 Beacon frame, SN=451, FN=0, Flags=C, BI=100, SSI
	1	7 202	1-04-13	16	:28:06	.076	015	Broa	adcast	802	.11	-37	7 dBm	ı (	Cerva	ntes	0.058116 Beacon frame, SN=1758, FN=0, Flags=C, BI=100, SS
	1	8 202	1-04-13	16	:28:06	.076	447	Broa	dcast	802	.11	-38	3 dBm	1			0.000432 Data, SN=3801, FN=0, Flags=.pF.C
	1	9 202	1-04-13	16	:28:06	. 120	322	Broa	dcast	802	.11	-75	5 dBm	ı (	Cerva	ntes	0.043875 Beacon frame, SN=452, FN=0, Flags=C, BI=100, SSI
	2	0 202	1-04-13	16	:28:06	.120	691	Broa	dcast	802	.11	-75	5 dBm	1			0.000369 Data, SN=150, FN=0, Flags=.pF.C
	2	1 202	1-04-13	16	:28:06	.178	412	Broa	dcast	802	.11	-37	/ dBm	. (	Cerva	ntes	0.057721 Beacon frame, SN=1761, FN=0, Flags=C, BI=100, SS
	2	2 202	1-04-13	16	:28:06	. 222	688	Broa	dcast	802	.11	-75	5 dBm	1 (	Cerva	ntes	0.044276 Beacon frame, SN=455, FN=0, Flags=C, BI=100, SSI
	2	3 202	1-04-13	16	:28:06	.280	977	Broa	dcast	802	. 11	-37	7 dBm	n (	Cerva	ntes	0.058289 Beacon frame, SN=1762, FN=0, Flags=C, BI=100, SS
	2	4 202	1-04-13	16	:28:06	. 281	240	Broa	adcast	802	. 11	-37	7 dBm	1			0.000263 Data, SN=3802, FN=0, Flags=.pmF.C
	2	5 202	1-04-13	16	:28:06	.282	697	IPv4	Imcas	802	.11	-37	7 dBm	1			0.001457 Data, SN=3803, FN=0, Flags=.pF.C
	2	6 202	1-04-13	16	:28:06	.325	085	Broa	dcast	802	. 11	-75	5 dBm	ı (	Cerva	ntes	0.042388 Beacon frame, SN=456, FN=0, Flags=C, BI=100, SSI
	2	7 202	1-04-13	16	:28:06	.325	444	Broa	adcast	802	.11	-76	6 dBm	1			0.000359 Data, SN=151, FN=0, Flags=.pmF.C
	2	8 202	1-04-13	16	:28:06	.327	019	IPv4	Imcas	802	.11	-76	5 dBm	1			0.001575 Data, SN=152, FN=0, Flags=.pF.C
	2	9 202	1-04-13	16	:28:06	. 383	259	Broa	dcast	802	.11	-37	7 dBm	1 (	Cerva	ntes	0.056240 Beacon frame, SN=1763, FN=0, Flags=C, BI=100, SS
	3	0 202	1-04-13	16	:28:06	.431	298	Broa	dcast	802	.11	-75	5 dBm	1 (	Cerva	ntes	0.048039 Beacon frame, SN=458, FN=0, Flags=C, BI=100, SSI
	3	1 202	1-04-13	16	:28:06	.491	274	Broa	dcast	802	.11	-37	/ dBm	. (	Cerva	ntes	0.059976 Beacon frame, SN=1765, FN=0, Flags=C, BI=100, SS

### 故障排除

目前没有针对此配置的故障排除信息。

## 相关信息

- 802.11无线嗅探的基础
- <u>技术支持和文档 Cisco Systems</u>