# 在802.1X SSID中解密無線資料包捕獲

目錄
<u>必要條件</u>
<u>採用元件</u>
<u>背景資訊</u>
<u>設定</u>
步驟 1.開始感興趣終端的放射性跟蹤
步驟2.獲取無線資料包捕獲
步驟 3.生成和導出裝置的放射性蹤跡
步驟 4.從放射性痕跡獲取MSK
步驟 5.在Wireshark中增加MSK作為IEEE 802.11解密金鑰
<u>步驟 6.分析解密的802.1X流量</u>

## 簡介

本檔案介紹如何使用Catalyst 9800 WLC上提供的疑難排解工具解密802.1X WLAN的無線封包擷取。

## 必要條件

### 需求

思科建議您瞭解以下主題:

- 如何在Catalyst 9800 WLC中配置802.1X WLAN
- 如何在Catalyst 9800 WLC中啟用條件調試的情況下進行放射性跟蹤
- 如何使用嗅探器模式下的存取點或具有無線診斷工具的Macbook進行無線資料包捕獲

### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Catalyst 9800-L WLC、Cisco IOS® XE Cupertino 17.9.3
- 採用監聽器模式的Catalyst 9130AXE存取點
- Cisco ISE版本3.3
- Wireshark 4.0.8

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

## 背景資訊

一旦透過EAP+8021X驗證身份,無線流量就會使用由請求方和驗證方之間的握手生成的Pairwise Transient Key (PTK)加密,後者使用要計算的Pairwise Master Key (PMK)進行加密。此PMK衍生自 主會話金鑰(MSK)。MSK包含在RADIUS Access-Accept消息的屬性值對中(使用RADIUS共用金鑰 加密)。因此,在無線資料包捕獲中,即使四向握手被第三方攔截,也無法透明地看到流量。

通常,生成PMK意味著在有線網路中捕獲資料包、瞭解RADIUS共用金鑰和某些編碼以提取興趣值。相反,透過此方法,可以使用可用於Catalyst 9800 WLC上的故障排除工具之一(放射性蹤跡)獲取MSK,然後將其用於任何已知資料包分析工具(如Wireshark)。



注意:此程式僅適用於WPA2,因為計算成對暫時性金鑰(PTK)所需的資訊會透過4次交涉 在空中交換。相反,在WPA3中,對等體同時身份驗證(SAE)透過所謂的蜻蜓握手來執行。

## 步驟 1.開始感興趣終端的放射性跟蹤

在Catalyst 9800 WLC上,轉到Troubleshooting > Radiative Traces,然後按一下Add按鈕以鍵入要 解密其流量的裝置的MAC地址。

÷	Cisco Cisco 17.9.3	Catal	lyst 9800-L Wireless Contro	bller	Welcome au Last login 10/03/20	<b>dmin</b> 22 15:13:03	*	0	A	6	<b>\$</b> (3
٩			Troubleshooting - > Radioactive	Trace							
	Dashboard		Conditional Debug Global State			🔅 Wire	eless Debi	ug Ana	lyzer		
	Monitoring		+ Add × Delete	✓ Start Stop			Last Ru	n Res	sult		
Z	Configuration		MAC/IP Address		No items to d						
ঠ্য					NO Items to d		MAC/IF				
C				Add MAC/IP Address							× <sup>19</sup>
X				MAC/IP Address*	Enter a MAC/IP Address every 0093.3794.2730	newline					de
				Cancel				🖹 Ap	ply to	Device	e

增加之後,請確保按一下清單頂部的Start按鈕以啟用Conditional Debug。這允許您檢視在資料平面 中交換的資訊(MSK在此)。

¢	Cisco Catalyst 9800-L Wireless Controller								Welco Last login
C	Search Menu Items		Troublest	nooting - > Radio	active Trac	e			
	Dashboard		Conditi	onal Debug Globa	l State: Star				🔅 Wireless De
	) Monitoring	>	+ Add	× Delete	✓ Start	Stop			
Ľ	Configuration	>		MAC/IP Address	۲	Trace file			
Ś	Administration	>	  4	1 N N	0 🔻				1 - 1 of 1 items
C	Licensing								
X	Troubleshooting								

在啟用條件調試的情況下增加到放射性跟蹤清單的裝置。

增加到放射性蹤跡清單的MAC地址



注意:如果未啟用條件調試,則只能看到控制平面中的流量,而不包括MSK。有關此過程 的詳細資訊,請參閱<u>Catalyst 9800 WLC故障排除文檔上的調試和日誌收集的條件調試和放</u> <u>射性跟蹤</u>部分。

步驟 2.獲取無線資料包捕獲

啟動無線資料包捕獲並將您的終端連線到802.1X WLAN。

您可以<u>使用處於嗅探器模式的存取點</u>獲取此無線資料包捕獲,也可以使用<u>Macbook內建的無線診斷</u> 工具獲取此無線資料包捕獲。



注意:請確保資料包捕獲包含所有802.11幀。最重要的是,在此過程中必須捕獲四向握手。

觀察透過四向握手(資料包475至478)的所有流量如何加密。

lo.		Time	Time delta from p	Source	Destination	Protocol	Length	Signa	il strenç	Signal/nois	i Info
	449	14:12:10.052518	0.001339000	IntelCor_94:27:30	Cisco_aa:18:8f	802.11	248	-59	dBm	35 dB	Reassociation Request, SN=22, FN=0, Flags=C, SSID="ota-dot1x"
	450	14:12:10.056200	0.003682000	Cisco_aa:18:8f	IntelCor_94:27:30	802.11	227	-34	dBm	60 dB	Reassociation Response, SN=3741, FN=0, Flags=C
	451	14:12:10.058303	0.002103000	IntelCor_94:27:30	Cisco_aa:18:8f	802.11	93	-59	dBm	35 dB	Action, SN=23, FN=0, Flags=C
	452	14:12:10.059417	0.001114000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	109	-34	dBm	60 dB	Request, Identity
	453	14:12:10.108429	0.049012000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146	-59	dBm	35 dB	Response, Identity
	454	14:12:10.116909	0.008480000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	110	-34	dBm	60 dB	Request, TLS EAP (EAP-TLS)
	455	14:12:10.119150	0.002241000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146	-59	dBm	35 dB	Response, Legacy Nak (Response Only)
	456	14:12:10.122792	0.003642000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	110	-33	dBm	61 dB	Request, Protected EAP (EAP-PEAP)
	457	14:12:10.124621	0.001829000	IntelCor_94:27:30	Cisco_aa:18:8f	TLSv1.2	330	-60	dBm	34 dB	Encrypted Handshake Message
	458	14:12:10.166650	0.042029000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	1116	-33	dBm	61 dB	Request, Protected EAP (EAP-PEAP)
	459	14:12:10.170039	0.003389000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146	-59	dBm	35 dB	Response, Protected EAP (EAP-PEAP)
	460	14:12:10.175814	0.005775000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	1112	-34	dBm	60 dB	Request, Protected EAP (EAP-PEAP)
	461	14:12:10.180069	0.004255000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146	-59	dBm	35 dB	Response, Protected EAP (EAP-PEAP)
	462	14:12:10.182929	0.002860000	Cisco_aa:18:8f	IntelCor_94:27:30	TLSv1.2	268	-34	dBm	60 dB	Server Hello, Certificate, Server Key Exchange, Server Hello Done
	463	14:12:10.236135	0.053206000	IntelCor_94:27:30	Cisco_aa:18:8f	TLSv1.2	308	-60	dBm	34 dB	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
	464	14:12:10.244438	0.008303000	Cisco_aa:18:8f	IntelCor_94:27:30	TLSv1.2	161	-34	dBm	60 dB	Change Cipher Spec, Encrypted Handshake Message
	465	14:12:10.248078	0.003640000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146	-60	dBm	34 dB	Response, Protected EAP (EAP-PEAP)
	466	14:12:10.251302	0.003224000	Cisco_aa:18:8f	IntelCor_94:27:30	TLSv1.2	144	-34	dBm	60 dB	Application Data
	467	14:12:10.259110	0.007808000	IntelCor_94:27:30	Cisco_aa:18:8f	TLSv1.2	149	-60	dBm	34 dB	Application Data
	468	14:12:10.263865	0.004755000	Cisco_aa:18:8f	IntelCor_94:27:30	TLSv1.2	175	-34	dBm	60 dB	Application Data
	469	14:12:10.271714	0.007849000	IntelCor_94:27:30	Cisco_aa:18:8f	TLSv1.2	203	-60	dBm	34 dB	Application Data
	470	14:12:10.285280	0.013566000	Cisco_aa:18:8f	IntelCor_94:27:30	TLSv1.2	190	-33	dBm	61 dB	Application Data
	471	14:12:10.287513	0.002233000	IntelCor_94:27:30	Cisco_aa:18:8f	TLSv1.2	146	-60	dBm	34 dB	Application Data
	472	14:12:10.291081	0.003568000	Cisco_aa:18:8f	IntelCor_94:27:30	TLSv1.2	143	-34	dBm	60 dB	Application Data
	473	14:12:10.294213	0.003132000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146	-60	dBm	34 dB	Response, Protected EAP (EAP-PEAP)
	474	14:12:10.315016	0.020803000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	108	-33	dBm	61 dB	Success
	475	14:12:10.316556	0.001540000	Cisco_aa:18:8f	IntelCor_94:27:30	EAPOL	221	-34	dBm	60 dB	Key (Message 1 of 4)
	476	14:12:10.321017	0.004461000	IntelCor_94:27:30	Cisco_aa:18:8f	EAPOL	223	-60	dBm	34 dB	Key (Message 2 of 4)
	477	14:12:10.322061	0.001044000	Cisco_aa:18:8f	IntelCor_94:27:30	EAPOL	255	-34	dBm	60 dB	Key (Message 3 of 4)
	478	14:12:10.323817	0.001756000	IntelCor_94:27:30	Cisco_aa:18:8f	EAPOL	199	-60	dBm	34 dB	Key (Message 4 of 4)
	479	14:12:10.324699	0.000882000	IntelCor_94:27:30	Cisco_aa:18:8f	802.11	148	-60	dBm	34 dB	Action, SN=24, FN=0, Flags=C, Dialog Token=3
	480	14:12:10.325899	0.001200000	Cisco_aa:18:8f	IntelCor_94:27:30	802.11	148	-34	dBm	60 dB	Action, SN=3746, FN=0, Flags=C, Dialog Token=3
	481	14:12:10.334956	0.009057000	IntelCor_94:27:30	IPv6mcast_02	802.11	207	-61	dBm	33 dB	QoS Data, SN=13, FN=0, Flags=.pTC
	482	14:12:10.348407	0.013451000	IntelCor_94:27:30	Broadcast	802.11	197	-61	dBm	33 dB	QoS Data, SN=14, FN=0, Flags=.pTC
	483	14:12:10.348903	0.000496000	Cisco_aa:18:8f	IntelCor_94:27:30	802.11	99	-34	dBm	60 dB	Action, SN=3747, FN=0, Flags=C, Dialog Token=90
	484	14:12:10.349222	0.000319000	Cisco_3f:80:f1	IntelCor_94:27:30	802.11	197	-30	dBm	64 dB	QoS Data, SN=0, FN=0, Flags=.pF.C
	485	14:12:10.349623	0.000401000	IntelCor_94:27:30	Cisco_aa:18:8f	802.11	99	-60	dBm	34 dB	Action, SN=25, FN=0, Flags=C, Dialog Token=90
	486	14:12:10.350046	0.000423000	IntelCor_94:27:30	Cisco_3f:80:f1	802.11	220	-61	dBm	33 dB	QoS Data, SN=15, FN=0, Flags=.pTC
	487	14:12:10.530286	0.180240000	IntelCor_94:27:30	Cisco_3f:80:f1	802.11	206	-61	dBm	33 dB	QoS Data, SN=16, FN=0, Flags=.pTC
	488	14:12:10.616297	0.086011000	Cisco_3f:80:f1	IntelCor_94:27:30	802.11	222	-30	dBm	64 dB	QoS Data, SN=1, FN=0, Flags=.pF.C
	489	14:12:10.623163	0.006866000	IntelCor_94:27:30	IPv4mcast_16	802.11	199	-61	dBm	33 dB	QoS Data, SN=17, FN=0, Flags=.pTC
	490	14:12:10.623515	0.000352000	IntelCor_94:27:30	IPv6mcast_16	802.11	267	-61	dBm	33 dB	QoS Data, SN=18, FN=0, Flags=.pTC
	491	14:12:10.623890	0.000375000	IntelCor_94:27:30	Cisco_3f:80:f1	802.11	243	-61	dBm	33 dB	QoS Data, SN=19, FN=0, Flags=.pTC
	492	14:12:10.625663	0.001773000	Cisco_3f:80:f1	IntelCor_94:27:30	802.11	207	-30	dBm	64 dB	QoS Data, SN=2, FN=0, Flags=.pF.C
	493	14:12:10.627395	0.001732000	IntelCor_94:27:30	Cisco_3f:80:f1	802.11	243	-61	dBm	33 dB	QoS Data, SN=20, FN=0, Flags=.pTC
	494	14:12:10.628807	0.001412000	Cisco_3f:80:f1	IntelCor_94:27:30	802.11	207	-30	dBm	64 dB	QoS Data, SN=3, FN=0, Flags=.pF.C
	495	14:12:10.632290	0.003483000	IntelCor_94:27:30	Cisco_3f:80:f1	802.11	243	-61	dBm	33 dB	QoS Data, SN=21, FN=0, Flags=.pTC
	496	14:12:10.632626	0.000336000	IntelCor_94:27:30	Cisco_3f:80:f1	802.11	211	-61	dBm	33 dB	QoS Data, SN=22, FN=0, Flags=.pTC

加密的無線流量。

步驟 3.生成和導出裝置的放射性蹤跡

在步驟1所在的螢幕中,捕捉到無線流量後,按一下綠色的Generate按鈕。

在「時間間隔」彈出窗口中,選擇符合您需求的時間範圍。無需在此啟用內部日誌。

按一下Apply to Device以生成放射性蹤跡。



RA跟蹤的時間間隔。

一旦放射性跟蹤就緒,download圖示將顯示在跟蹤檔名旁邊。點選它下載你的放射性痕跡。

Troubleshooting - > Radioactive Tra	ce		
Conditional Debug Global State: State	arted		A Wireless Deb
	rt Stop		Wileless Deb
MAC/IP Address T	Trace file		
0093.3794.2730	debugTrace_0093.3794.2730.tx: 📥	È	► Generate
			1 - 1 of 1 items

放射性痕跡可供下載。

步驟 4.從放射性痕跡獲取MSK

打開下載的放射性跟蹤檔案,然後在Access-Accept消息後搜尋eap-msk屬性。

#### <#root>

2022/09/23 20:00:08.646494126 {wncd\_x\_R0-0}{1}: [radius] [15612]: (info): RADIUS: Received from id 1812

#### Access-Accept

, len 289			
2022/09/23	20:00:08.646504952	{wncd_x_R0-0}{1}:	[radius] [15612]: (info): RADIUS: authenticator 8b 11 2
2022/09/23	20:00:08.646511532	{wncd_x_R0-0}{1}:	<pre>[radius] [15612]: (info): RADIUS: User-Name [1] 7 "Alic</pre>
2022/09/23	20:00:08.646516250	{wncd_x_R0-0}{1}:	[radius] [15612]: (info): RADIUS: Class [25] 55
2022/09/23	20:00:08.646566556	{wncd_x_R0-0}{1}:	<pre>[radius] [15612]: (info): RADIUS: EAP-Message [79] 6</pre>
2022/09/23	20:00:08.646577756	{wncd_x_R0-0}{1}:	[radius] [15612]: (info): RADIUS: Message-Authenticator
2022/09/23	20:00:08.646601246	{wncd_x_R0-0}{1}:	[radius] [15612]: (info): RADIUS: EAP-Key-Name [102] 67
2022/09/23	20:00:08.646610188	{wncd_x_R0-0}{1}:	[radius] [15612]: (info): RADIUS: Vendor, Microsoft [26
2022/09/23	20:00:08.646614262	{wncd_x_R0-0}{1}:	<pre>[radius] [15612]: (info): RADIUS: MS-MPPE-Send-Key [16]</pre>
2022/09/23	20:00:08.646622868	{wncd_x_R0-0}{1}:	[radius] [15612]: (info): RADIUS: Vendor, Microsoft [26
2022/09/23	20:00:08.646642158	{wncd_x_R0-0}{1}:	<pre>[radius] [15612]: (info): RADIUS: MS-MPPE-Recv-Key [17]</pre>
2022/09/23	20:00:08.646668839	{wncd_x_R0-0}{1}:	[radius] [15612]: (info): Valid Response Packet, Free t
2022/09/23	20:00:08.646843647	{wncd_x_R0-0}{1}:	[dot1x] [15612]: (info): [0093.3794.2730:capwap_9000000
2022/09/23	20:00:08.646878921	{wncd_x_R0-0}{1}:	[dot1x] [15612]: (info): [0093.3794.2730:capwap_9000000
2022/09/23	20:00:08.646884283	{wncd_x_R0-0}{1}:	[dot1x] [15612]: (info): [0093.3794.2730:capwap_9000000
2022/09/23	20:00:08.646913535	{wncd_x_R0-0}{1}:	[dot1x] [15612]: (info): [0000.0000.0000:capwap_9000000
2022/09/23	20:00:08.646914875	{wncd_x_R0-0}{1}:	[dot1x] [15612]: (info): [0000.0000.0000:capwap_9000000
2022/09/23	20:00:08.646996798	{wncd_x_R0-0}{1}:	[dot1x] [15612]: (info): [0093.3794.2730:capwap_9000000
2022/09/23	20:00:08.646998966	{wncd_x_R0-0}{1}:	[dot1x] [15612]: (info): [0093.3794.2730:capwap_9000000
2022/09/23	20:00:08.647000954	{wncd_x_R0-0}{1}:	[dot1x] [15612]: (info): [0000.0000.0000:unknown] Pkt b
2022/09/23	20:00:08.647004108	{wncd_x_R0-0}{1}:	[dot1x] [15612]: (info): [0093.3794.2730:capwap_9000000
2022/09/23	20:00:08.647008702	{wncd_x_R0-0}{1}:	[auth-mgr] [15612]: (info): [0093.3794.2730:capwap_9000
2022/09/23	20:00:08.647025898	{wncd_x_R0-0}{1}:	[auth-mgr] [15612]: (info): [0093.3794.2730:capwap_9000
2022/09/23	20:00:08.647033682	{wncd_x_R0-0}{1}:	[auth-mgr] [15612]: (info): [0093.3794.2730:capwap_9000
2022/09/23	20:00:08.647101204	{wncd_x_R0-0}{1}:	[aaa-attr-inf] [15612]: (info): Applying Attribute : us
2022/09/23	20:00:08.647115452	{wncd_x_R0-0}{1}:	[aaa-attr-inf] [15612]: (info): Applying Attribute : cl
2022/09/23	20:00:08.647116846	{wncd_x_R0-0}{1}:	[aaa-attr-inf] [15612]: (info): Applying Attribute : EA
2022/09/23	20:00:08.647118074	{wncd_x_R0-0}{1}:	[aaa-attr-inf] [15612]: (info): Applying Attribute : Me
2022/09/23	20:00:08.647119674	{wncd_x_R0-0}{1}:	[aaa-attr-inf] [15612]: (info): Applying Attribute : EA
2022/09/23	20:00:08.647128748	{wncd_x_R0-0}{1}:	[aaa-attr-inf] [15612]: (info): Applying Attribute : MS
2022/09/23	20:00:08.647137606	{wncd_x_R0-0}{1}:	[aaa-attr-inf] [15612]: (info): Applying Attribute : MS
2022/09/23	20:00:08.647139194	{wncd_x_R0-0}{1}:	[aaa-attr-inf] [15612]: (info): Applying Attribute : dn
2022/09/23	20:00:08.647140612	{wncd_x_R0-0}{1}:	[aaa-attr-inf] [15612]: (info): Applying Attribute : fo
2022/09/23	20:00:08.647141990	{wncd_x_R0-0}{1}:	[aaa-attr-inf] [15612]: (info): Applying Attribute : au
2022/09/23	20:00:08.647158674	{wncd_x_R0-0}{1}:	[aaa-attr-inf] [15612]: (info): Applying Attribute :

#### eap-msk

#### 0

fb c1 c3 f8 2c 13 66 6e 4d dc 26 b8 79 7e 89 83 f0 12 54 73 cb 61 51 da fa af 02 bf 96 87 67 4c c7 22 cl

2022/09/23 20:00:08.647159912 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [15612]: (info): Applying Attribute : ea 2022/09/23 20:00:08.647161666 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [15612]: (info): Applying Attribute : me 2022/09/23 20:00:08.647164452 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [15612]: (info): Applying Attribute : cl 2022/09/23 20:00:08.647166150 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [15612]: (info): Applying Attribute : in 2022/09/23 20:00:08.647202312 {wncd\_x\_R0-0}{1}: [auth-mgr] [15612]: (info): [0093.3794.2730:capwap\_9000

eap-msk字串之後的值是MSK。複製並儲存它,以便在下一步中使用它。

#### <#root>

```
2022/09/23 20:00:08.647158674 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15612]: (info): Applying Attribute : eap-msk
```

0

fb cl c3 f8 2c 13 66 6e 4d dc 26 b8 79 7e 89 83 f0 12 54 73 cb 61 51 da fa af 02 bf 96 87 67 4c c7 22 cl

步驟 5.在Wireshark中增加MSK作為IEEE 802.11解密金鑰

在Wireshark上,轉到Wireshark > Preferences > Protocols > IEEE 802.11。

選中Enable decryption覈取方塊,然後選擇Decryption keys旁邊的Edit。

按一下底部的「+」按鈕以增加新的解密金鑰,然後選擇msk作為金鑰型別。

貼上步驟4中取得的eap-msk值(不含空格)。

最後,按一下OK關閉「Decryption keys」窗口,然後按一下OK關閉「Preferences」窗口並應用解 密金鑰。

•••	Wireshark · Preferences	
ICP ICQ IEC 60870-5-101 IEC 60870-5-103 IEC 60870-5-104 IEEE 802.15.4 IEEE 802.15.4 IEEE 802.1AH IEEE 1722 IFCP ILP IMAP IMAP IMAP IMF INAP Infiniband SDP Interlink IPDC IPDR/SP IPPR/SP	IEEE 802.11 wireless LAN   Reassemble fragmented 802.11 datagrams  Ignore vendor-specific HT elements  Call subdissector for retransmitted 802.11 frames  Assume packets have FCS Validate the FCS checksum if possible  Ignore the Protection bit  No  Yes - without IV  Fraable WPA Key MIC Length override  WPA Key MIC Length override  WPA Key MIC Length override  Decryption  Decryption keys Edit	
IPMI IPPUSB	WEP and WPA Decryption Keys	
IPSICIL IPv4 IPv6 IPV5 IPX ISCSI ISDN ISER ISMACRYP ISNS ISO 10681 ISO 15765 ISO 8583 ISObus VT ISUP	Key type         Key           msk         fbc1c3f82c13666e4ddc26b8797e8983f0125473cb6151dafaaf02bf9687674cc722cbf0933102a41bb02f0a769bb223810ct	
Help	+ - Pa A V E	Cancel OK
sco_3f:80:f1 802 sco_3f:80:f1 802	Help Copy from Cancel OK	

解密金鑰已增加到wireshark首選項。

## 步驟 6.分析解密的802.1X流量

觀察無線流量現在是如何顯示的。在熒幕擷取畫面中,您可以看到ARP流量(封包482和484)、

DNS查詢和回應(封包487和488)、ICMP流量(封包491到497),甚至是TCP作業階段三向交涉 的開始(封包507)。

No.	11	Time	Time delta from p	Source	Destination	Protocol  L	Length   Signal strens	Signal/nois	1100
	449	14:12:10.052518	0.001339000	IntelCor_94:27:30	Cisco_aa:18:8f	802.11	248 -59 dBm	35 dB	Reassociation Request, SN=22, FN=0, Flags=C, SSID="ota-dot1x"
	450	14:12:10.056200	0.003682000	Cisco_aa:18:8f	IntelCor_94:27:30	802.11	227 -34 dBm	60 dB	Reassociation Response, SN=3741, FN=0, Flags=C
	451	14:12:10.058303	0.002103000	IntelCor 94:27:30	Cisco aa:18:8f	802.11	93 -59 dBm	35 dB	Action, SN=23, FN=0, Flags=C
	452	14:12:10.059417	0.001114000	Cisco aa:18:8f	IntelCor 94:27:38	EAP	109 -34 dBm	60 dB	Request. Identity
	453	14:12:10.108429	0.049012000	IntelCor 94:27:38	Cisco aa:18:8f	FAP	146 -59 dBm	35 dB	Resonase. Identity
	454	14:12:18 116080	0.000400000	Circo anile.ef	IntelCor 94:27:28	EAD	110 -24 dBm	60 dB	Dequest TIC EAD (EAD_TIC)
	454	14.12.10.110909	0.000400000	Tate1Car 04:27:30	Cieco ant 10.0f	EAD	146 -50 dBm	35 40	
	433	14:12:10.119150	0.002241000	Intettor_94:27:30	C15C0_88118181	EAP	140 -39 dbm	35 08	Response, Legacy war (Response only)
	450	14:12:10.122/92	0.003642000	Cisco_aa:18:81	IntelCor_9412/130	EAP	110 -33 dBm	61 dB	Request, Protected EAP (EAP-PEAP)
	457	14:12:10.124621	0.001829000	IntelCor_94:27:30	Cisco_aa:18:8f	TLSV1.2	330 -60 dBm	34 dB	Encrypted Handshake Message
	458	14:12:10.166650	0.042029000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	1116 -33 dBm	61 dB	Request, Protected EAP (EAP-PEAP)
	459	14:12:10.170039	0.003389000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146 -59 dBm	35 dB	Response, Protected EAP (EAP-PEAP)
	460	14:12:10.175814	0.005775000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	1112 -34 dBm	60 dB	Request, Protected EAP (EAP-PEAP)
	461	14:12:10.180069	0.004255000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146 -59 dBm	35 dB	Response, Protected EAP (EAP-PEAP)
	462	14:12:10.182929	0.002860000	Cisco_aa:18:8f	IntelCor_94:27:30	TLSv1.2	268 -34 dBm	60 dB	Server Hello, Certificate, Server Key Exchange, Server Hello Done
	463	14:12:10.236135	0.053206000	IntelCor_94:27:30	Cisco_aa:18:8f	TLSv1.2	308 -60 dBm	34 dB	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
	464 :	14:12:10.244438	0.008303000	Cisco_aa:18:8f	IntelCor_94:27:30	TLSv1.2	161 -34 dBm	60 dB	Change Cipher Spec, Encrypted Handshake Message
	465	14:12:10.248078	0.003640000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146 -60 dBm	34 dB	Response, Protected EAP (EAP-PEAP)
	466	14:12:10.251302	0.003224000	Cisco_aa:18:8f	IntelCor_94:27:30	TLSv1.2	144 -34 dBm	60 dB	Application Data
	467	14:12:10.259110	0.007808000	IntelCor 94:27:30	Cisco aa:18:8f	TLSv1.2	149 -60 dBm	34 dB	Application Data
	468	14:12:10.263865	0.004755000	Cisco aa:18:8f	IntelCor 94:27:38	TLSv1.2	175 -34 dBm	60 dB	Application Data
	469	14:12:10.271714	0.007849000	IntelCor 94:27:38	Cisco aa:18:8f	TI 5v1.2	203 -60 dBm	34 dB	Apolication Data
	478	14:12:18 205208	0.012566000	Cisco anil9.9f	IntelCor 94:27:38	TI Su1 2	198 -22 dBa	61 dB	Anolication Data
	471	14-12-10 207513	0.013300000	Tatel Car 04:27:30	Cisco anile of	TI Cut 2	146 -60 dBm	34 dB	Application bata
	471	14:12:10.20/515	0.002233000	Intettor_94:27:30	C15C0_88:10:01	TLOVI.2	140 -00 000	34 db	Application bata
	4/2	14:12:10.291081	0.003568000	Cisco_aa:18:81	Inte(Cor_94:27:30	TLSV1.2	143 -34 dBm	00 dB	Application bata
	4/3	14:12:10.294213	0.003132000	IntelCor_94:27:30	C15C0_88:18:81	EAP	146 -68 dbm	34 08	Response, Protected EAP (EAP-PEAP)
	474	14:12:10.315016	0.020803000	Cisco_aa:18:81	IntelCor_94:27:30	EAP	108 -33 dBm	61 dB	Success
	475	14:12:10.316556	0.001540000	Cisco_aa:18:8f	IntelCor_94:27:30	EAPOL	221 -34 dBm	60 dB	Key (Message 1 of 4)
	476	14:12:10.321017	0.004461000	IntelCor_94:27:30	Cisco_aa:18:8f	EAPOL	223 -60 dBm	34 dB	Key (Message 2 of 4)
	477	14:12:10.322061	0.001044000	Cisco_aa:18:8f	IntelCor_94:27:30	EAPOL	255 -34 dBm	60 dB	Key (Message 3 of 4)
	478	14:12:10.323817	0.001756000	IntelCor_94:27:30	Cisco_aa:18:8f	EAPOL	199 -60 dBm	34 dB	Key (Message 4 of 4)
	479	14:12:10.324699	0.000882000	IntelCor_94:27:30	Cisco_aa:18:8f	802.11	148 -60 dBm	34 dB	Action, SN=24, FN=8, Flags=C, Dialog Token=3
	488 :	14:12:10.325899	0.001200000	Cisco_aa:18:8f	IntelCor_94:27:30	882.11	148 -34 dBm	60 dB	Action, SN=3746, FN=0, Flags=C, Dialog Token=3
	481	14:12:10.334956	0.009057000	fe80::badf:865b:f10_	ff02::2	ICMPv6	207 -61 dBm	33 dB	Router Solicitation from 00:93:37:94:27:30
	482 :	14:12:10.348407	0.013451000	IntelCor_94:27:30	Broadcast	ARP	197 -61 dBm	33 dB	Who has 172.16.5.1? Tell 172.16.5.66
	483	14:12:10.348903	0.000495000	Cisco_aa:18:8f	IntelCor_94:27:30	802.11	99 -34 dBm	60 dB	Action, SN=3747, FN=0, Flags=C, Dialog Token=90
	484	14:12:10.349222	0.000319000	Cisco_3f:80:f1	IntelCor 94:27:38	ARP	197 -30 dBm	64 dB	172.16.5.1 is at 78:da:6e:3f:80:f1
	485	14:12:10.349623	0.000401000	IntelCor 94:27:30	Cisco aa:18:8f	802.11	99 -60 dBm	34 dB	Action, SN=25, FN=0, Flags=C, Dialog Token=90
	486	14:12:10.350846	0.000423000	172.16.5.66	172.18.188.43	DNS	220 -61 dBm	33 dB	Standard query 0x3c48 A www.msftconnecttest.com
	487	14:12:18.530286	0.180240000	172, 16, 5, 66	172.18.108.43	DNS	206 -61 dBm	33 dB	Standard guery 8xad51 A cisco.com
1	488	14:12:10.616297	8,885811888	172.18.188.43	172.16.5.66	DNS	222 -30 dBm	64 dB	Standard query researce exad51 A cisco.com A 72.163.4.161
	489	14:12:18.623163	0.005855000	172 16 5 66	224 8 8 22	TOMPUS	199 -61 dBa	33 dB	Membership Report / Join group 224 & 8,251 for any courses / Join group 230,255,258 for any courses
	498	14:12:18.623515	0.000000000	fe88: : hadf: 865h: f18	ff82::16	TOMPus	267 -61 dBa	33 dB	Multicast lictorer Benert Mecsane v2
	401	14:12:10.023313	0.000332000	173 16 5 66	172 252 62 00	TONP	242 -61 dBa	33 48	Techo (a result in equiption and a second se
	491	14:12:10.023090	0.000373000	10 152 216 102	172.253.03.99	TONP	243 -01 dbs	55 db	Ecto (pang) request in exceeds, sequels//sites/, (cto (no response round:/
	492	14:12:10.023003	0.001773000	10.152.210.193	172.10.5.00	TONP	207 -30 dom	04 00	Time-to-tive exceeded (time to tive exceeded in transit)
_	493	14:12:10.627395	0.001/32000	1/2.10.5.66	172.253.63.99	TONP	243 -01 dbm	33 db	Echo (ping) request id=exeeds, seq=alse/S1/43, tttm9 (no response tound:)
	494	14:12:10.628807	0.001412000	10.152.216.129	172.16.5.66	TONP	207 -30 dBm	64 dB	Time-to-live exceeded (Time to live exceeded in transit)
	495	14:12:10.632290	0.003483000	172.16.5.66	172.253.63.99	ICMP	243 -61 dBm	33 dB	Echo (ping) request 1d=0x0001, seq=8139/51999, ttl=10 (no response Tound!)
_	496	14:12:10.632626	0.000336000	1/2.16.5.66	72.163.4.161	ICMP	211 -61 dBm	33 dB	Ecno (ping) request 10=0X0001, seq=8140/52255, ttl=128 (reply in 501)
	497	14:12:10.632626	0.000000000	10.152.192.145	172.16.5.66	ICHP	207 -30 dBm	64 dB	Time-to-live exceeded (Time to live exceeded in transit)
	498	14:12:10.632695	0.000069000	IntelCor_94:27:30	Cisco_aa:18:8f	802.11	99 -60 dBm	34 dB	Action, SN=26, FN=0, Flags=C, Dialog Token=6
	499 :	14:12:10.632972	0.000277000	Cisco_aa:18:8f	IntelCor_94:27:30	802.11	99 -34 dBm	60 dB	Action, SN=3754, FN=0, Flags=C, Dialog Token=6
	500	14:12:10.634467	0.001495000	172.16.5.66	172.253.63.99	ICMP	243 -61 dBm	33 dB	Echo (ping) request id=0x0001, seq=8141/52511, ttl=11 (no response found!)
	501	14:12:10.666791	0.032324000	72.163.4.161	172.16.5.66	ICMP	211 -30 dBm	64 dB	Echo (ping) reply id=0x0001, seq=8140/52255, ttl=236 (request in 496)
_	502	14:12:10.668564	0.001773000	10.152.216.189	172.16.5.66	ICMP	207 -30 dBm	64 dB	Time-to-live exceeded (Time to live exceeded in transit)
	503	14:12:10.669017	0.000453000	10.152.216.189	172.16.5.66	ICMP	207 -30 dBm	64 dB	Time-to-live exceeded (Time to live exceeded in transit)
	584	14:12:10.718518	0.049501000	172.16.5.66	239.255.255.250	SSDP	354 -61 dBm	33 dB	M-SEARCH * HTTP/1.1
	505	14:12:10.747832	0.029314000	172.18.108.43	172.16.5.66	DNS	364 -30 dBm	64 dB	Standard query response 0x3c48 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msf
	506	14:12:10.748179	0.000347080	172.18.108.43	172.16.5.66	DNS	364 -30 dBm	64 dB	Standard guery response 0x3c48 A www.msftconnecttest.com ONAME ncsi-geo.trafficmanager.net ONAME www.msf
				133 16 5 55		<b>2.40</b>	242 64 40-	22 42	const. as feasily and a second second and and a second and

解密的無線流量。

### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。