在802.1X SSID中解密無線資料包捕獲

目錄

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：

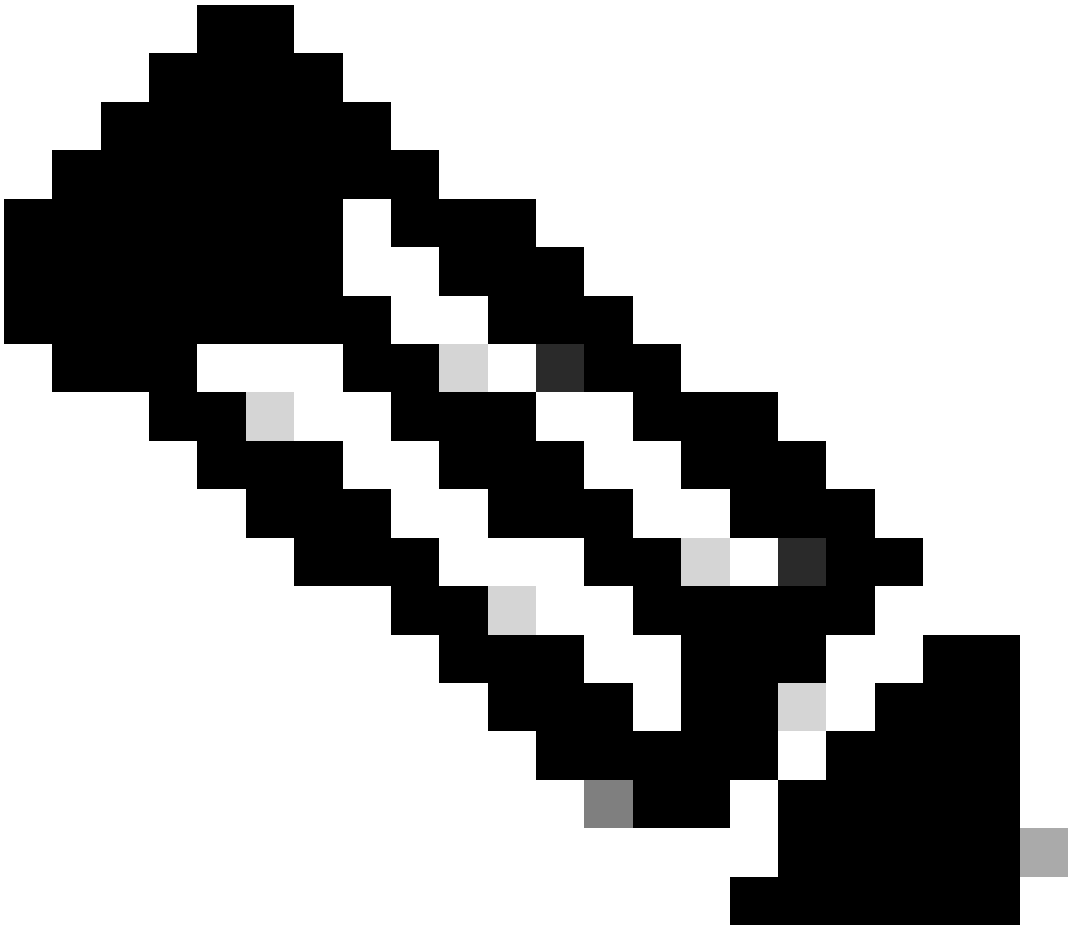
- Catalyst 9800-L WLC、Cisco IOS® XE Cupertino 17.9.3
- 採用監聽器模式的Catalyst 9130AXE存取點
- Cisco ISE版本3.3
- Wireshark 4.0.8

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）。

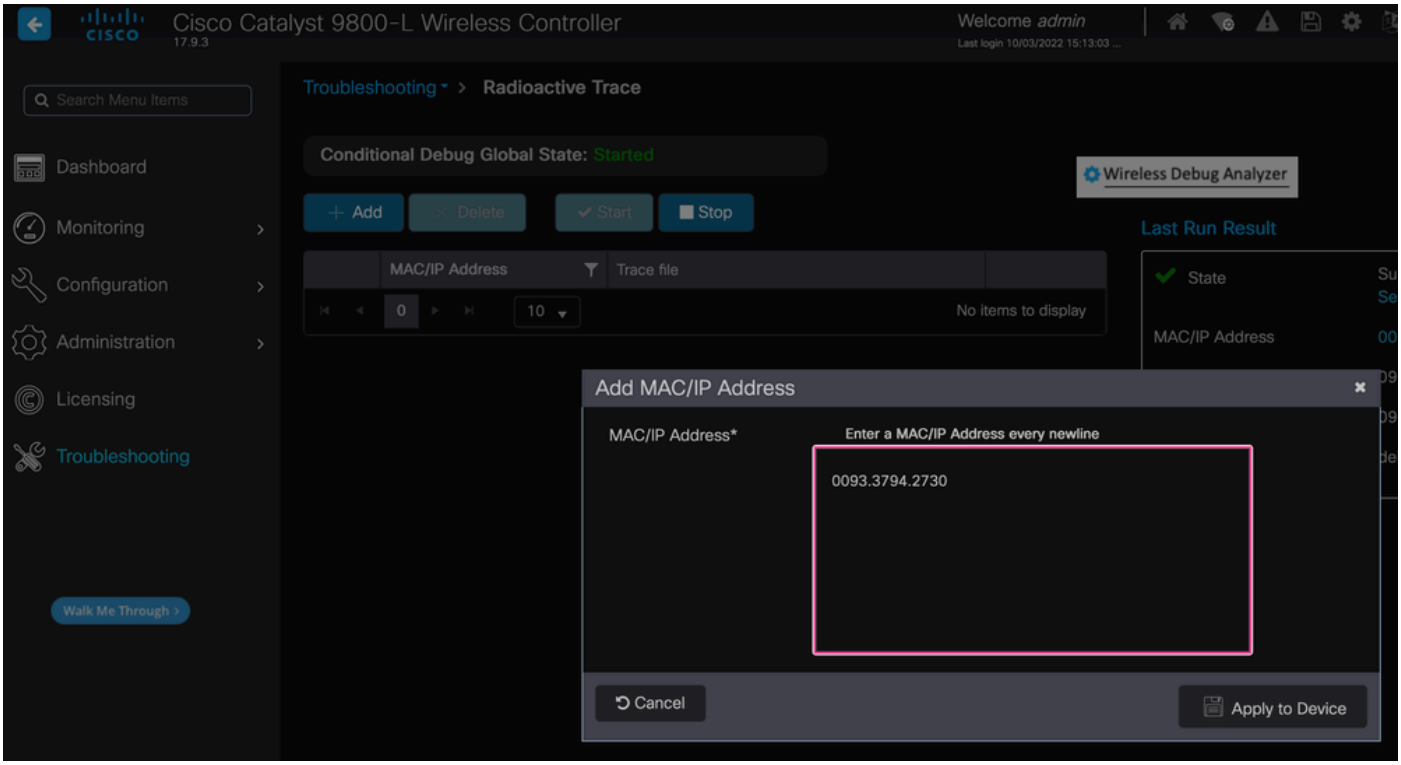


注意：此程式僅適用於WPA2，因為計算成對暫時性金鑰(PTK)所需的資訊會透過4次交涉在空中交換。相反，在WPA3中，對等體同時身份驗證(SAE)透過所謂的蜻蜓握手來執行。

設定

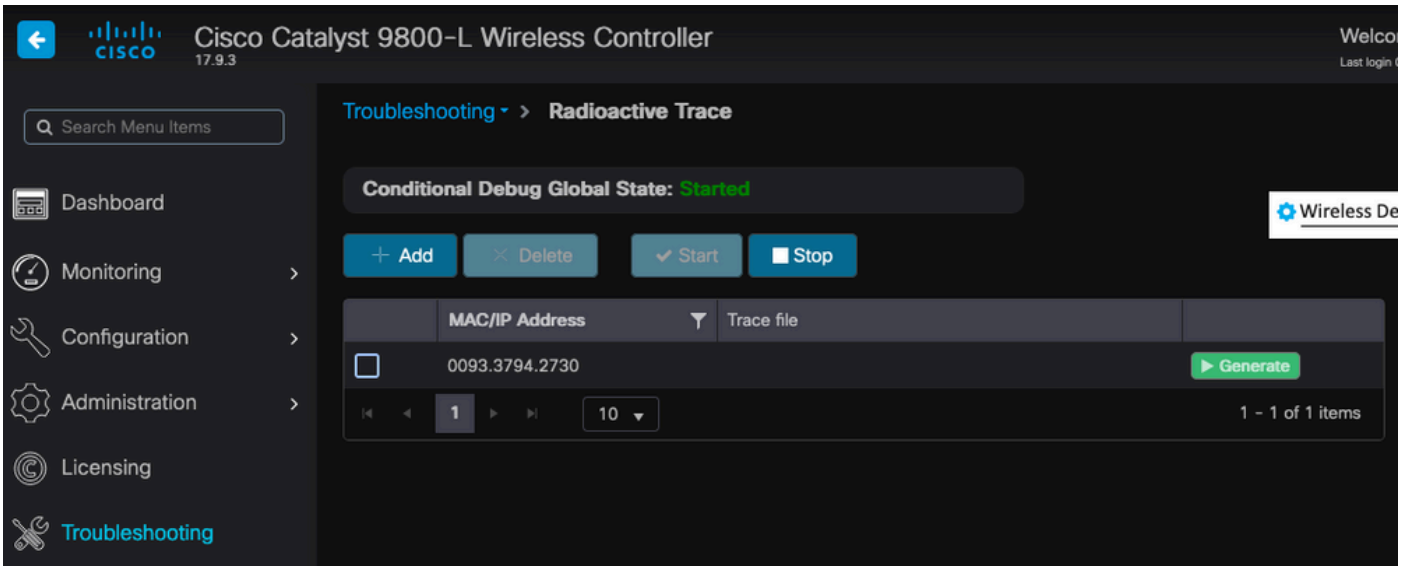
步驟 1.開始感興趣終端的放射性跟蹤

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。

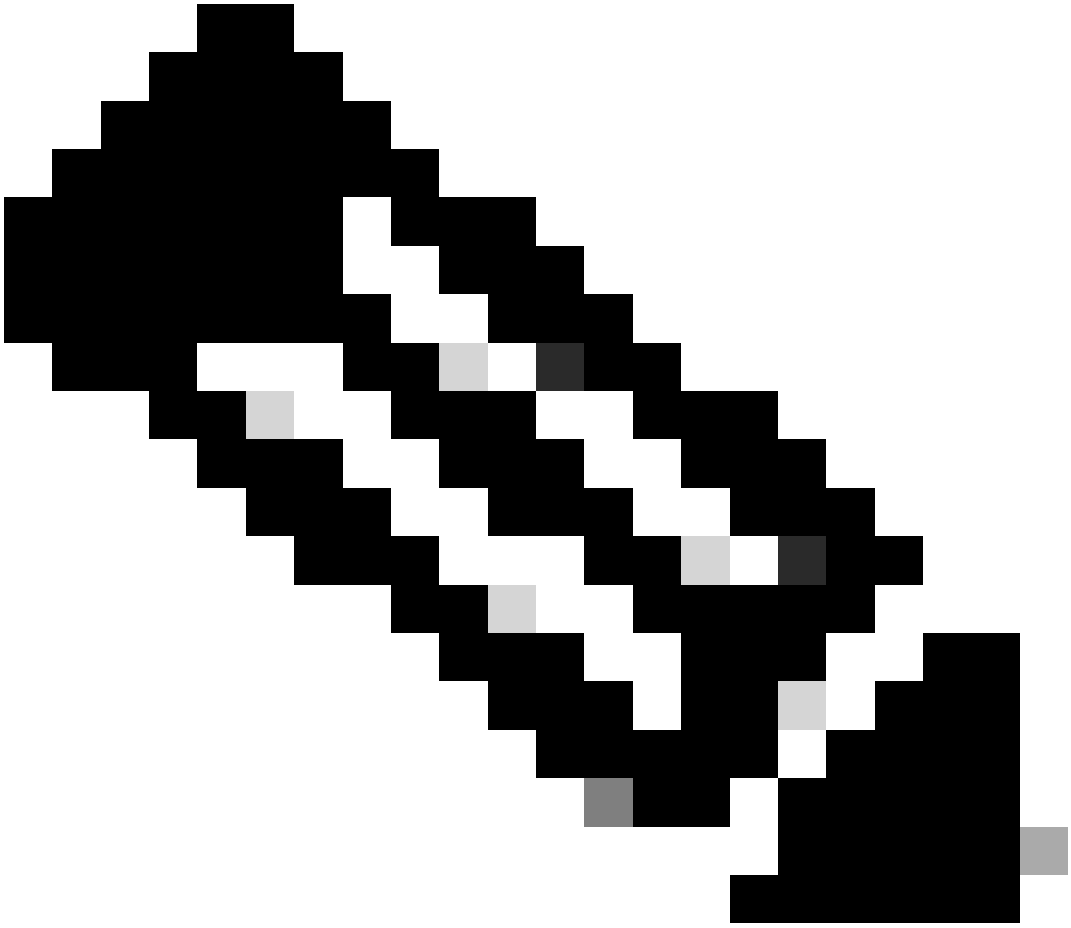


增加到放射性蹤跡清單的MAC地址

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）。



在啟用條件調試的情況下增加到放射性跟蹤清單的裝置。

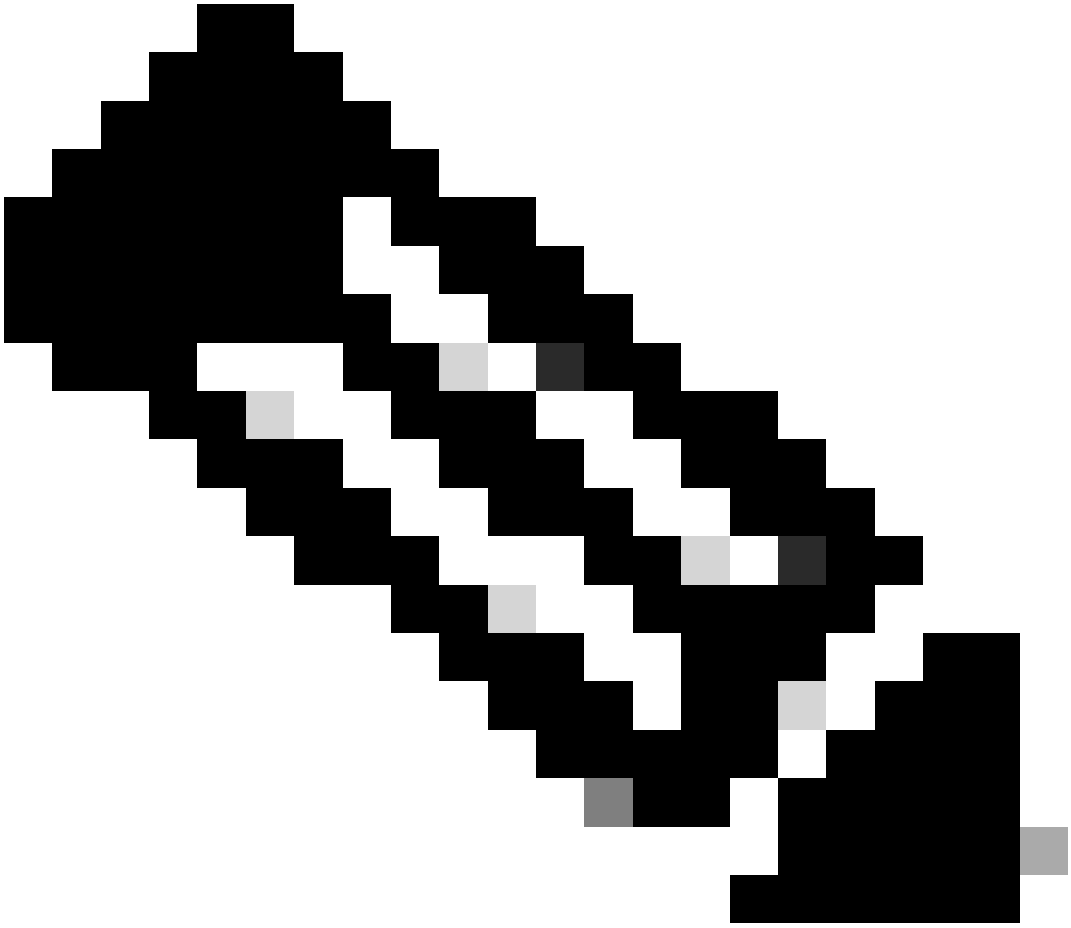


注意：如果未啟用條件調試，則只能看到控制平面中的流量，而不包括MSK。有關此過程的詳細資訊，請參閱Catalyst 9800 WLC故障排除文檔上的調試和日誌收集的條件調試和放射性跟蹤部分。

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。

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

No.	Time	Time delta from p	Source	Destination	Protocol	Length	Signal streng	Signal/nois	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=.p.....TC
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=.p.....TC
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=.p....F.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=.p.....TC
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=.p.....TC
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=.p....F.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=.p.....TC
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=.p.....TC
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=.p.....TC
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=.p....F.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=.p.....TC
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=.p....F.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=.p.....TC
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=.p.....TC

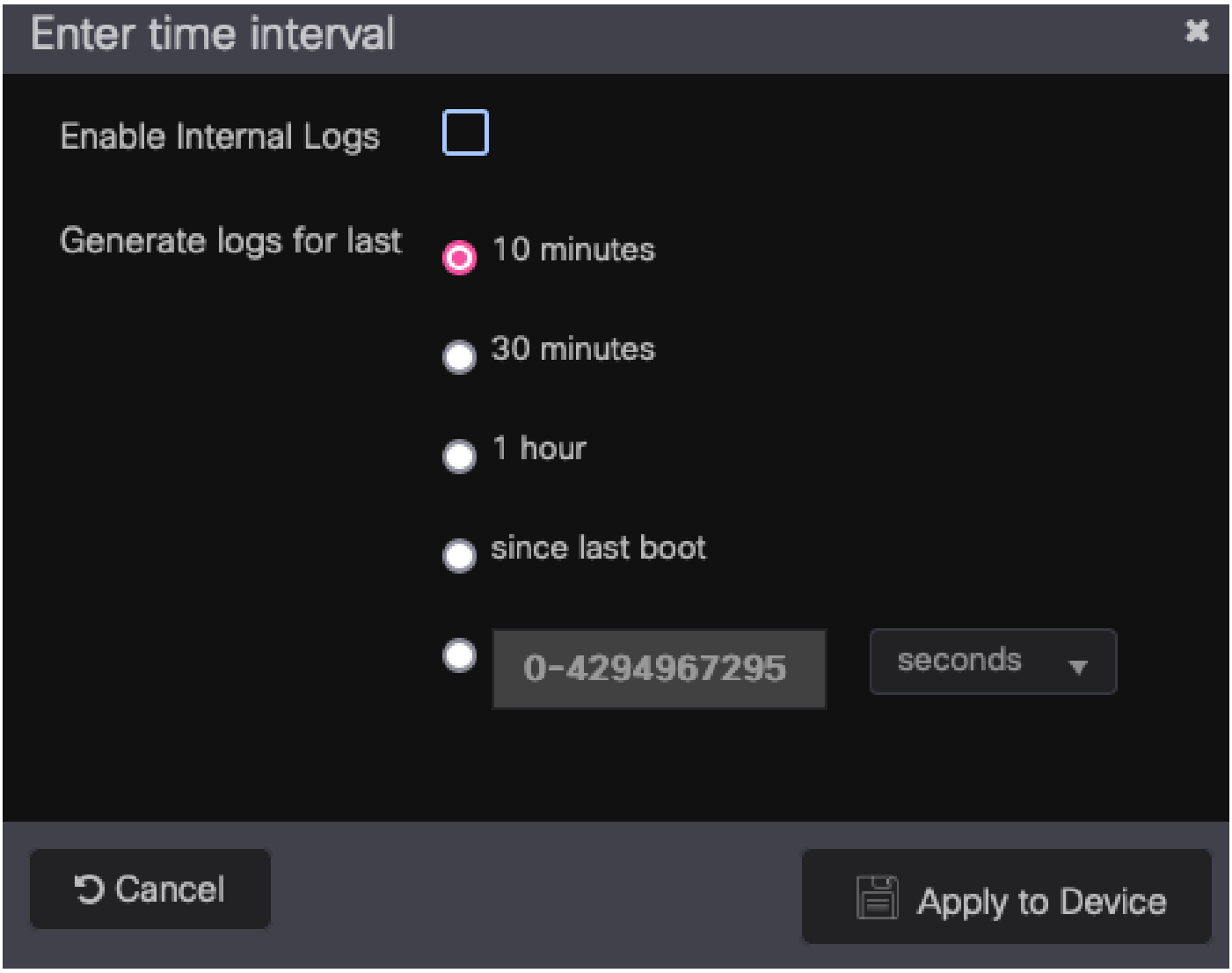
加密的無線流量。

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。

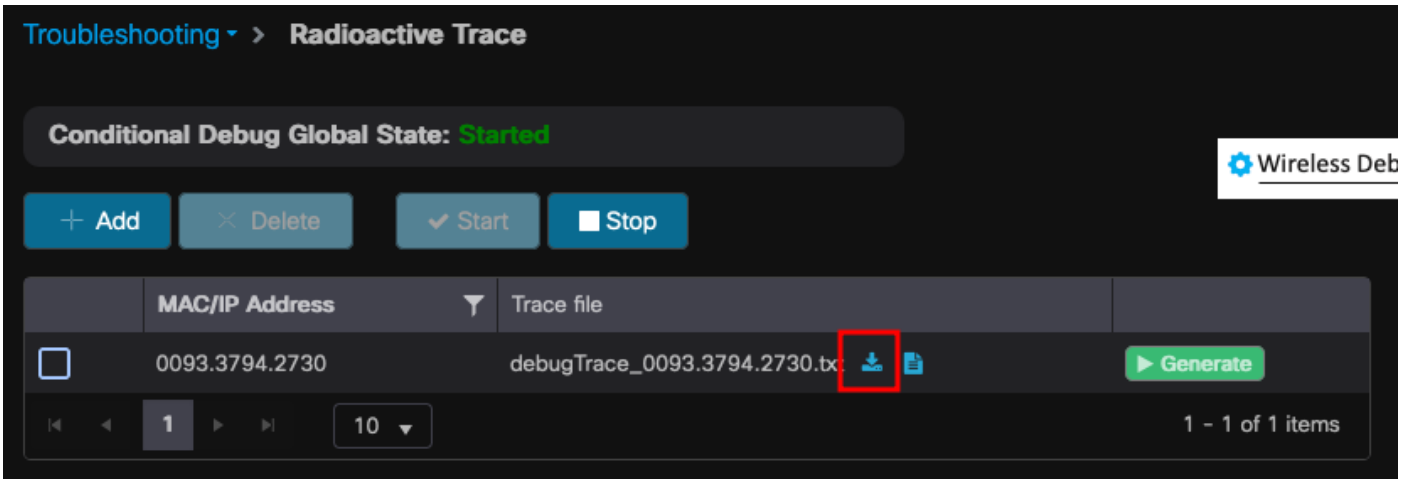
在「時間間隔」彈出窗口中，選擇符合您需求的時間範圍。無需在此啟用內部日誌。

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。



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}: [radius] [15612]: (info): RADIUS: User-Name [1] 7 "Alic
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}: [radius] [15612]: (info): RADIUS: EAP-Message [79] 6 ..
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}: [radius] [15612]: (info): RADIUS: MS-MPPE-Send-Key [16]
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}: [radius] [15612]: (info): RADIUS: MS-MPPE-Recv-Key [17]
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 cb

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 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 cb
```

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

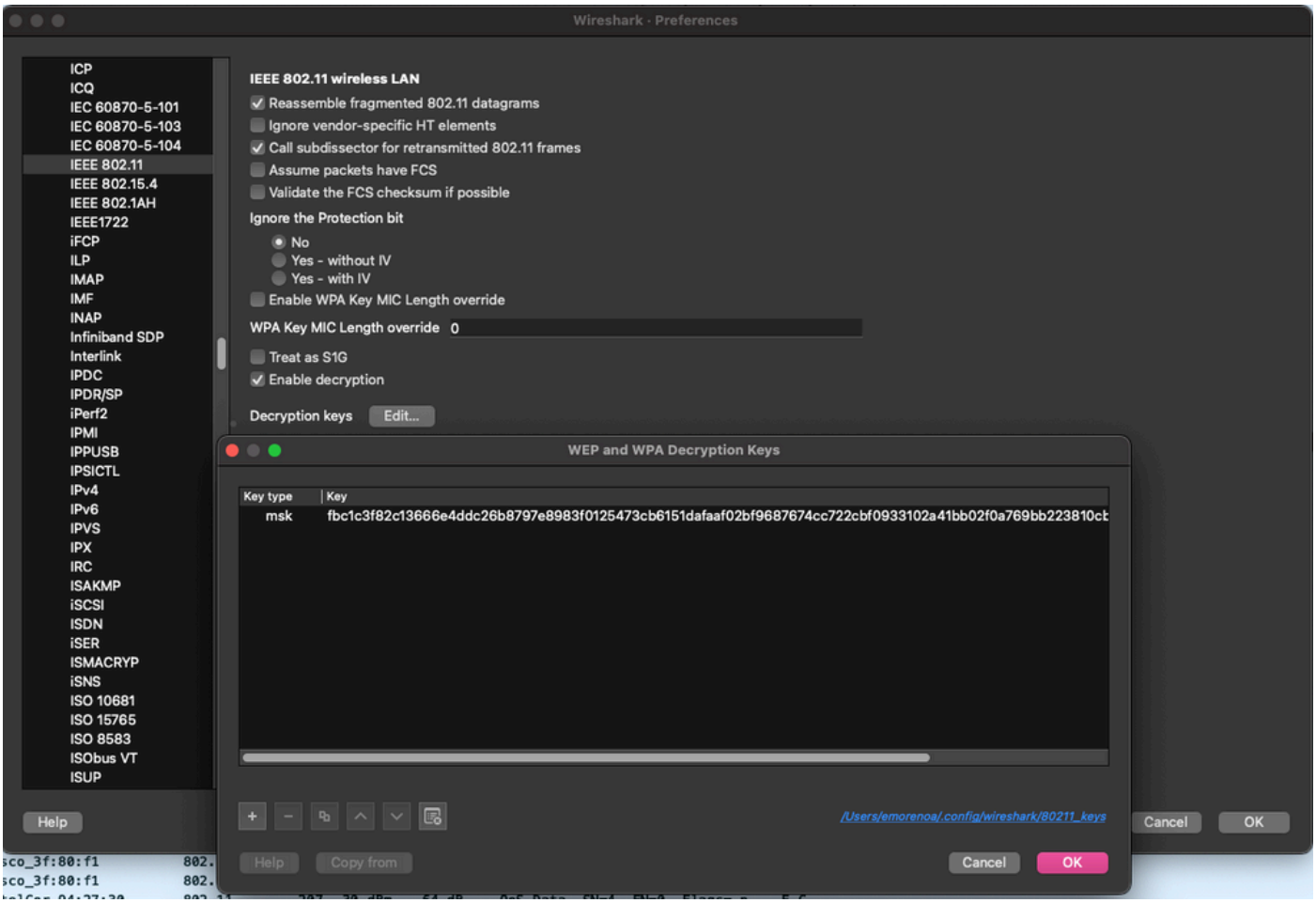
在Wireshark上，轉到Wireshark > Preferences > Protocols > IEEE 802.11。

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。

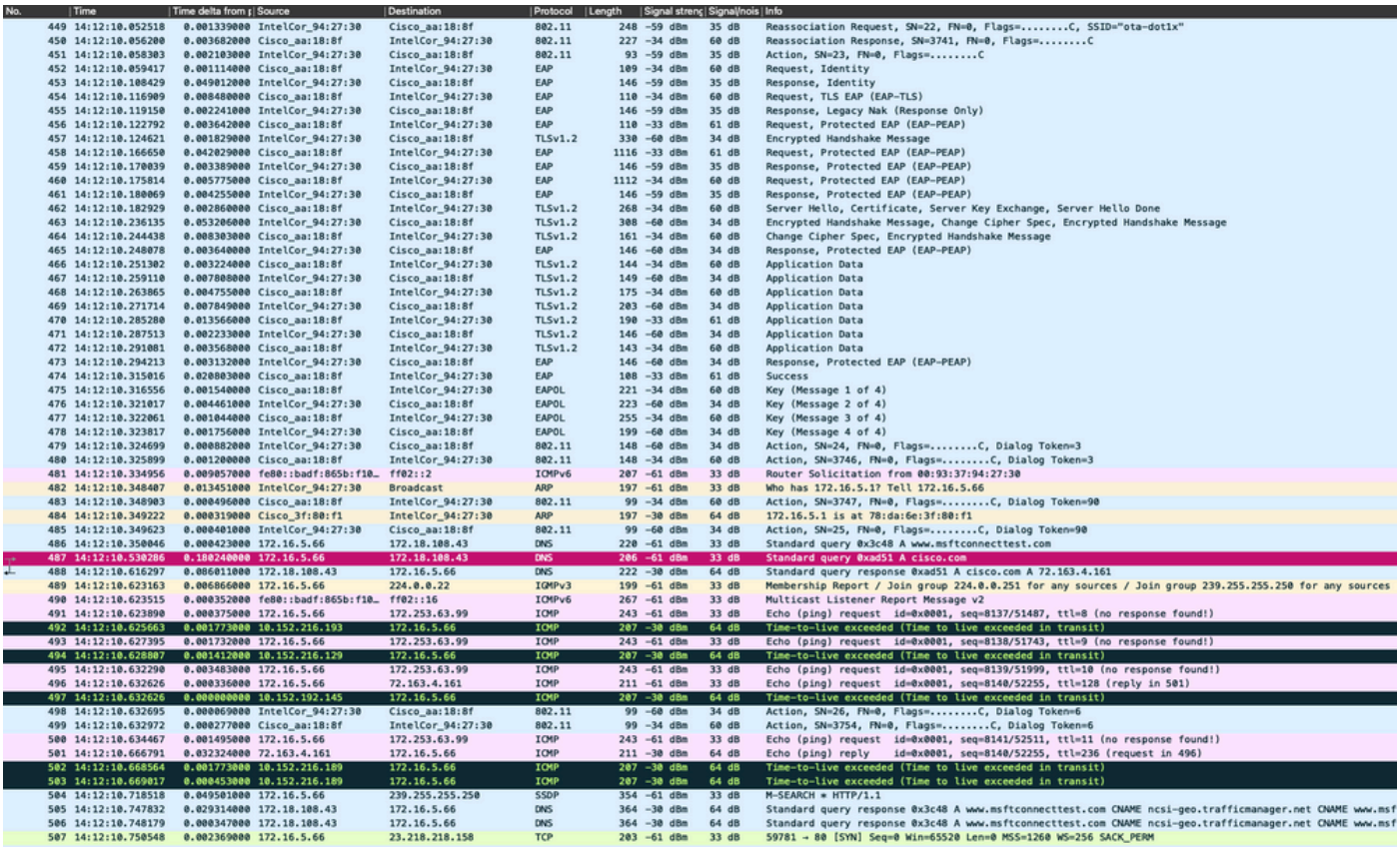


解密金鑰已增加到wireshark首選項。

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.	Time	Time delta from p	Source	Destination	Protocol	Length	Signal streng	Signal/nois	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	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	0.000496000	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	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	14:12:10.350046	0.000423000	172.16.5.66	172.18.108.43	DNS	220	-61 dBm	33 dB	Standard query 0x3c48 A www.msftconnecttest.com
487	14:12:10.530286	0.180240000	172.16.5.66	172.18.108.43	DNS	206	-61 dBm	33 dB	Standard query 0xad51 A cisco.com
488	14:12:10.616297	0.086011000	172.18.108.43	172.16.5.66	DNS	222	-30 dBm	64 dB	Standard query response 0xad51 A cisco.com A 72.163.4.161
489	14:12:10.623163	0.006866000	172.16.5.66	224.0.0.22	IGMPv3	199	-61 dBm	33 dB	Membership Report / Join group 224.0.0.251 for any sources / Join group 239.255.255.250 for any sources
490	14:12:10.623515	0.000352000	fe80::badf:865b:f10…	ff02::16	ICMPv6	267	-61 dBm	33 dB	Multicast Listener Report Message v2
491	14:12:10.623890	0.000375000	172.16.5.66	172.253.63.99	ICMP	243	-61 dBm	33 dB	Echo (ping) request id=0x0001, seq=8137/51487, ttl=8 (no response found!)
492	14:12:10.625663	0.001773000	10.152.216.193	172.16.5.66	ICMP	207	-30 dBm	64 dB	Time-to-live exceeded (Time to live exceeded in transit)
493	14:12:10.627395	0.001732000	172.16.5.66	172.253.63.99	ICMP	243	-61 dBm	33 dB	Echo (ping) request id=0x0001, seq=8138/51743, ttl=9 (no response found!)
494	14:12:10.628807	0.001412000	10.152.216.129	172.16.5.66	ICMP	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 id=0x0001, seq=8139/51999, ttl=10 (no response found!)
496	14:12:10.632626	0.000336000	172.16.5.66	72.163.4.161	ICMP	211	-61 dBm	33 dB	Echo (ping) request id=0x0001, seq=8140/52255, ttl=128 (reply in 501)
497	14:12:10.632626	0.000000000	10.152.192.145	172.16.5.66	ICMP	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)
504	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	0.000347000	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
507	14:12:10.750548	0.002369000	172.16.5.66	23.218.218.158	TCP	203	-61 dBm	33 dB	59781 → 80 [SYN] Seq=0 Win=65520 Len=0 MSS=1260 WS=256 SACK_PERM

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）。