Entschlüsseln von Over-the-Air-Paketerfassungen in 802.1x-SSIDs

Inhalt

Einleitung

In diesem Dokument wird die Entschlüsselung von Over-the-Air Packet Captures für 802.1X-WLANs mithilfe der auf dem Catalyst 9800 WLC verfügbaren Tools zur Fehlerbehebung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- So konfigurieren Sie ein 802.1X-WLAN im Catalyst 9800 WLC
- Aufnahme radioaktiver Spuren mit aktiviertem bedingtem Debugging im Catalyst 9800 WLC
- Übernahme von Over-the-Air-Paketerfassungen über einen Access Point im Sniffer-Modus oder ein Macbook mit dem Wireless-Diagnosetool

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 9800-L WLC, Cisco IOS® XE Cupertino 17.9.3
- Catalyst 9130AX Access Point im Sniffer-Modus

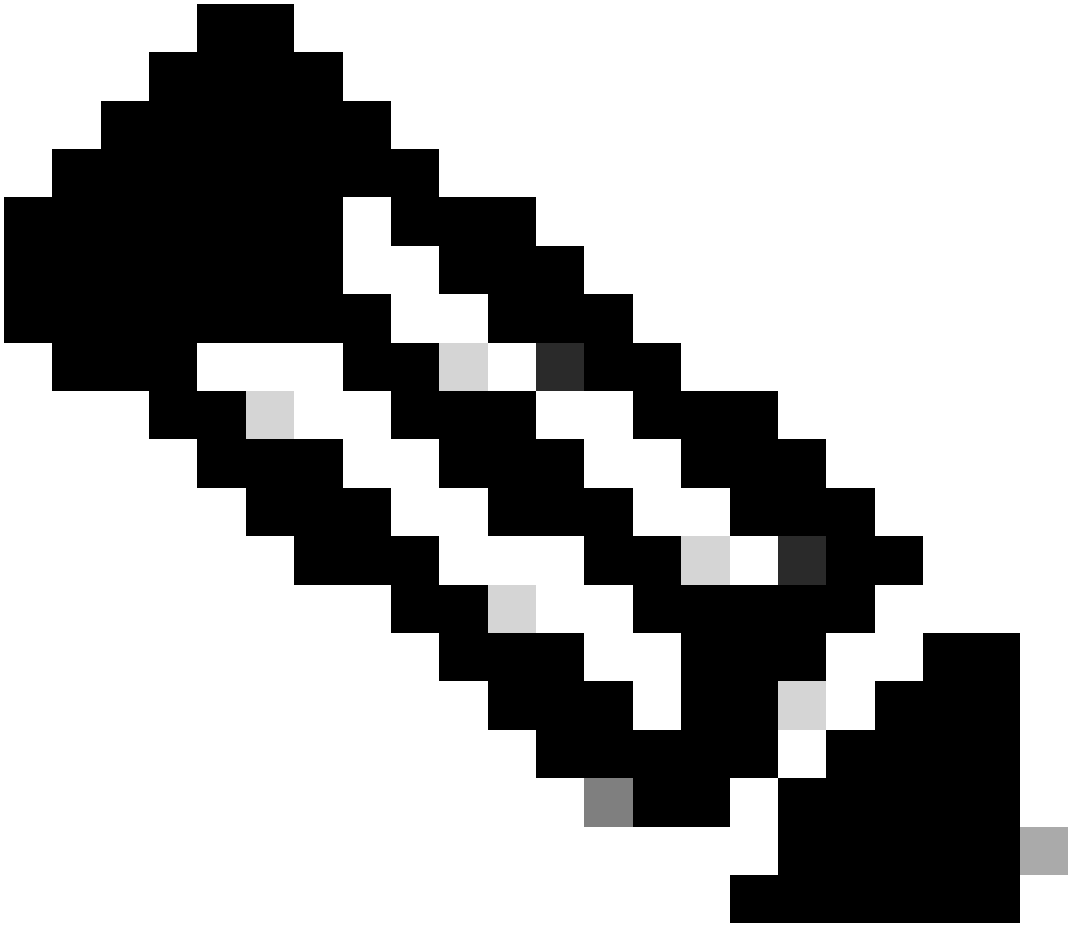
- Cisco ISE Version 3.3
- Wireshark 4.0.8

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Nachdem eine Identität über EAP+8021X validiert wurde, wird der Wireless-Datenverkehr mit dem Pairwise Transient Key (PTK) verschlüsselt, der aus dem Handshake zwischen dem Supplicant und dem Authentifikator generiert wird. Dabei wird der Pairwise Master Key (PMK) zur Berechnung verwendet. Diese PMK wird vom Master Session Key (MSK) abgeleitet. Das MSK ist in den Attributwertpaaren der RADIUS Access-Accept-Nachricht enthalten (verschlüsselt mit dem RADIUS Shared Secret). Daher kann der Datenverkehr bei einer Over-the-Air-Paketerfassung nicht transparent angezeigt werden, selbst wenn der Vier-Wege-Handshake von einem Drittanbieter abgefangen wird.

Normalerweise umfasst die Erzeugung des PMK die Paketerfassung im kabelgebundenen Netzwerk, die Kenntnis des gemeinsamen geheimen RADIUS-Schlüssels und eine Codierung, um die gewünschten Werte zu extrahieren. Bei dieser Methode wird stattdessen eines der Tools zur Fehlerbehebung auf dem Catalyst 9800 WLC (Radioactive Traces) verwendet, um die MSK zu erhalten. Diese kann dann in jedem bekannten Paketanalyse-Tool wie Wireshark verwendet werden.

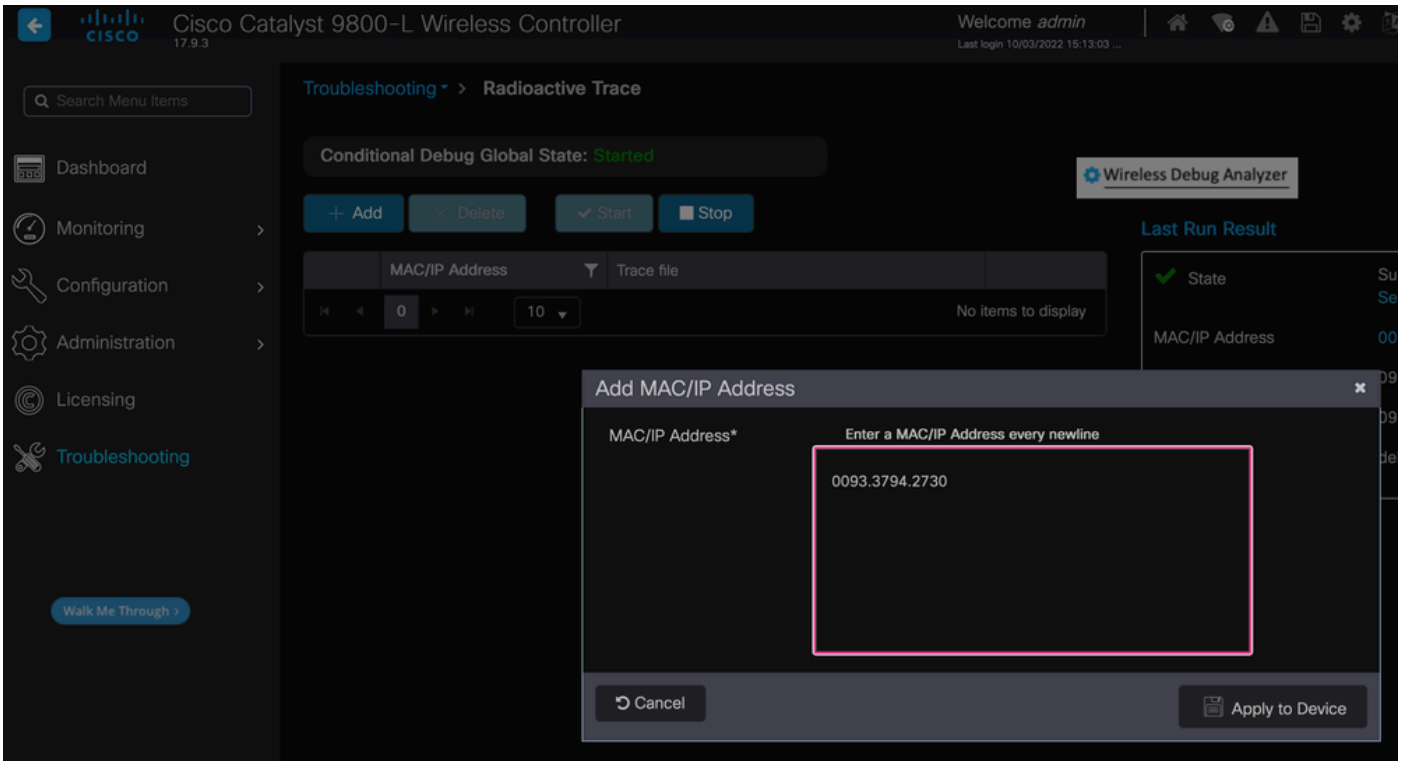


Hinweis: Dieses Verfahren funktioniert nur bei WPA2, da die zur Berechnung der paarweisen Übergangsschlüssel (Pairwise Transient Keys, PTK) erforderlichen Informationen über den 4-Wege-Handshake per Funk ausgetauscht werden. Stattdessen wird in WPA3 die gleichzeitige Authentifizierung von Gleichen (SAE) durch den so genannten Dragonfly-Handshake durchgeführt.

Konfigurieren

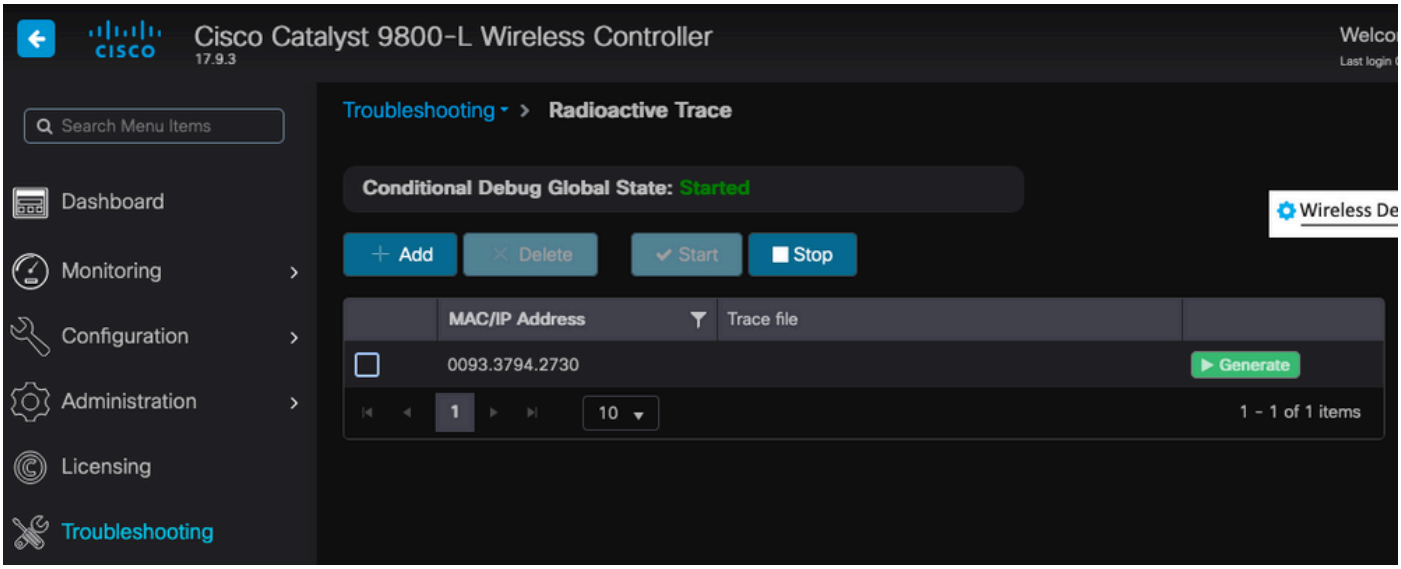
Schritt 1: Radioaktive Spur des interessierenden Endpunkts starten

Gehen Sie auf Ihrem Catalyst 9800 WLC zu Troubleshooting > Radioactive Traces, und klicken Sie auf die Schaltfläche Add, um die MAC-Adresse des Geräts einzugeben, dessen Datenverkehr entschlüsselt werden soll.

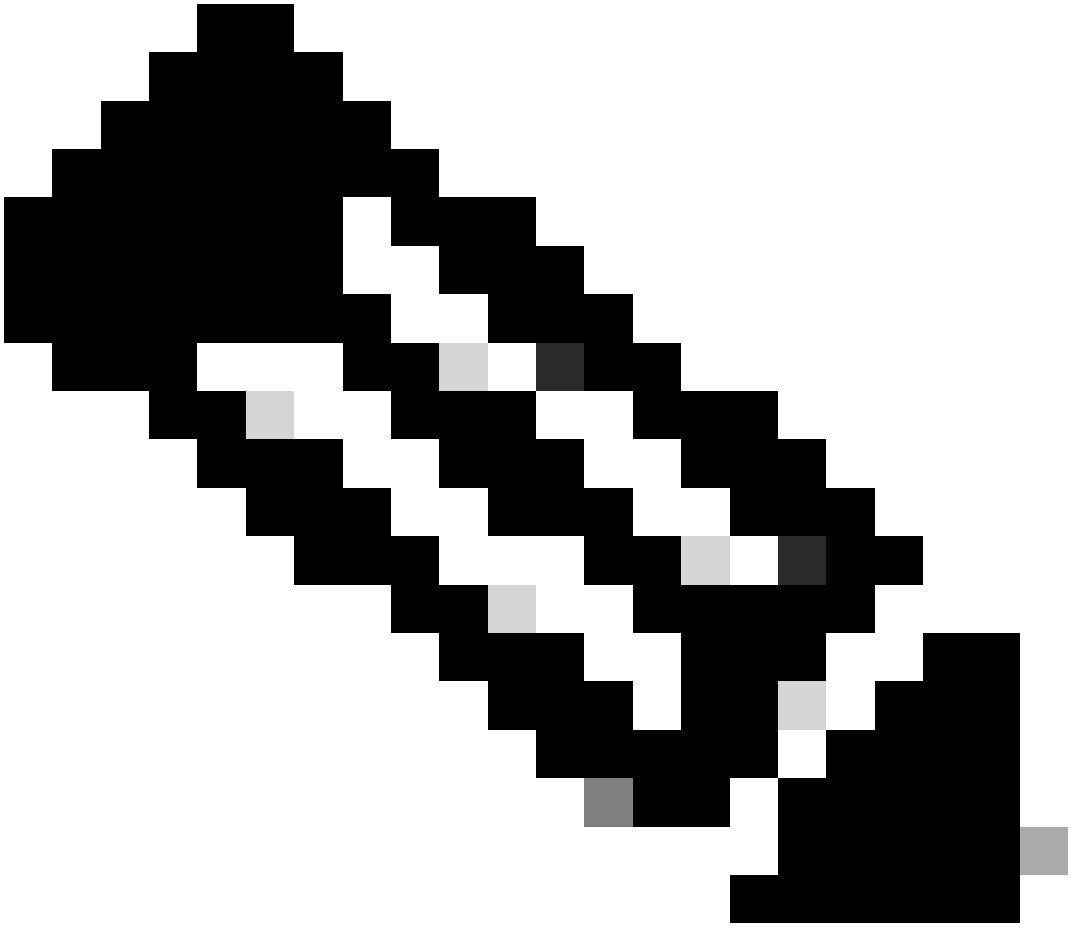


MAC-Adresse zur Liste der radioaktiven Spuren hinzugefügt

Klicken Sie nach dem Hinzufügen auf die Schaltfläche Start oben in der Liste, um Bedingtes Debuggen zu aktivieren. Dadurch können Sie die Informationen sehen, die auf der Datenebene ausgetauscht werden (hier ist das MSK).



Gerät wurde der Liste radioaktiver Spuren mit aktiviertem bedingtem Debugging hinzugefügt.

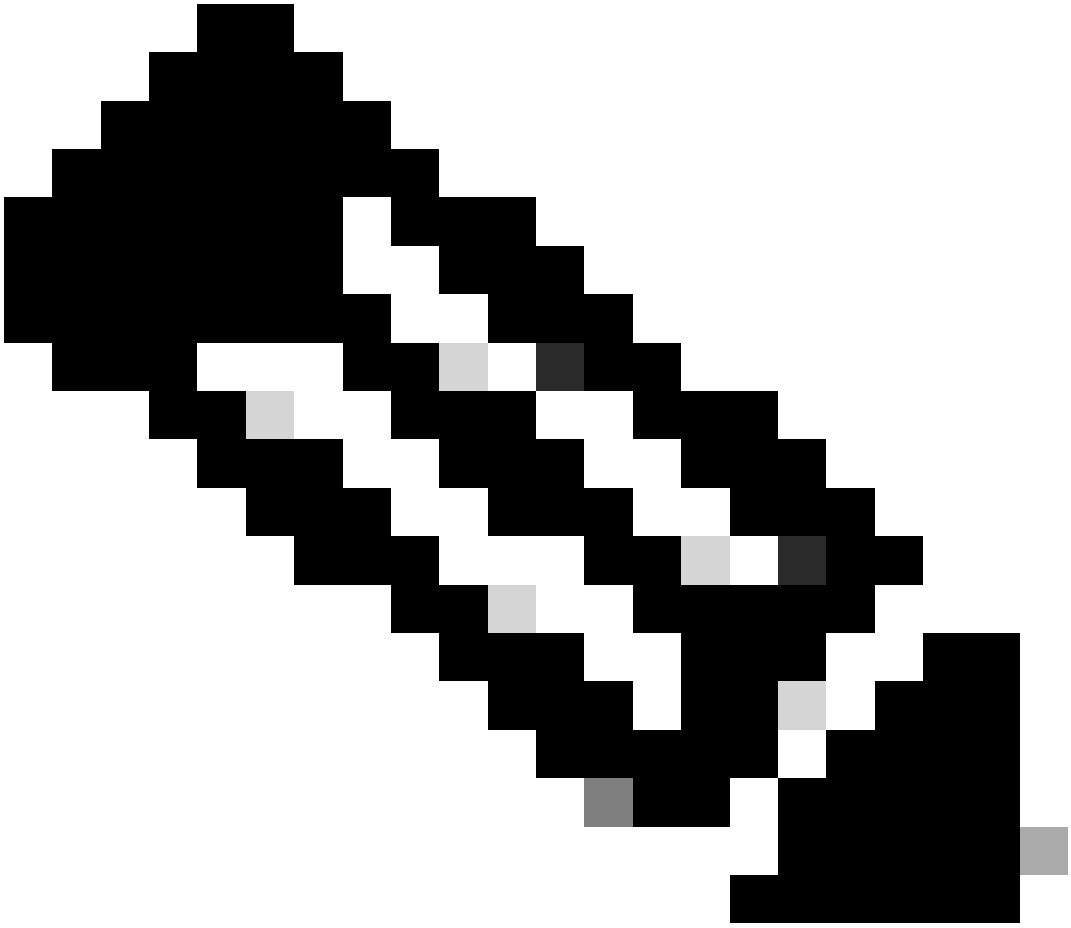


Hinweis: Wenn Sie das bedingte Debuggen nicht aktivieren, wird nur der Datenverkehr auf der Kontrollebene angezeigt, der das MSK nicht enthält. Weitere Informationen hierzu finden Sie im Abschnitt Bedingtes Debuggen und Radioaktive Ablaufverfolgung der Debug & Log Collection im Dokument Catalyst 9800 WLC Troubleshooting.

Schritt 2: Erhalten einer Over-the-Air-Paketerfassung

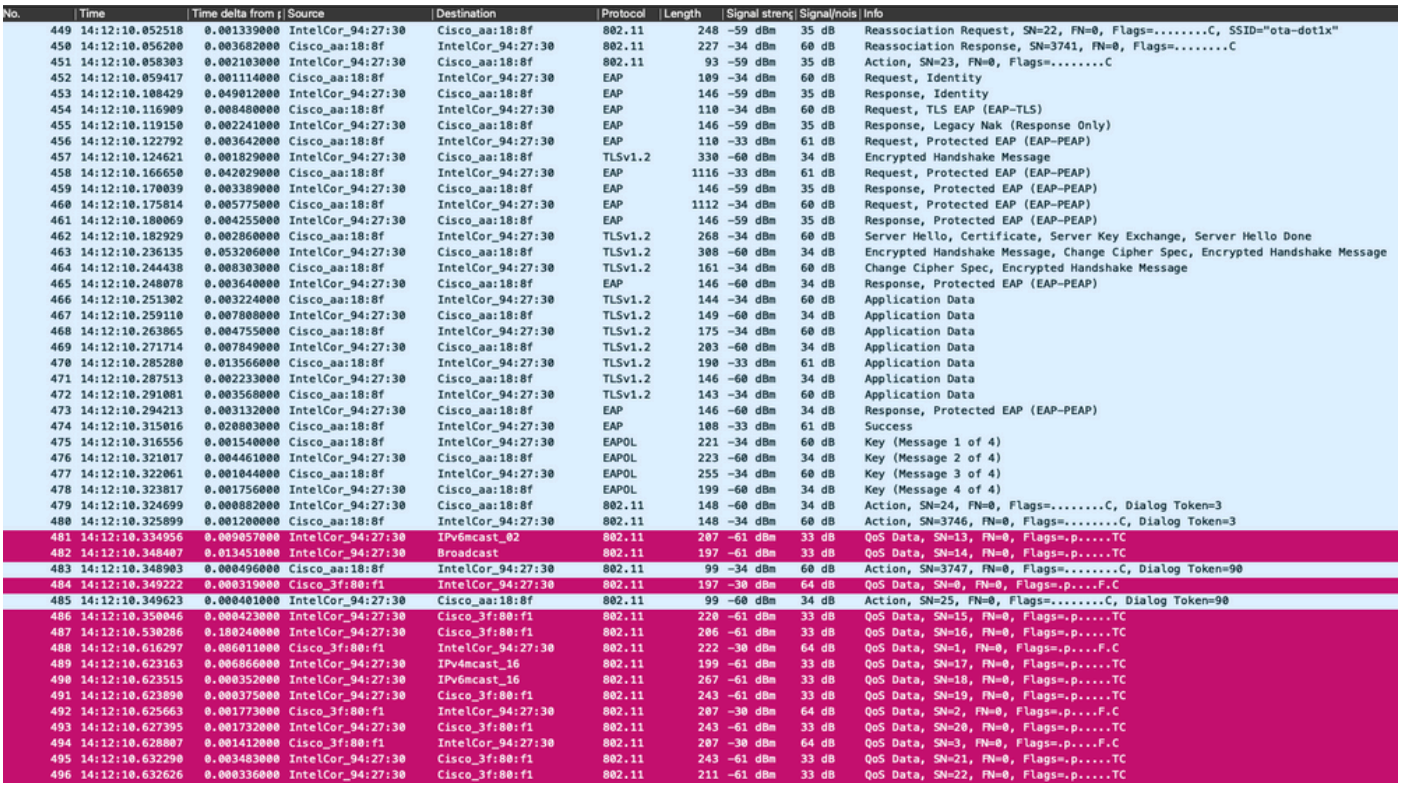
Starten Sie die Over-the-Air-Paketerfassung, und verbinden Sie Ihren Endpunkt mit dem 802.1X-WLAN.

Sie können diese Over-the-Air-Paketerfassung entweder mit einem Access Point im Sniffer-Modus oder mit einem Macbook mit dem integrierten Wireless Diagnostics-Tool erhalten.



Hinweis: Stellen Sie sicher, dass die Paketerfassung alle 802.11-Frames enthält. Am wichtigsten ist, dass der Vier-Wege-Handshake während des Vorgangs aufgefangen wird.

Beobachten Sie, wie der gesamte Datenverkehr nach dem Vier-Wege-Handshake (Pakete 475 bis 478) verschlüsselt wird.



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

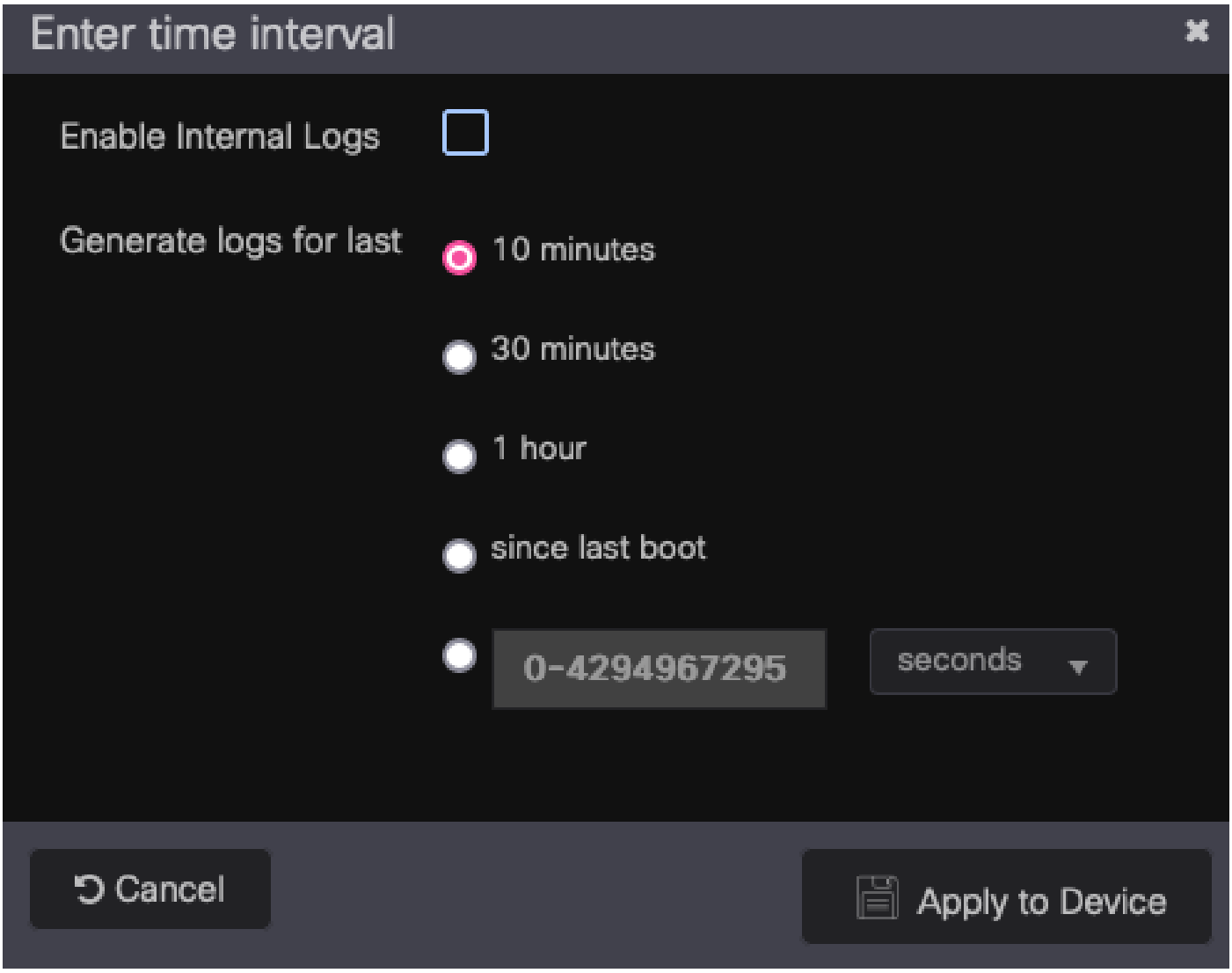
Verschlüsselter Wireless-Datenverkehr

Schritt 3: Generieren und Exportieren der radioaktiven Spur des Geräts

Klicken Sie auf derselben Seite wie in Schritt 1 auf die grüne Schaltfläche Generate (Generieren), sobald Sie den Wireless-Datenverkehr erfasst haben.

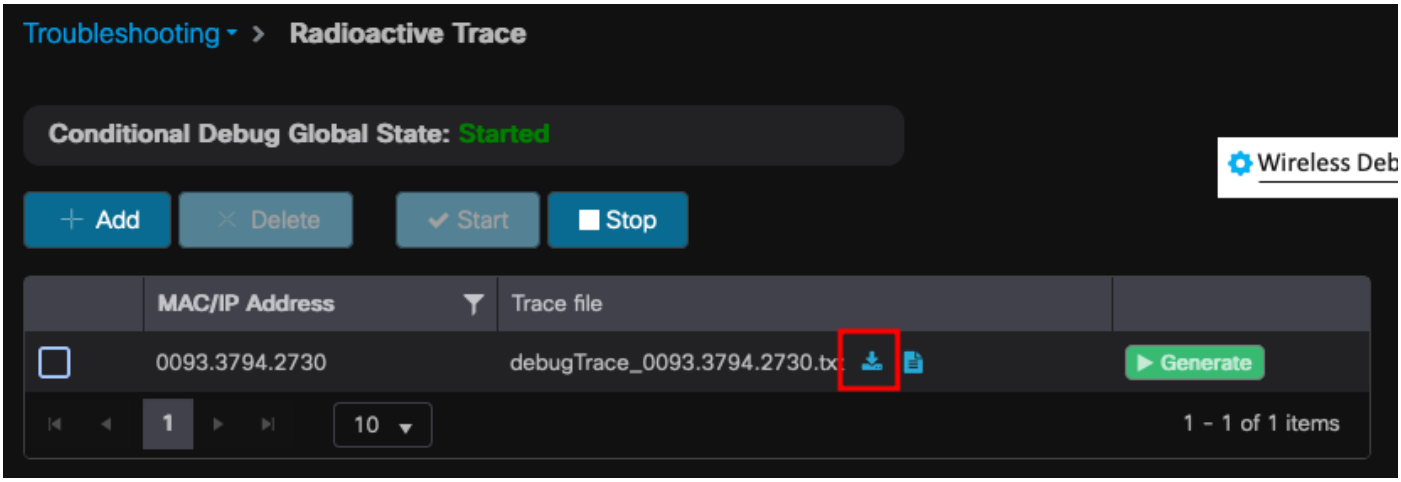
Wählen Sie im Zeitintervall-Popup-Fenster den Zeitrahmen aus, der Ihren Anforderungen entspricht. Interne Protokolle müssen hier nicht aktiviert werden.

Klicken Sie auf Auf Gerät anwenden, um die radioaktive Spur zu generieren.



Zeitintervall für RA Trace.

Sobald die Radioactive Trace fertig ist, wird neben dem Namen der Trace-Datei ein Download-Symbol angezeigt. Klicken Sie darauf, um Ihre Radioactive Trace herunterzuladen.



Radioactive Trace zum Download verfügbar.

Schritt 4: MSK aus der radioaktiven Spur abrufen

Öffnen Sie die heruntergeladene Radioactive Trace-Datei und suchen Sie nach dem eap-msk-Attribut nach der Access-Accept-Nachricht.

<#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
```

Der Wert, auf den die eap-msk-Zeichenfolge folgt, ist MSK. Kopieren Sie diese Datei, und

speichern Sie sie, um sie im nächsten Schritt zu verwenden.

<#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
```

Schritt 5: MSK als IEEE 802.11-Entschlüsselungsschlüssel in Wireshark hinzufügen

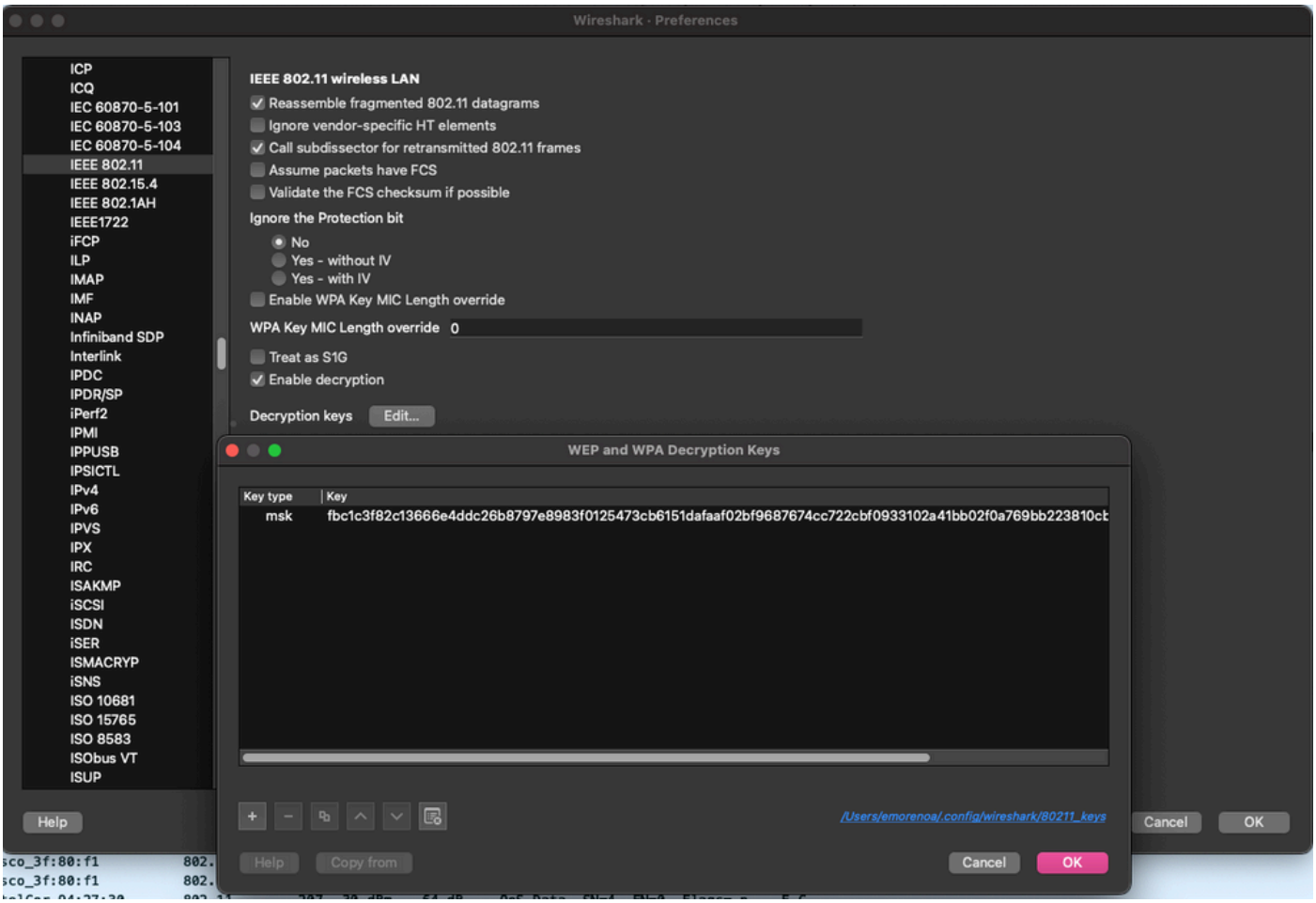
Gehen Sie auf Wireshark zu Wireshark > Preferences > Protocols > IEEE 802.11.

Aktivieren Sie das Kontrollkästchen "Entschlüsselung aktivieren", und wählen Sie dann Bearbeiten direkt neben Entschlüsselungsschlüssel aus.

Klicken Sie auf die "+"-Schaltfläche am unteren Rand, um einen neuen Entschlüsselungsschlüssel hinzuzufügen, und wählen Sie msk als Schlüsseltyp aus.

Fügen Sie den in Schritt 4 erhaltenen eap-msk-Wert (ohne Leerzeichen) ein.

Klicken Sie abschließend auf OK, um das Fenster Entschlüsselungsschlüssel zu schließen, und klicken Sie dann ebenfalls auf OK, um das Fenster Einstellungen zu schließen und den Entschlüsselungsschlüssel anzuwenden.



Entschlüsselungsschlüssel wurde den Wireshark-Einstellungen hinzugefügt.

Schritt 6: Analyse des entschlüsselten 802.1X-Datenverkehrs

Beobachten Sie, wie der Wireless-Datenverkehr jetzt sichtbar ist. Im Screenshot sehen Sie ARP-Datenverkehr (Pakete 482 und 484), DNS-Abfragen und -Antworten (Pakete 487 und 488), ICMP-Datenverkehr (Pakete 491 bis 497) und sogar den Start des Drei-Wege-Handshakes für eine TCP-Sitzung (Paket 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

Entschlüsselter Wireless-Datenverkehr

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.