Décrypter les captures de paquets en direct dans les SSID 802.1X

Table des matières

Introduction

Ce document décrit comment décrypter les captures de paquets en direct pour les WLAN 802.1X avec les outils de dépannage disponibles sur le WLC Catalyst 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment configurer un WLAN 802.1X dans le WLC Catalyst 9800
- Comment prendre des traces radioactives avec le débogage conditionnel activé dans le WLC Catalyst 9800
- Comment effectuer des captures de paquets Over-the-Air à l'aide d'un point d'accès en mode renifleur ou d'un Macbook avec son outil de diagnostic sans fil

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC Catalyst 9800-L, Cisco IOS® XE Cupertino 17.9.3
- Point d'accès Catalyst 9130AX en mode Sniffer

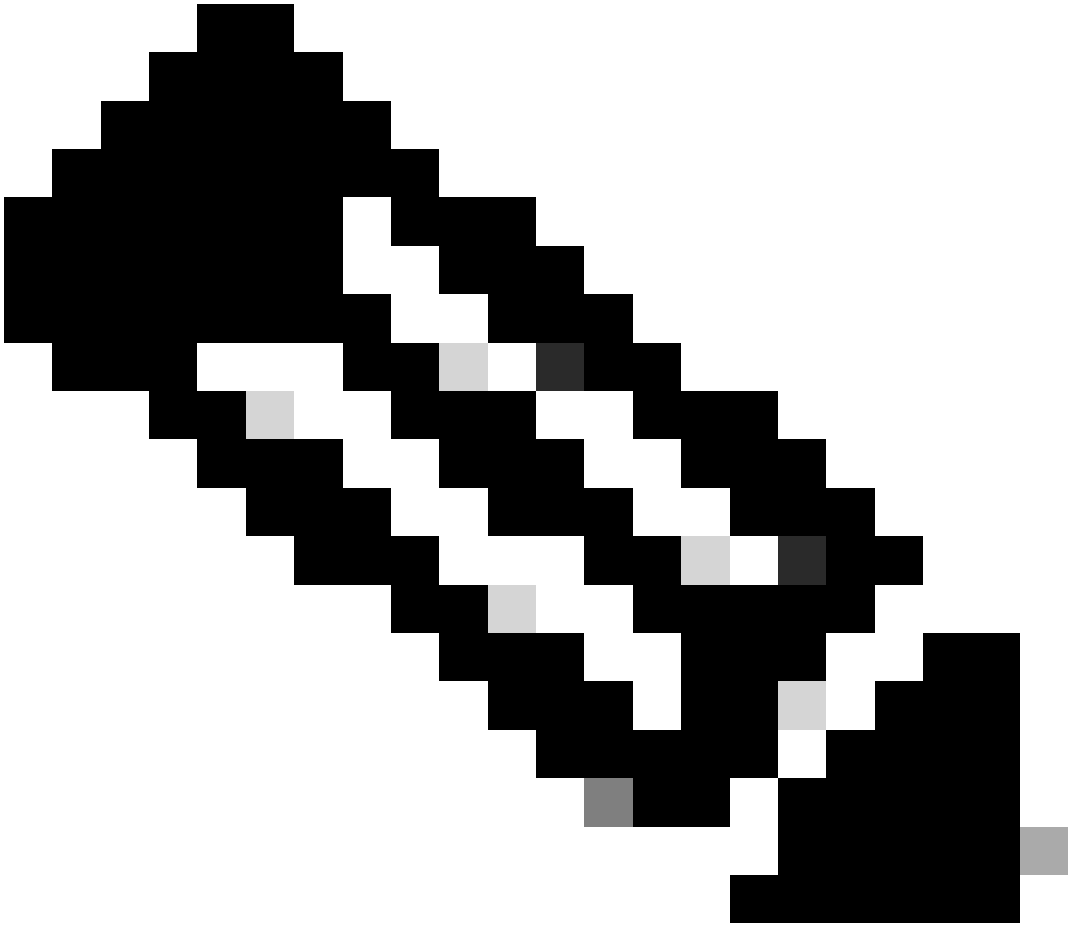
- Cisco ISE version 3.3
- Wireshark 4.0.8

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Une fois qu'une identité est validée via EAP+8021X, le trafic sans fil est chiffré à l'aide de la clé PTK (Pairwise Transient Key) générée à partir de la connexion entre le demandeur et l'authentificateur, qui utilise la clé PMK (Pairwise Master Key) à calculer. Cette clé PMK est dérivée de la clé de session principale (MSK). Le MSK est inclus dans les paires de valeurs d'attribut du message d'acceptation d'accès RADIUS (chiffré à l'aide du secret partagé RADIUS). Par conséquent, le trafic ne peut pas être vu de manière transparente lors d'une capture de paquets Over-the-Air, même si la connexion en quatre étapes est interceptée par un tiers.

Généralement, la génération de la clé PMK implique des captures de paquets dans le réseau câblé, la connaissance du secret partagé RADIUS et un certain codage pour extraire les valeurs d'intérêt. Au lieu de cela, avec cette méthode, l'un des outils disponibles pour dépanner le WLC (Radioactive Traces) du Catalyst 9800 est utilisé pour obtenir le MSK, qui peut ensuite être utilisé dans n'importe quel outil d'analyse de paquets bien connu, tel que Wireshark.

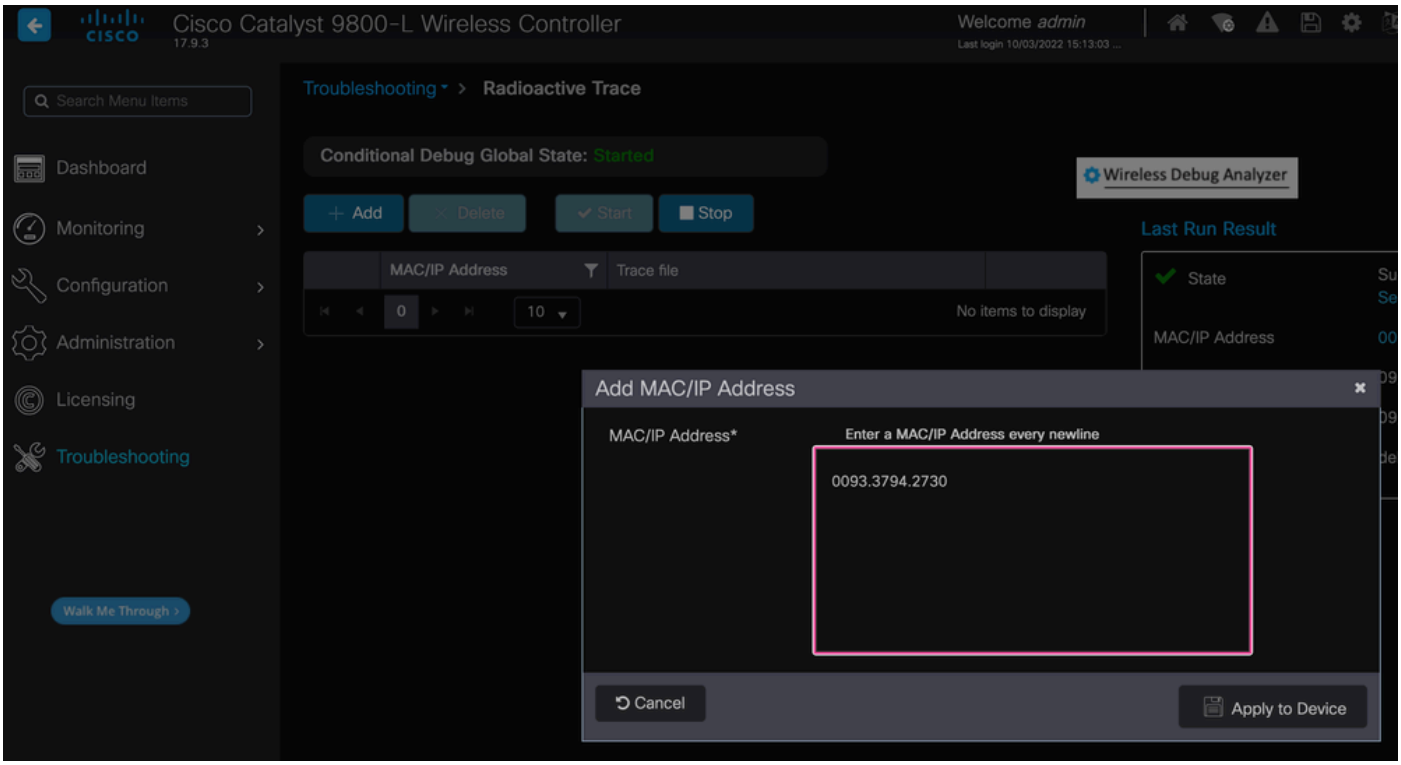


Remarque : cette procédure ne fonctionne que pour WPA2, car les informations nécessaires au calcul des clés PTK (Pairwise Transient Keys) sont échangées par liaison radio via la connexion en 4 étapes. Dans WPA3, l'authentification simultanée d'égaux (SAE) est effectuée par le biais de ce que l'on appelle la connexion Dragonfly.

Configurer

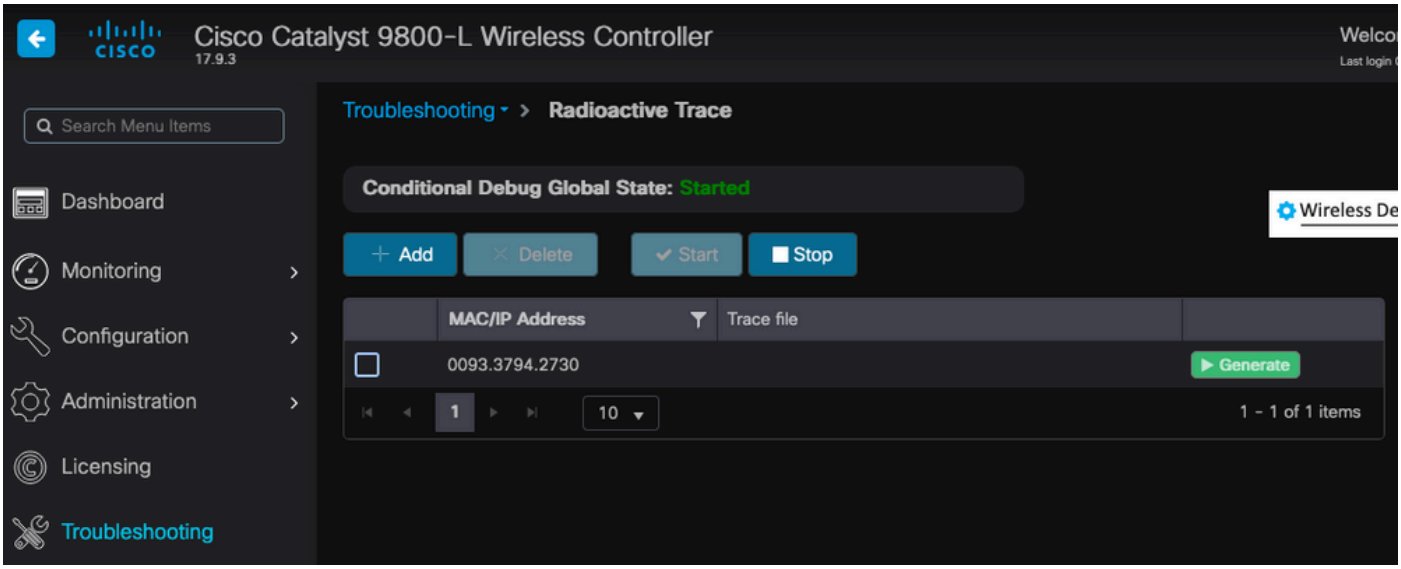
Étape 1. Démarrer le suivi radioactif du point d'extrémité concerné

Sur votre WLC Catalyst 9800, accédez à Troubleshooting > Radioactive Traces et cliquez sur le bouton Add pour taper l'adresse MAC du périphérique dont le trafic doit être décrypté.

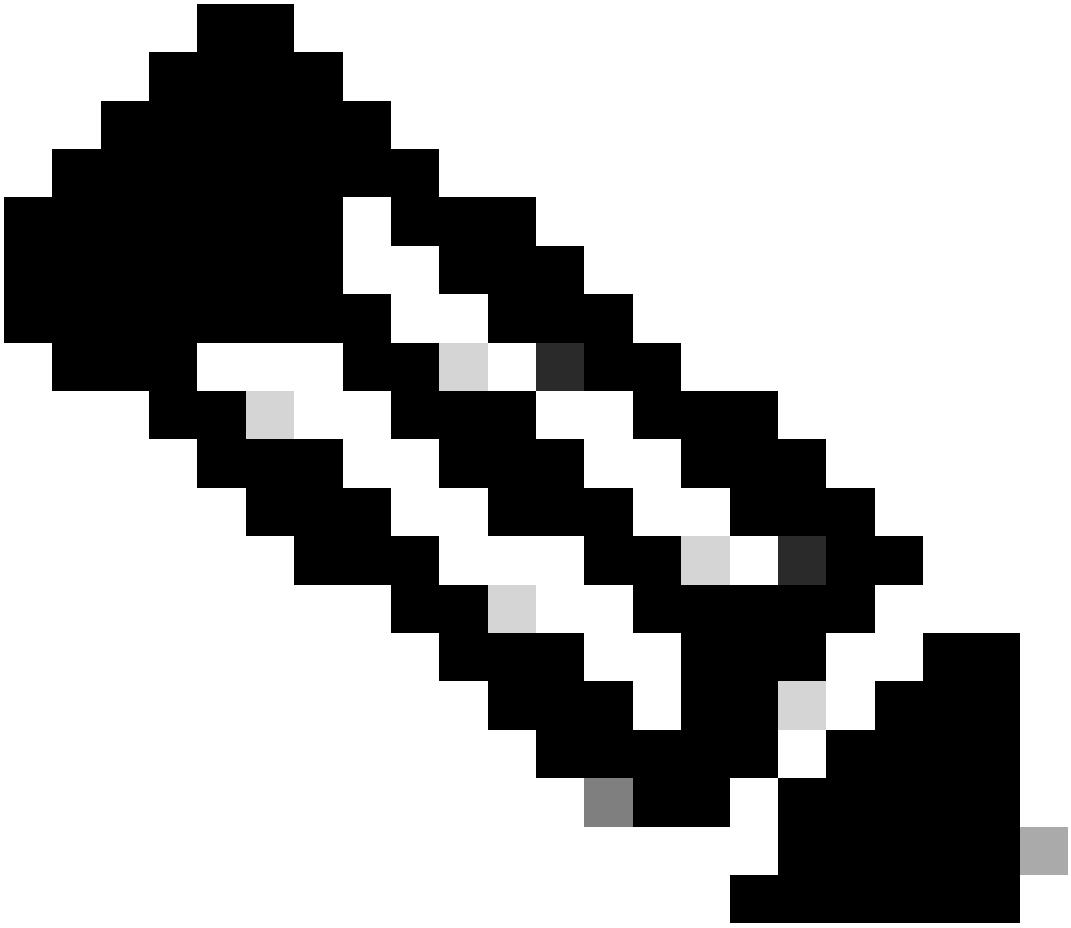


Adresse MAC ajoutée à la liste des traces radioactives

Une fois que vous l'avez ajouté, assurez-vous de cliquer sur le bouton Start en haut de la liste pour activer le débogage conditionnel. Cela vous permet de voir les informations échangées dans le plan de données (le MSK est ici).



Périphérique ajouté à la liste des traces radioactives avec le débogage conditionnel activé.

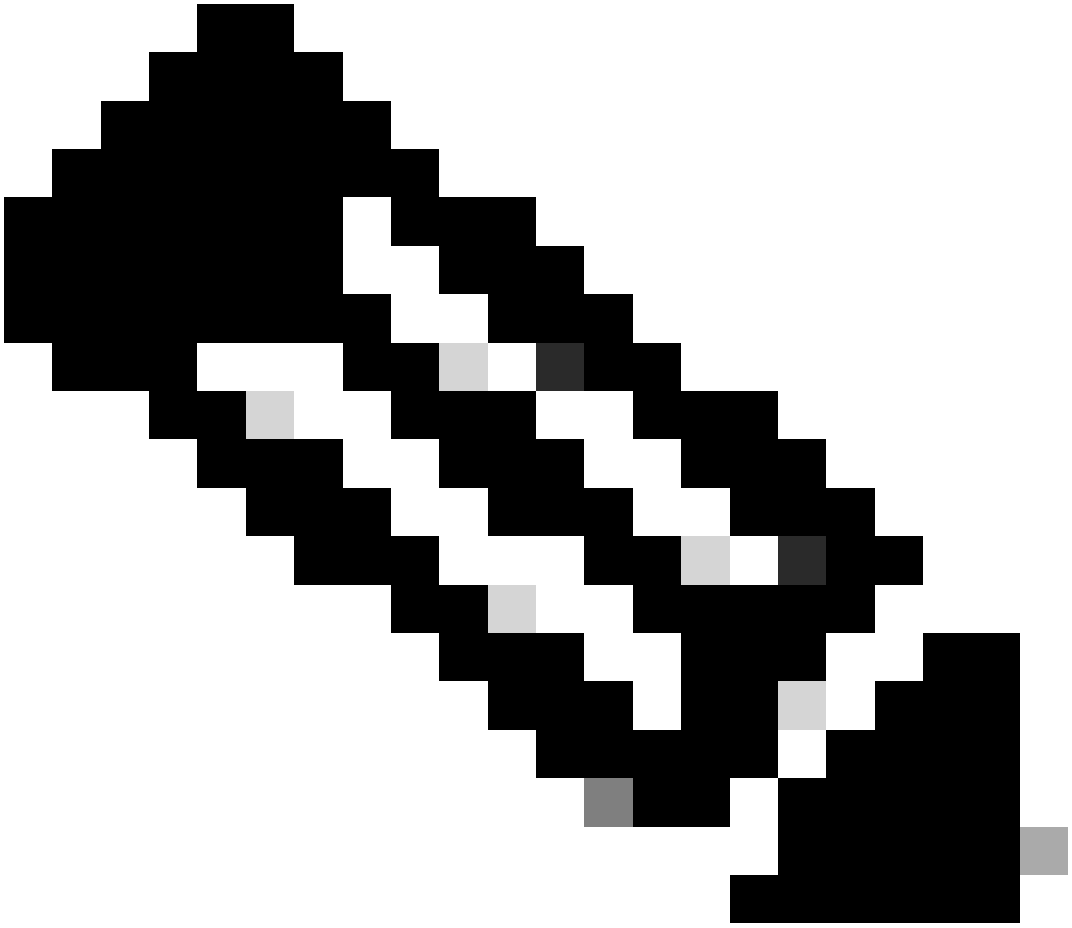


Remarque : si vous n'activez pas le débogage conditionnel, seul le trafic dans le plan de contrôle peut être vu, ce qui n'inclut pas le MSK. Référez-vous à la section Débogage conditionnel et suivi radioactif de la collection Debug & Log sur le document de dépannage du WLC Catalyst 9800 pour plus d'informations sur ceci.

Étape 2. Obtention d’une capture de paquets par liaison radio

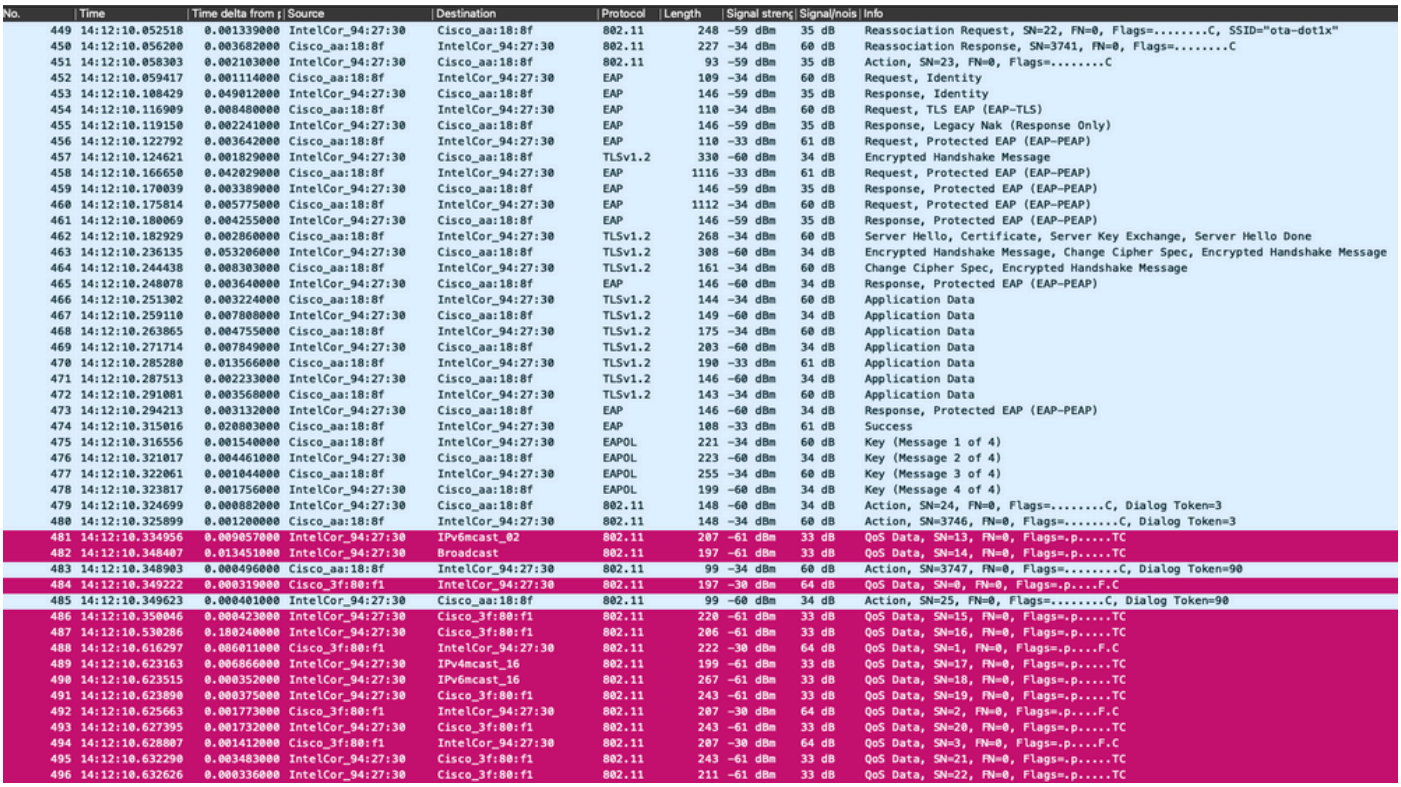
Lancez la capture de paquets en direct et connectez votre terminal au réseau local sans fil 802.1X.

Vous pouvez obtenir cette capture de paquets Over-the-Air en utilisant un point d'accès en mode Sniffer, ou avec un Macbook en utilisant son outil intégré de diagnostic sans fil.



Remarque : assurez-vous que la capture de paquets inclut toutes les trames 802.11. Plus important encore, il est impératif que la connexion en quatre étapes soit capturée au cours du processus.

Observez comment tout le trafic passé la connexion en quatre étapes (paquets 475 à 478) est chiffré.



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

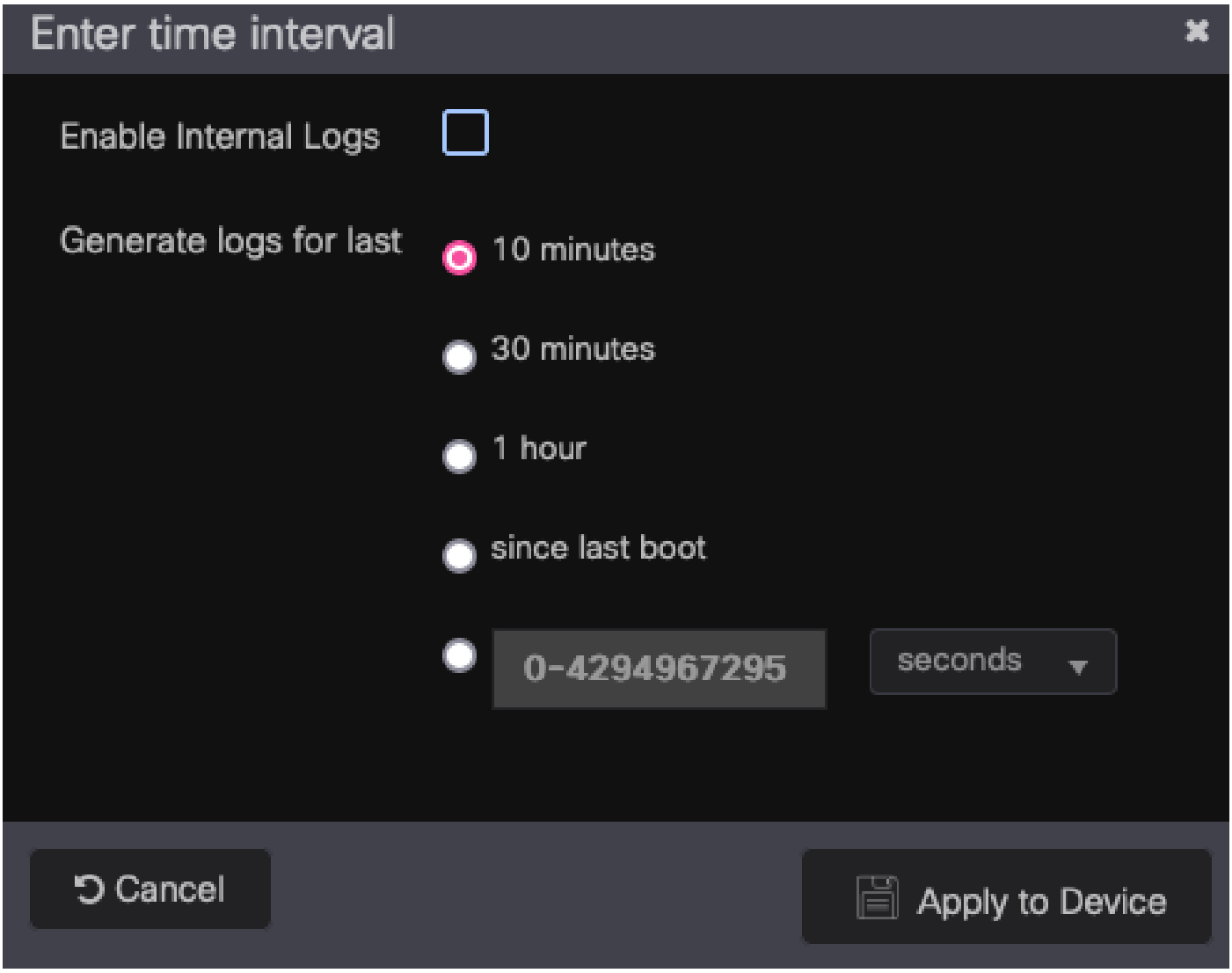
Trafic sans fil chiffré.

Étape 3. Générer et exporter le suivi radioactif du périphérique

Dans le même écran que l'étape 1, cliquez sur le bouton vert Generate une fois que vous avez capturé le trafic sans fil.

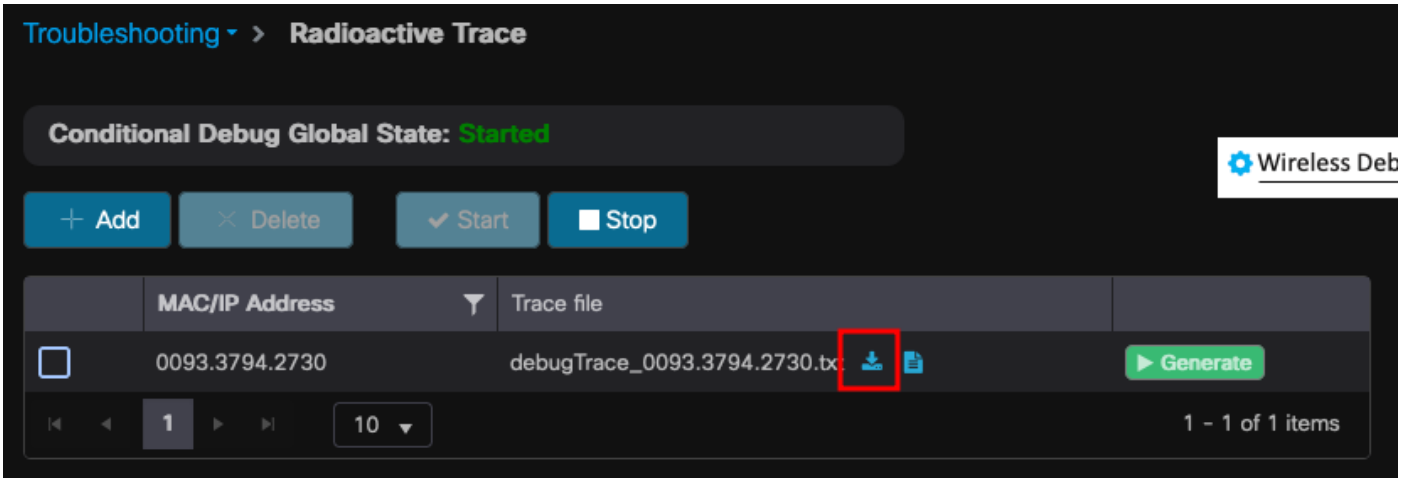
Dans la fenêtre contextuelle Intervalle de temps, sélectionnez le délai qui correspond à vos besoins. Il n'est pas nécessaire d'activer les journaux internes ici.

Cliquez sur Apply to Device pour générer le suivi radioactif.



Intervalle de temps pour RA Trace.

Une fois que le suivi radioactif est prêt, une icône de téléchargement s'affiche juste à côté du nom du fichier de suivi. Cliquez dessus pour télécharger votre suivi radioactif.



Radioactive Trace est disponible en téléchargement.

Étape 4. Obtenir le MSK à partir du suivi radioactif

Ouvrez le fichier de trace radioactif téléchargé et recherchez l'attribut eap-msk après le message Access-Accept.

<#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
```

La valeur suivie de la chaîne eap-msk est le MSK. Copiez-le et enregistrez-le pour l'utiliser à

l'étape suivante.

<#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

Étape 5. Ajoutez le MSK en tant que clé de déchiffrement IEEE 802.11 dans Wireshark

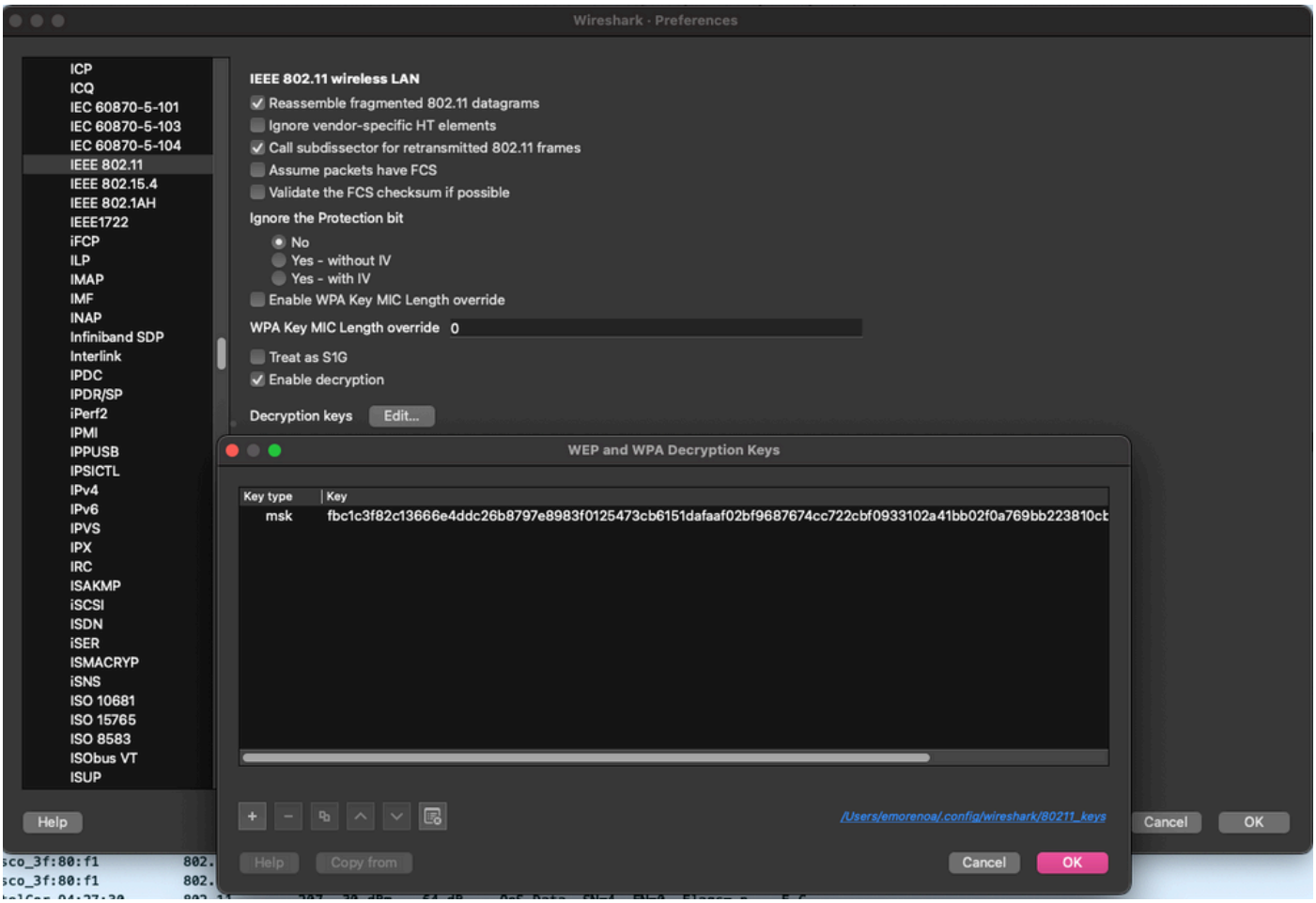
Sur Wireshark, accédez à Wireshark > Préférences > Protocoles > IEEE 802.11.

Cochez la case « Enable decryption » (Activer le décodage), puis sélectionnez Edit, juste à côté de Decryption keys (Clés de décodage).

Cliquez sur le bouton « + » en bas pour ajouter une nouvelle clé de déchiffrement et sélectionner msk comme type de clé.

Collez la valeur eap-msk obtenue à l'étape 4 (sans espaces).

Enfin, cliquez sur OK pour fermer la fenêtre Clés de déchiffrement, puis cliquez également sur OK pour fermer la fenêtre Préférences et appliquer la clé de déchiffrement.



Clé de décodage ajoutée aux préférences Wireshark.

Étape 6. Analyse du trafic 802.1X déchiffré

Observez comment le trafic sans fil est désormais visible. Dans la capture d'écran, vous pouvez voir le trafic ARP (paquets 482 et 484), les requêtes et réponses DNS (paquets 487 et 488), le trafic ICMP (paquets 491 à 497) et même le début de la connexion en trois étapes pour une session TCP (paquet 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

Trafic sans fil décrypté.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.