

# Decrittografa le acquisizioni di pacchetti via etere negli SSID 802.1X

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Passaggio 1. Avvia la traccia radioattiva dell'endpoint di interesse](#)

[Passaggio 2. Acquisizione di pacchetti via etere](#)

[Passaggio 3. Genera ed esporta la traccia radioattiva del dispositivo](#)

[Passaggio 4. Ottenere il codice MSK dalla traccia radioattiva](#)

[Passaggio 5. Aggiungere MSK come chiave di decrittografia IEEE 802.11 in Wireshark](#)

[Passaggio 6. Analisi del traffico 802.1X decrittografato](#)

---

## Introduzione

In questo documento viene descritto come decrittografare le acquisizioni di pacchetti via etere per WLAN 802.1X con gli strumenti di risoluzione dei problemi disponibili sul WLC di Catalyst 9800.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Come configurare una WLAN 802.1X in Catalyst 9800 WLC
- Come utilizzare le tracce radioattive con il debug condizionale abilitato nel WLC di Catalyst 9800
- Come acquisire pacchetti over-the-air utilizzando un access point in modalità sniffer o un Macbook con il suo strumento di diagnostica wireless

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst 9800-L WLC, Cisco IOS® XE Cupertino 17.9.3
- Access point Catalyst 9130AXE in modalità sniffer

- Cisco ISE versione 3.3
- Wireshark 4.0.8

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Una volta convalidata un'identità tramite EAP+8021X, il traffico wireless viene crittografato utilizzando la chiave temporanea Pairwise (PTK) generata dall'handshake tra il supplicant e l'autenticatore, che utilizza la chiave master Pairwise (PMK) per il calcolo. Questa chiave PMK è derivata dalla chiave di sessione master (MSK). Il codice MSK è incluso nelle coppie valore attributo del messaggio di accettazione dell'accesso RADIUS (crittografato utilizzando il segreto condiviso RADIUS). Di conseguenza, il traffico non può essere visto in modo trasparente in un'acquisizione di pacchetti over-the-air, anche se l'handshake a quattro vie viene intercettato da una terza parte.

In genere, la generazione della chiave PMK implica l'acquisizione dei pacchetti nella rete cablata, la conoscenza del segreto condiviso RADIUS e una certa codifica per estrarre i valori di interesse. Con questo metodo, uno degli strumenti disponibili per la risoluzione dei problemi sul Catalyst 9800 WLC (Radioactive Traces) viene usato per ottenere il MSK, che può essere usato in qualsiasi strumento conosciuto di analisi dei pacchetti, ad esempio Wireshark.



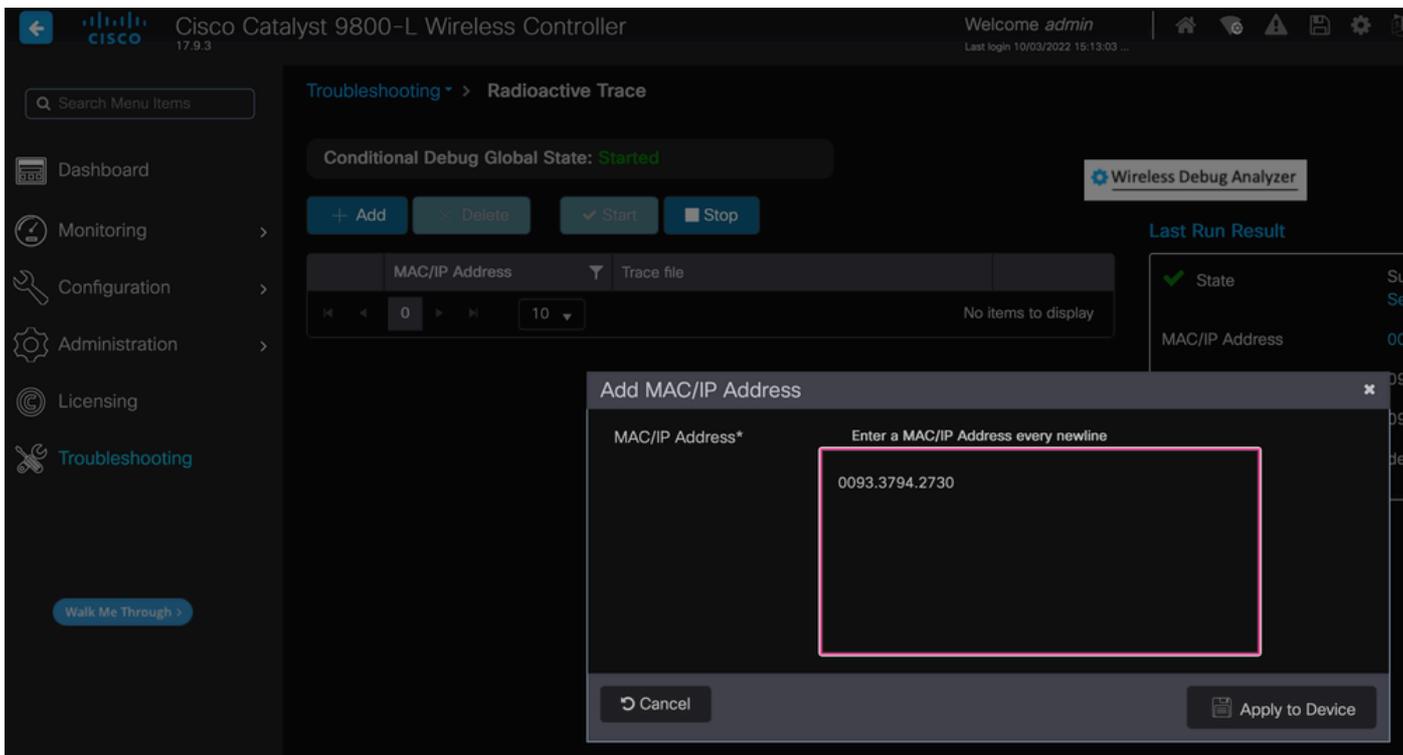
Nota: questa procedura funziona solo per WPA2, poiché le informazioni necessarie per calcolare le chiavi transitorie Pairwise (PTK) vengono scambiate via etere tramite handshake a 4 vie. In WPA3, invece, l'autenticazione simultanea di Equals (SAE) viene eseguita attraverso quello che è noto come handshake Dragonfly.

---

## Configurazione

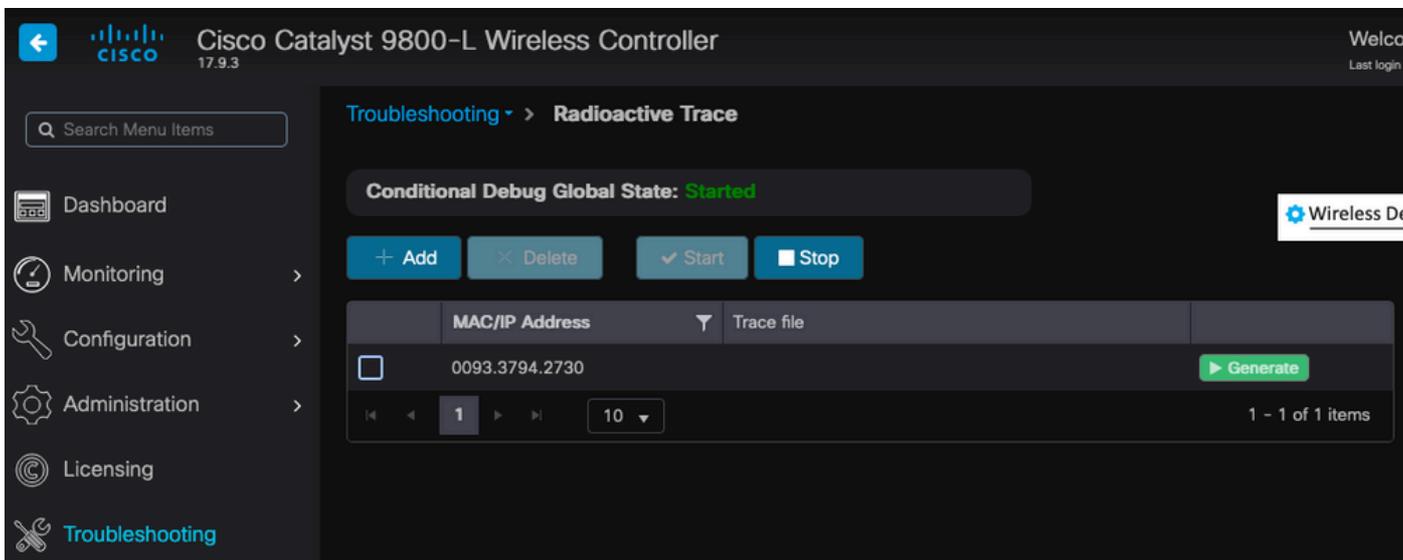
### Passaggio 1. Avvia la traccia radioattiva dell'endpoint di interesse

Sul proprio Catalyst 9800 WLC, andare a Risoluzione dei problemi > Tracce radioattive e fare clic sul pulsante Add per digitare l'indirizzo MAC del dispositivo il cui traffico deve essere decriptato.



Indirizzo MAC aggiunto all'elenco delle tracce radioattive

Dopo averlo aggiunto, accertarsi di fare clic sul pulsante Start all'inizio dell'elenco per abilitare il debug condizionale. In questo modo è possibile visualizzare le informazioni scambiate nel data plane (il codice MSK si trova qui).



Dispositivo aggiunto all'elenco di tracce radioattive con debug condizionale abilitato.



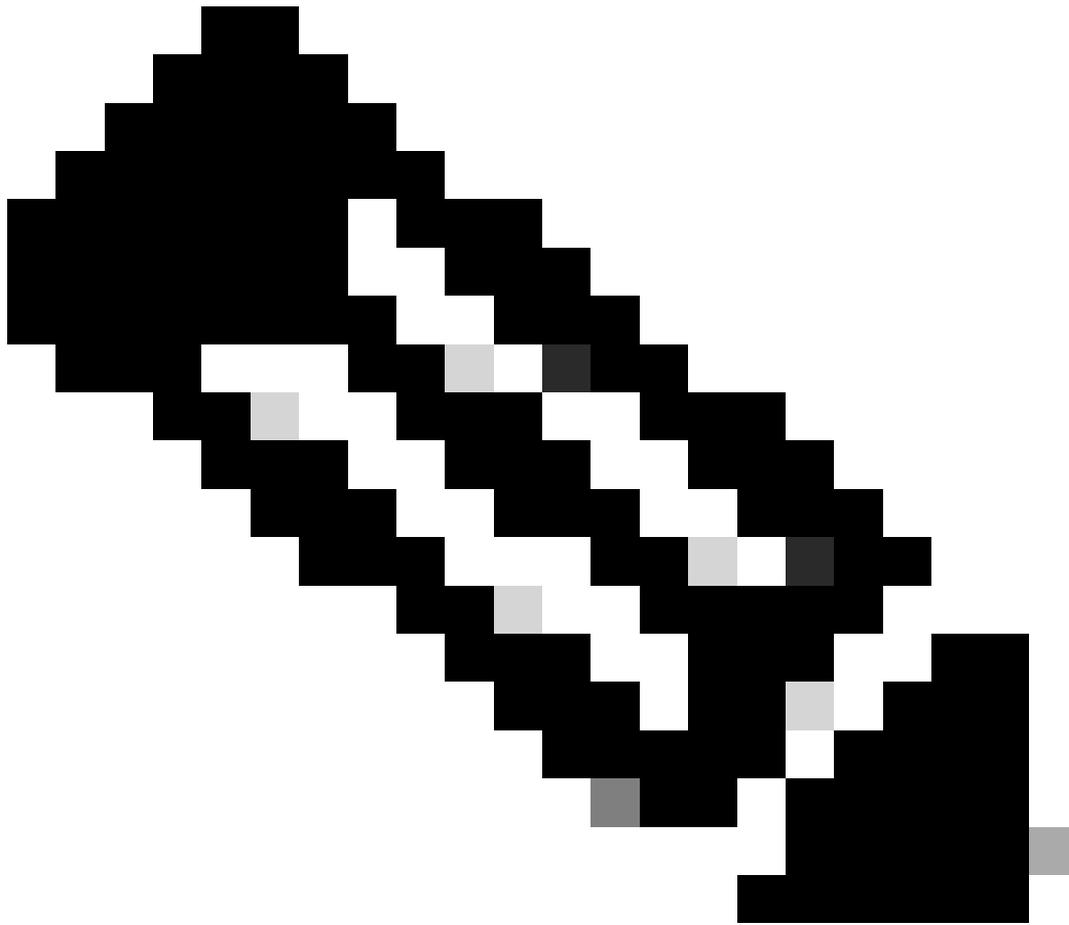
Nota: se non si abilita il debug condizionale, sarà possibile visualizzare solo il traffico nel control plane, che non include il codice MSK. Per ulteriori informazioni, consultare la sezione [Debug condizionale e traccia radioattiva](#) del [documento](#) sulla [risoluzione dei problemi di Debug e Log Collection sul Catalyst 9800 WLC](#).

---

## Passaggio 2. Acquisizione di pacchetti via etere

Avviare l'acquisizione dei pacchetti via etere e collegare l'endpoint alla WLAN 802.1X.

È possibile acquisire questo pacchetto over-the-air [utilizzando un Access Point in modalità Sniffer](#), o con un [Macbook utilizzando lo strumento integrato Wireless Diagnostics](#).



Nota: assicurarsi che l'acquisizione del pacchetto includa tutti i frame 802.11. Ma soprattutto, è fondamentale che la stretta di mano a quattro vie venga acquisita durante il processo.

---

Osservare come tutto il traffico che supera l'handshake a quattro vie (pacchetti da 475 a 478) è crittografato.

No.	Time	Time delta from j	Source	Destination	Protocol	Length	Signal strength	Signal/noise	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	TLV1.2	330	-60 dBm	34 dB	Encrypted Handshake Message
458	14:12:10.166650	0.042829000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	1116	-33 dBm	61 dB	Request, Protected EAP (EAP-PEAP)
459	14:12:10.170839	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	TLV1.2	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	TLV1.2	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	TLV1.2	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	TLV1.2	144	-34 dBm	60 dB	Application Data
467	14:12:10.259110	0.007800000	IntelCor_94:27:30	Cisco_aa:18:8f	TLV1.2	149	-60 dBm	34 dB	Application Data
468	14:12:10.263865	0.004755000	Cisco_aa:18:8f	IntelCor_94:27:30	TLV1.2	175	-34 dBm	60 dB	Application Data
469	14:12:10.271714	0.007849000	IntelCor_94:27:30	Cisco_aa:18:8f	TLV1.2	203	-60 dBm	34 dB	Application Data
470	14:12:10.285280	0.013566000	Cisco_aa:18:8f	IntelCor_94:27:30	TLV1.2	190	-33 dBm	61 dB	Application Data
471	14:12:10.287513	0.002233000	IntelCor_94:27:30	Cisco_aa:18:8f	TLV1.2	146	-60 dBm	34 dB	Application Data
472	14:12:10.291081	0.003560000	Cisco_aa:18:8f	IntelCor_94:27:30	TLV1.2	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	IntelCor_94:27:30	Cisco_aa:18:8f	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	0.001750000	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_62	802.11	287	-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	14:12:10.330286	0.100240000	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	14:12:10.316297	0.008611000	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	0.008966000	IntelCor_94:27:30	IPv6mcast_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	14:12:10.628007	0.001413000	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	0.000360000	IntelCor_94:27:30	Cisco_3f:80:f1	802.11	211	-61 dBm	33 dB	QoS Data, SN=22, FN=0, Flags=p.....TC

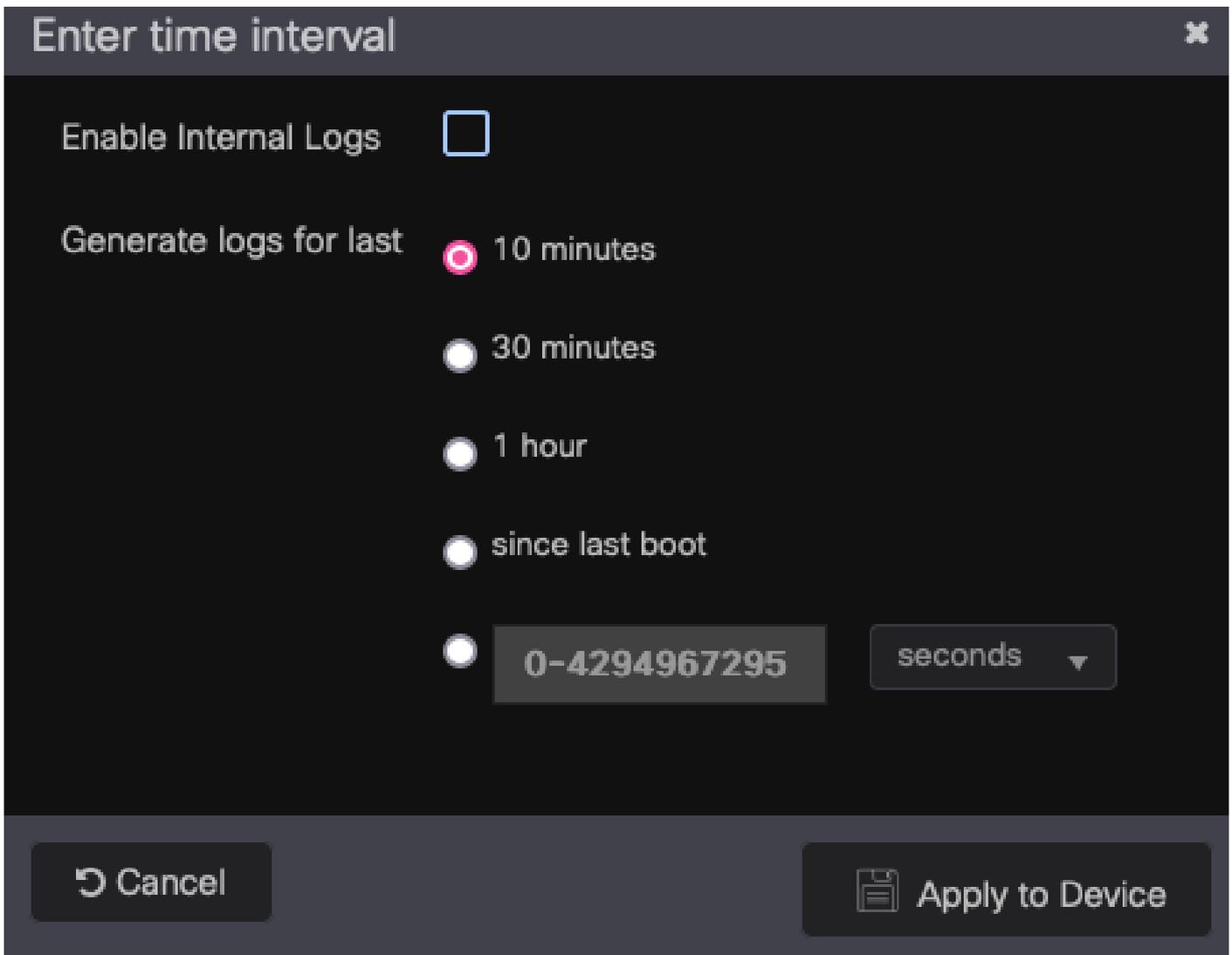
Traffico wireless crittografato.

### Passaggio 3. Genera ed esporta la traccia radioattiva del dispositivo

Nella stessa schermata del Passaggio 1, fare clic sul pulsante verde Genera una volta acquisito il traffico wireless.

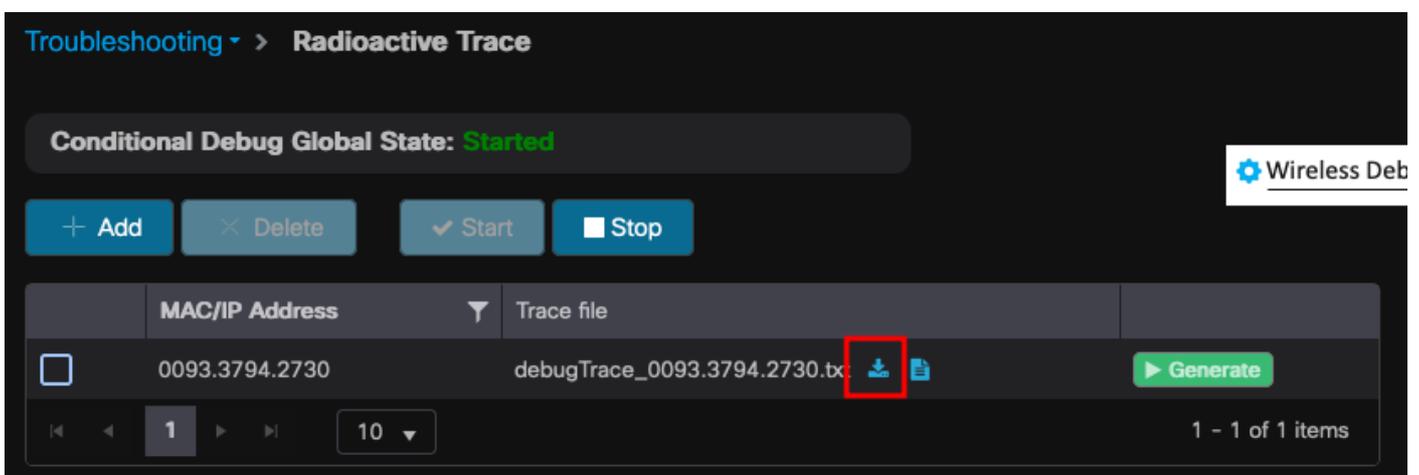
Nella finestra a comparsa Intervallo di tempo, selezionare l'intervallo di tempo che corrisponde alle proprie esigenze. Non è necessario abilitare i registri interni.

Fare clic su Applica a dispositivo per generare la traccia radioattiva.



Intervallo di tempo per la traccia RA.

Quando la traccia radioattiva è pronta, accanto al nome del file di traccia viene visualizzata un'icona di download. Fare clic su di esso per scaricare la traccia radioattiva.



Traccia radioattiva disponibile per il download.

Passaggio 4. Ottenere il codice MSK dalla traccia radioattiva

Aprire il file di traccia radioattiva scaricato e cercare l'attributo eap-msk dopo il messaggio 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

Il valore seguito dalla stringa eap-msk è MSK. Copiare e salvare il file per utilizzarlo nel passaggio

successivo.

<#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

## Passaggio 5. Aggiungere MSK come chiave di decrittografia IEEE 802.11 in Wireshark

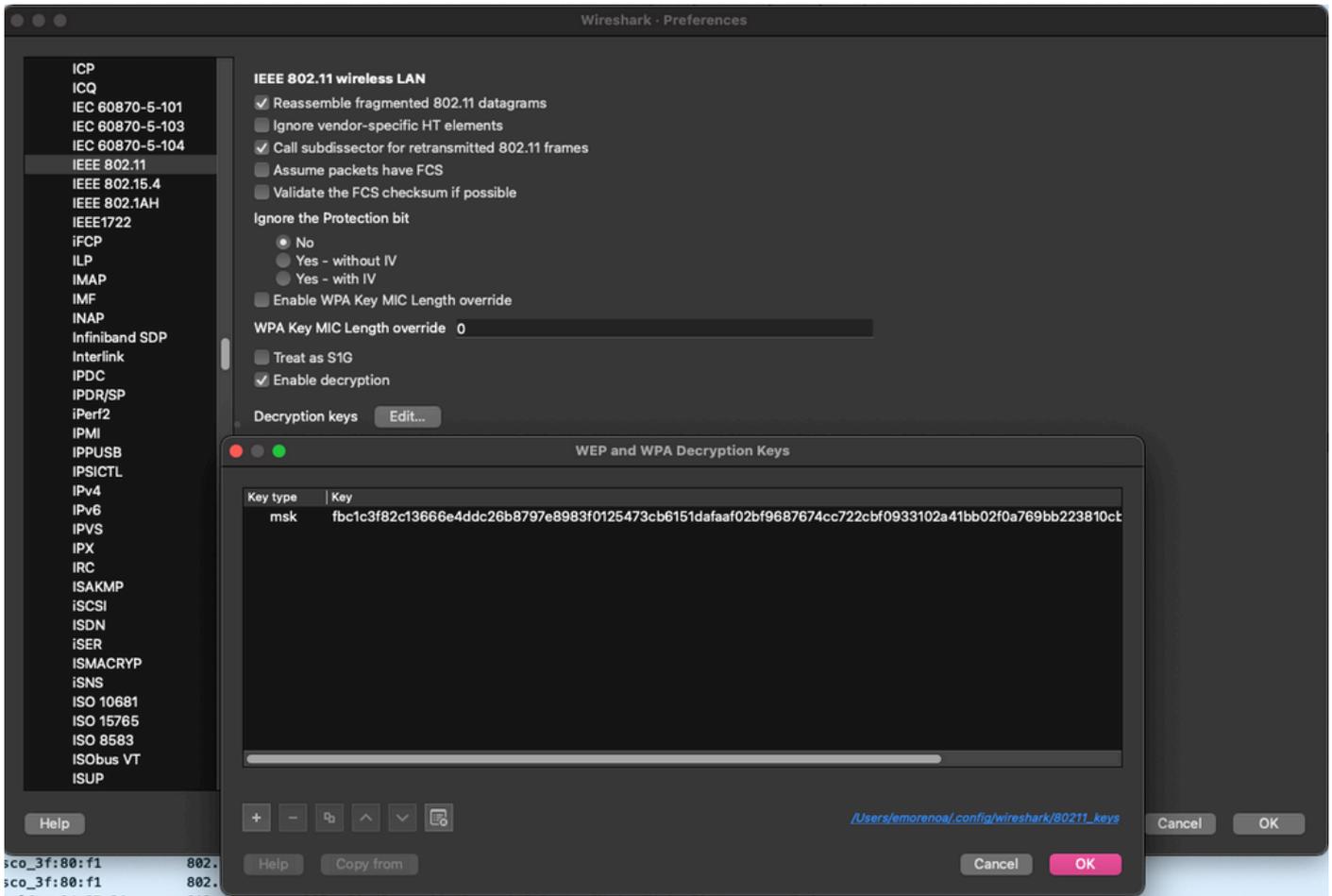
Su Wireshark, selezionare Wireshark > Preferences > Protocols > IEEE 802.11.

Selezionare la casella "Abilita decrittografia", quindi selezionare Modifica, accanto a Chiavi di decrittografia.

Fare clic sul pulsante "+" in basso per aggiungere una nuova chiave di decrittografia e selezionare msk come tipo di chiave.

Incollare il valore eap-msk ottenuto al punto 4 (senza spazi).

Infine, fare clic su OK per chiudere la finestra Chiavi di decrittografia e quindi fare clic su OK per chiudere la finestra Preferenze e applicare la chiave di decrittografia.



Chiave di decrittografia aggiunta alle preferenze di wireshark.

## Passaggio 6. Analisi del traffico 802.1X decrittografato

Osservate come il traffico wireless è ora visibile. Nello screenshot, è possibile vedere il traffico ARP (pacchetti 482 e 484), le query e le risposte DNS (pacchetti 487 e 488), il traffico ICMP (pacchetti da 491 a 497) e persino l'avvio dell'handshake a tre vie per una sessione TCP (pacchetto 507).

No.	Time	Time delta from j	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	14:12:10.056280	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	14:12:10.058383	0.002183000	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	118	-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	118	-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	338	-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	14:12:10.178039	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	14:12:10.180669	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	0.053260000	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	14:12:10.251382	0.003224000	Cisco_aa:18:8f	IntelCor_94:27:30	TLSv1.2	144	-34 dBm	60 dB	Application Data
467	14:12:10.259110	0.007800000	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	198	-33 dBm	61 dB	Application Data
471	14:12:10.287531	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	188	-33 dBm	61 dB	Success
475	14:12:10.348487	0.013451000	IntelCor_94:27:30	Broadcast	ARP	197	-61 dBm	33 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	0.001040000	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::f902:12		ICMPv6	207	-61 dBm	33 dB	Router Solicitation from 00:93:37:94:27:30
482	14:12:10.348487	0.013451000	IntelCor_94:27:30	Broadcast	ARP	197	-61 dBm	33 dB	Who has 172.16.5.1? Tel: 172.16.5.66
483	14:12:10.348983	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	172.18.100.43	DNS	228	-61 dBm	33 dB	Standard query 0x3c48 A www.msftconnecttest.com
487	14:12:10.530286	0.100240000	172.16.5.66	172.18.100.43	DNS	206	-61 dBm	33 dB	Standard query 0xad51 A cisco.com
488	14:12:10.516297	0.006011000	172.18.100.43	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	0.006860000	172.16.5.66	224.0.0.22	ICMPv3	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	14:12:10.623155	0.000352000	fe80::badf:865b:f10::f902:16		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	0.001730000	10.152.216.103	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 581)
497	14:12:10.632626	0.000000000	10.152.216.145	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	0.000000000	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	172.18.100.43	172.16.5.66	DNS	364	-30 dBm	64 dB	Standard query response 0x3c48 A www.msftconnecttest.com ONAME ncsi-geo.trafficmanager.net ONAME www.msft
506	14:12:10.748179	0.000347000	172.18.100.43	172.16.5.66	DNS	364	-30 dBm	64 dB	Standard query response 0x3c48 A www.msftconnecttest.com ONAME ncsi-geo.trafficmanager.net ONAME www.msft
507	14:12:10.750548	0.002309000	172.16.5.66	23.218.218.158	TCP	203	-61 dBm	33 dB	50781 - 80 [SYN] Seq=0 Min=65520 Len=0 MSS=1260 WS=256 SACK_PERM

Traffico wireless decrittografato.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).