

802.1X SSID에서 Over-the-Air 패킷 캡처 해독

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1단계. 관심 엔드포인트의 방사능 추적 시작](#)

[2단계. Over-the-Air 패킷 캡처 얻기](#)

[3단계. 디바이스의 방사선 추적 생성 및 내보내기](#)

[4단계. Radioactive Trace\(방사능 흔적\)에서 MSK 얻기](#)

[5단계. Wireshark에서 MSK를 IEEE 802.11 암호 해독 키로 추가](#)

[6단계. 해독된 802.1X 트래픽 분석](#)

소개

이 문서에서는 Catalyst 9800 WLC에서 사용 가능한 문제 해결 툴을 사용하여 802.1X WLAN에 대한 OTA(Over-the-Air) 패킷 캡처를 해독하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Catalyst 9800 WLC에서 802.1X WLAN을 구성하는 방법
- Catalyst 9800 WLC에서 조건부 디버깅을 활성화하여 방사성 추적을 수행하는 방법
- 스니퍼 모드의 액세스 포인트 또는 무선 진단 도구가 있는 Macbook을 사용하여 OTA(Over-the-Air) 패킷 캡처를 가져오는 방법

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9800-L WLC, Cisco IOS® XE Cupertino 17.9.3
- 스니퍼 모드의 Catalyst 9130AX Access Point
- Cisco ISE 버전 3.3
- Wireshark 4.0.8

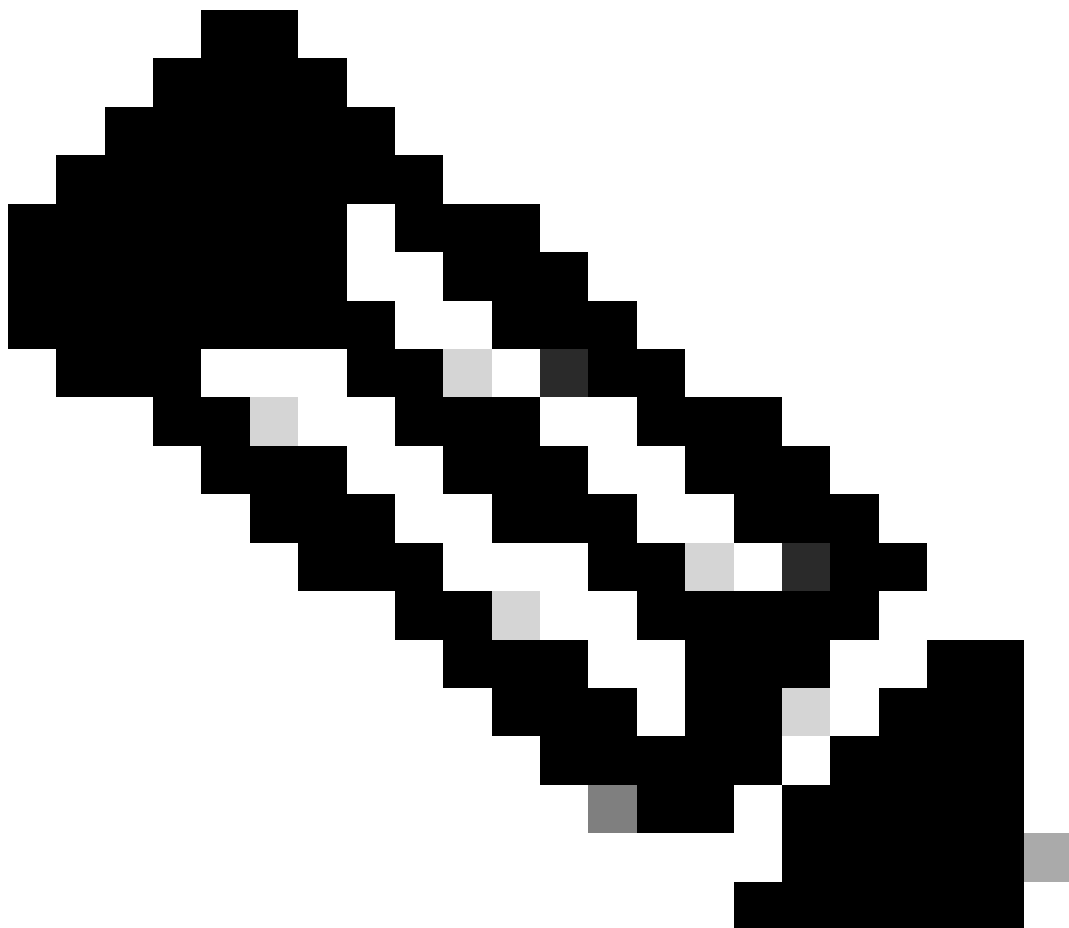
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

EAP+8021X를 통해 ID가 검증되면 신청자와 인증자 간의 핸드셰이크에서 생성된 PTK(Pairwise Transient Key)를 사용하여 무선 트래픽이 암호화됩니다. PTK는 PMK(Pairwise Master Key)를 사용하여 계산됩니다. 이 PMK는 MSK(마스터 세션 키)에서 파생됩니다. MSK는 RADIUS Access-Accept 메시지(RADIUS 공유 암호를 사용하여 암호화됨)의 특성 값 쌍에 포함됩니다. 따라서 4방향 핸드셰이크가 제3자에 의해 가로채어지더라도 OTA(Over-the-Air) 패킷 캡처에서 트래픽을 투명하게 볼 수 없습니다.

일반적으로, PMK의 생성은 유선 네트워크에서 취해지는 패킷 캡처, RADIUS 공유 비밀에 대한 지식 및 관심 값을 추출하기 위한 일부 코딩을 의미합니다. 대신 이 방법을 사용하면 Catalyst 9800 WLC(Radioactive Traces)에서 문제 해결에 사용할 수 있는 도구 중 하나를 사용하여 MSK를 얻은 다음 Wireshark와 같은 잘 알려진 패킷 분석 도구에서 사용할 수 있습니다.



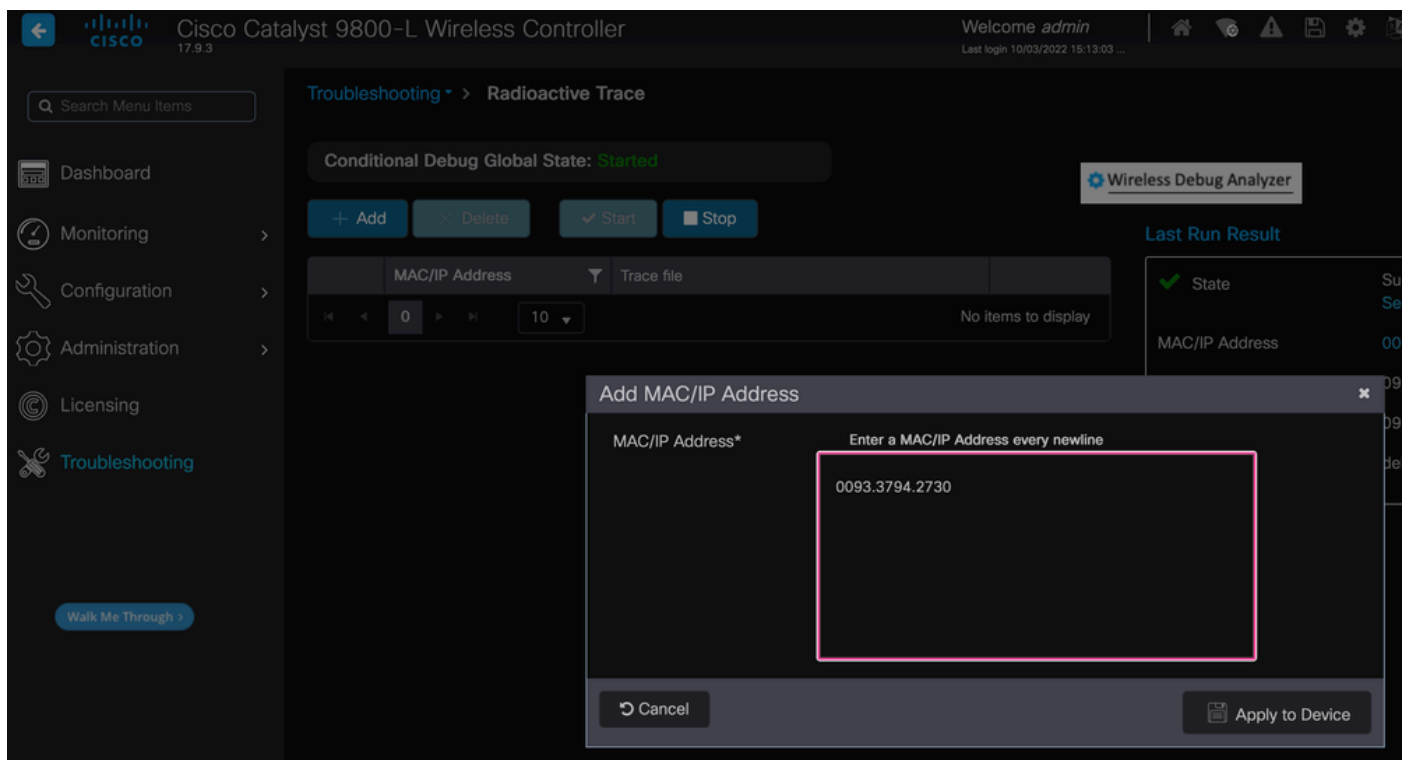
참고: PTK(Pairwise Transient Keys)를 계산하는 데 필요한 정보가 4방향 핸드셰이크를 통

해 공중을 통해 교환되므로 이 절차는 WPA2에서만 작동합니다. 대신 WPA3에서는 Dragonfly 핸드셰이크라고 하는 것을 통해 SAE(Simultaneous Authentication of Equals)가 수행됩니다.

구성

1단계. 관심 엔드포인트의 방사능 추적 시작

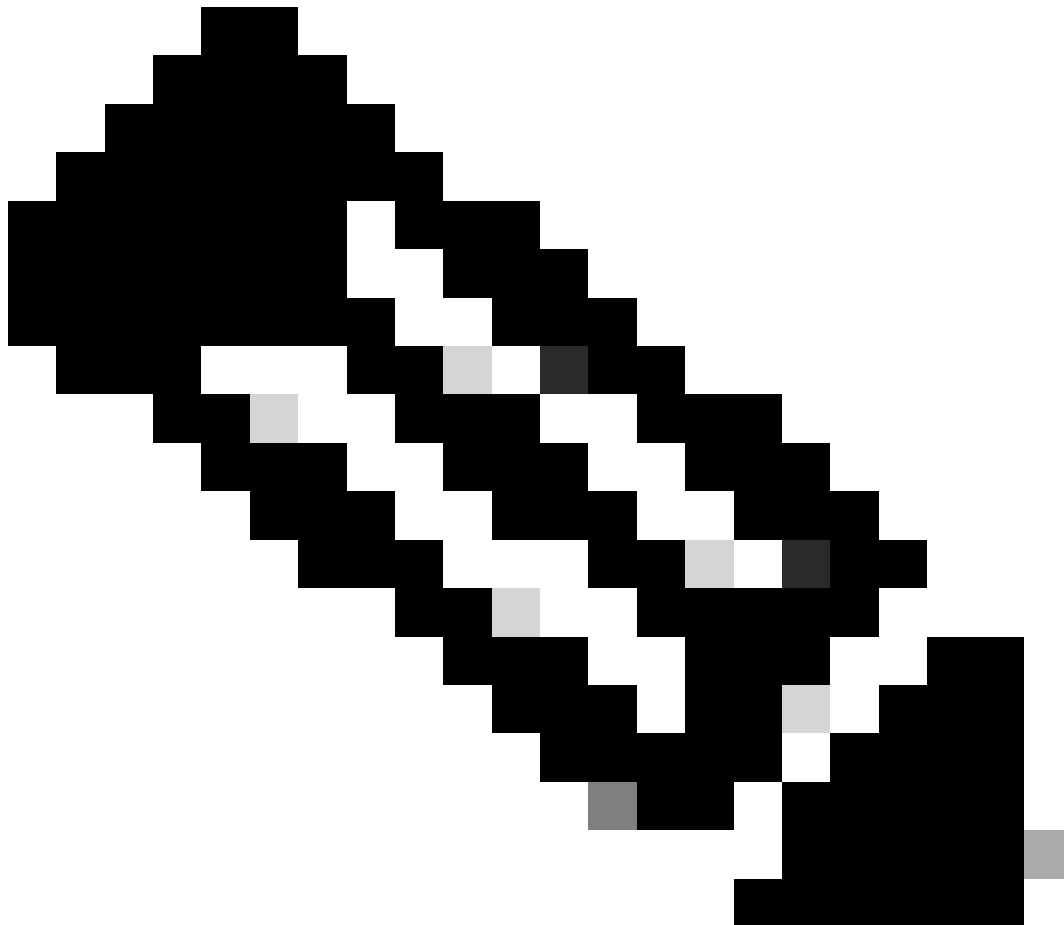
Catalyst 9800 WLC에서 Troubleshooting(문제 해결) > Radioactive Traces(방사능 추적)로 이동하고 Add(추가) 버튼을 클릭하여 트래픽을 해독할 디바이스의 MAC 주소를 입력합니다.



방사성 추적 목록에 추가된 MAC 주소

추가한 후에는 목록 상단에서 Start(시작) 버튼을 클릭하여 Conditional Debug(조건부 디버그)를 활성화해야 합니다. 이렇게 하면 데이터 평면에서 교환된 정보를 볼 수 있습니다(MSK는 여기에 있음).

조건부 디버그가 활성화된 상태로 디바이스가 방사성 추적 목록에 추가되었습니다.



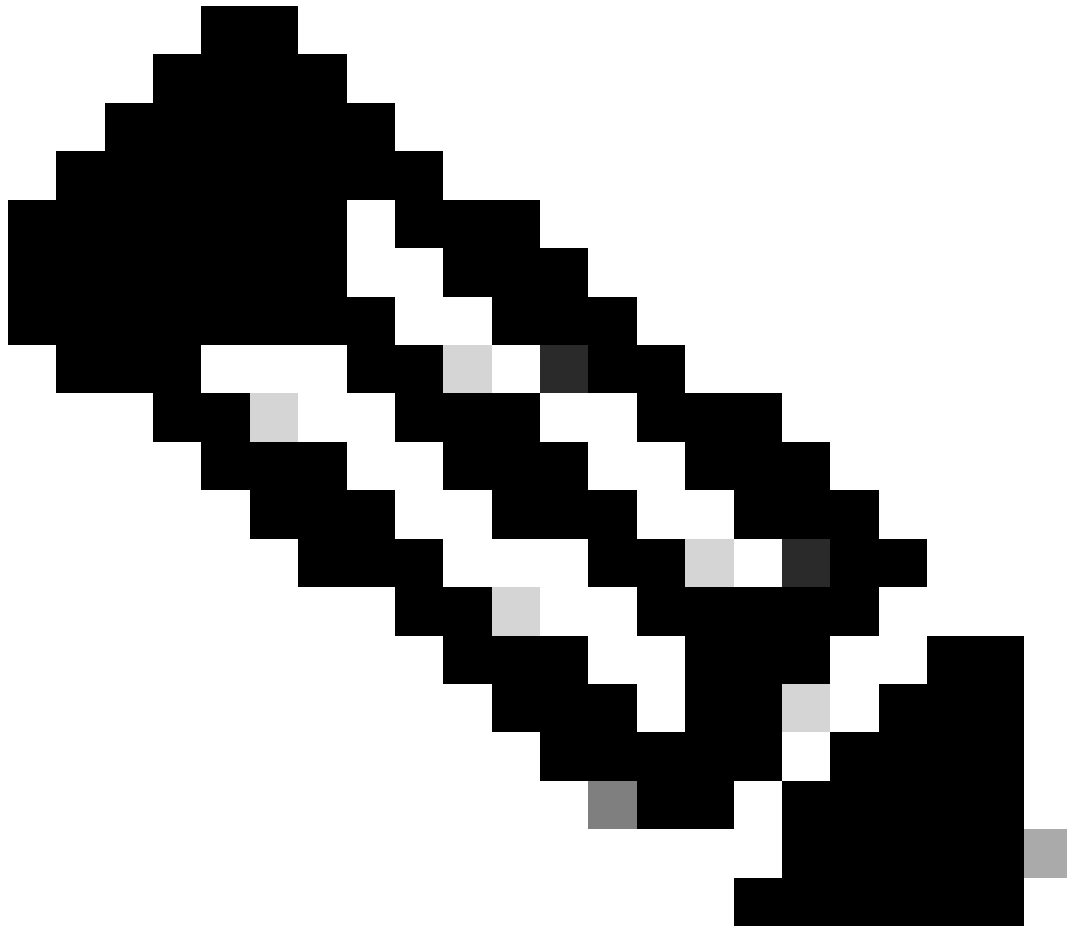
참고: Conditional Debugging을 활성화하지 않으면 컨트롤 플레인의 트래픽만 볼 수 있으며, 여기에는 MSK가 포함되지 않습니다. 이에 대한 자세한 내용은 [내용은 Catalyst 9800 WLC](#) 트러

블슈팅 문서의 [디버그 및 로그 수집의 조건부 디버깅 및 방사성 추적](#) 섹션을 참조하십시오.

2단계. Over-the-Air 패킷 캡처 얻기

Over-the-Air 패킷 캡처를 시작하고 엔드포인트를 802.1X WLAN에 연결합니다.

이 무선 패킷 캡처는 스니퍼 모드에서 액세스 포인트를 [사용하거나 무선 진단 기본 제공 도구를 사용하여 Macbook](#)에서 얻을 수 있습니다.



참고: 패킷 캡처에 모든 802.11 프레임이 포함되었는지 확인합니다. 가장 중요한 것은 이 과정에서 4자 약수를 포착하는 것이 필수다.

4방향 핸드셰이크(패킷 475~478)를 지나는 모든 트래픽이 어떻게 암호화되는지 확인합니다.

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	0.003662000	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	EAP	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	0.001844000	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	IntelCor_94:27:30	Cisco_aa:18:8f	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	IPvmcast_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	14:12:10.338286	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	0.006811000	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	IPvmcast_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	IPvmcast_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	0.000336000	IntelCor_94:27:30	Cisco_3f:80:f1	802.11	211	-61 dBm	33 dB	QoS Data, SN=22, FN=0, Flags=p.....TC

암호화된 무선 트래픽.

3단계. 디바이스의 방사선 추적 생성 및 내보내기

1단계와 동일한 화면에서 무선 트래픽을 캡처한 후 녹색 Generate(생성) 버튼을 클릭합니다.

시간 간격 팝업 창에서 요구 사항에 맞는 시간 프레임을 선택합니다. 여기서 내부 로그를 활성화할 필요는 없습니다.

Apply to Device(디바이스에 적용)를 클릭하여 Radioactive Trace(방사능 추적)를 생성합니다.

Enter time interval ✕

Enable Internal Logs

Generate logs for last

- 10 minutes
- 30 minutes
- 1 hour
- since last boot
-

RA 추적을 위한 시간 간격입니다.

Radioactive Trace(방사성 추적)가 준비되면 Trace(추적) 파일 이름 바로 옆에 다운로드 아이콘이 표시됩니다. Radioactive Trace(방사능 추적)를 다운로드하려면 클릭하십시오.

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Started**

Wireless Deb

+ Add × Delete ✓ Start ■ Stop

	MAC/IP Address	Trace file	
<input type="checkbox"/>	0093.3794.2730	debugTrace_0093.3794.2730.tx	<input checked="" type="button" value="Download"/> <input type="button" value="File"/> <input type="button" value="Generate"/>

1 10

1 - 1 of 1 items

Radioactive Trace 다운로드 가능.

4단계. Radioactive Trace(방사능 흔적)에서 MSK 얻기

다운로드한 Radioactive Trace(방사능 추적) 파일을 열고 Access-Accept(액세스 수락) 메시지 이후 eap-msk 특성을 검색합니다.

<#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 문자열 뒤의 값은 MSK입니다. 복사한 다음 저장하여 다음 단계에서 사용합니다.

<#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

5단계. Wireshark에서 MSK를 IEEE 802.11 암호 해독 키로 추가

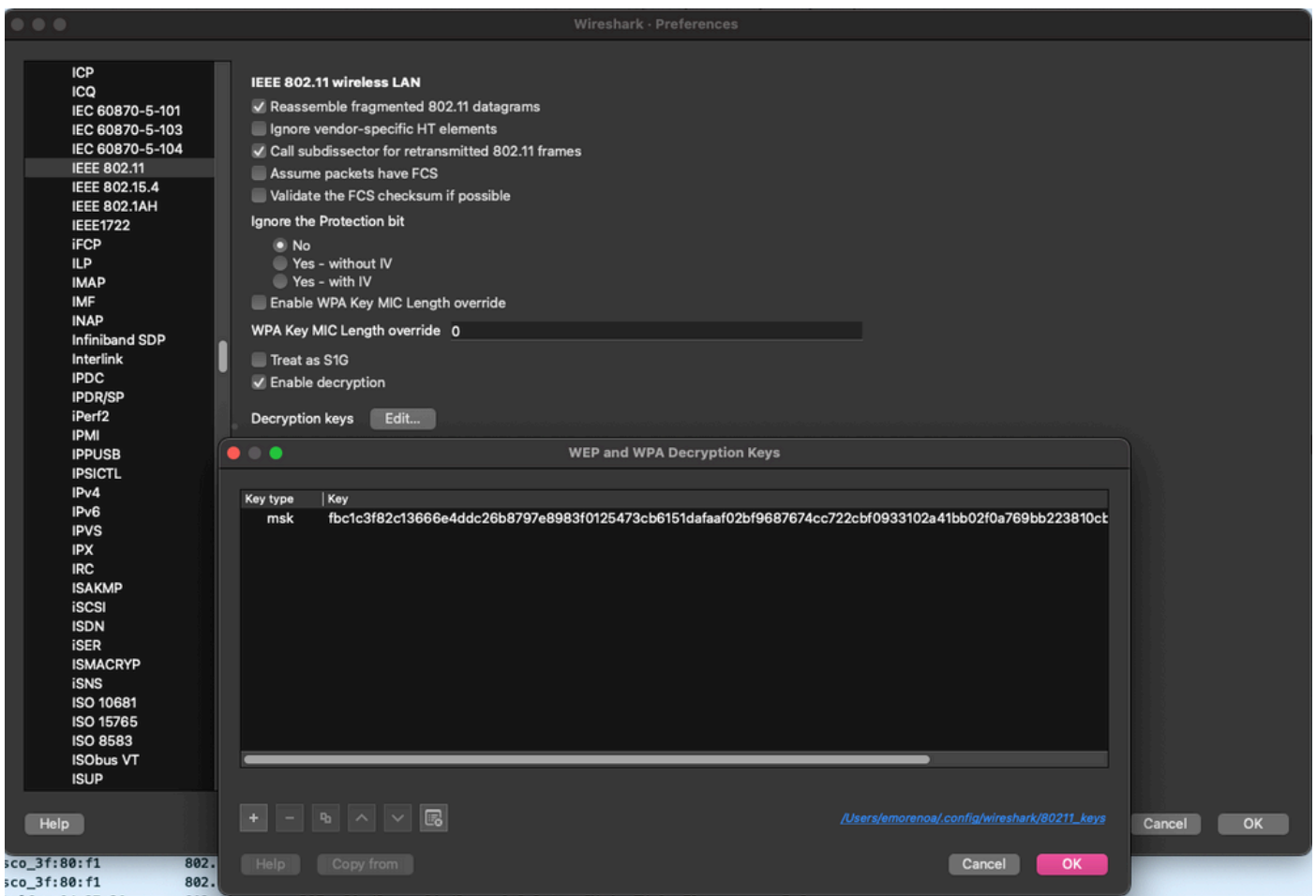
Wireshark에서 Wireshark > Preferences > Protocols > IEEE 802.11로 이동합니다.

"Enable decryption(해독 활성화)"이라고 표시된 상자를 선택한 다음 Decryption keys(해독 키) 바로 옆에 있는 Edit(편집)를 선택합니다.

하단의 "+" 버튼을 클릭하여 새 암호 해독 키를 추가하고 키 유형으로 msk를 선택합니다.

4단계에서 얻은 eap-msk 값을 공백 없이 붙여넣습니다.

마지막으로 OK(확인)를 클릭하여 Decryption keys(암호 해독 키) 창을 닫은 다음 OK(확인)를 클릭하여 Preferences(기본 설정) 창을 닫고 암호 해독 키를 적용합니다.



wireshark 기본 설정에 암호 해독 키가 추가되었습니다.

6단계. 해독된 802.1X 트래픽 분석

이제 무선 트래픽이 어떻게 표시되는지 확인합니다. 스크린샷에서는 ARP 트래픽(패킷 482 및 484), DNS 쿼리 및 응답(패킷 487 및 488), ICMP 트래픽(패킷 491~497) 및 TCP 세션에 대한 3방향 핸드셰이크의 시작(패킷 507)을 볼 수 있습니다.

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-dotix"
450	14:12:10.056200	0.003662000	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	0.002163000	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	14:12:10.166550	0.042029000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	1116	-33 dBm	61 dB	Request, Protected EAP (EAP-PEAP)
459	14:12:10.170939	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	14:12:10.180969	0.004255000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146	-59 dBm	35 dB	Response, Protected EAP (EAP-PEAP)
462	14:12:10.182870	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	0.053266000	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	14:12:10.248070	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	14:12:10.263965	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	14:12:10.287513	0.002233000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146	-60 dBm	34 dB	Application Data
472	14:12:10.291081	0.003569000	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	0.028083000	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	IntelCor_94:27:30	Cisco_aa:18:8f	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	14:12:10.325999	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:f1a...	ff02::12	ICMPv6	287	-61 dBm	33 dB	Router Solicitation from 08:03:37:94:27:30
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	0.000481000	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	228	-61 dBm	33 dB	Standard query 0x3c48 A www.msftconnecttest.com
487	14:12:10.350206	0.000240000	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	0.006018000	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	0.000606000	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	14:12:10.623515	0.000352000	fe80::badf:865b:f1a...	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	14:12:10.628007	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=8 (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	14:12:10.633620	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	0.000069000	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	0.000423000	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	14:12:10.718510	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.msft
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.msft
507	14:12:10.758548	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

암호 해독된 무선 트래픽.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.