解密802.1X SSID中的无线数据包捕获

目录
先决条件
要求
使用的组件
<u>背景信息</u>
步骤1:启动目标终端的放射性跟踪
<u>第二步:获取空中数据包捕获</u>
第三步:生成并导出设备的放射性踪迹
<u>第四步:从放射性踪迹中获取MSK</u>
<u>第五步:在Wireshark中添加MSK作为IEEE 802.11解密密钥</u>
<u>第六步:分析解密的802.1X流量</u>

简介

本文档介绍如何使用Catalyst 9800 WLC上提供的故障排除工具解密802.1X WLAN的空口数据包捕获。

先决条件

要求

Cisco 建议您了解以下主题:

- 如何在Catalyst 9800 WLC中配置802.1X WLAN
- 如何在Catalyst 9800 WLC中启用条件调试的情况下进行放射性跟踪
- 如何在嗅探器模式下使用接入点或Macbook及其无线诊断工具进行空中数据包捕获

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Catalyst 9800-L WLC、Cisco IOS® XE Cupertino 17.9.3
- 嗅探器模式下的Catalyst 9130AX接入点
- 思科ISE版本3.3
- Wireshark 4.0.8

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

一旦通过EAP+8021X验证身份,无线流量就会使用从请求方和身份验证方之间的握手生成的成对临时密钥(PTK)加密,使用成对主密钥(PMK)进行计算。此PMK派生自主会话密钥(MSK)。MSK包含在RADIUS访问接受消息的属性值对中(使用RADIUS共享密钥加密)。因此,即使四次握手被第三方拦截,也无法通过空中数据包捕获透明地看到流量。

通常,PMK的生成意味着有线网络中捕获的数据包、了解RADIUS共享密钥以及一些用于提取兴趣 值的编码。相反,通过这种方法,可以使用可用于Catalyst 9800 WLC上故障排除的工具之一(放 射性跟踪)来获取MSK,然后将其用于任何众所周知的数据包分析工具(例如Wireshark)。



注意:此过程仅适用于WPA2,因为计算成对临时密钥(PTK)所需的信息会通过四次握手在 空中交换。相反,在WPA3中,对等同时身份验证(SAE)通过所谓的蜻蜓握手来执行。

步骤1:启动目标终端的放射性跟踪

在您的Catalyst 9800 WLC上,转到故障排除>放射性跟踪,并单击Add按钮,键入要解密其流量的 设备的MAC地址。

	Cisco Cisco (Catal	yst 9800-L Wireless Controller	Welcome <i>admin</i>	
Q			Troubleshooting - > Radioactive Trace		
	Dashboard		Conditional Debug Global State: Started	🔹 Wireless Debu	ıg Analyzer
	Monitoring		+ Add × Delete ✓ Start Stop	Last Ru	n Result
Z	Configuration		MAC/IP Address T Trace file	→ St No items to display	
হ্ট্য				MAC/IF	Address 0
C			Add MAC/IP Addres	SS	*
X			MAC/IP Address*	Enter a MAC/IP Address every newline 0093.3794.2730	
			Cancel		Apply to Device

添加完成后,请确保单击列表顶部的Start按钮以启用Conditional Debug。这允许您查看数据平面(MSK位于此处)交换的信息。

¢	Cisco Catalyst 9800-L Wireless Controller								Welco Last login
C	Search Menu Items		Troublest	nooting - > Radio	active Trac	e			
	Dashboard		Conditi	onal Debug Globa	l State: Star				🔅 Wireless De
) Monitoring	>	+ Add	× Delete	✓ Start	Stop			
Ľ	Configuration	>		MAC/IP Address	۲	Trace file			
Ś	Administration	>	 4	1 N N	0 🔻				1 - 1 of 1 items
C	Licensing								
X	Troubleshooting								

设备已添加到放射性跟踪列表,并且启用了条件调试。

添加到放射性踪迹列表的MAC地址



注意:如果您不启用条件调试,则只能看到控制平面中的流量,这还不包括MSK。有关此 过程的详细信息,请参阅<u>Catalyst 9800 WLC故障排除文档上的调试和日志收集</u>的<u>条件调试</u> <u>和放射性跟踪</u>部分。

第二步:获取空中数据包捕获

开始空中数据包捕获,并将您的终端连接到802.1X WLAN。

您可以在<u>嗅探器模式下使用接入点</u>或使用<u>Macbook内置无线诊断工具</u>来获取此空中数据包捕获。



注意:确保数据包捕获包括所有802.11帧。最重要的是,在此过程中必须捕获四次握手。

观察通过四次握手的所有流量(数据包475至478)如何加密。

lo.		Time	Time delta from p	Source	Destination	Protocol	Length	Signa	il strenç	Signal/nois	i 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=.pTC
	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=.pTC
	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=.pF.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=.pTC
	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=.pTC
	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=.pF.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=.pTC
	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=.pTC
	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=.pTC
	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=.pF.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=.pTC
	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=.pF.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=.pTC
	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=.pTC

加密的无线流量。

第三步:生成并导出设备的放射性踪迹

在步骤1所在的屏幕中,捕获无线流量之后,单击绿色的Generate按钮。

在"时间间隔"弹出窗口中,选择符合您需求的时间范围。无需在此启用内部日志。

单击Apply to Device以生成放射性跟踪。



RA跟踪的时间间隔。

一旦放射性跟踪准备就绪,跟踪文件名旁边就会显示一个download图标。单击它下载你的放射性核素追踪

Troublesh	nooting - > Radioactive Tr	ace	
Conditi	onal Debug Global State: S	arted	🗘 Wireless Deb
+ Add	X Delete 🗸 St	art Stop	
	MAC/IP Address	Trace file	
	0093.3794.2730	debugTrace_0093.3794.2730.tx 📩	► Generate
	1 ▶ ⊨ 10 ▼		1 - 1 of 1 items

放射性痕迹软件可以下载。

第四步:从放射性踪迹中获取MSK

<#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}:	<pre>[radius] [15612]: (info): RADIUS: MS-MPPE-Recv-Key [17]</pre>
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 : dr
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 cl

2022/09/23 20:00:08.647159912 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15612]: (info): Applying Attribute : ea 2022/09/23 20:00:08.647161666 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15612]: (info): Applying Attribute : me 2022/09/23 20:00:08.647164452 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15612]: (info): Applying Attribute : cl 2022/09/23 20:00:08.647166150 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15612]: (info): Applying Attribute : in 2022/09/23 20:00:08.647202312 {wncd_x_R0-0}{1}: [auth-mgr] [15612]: (info): [0093.3794.2730:capwap_9000

eap-msk字符串后面的值是MSK。复制并保存此文件,以便在下一步中使用。

<#root>

2022/09/23 20:00:08.647158674 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15612]: (info): Applying Attribute : eap-msk

0

fb cl 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 ck

第五步:在Wireshark中添加MSK作为IEEE 802.11解密密钥

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

选中Enable decryption复选框,然后选择Decryption keys旁边的Edit。

单击底部的+按钮以添加新的解密密钥,并选择msk作为密钥类型。

粘贴在步骤4中获得的eap-msk值(不含空格)。

最后,单击OK关闭解密密钥窗口,然后单击OK关闭首选项窗口并应用解密密钥。

•••	Wireshark · Preferences
ICP ICQ IEC 60870-5-101 IEC 60870-5-103 IEC 60870-5-104 IEEE 802.11 IEEE 802.15.4 IEEE 802.1AH IEEE 722 IFCP ILP IMAP IMF INAP Infiniband SDP Interlink IPDC IPDR/SP iPerf2	IEEE 802.11 wireless LAN ✓ Reassemble fragmented 802.11 datagrams Ignore vendor-specific HT elements ✓ Call subdissector for retransmitted 802.11 frames Assume packets have FCS Validate the FCS checksum if possible Ignore the Protection bit ● No ● Yes - without IV ● Yes - with IV Enable WPA Key MIC Length override WPA Key MIC Length override O ● Treat as S1G ✓ Enable decryption Decryption keys
IPMI IPPUSB	WEP and WPA Decryption Keys
IPSICTL IPv4 IPv6 IPVS IRC ISAKMP ISCSI ISDN ISER ISMACRYP ISNS ISO 10681 ISO 15765 ISO 8583 ISO 15765 ISO 8583 ISObus VT ISUP	Key type Key msk fbc1c3f82c13666e4ddc26b8797e8983f0125473cb6151dafaaf02bf9687674cc722cbf0933102a41bb02f0a769bb223810ct
Help	+ - Pa ^ V E Cancel OK
sco_3f:80:f1 802 sco_3f:80:f1 802	Help Copy from Cancel OK

解密密钥已添加到wireshark首选项。

第六步:分析解密的802.1X流量

观察无线流量现在如何可见。在屏幕截图中,您可以看到ARP流量(数据包482和484)、DNS查询

和响应(数据包487和488)、ICMP流量(数据包491到497),甚至可以看到TCP会话三次握手的 开始(数据包507)。

No.	_ T	ime	Time delta from p	Source	Destination	Protocol Len	gth Signal streng	Signal/nois	i Info
44	9 1	4:12:10.052518	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"
45	0 1	4:12:10.056200	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
45	1 1	4:12:10.058303	0.002103000	IntelCor 94:27:38	Cisco aa:18:8f	802.11	93 -59 dBm	35 dB	Action. SN=23. FN=0. Flans=C
45	2 1	4:12:18.859417	0.001114000	Cisco aa:18:8f	IntelCor 94:27:38	FAP	109 -34 dBm	60 dB	Request Identity
45	2 1	4:12:10 100420	0.000112000	IntelCor 04:27:20	Circo an: 19: Pf	EAD	146 -50 dBm	25 dB	Decourse Identity
45		4.12.10.1160429	0.00000000	Cisco anila de	TatelCas 04:27:30	EAD	110 -34 dBm	50 40	Response, Tie Can Tiel
43		4:12:10.110909	0.000400000	C15C0_88118181	Inceccor_94127130	EAP	110 -34 Ubm	OD OD	Request, ILS EAP (EAP=ILS)
45	5 1	4:12:10.119150	0.002241000	Inte(Cor_9412/130	Cisco_aa:18:87	EAP	146 -59 dBm	35 dB	Response, Legacy Nak (Response Unity)
45	6 1	4:12:10.122792	0.003642000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	110 -33 dBm	61 dB	Request, Protected EAP (EAP-PEAP)
45	7 1	4:12:10.124621	0.001829000	IntelCor_94:27:30	Cisco_aa:18:8f	TLSv1.2	330 -60 dBm	34 dB	Encrypted Handshake Message
45	8 1	4:12:10.166650	0.042029000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	1116 -33 dBm	61 dB	Request, Protected EAP (EAP-PEAP)
45	9 1	4:12:10.170039	0.003389000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146 -59 dBm	35 dB	Response, Protected EAP (EAP-PEAP)
46	0 1	4:12:10.175814	0.005775000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	1112 -34 dBm	60 dB	Request, Protected EAP (EAP-PEAP)
46	1 1	4:12:10.180069	0.004255000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146 -59 dBm	35 dB	Response, Protected EAP (EAP-PEAP)
46	2 1	4:12:10.182929	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
46	3 1	4:12:10.236135	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
46	4 1	4:12:10.244438	0.008303000	Cisco aa:18:8f	IntelCor 94:27:30	TLSv1.2	161 -34 dBm	60 dB	Change Cipher Spec, Encrypted Handshake Message
46	5 1	4:12:10.248078	0.003640000	IntelCor 94:27:30	Cisco aa:18:8f	EAP	146 -60 dBm	34 dB	Response, Protected EAP (EAP-PEAP)
46	6 1	4:12:18.251382	0.003224000	Cisco aa:18:8f	IntelCor 94:27:38	TI 5v1.2	144 -34 dBm	60 dB	Application Data
46	7 1	4:12:18.259118	0.007808000	IntelCor 94:27:38	Cisco aa:18:8f	TI 5v1.2	149 -68 dBa	34 dB	Application Data
46		4:12:18 262865	0.004755000	Cisco anil9.9f	IntelCor 94:27:38	TI Su1 2	175 -34 dBm	60 dB	Application Data
40		4.12.10.203003	0.0047330000	Tatel Car 04:27:30	Cisco aprile Rf	TI Cut 2	203 -60 dBm	34 dB	Application bata
40		4:12:10.2/1/14	0.007049000	Intettor_94:27:30	C15C0_00:10:01	TLSVI.2	203 -00 000	34 db	Application bata
4/	0 1	4:12:10.285280	0.013566000	C15C0_88:18:81	IntelCor_94:27:30	TLSV1.2	190 -33 dBm	61 dB	Application Data
47	1 1	4:12:10.287513	0.002233000	IntelCor_94:27:30	C1sco_aa:18:8f	TLSV1.2	146 -60 dBm	34 dB	Application Data
47	2 1	4:12:10.291081	0.003568000	Cisco_aa:18:8f	IntelCor_94:27:30	TLSv1.2	143 -34 dBm	60 dB	Application Data
47	3 1	4:12:10.294213	0.003132000	IntelCor_94:27:30	Cisco_aa:18:8f	EAP	146 -60 dBm	34 dB	Response, Protected EAP (EAP-PEAP)
47	4 1	4:12:10.315016	0.020803000	Cisco_aa:18:8f	IntelCor_94:27:30	EAP	108 -33 dBm	61 dB	Success
47	5 1	4:12:10.316556	0.001540000	Cisco_aa:18:8f	IntelCor_94:27:38	EAPOL	221 -34 dBm	60 dB	Key (Message 1 of 4)
47	6 1	4:12:10.321017	0.004461000	IntelCor_94:27:30	Cisco_aa:18:8f	EAPOL	223 -60 dBm	34 dB	Key (Message 2 of 4)
47	7 1	4:12:10.322061	0.001044000	Cisco_aa:18:8f	IntelCor_94:27:30	EAPOL	255 -34 dBm	60 dB	Key (Message 3 of 4)
47	8 1	4:12:10.323817	0.001756000	IntelCor_94:27:30	Cisco_aa:18:8f	EAPOL	199 -68 dBm	34 dB	Key (Message 4 of 4)
47	9 1	4:12:10.324699	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
48	8 1	4:12:10.325899	0.001200000	Cisco aa:18:8f	IntelCor 94:27:38	802.11	148 -34 dBm	60 dB	Action, SN=3746, FN=0, Flags=C, Dialog Token=3
48	1 1	4:12:18.334956	0.009857888	fe88::badf:865b:f18_	ff82::2	ICMPv6	207 -61 dBm	33 dB	Router Solicitation from 00:93:37:94:27:30
48	12 1	4:12:10.348407	0.013451000	IntelCor 94:27:38	Broadcast	ARP	197 -61 dBm	33 dB	Who has 172.16.5.17 Tell 172.16.5.66
48	3 1	4:12:18.348983	0.000495000	Cisco aa:18:8f	IntelCor 94:27:38	882.11	99 -34 dBm	60 dB	Action, SN=3747, FN=0, FlagssC. Dialog Token=90
48	4 1	4:12:18.349222	0.000319000	Cisco 3f:88.f1	IntelCor 94:27:38	ARP	197 -38 dBa	64 dB	172 16 5 1 ic at 78 dai 56 25 da 61
40		4.12.10.349222	0.000319000	Tatel Car 04:27:20	Cicco apil9:0f	992 11	00 -60 dBm	24 dB	Action Shirts Elling Children C Dislog Takan-Da
40	10 1	4:12:10.349023	0.000401000	172 16 5 66	173 10 100 43	DAIC	220 -61 dBm	34 db	Action, Smech, Field, Field, State State Com
40	10 1	4:12:10.330040	0.00042.3000	172.10.5.00	172.10.100.43	UND	220 -01 000	33 00	Standard query 0x3c40 A www.msrtconnecttest.com
7* 48	1 1	4:12:10.530286	0.180240000	172.16.5.66	172.18.108.43	uno	200 -01 008	33 08	Standard query 8xadbi A cisco.com
- 48	18 1	4:12:10.616297	0.085011000	172.18.108.43	172.16.5.66	DNS	222 -30 dBm	64 dB	Standard query response Wxad51 A c1sco.com A 72.163.4.161
48	9 1	4:12:10.623163	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 239.255.250 for any sources
49	0 1	4:12:10.623515	0.000352000	fe80::badf:865b:f10_	ff02::16	ICMPv6	267 -61 dBm	33 dB	Multicast Listener Report Message v2
49	1 1	4:12:10.623890	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!)
49	2 1	4:12:10.625663	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)
49	3 1	4:12:10.627395	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!)
49	14 1	4:12:10.628807	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)
49	5 1	4:12:10.632290	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!)
49	6 1	4:12:10.632626	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)
49	7 1	4:12:10.632626	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)
49	8 1	4:12:10.632695	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
49	9 1	4:12:10.632972	0.000277000	Cisco_aa:18:8f	IntelCor_94:27:38	802.11	99 -34 dBm	60 dB	Action, SN=3754, FN=0, Flags=C, Dialog Token=6
50	00 1	4:12:10.634467	0.001495000	172.16.5.66	172.253.63.99	ICMP	243 -61 dBm	33 dB	Echo (ping) request id=0x0001, seg=8141/52511, ttl=11 (no response found!)
58	1 1	4:12:10.666791	0.032324000	72, 163, 4, 161	172.16.5.66	ICMP	211 -30 dBm	64 dB	Echo (ping) reply id=0x0001, seg=8140/52255, ttl=236 (request in 496)
50	2 1	4:12:18.668564	0.001773000	10.152.216.189	172, 16, 5, 66	TOMP	207 -30 dBm	64 dB	Time-to-live exceeded (Time to live exceeded in transit)
50	3 1	4:12:18.669817	0.000453000	10, 152, 216, 189	172.16.5.66	TOMP	207 -38 dBm	64 dB	Time-to-live exceeded (Time to live exceeded in transit)
50	4 1	4-12-18.718518	8.849581888	172 16 5 66	230 255 255 258	SSDP	354 -61 dBa	33 dB	M_SEARCH + HTTP/1.1
50		4.12.10 747022	0.030314000	173 10 100 43	173 16 5 66	DAIE	264 -20 dBa	64 48	Condensed among account of August A line and connections on ANAME acci-and testficeneous ant ANAME line are
50		4.12.10.74/032	0.029314000	172.10.100.43	172.10.3.00	CAN'S	304 -30 dbm	64 48	Standard query response 0.3cHo A www.mstcommectest.com CMME htsl-geo.trafficmanger.het CMME WW.mst
50	1 07	4:12:10.748179	0.000347000	1/2.10.100.43	1/2.10.3.00	uno	304 -38 dBm	on dB	standard query response exacto A www.msttconnecttest.com CNAME ncsi-geo.tratticmanager.net CNAME www.mst

解密的无线流量。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。