Configurez Wireshark et FreeRADIUS afin de déchiffrer l'analyseur sans fil 802.11 WPA2-Enterprise/EAP/dot1x en direct

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Procédure Étape 1 : déchiffrement des PMK à partir du paquet Access-accept Étape 2. Extraire les PMK. Étape 3. Décryptage de l'analyseur OTA Exemple de paquet 802.11 déchiffré Exemple de paquet 802.11 chiffré Informations connexes

Introduction

Ce document décrit la procédure à suivre pour déchiffrer l'analyseur d'accès sans fil en direct (OTA) crypté Wi-Fi Protected Access 2 - Enterprise (WPA2-Enterprise) ou 802.1x (dot1x), avec toute méthode EAP (Extensible Authentication Protocol).

Il est relativement facile de décrypter la capture OTA 802.11 basée sur PSK/WPA2 personnel, à condition que les échanges EAPoL à quatre voies complets soient capturés. Cependant, la clé prépartagée (PSK) n'est pas toujours recommandée du point de vue de la sécurité. Il ne s'agit que d'une question de temps.

Par conséquent, de nombreuses entreprises choisissent dot1x avec Remote Authentication Dial-In User Service (RADIUS) comme meilleure solution de sécurité pour leur réseau sans fil.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FreeRADIUS avec radsniff installé
- Wireshark/Omnipeek ou tout logiciel capable de déchiffrer le trafic sans fil 802.11
- Privilège pour obtenir le secret partagé entre le serveur d'accès au réseau (NAS) et Authenticator
- Possibilité de capturer la capture de paquets radius entre le NAS et l'authentificateur à partir

de la première demande d'accès (du NAS à l'authentificateur) jusqu'à la dernière acceptation d'accès (de l'authentificateur au NAS) tout au long de la session EAP

 Possibilité d'effectuer une capture OTA (Over-the-Air) contenant des échanges EAPoL à quatre voies

Components Used

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

- Serveur Radius (FreeRADIUS ou ISE)
- Périphérique de capture en vol
- Appareil Apple macOS/OS X ou Linux

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

Dans cet exemple, deux clés maître par paire (PMK) sont dérivées de paquets Radius capturés à partir de ISE 2.3, car le délai d'attente de session sur ce SSID est de 1800 secondes et la capture donnée ici est de 34 minutes (2040 secondes).

Comme l'illustre l'image, EAP-PEAP est utilisé comme exemple, mais cela peut être appliqué à toute authentification sans fil basée sur dot1x.

	wlan.addr==04:f1:28:6a:69:11 && (eapol or eap)			🔀 📼 🔹 Expression	4
No	o. Time	Source	Destination	Protocol	Length Info	1
Т	4325 2018-11-16 00:04:02.812197	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP	109 Request, TLS EAP (EAP-TLS)	
	4327 2018-11-16 00:04:02.812927	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	73 Response, Legacy Nak (Response Only)	-
	4329 2018-11-16 00:04:02.816752	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP	109 Request, Protected EAP (EAP-PEAP)	
T	4332 2018-11-16 00:04:02.818331	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSV1.2	244 Client Hello	- P
	4349 2018-11-16 00:04:02.828460	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	1079 Server Hello. Certificate. Server Key Exchange. Server Hell	
T	4352 2018-11-16 00:04:02.829281	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	73 Response, Protected EAP (EAP-PEAP)	
	4354 2018-11-16 00:04:02.833165	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	1075 Server Hello, Certificate, Server Key Exchange, Server Hell	
	4356 2018-11-16 00:04:02.834110	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	73 Response, Protected EAP (EAP-PEAP)	
	4361 2018-11-16 00:04:02.839052	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	738 Server Hello, Certificate, Server Key Exchange, Server Hello	
	4363 2018-11-16 00:04:02.845892	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	199 Client Key Exchange, Change Cipher Spec, Encrypted Handshak	
	4365 2018-11-16 00:04:02.851843	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	124 Change Cipher Spec, Encrypted Handshake Message	
	4367 2018-11-16 00:04:02.853063	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	73 Response, Protected EAP (EAP-PEAP)	
1						

		≊*® ⊒ ≣≪≪≪∞			
	lan.addr==04:f1:28:6a:69:11 && (eapol or eap))		🔀 📩 💌 Expression	+
No.	Time	Source	Destination	Protocol Length Info	^
1	095. 2018-11-16 00:34:07.507960	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 754 Encrypted Handshake Message, Encrypted Handshake Message, En	
1	095. 2018-11-16 00:34:07.519109	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2 215 Encrypted Handshake Message, Change Cipher Spec, Encrypted I	
9	095. 2018-11-16 00:34:07.524344	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 140 Change Cipher Spec, Encrypted Handshake Message	
9	095 2018-11-16 00:34:07.525423	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 89 Response, Protected EAP (EAP-PEAP)	
1	095_ 2018-11-16 00:34:07.528660	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 125 Application Data	
1	095_ 2018-11-16 00:34:07.529567	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2 129 Application Data	
1	095_ 2018-11-16 00:34:07.532409	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 151 Application Data	
1	095. 2018-11-16 00:34:07.536570	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2 183 Application Data	
9	095_ 2018-11-16 00:34:07.569469	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 169 Application Data	
1	095_ 2018-11-16 00:34:07.570964	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2 124 Application Data	-
1	095_ 2018-11-16 00:34:07.574596	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 125 Application Data	
1	095_ 2018-11-16 00:34:07.575693	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 89 Response, Protected EAP (EAP-PEAP)	~

Procédure

Étape 1 : déchiffrement des PMK à partir du paquet Access-accept

Exécutez le **radsniff** contre la capture radius entre NAS et Authenticator afin d'extraire PMK. La raison pour laquelle deux paquets d'acceptation d'accès sont extraits au cours de la capture est que le délai d'expiration de la session est défini sur 30 minutes sur ce SSID particulier et la

capture dure 34 minutes. L'authentification est effectuée deux fois.

```
FRLU-M-51X5:pcaps frlu$ radsniff -I /Users/frlu/Downloads/radius_novlan_merged.pcapng -
s <shared-secret between NAS and Authenticator> -x
<snip>
2018-11-16 11:39:01.230000 (24) Access-Accept Id 172
/Users/frlu/Downloads/radius_novlan_merged.pcapng:10.66.79.42:32771 <- 10.66.79.36:1812 +0.000
+0.000
User-Name = "frlu_2"
State = 0x52656175746853657373696f6e3a306134323466326130303030303565373562656530393732
Class =
2f33303432
EAP-Message = 0x03c50004
Message-Authenticator = 0x38c67b9ba349842c9624889a45cabdfb
MS-MPPE-Send-Key = 0xa464cc15c0df8f09edc249c28711eb13a6db2d1a176f1196edcc707579fd6793
MS-MPPE-Recv-Key =
0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b<<<<<<<<<PMK
Authenticator-Field = 0x6cd33b4d4dde05c07d9923e17ad6c218
<snip>
2018-11-16 11:39:01.470000 (48) Access-Accept Id 183
/Users/frlu/Downloads/radius_novlan_merged.pcapng:10.66.79.42:32771 <- 10.66.79.36:1812 +0.000
+0.000
User-Name = "frlu_2"
State = 0x52656175746853657373696f6e3a30613432346632613030303030303565373562656530393732
Class =
0x434143533a30613432346632613030303035653735626565303937323a4953452d322d332f33323832373132338
2f33303434
EAP-Message = 0x03910004
Message-Authenticator = 0x81c572651679e15e54a900f3360c0aa9
MS-MPPE-Send-Key = 0xeae42cf7c6cd26371eee29856c51824fbb5bbb298874125928470114d009b5fb
MS-MPPE-Recv-Key =
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfblcfb0e<<<<<<<<<PMK
Authenticator-Field = 0xa523dd9ec2ce93d19fe4fc2e21537a5d
```

Note: Supprimez toute étiquette de réseau local virtuel (VLAN) de la capture de paquets Radius, sinon **radsniff** ne reconnaîtra pas le fichier pcap d'entrée. Afin de supprimer toute balise VLAN, par exemple, <u>editcap</u> peut être utilisé.

Astuce : En règle générale, le temps d'exécution de la commande radsniff par rapport à un

fichier pcap RADIUS peut être compté comme une échelle de secondes. Cependant, si le **radsniff** est coincé dans cet état indiqué dans le journal, mettez en cascade cette capture de paquets (A) avec une autre capture de paquets plus longue (B) entre le même NAS et l'authentificateur. Ensuite, exécutez la commande radsniff sur le paquet en cascade (A+B). La seule exigence de la capture de paquets (B) est que vous pouvez exécuter la commande radsniff contre elle et voir le résultat verbose.

FRLU-M-51X5:pcaps frlu\$ radsniff -I /Users/frlu/Downloads/radius_novlan.pcap -s Cisco123 -x

Logging all events

Sniffing on (/Users/frlu/Downloads/radius_novlan.pcap)

Dans cet exemple, la journalisation du plan de contrôle du contrôleur de réseau local sans fil (WLC) (A) capturée via la fonctionnalité de journalisation des paquets du WLC, est en cascade avec une capture plus longue à partir du TCPdump (B) d'ISE. La journalisation des paquets WLC est utilisée comme exemple car elle est généralement de très petite taille.

Journalisation des paquets WLC (A)

radius_novlan.pcap	Pcap Napture	22 KB	Today at '	11:56 am	
Tcpdump ISE (B)					
adius_eap_decode_Cisco123.pcap	Yesterday at 12:04 pm		850 KB P	Cap Napture	
Fusion (A+B)					
👼 radius novlan merged.pcapng	PcapnCapture 9	927 KB	Today at 12	:28 pm	

Ensuite, exécutez le **radsniff** contre le pcap fusionné (A+B) et vous pourrez voir la sortie du verbose.

FRLU-M-51X5:pcaps frlu\$ radsniff -I /Users/frlu/Downloads/radius_novlan_merged.pcapng -s
<shared-secret between NAS and Authenticator> -x

<snip>

```
2018-11-16 11:39:01.230000 (24) Access-Accept Id 172
/Users/frlu/Downloads/radius_novlan_merged.pcapng:10.66.79.42:32771 <- 10.66.79.36:1812 +0.000
+0.000
```

<snip>

Étape 2. Extraire les PMK.

La suppression de 0x dans chaque **MS-MPPE-Recv-Key** à partir de la sortie détaillée et des PMK nécessaires au décodage du trafic sans fil est ensuite présentée.

MS-MPPE-Recv-Key = 0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a 066d8b3b fb0e

PMK: 7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

Étape 3. Décryptage de l'analyseur OTA

Accédez à **Wireshark > Préférences > Protocoles > IEEE 802.11.** Ensuite, cochez **Enable Decryption** et cliquez sur le bouton **Edit** en regard de **Decryption Keys**, comme indiqué dans l'image.

4	Wireshark · Preferences ? ×
HCrt HDFS HDFSDATA HIP HiQnet HISLIP HL7 HNBAP HP_ERM HPFEEDS HSMS HSRP HTTP HTTP2 LAPP IAX2 IB ICAP ICCP ICCQ IEEE 802.11 IEEE 802.11 IEEE 802.11	▲ Itel 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 - without IV ○ Yes - without IV ○ Tes - with IV WPA Key MIC Length override ● Coryption keys Edit

Ensuite, sélectionnez **wpa-psk** comme type de clé, puis placez les PMK dérivés dans le champ **Key**, puis cliquez sur **OK**. Une fois cette opération terminée, la capture OTA doit être déchiffrée et vous pouvez voir des informations de couche supérieure (3+).

4	Wireshark - Preferences	?	x
	WEP and WPA Decryption Keys ? X		
	Key wpa-psk ddb0b09a7d6980515825950b5929d02f236799f3e8a87t163c8ca41a066d8b3b wpa-psk 7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e		
٤	+ - 9 A V B Ckters Habitator HacOsta Roaming Hitreshark (80211 Jans OK Cancel Help OK Cancel	Help	,

Exemple de paquet 802.11 déchiffré

File Edit	View Go Capture Analyze Statistics	Telephony Wireless Tools Help			
A = 1	۵ 🗿 🕾 🗢 🕻 🗖 🖉 🖉 🕘	l 🚍 🔳 @, Q, @, II			
wlan.addr	==04:f1:28:6a:69:11				🔀 🔜 💌 Expression +
No.	Time	Source	Destination Pr	rotocol	Length Info
	397877 2018-11-16 00:17:08.095884	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 80	02.11	45 Request-to-send, Flags=C
	397879 2018-11-16 00:17:08.097877	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 80	02.11	45 Request-to-send, Flags=C
	397881 2018-11-16 00:17:08.098393	40.127.66.24	172.16.255.13 TO	CP	1438 [TCP Retransmission] 80 → 45658 [ACK] Seq=3999908
	397882 2018-11-16 00:17:08.098444	104.17.57.239	172.16.255.13 TO	CP	154 80 → 37553 [ACK] Seq=1 Ack=310 Win=65344 Len=0 TS
	397883 2018-11-16 00:17:08.098495	HmdGloba_6a:69:11 (04:f1:28:6a:69:11)_	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (RA) 80	02.11	57 802.11 Block Ack, Flags=C
_	397884 2018-11-16 00:17:08.098999	104.17.57.239	172.16.255.13 TO	CP	162 80 → 37555 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
	397886 2018-11-16 00:17:08.099099	172.16.255.13	40.127.66.24 TO	CP	154 45658 → 80 [ACK] Seq=128 Ack=4001196 Win=788480 L
-	397887 2018-11-16 00:17:08.099181	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (1_	HmdGloba_6a:69:11 (84:11:28:6a:69:11) (RA) 88	82.11	57 802.11 Block Ack, Flags=
	397888 2018-11-16 00:17:08.099606	172.16.255.13	104.17.57.239 TO	CP	154 37555 → 80 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSva
	397889 2018-11-16 00:17:08.099655	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 80	02.11	57 802.11 Block Ack, Flags=C
	397890 2018-11-16 00:17:08.101762	172.16.255.13	104.17.57.239 HT	ттр	479 GET /s100264/images/logoq.png?t=636366 HTTP/1.1
	397891 2018-11-16 00:17:08.101812	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 80	02.11	57 802.11 Block Ack, Flags=C
<					>
Frame 3	97886: 154 bytes on wire (1232 bits),	, 154 bytes captured (1232 bits)			
Radiota	p Header v0, Length 48				
▶ 802.11	radio information		and the second		
D IEEE 80	2.11 QoS Data, Flags: .pTC				
Logical	-Link Control				
▷ Interne	t Protocol Version 4, Src: 172.16.255	5.13, Dst: 40.127.66.24			
Transmi	ssion Control Protocol, Src Port: 456	658, Dst Port: 80, Seq: 128, Ack: 4001196	, Len: 0		
0000 00	00 20 00 ch 00 4. 00 ch 40 20 20 00	00 00 00 0 k - 04			
0000 00	00 30 00 60 08 10 00 6d 19 30 31 00	00 00 00 ·····················			
0010 14 0020 9e	00 90 09 00 04 09 84 00 00 00 00 00 00 80 89 85 22 1f 88 85 88 55 88 88 88 84	00 00 00			
0030 88	41 30 00 00 a3 8e b4 3d e4 04 f1 28	6a 69 11 · A0·			
0040 00	0c 29 28 89 dd 50 06 00 00 c8 84 00	20 01 00 ···)(··P· ·····			
0050 00	00 af f4 c2 2f 90 d1 14 52 a5 8b 2e	57 27 3a ····/·· ·R··.W':			
0060 d8	54 a5 55 0a 12 92 da fc a9 1f c2 c8	34 39 ca ·T·U···· 49·			
0070 Sc	08 7a 36 57 cd e2 43 89 86 f5 92 24	17 d0 db \.z6WC\$			
0050 42	az ze 6z 35 c7 36 9b 54 d0 00 91 78	7d 44 87 B			
0030 23	or to so to op st to 30 TT	#Tf A.			

Si vous comparez le deuxième résultat où le PMK n'est pas inclus, avec le premier résultat, où le PMK est inclus, le paquet 397886 est déchiffré en données QoS 802.11.

Exemple de paquet 802.11 chiffré

Tme Source Destination Protocol Length Info 397881 2018-11-16 00:17:08.0980343 Wmare_28:89:dd Hiddloba_6a:69:11 802.11 1438 Q6S Data, SN=4344, FN=0, Flags=.pF.G 397882 2018-11-16 00:17:08.0980445 Wmare_28:89:dd Hiddloba_6a:69:11 802.11 154 Q5 Data, SN=4344, FN=0, Flags=.pF.G 397883 2018-11-16 00:17:08.098045 Hiddloba_6a:69:11 Cisco_b4:3i:e:104:33:8::b4:3d:e4) 802.11 57 802.11 Block Ack, Flags=C 397884 2018-11-16 00:17:08.098049 Hiddloba_6a:69:11 Vmare_28:89:dd 802.11 154 Q6S Data, SN=408, Flags=.pTC 397885 2018-11-16 00:17:08.098049 Hiddloba_6a:69:11 Vmare_28:89:dd 802.11 154 Q6S Data, SN=408, Flags=.pTC 397885 2018-11-16 00:17:08.098055 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. Hiddloba_6a:69:11) (R4:f1:28:6a:69:11) (RA) 802.11 154 QOS Data, SN=408, Flags=.pTC 397895 2018-11-16 00:17:08.098055 Vmare_28:89:dd Hiddloba_6a:69:11 Vmare_28:89:dd 802.11 397891	Tme Source Destination Protocol Length Info 397881 2016-11-16 00:17:08.0984933 Wimare_28:09:idd HindGloba_6a:69:11 082.11 138< QoS Data, SN=1335, FN=0, Flags=.pF.C 397882 2018-11-16 00:17:08.098495 HindGloba_6a:69:11 082.11 154 QoS Data, SN=1335, FN=0, Flags=.pF.C 397883 2018-11-16 00:17:08.098495 HindGloba_6a:69:11 082.11 154 QoS Data, SN=101, FN=0, Flags=.pF.C 397884 2018-11-16 00:17:08.099499 HindGloba_6a:69:11 Wimare_28:89:1d 082.11 154 QoS Data, SN=101, FN=0, Flags=.p,TC 397887 2018-11-16 00:17:08.099499 HindGloba_6a:69:11 Wimare_28:89:1d 082.11 154 QoS Data, SN=104, FN=0, Flags=.p,TC 397887 2018-11-16 00:17:08.099455 HindGloba_6a:69:11 Wimare_28:89:1d 082.11 154 QoS Data, SN=104, FN=0, Flags=.p,TC 397889 2018-11-16 00:17:08.099455 HindGloba_6a:69:11 Wimare_28:89:1d Wimare_28:89:1d 802.11 57 802.11 Block Ack, Flags=,C 397890 2018-11-16 00:17:08.094555		==04:f1:28:6a:69:11				×
397881 2012-11-16 00:17:08.098393 Vmare_28:89:dd HedGloba_68:69:11 802.11 1438 005 Data, SM=1434, FN=0, Flags=.pF.C 397882 2018-11-16 00:17:08.098445 Vmare_28:89:dd HedGloba_68:69:11 802.11 154 Qo5 Data, SM=1435, FN=0, Flags=.pF.C 397882 2018-11-16 00:17:08.098495 Vmare_28:89:dd HedGloba_68:69:11 802.11 154 Qo5 Data, SM=1435, FN=0, Flags=.pF.C 397882 2018-11-16 00:17:08.098099 MmdGloba_68:69:11 Vmare_28:89:dd 802.11 154 Qo5 Data, SM=101, FN=0, Flags=.pTC 397882 2018-11-16 00:17:08.099109 HedGloba_68:69:11 Vmare_28:89:dd 802.11 154 Qo5 Data, SM=101, FN=0, Flags=.pTC 397882 2018-11-16 00:17:08.099108 Clisco_b4:3de:4 (00:a3:8e:b4:3d:e4) (T. HedGloba_68:69:11) (AA1 802.11 154 Qo5 Data, SM=101, FN=0, Flags=.pTC 397882 2018-11-16 00:17:08.099108 Clisco_b4:3de:e4(00:a3:8e:b4:3d:e4) (T. HedGloba_68:69:11) (AA1 802.11 154 Qo5 Data, SN=103, FN=0, Flags=.pTC 397892 2018-11-16 00:17:08.09108 Clisco_b4:3de:e4(00:a3:8e:b4:3d:e4) (T. HedGloba_68:69:11) (AA1 802.11 154 Qo5 Data, SN=108, FN=0, Flags=.pTC 397892 2018-11-16 00:17:08.10120 Clisco_b4:3de:e4(00:a3:8e:b4:3d:e4) (T. HedGloba_68:69:11) (AA1 802.11 154 Qo5 Data, SN=108, FN=0, Flags=.pFC 397892 2018-11-16 00:17:08.108121	397881 2018-11-16 00:17:08.098493 Wmare_28:89:dd HedGloba_6s:69:11 602.11 1438 Qc5 Data, SH=1434, FN=0, Flags=, p, F, C 397882 2018-11-16 00:17:08.098494 Wmare_28:89:dd HedGloba_6s:69:11 602.11 154 Qc5 Data, SN=1434, FN=0, Flags=, p, F, C 397882 2018-11-16 00:17:08.098495 Wmare_28:89:dd HedGloba_6s:69:11 602.11 154 Qc5 Data, SN=1435, FN=0, Flags=, p, F, C 397882 2018-11-16 00:17:08.099095 HedGloba_6s:69:11 Wmare_28:89:dd 602.11 154 Qc5 Data, SN=01, FN=0, Flags=, p, TC 397882 2018-11-16 00:17:08.099095 HedGloba_6s:69:11 Wmare_28:89:dd 602.11 154 Qc5 Data, SN=01, FN=0, Flags=, p, TC 397882 2018-11-16 00:17:08.099056 HedGloba_6s:69:11 Wmare_28:89:dd 602.11 154 Qc5 Data, SN=01, FN=0, Flags=, p, TC 397882 2018-11-16 00:17:08.010760 HedGloba_6s:69:11 Wmare_28:89:dd 602.11 154 Qc5 Data, SN=01, FN=0, Flags=, p, TC 397892 2018-11-16 00:17:08.010760 HedGloba_6s:69:11 Wmare_28:89:dd 602.11 57 802.11 Block Ack, Flags=, p, F, C 397892 2018-11-16 00:17:08.010805 Wmare_28:89:dd Mo2.11 57 802.11 Block Ack, Flags=, p, F, C 397892 2018-11-16 00:17:08.010805 Wmare_28:89:dd HedGloba_6s:69:11 602.11 5		Time	Source	Destination	Protocol	Length Info
397882 2018-11-16 00:17:08.098444 Vmare_28:89:dd HmdGloba_6s:69:11 802.11 154 QoS Data, Sh=1435, FN-0, Flags=, p,F.C 397883 2018-11-16 00:17:08.098495 Vmare_28:89:dd HmdGloba_6s:69:11 802.11 157 802.11 Block Ack, Flags=, p,F.C 397884 2018-11-16 00:17:08.098495 Vmare_28:89:dd HmdGloba_6s:69:11 802.11 154 QoS Data, Sh=1435, FN-0, Flags=, p,F.C 397885 2018-11-16 00:17:08.099095 HmdGloba_6s:69:11 Vmare_28:89:dd 802.11 154 QoS Data, Sh=103, FN=0, Flags=, p,TC 397885 2018-11-16 00:17:08.099095 HmdGloba_6s:69:11 Vmare_28:89:dd 802.11 154 QoS Data, Sh=102, FN=0, Flags=, p,TC 397885 2018-11-16 00:17:08.099095 HmdGloba_6s:69:11 Vmare_28:89:dd 802.11 154 QoS Data, Sh=102, FN=0, Flags=, p,TC 397887 2018-11-16 00:17:08.099055 Cisco_b4:3id:e4 (00:a3:8e:b4:3d:e4) (T_L HmdGloba_6s:69:11) (04:f1:28:6a:69:11) (RA) 802.11 154 QoS Data, Sh=103, FN=0, Flags=, p,TC 397892 2018-11-16 00:17:08.10172 Cisco_b4:3id:e4 (00:a3:8e:b4:3d:e4) (T_L HmdGloba_6a:69:11) (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=, p,FC 397892 2018-11-16 00:17:08.10172 Cisco_b4:3id:e4 (00:a3:8e:b4:3d:e4) (T_L HmdGloba_6a:69:11) (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=, p,FC 397892 2018-11-16 00:17:08.10182 Cisco_b4:3id:e4 (00:a3:8e:b4:3d:e4) (T_L HmdGloba_6a:69:11) (04:f1:28:6a:69:11) (RA) 802	397882 2018-11-16 00:17:08.098444 Vmmare_28:89:dd HmdGloba_6a:69:11 002.11 154 qoS Data, SN=1435, FN=0, Flags-, pF.C 397883 2018-11-16 00:17:08.098495 HmdGloba_6a:69:11 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (RA) 802.11 154 qoS Data, SN=101, FN=0, Flags-, pF.C 397884 2018-11-16 00:17:08.098495 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 154 qoS Data, SN=101, FN=0, Flags-, pF.C 397887 2018-11-16 00:17:08.099090 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 154 qoS Data, SN=101, FN=0, Flags-, pTC 397887 2018-11-16 00:17:08.099050 HmdGloba_6a:69:11 Vmmare_28:89:dd 802.11 154 qoS Data, SN=102, FN=0, Flags-, pTC 397887 2018-11-16 00:17:08.099050 HmdGloba_6a:69:11 Vmmare_28:89:dd 802.11 154 qoS Data, SN=102, FN=0, Flags-, pTC 397887 2018-11-16 00:17:08.099050 HmdGloba_6a:69:11 Vmmare_28:89:dd 802.11 154 qoS Data, SN=102, FN=0, Flags-, pTC 397891 2018-11-16 00:17:08.01052 Cisco_b4:31:et:04:31:et:04:61:11 Vmmare_28:89:dd 802.11 57 802.11 Block Ack, Flags-, pFC 397891 2018-11-16 00:17:08.01052 Cisco_b4:31:et:04:31:et:04:61:11 802.11 57 802.11 Block Ack, Flags-, p,FC 397891 2018-11-16 00:17:08.010545 Wmmare_28:89:dd HmdGloba_6a:69:11 802.11 57 802.11 Block Ack, Flags-, p,FC 397892 2018-11-16 00:17:08.10545		397881 2018-11-16 00:17:08.098393	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	1438 QoS Data, SN=1434, FN=0, Flags=.pR.F.C
397883 2018-11-16 00:17:08.098499 HmdGloba_6a:69:11 (04:f1:28:6a:69:11) Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (RA) 802.11 57 802.11 Block Ack, Flags-,,CC 397884 2018-11-16 00:17:08.098999 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 154 QoS Data, Sh=143, FN=0, Flags-, p,TC 397885 2018-11-16 00:17:08.099099 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 154 QoS Data, Sh=143, FN=0, Flags-, p,TC 397885 2018-11-16 00:17:08.099099 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 154 QoS Data, Sh=143, FN=0, Flags-, p,TC 397885 2018-11-16 00:17:08.09966 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 154 QoS Data, Sh=143, FN=0, Flags-, p,TC 397885 2018-11-16 00:17:08.09966 HmdGloba_6a:69:11 Wmare_28:89:dd 802.11 154 QoS Data, Sh=143, FN=0, Flags-, p,TC 397885 2018-11-16 00:17:08.101726 HmdGloba_6a:69:11 Wmare_28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, Sh=143, FN=0, Flags-, p,FC 397892 2018-11-16 00:17:08.10812 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_H HmdGloba_6a:69:11] 802.11 57 802.11 Block Ack, Flags-, p,FC 397894 2018-11-16 00:17:08.10812 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_H HmdGloba_6a:69:11] 802.11 57 802.11 Block Ack, Flags-, p,FC 397894 2018-11-16 00:17:0	397883 2018-11-16 00:17:08.098499 Hediclobs_6a:69:11 (04:f1:28:6a:69:11) Cisco_b4:3d:re4 (00:a3:8e:b4:3d:e4) (RA) 802.11 57 802.11 Block Ack, Flags=C 397864 2018-11-16 00:17:08.098999 Wender_28:89:dd Wonare_28:89:dd 802.11 154 Qc5 Data, SN=104, FH=0, Flags=.pTC 397867 2018-11-16 00:17:08.099090 Hediclobs_6a:69:11 Venare_28:89:dd 802.11 57 802.11 Block Ack, Flags=.pTC 397867 2018-11-16 00:17:08.099060 Hediclobs_6a:69:11 Venare_28:89:dd 802.11 57 802.11 Block Ack, Flags=.pTC 397869 2018-11-16 00:17:08.099660 Hediclobs_6a:69:11 Venare_28:89:dd 802.11 57 802.11 Block Ack, Flags=.pTC 397899 2018-11-16 00:17:08.010762 Hediclobs_6a:69:11 Venare_28:89:dd 802.11 57 802.11 Block Ack, Flags=.pTC 397891 2018-11-16 00:17:08.010762 Hediclobs_6a:69:11 Venare_28:89:dd Hediclobs_6a:69:11 602.11 57 802.11 Block Ack, Flags=.pTC 397892 2018-11-16 00:17:08.010762 Hediclobs_6a:69:11 Venare_28:89:dd Hediclobs_6a:69:11 602.11 57 802.11 Block Ack, Flags=.p, C 397892 2018-11-16 00:17:08.010762 Hediclobs_6a:69:11 Wenare_28:89:dd Hediclobs_6a:69:11 58 201.11 50 20.14 57 802.11 Block Ack, Flags=.p, F.C 397892		397882 2018-11-16 00:17:08.098444	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	154 QoS Data, SN=1435, FN=0, Flags=.pF.C
397884 2018-11-16 00:17:08.099099 Vmare_28:89:dd HmdGloba_6a:69:11 802.11 164 265 Oste, 5N-1435; FN-0, FlagsprTC 397886 2018-11-16 00:17:08.099099 HmdGloba_6a:69:11 Vmare_28:89:dd 802.11 154 QoS Data, SN=101; FN=0, FlagsprTC 397887 2018-11-16 00:17:08.099099 HmdGloba_6a:69:11 Vmare_28:89:dd 802.11 37 602.11 154 QoS Data, SN=101; FN=0, FlagsprTC 397887 2018-11-16 00:17:08.099055 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_L HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 802.11 154 QoS Data, SN=102; FN=0, FlagsprTC 397889 2018-11-16 00:17:08.101702 HmdGloba_6a:69:11 Vmare_28:89:dd 802.11 157 002.11 Block Ack, FlagsprTC 397890 2018-11-16 00:17:08.101702 HmdGloba_6a:69:11 Vmare_28:89:dd 802.11 57 802.11 Block Ack, FlagsprTC 397892 2018-11-16 00:17:08.101702 HmdGloba_6a:69:11 Vmare_28:89:dd HmdGloba_6a:69:11 802.11 57 802.11 Block Ack, Flagspr,FC 397892 2018-11-16 00:17:08.101655 Vmare_28:89:dd HmdGloba_6a:69:11 802.11 55 QoS Data, SN=1437, FN=0, Flagspr,FC 397892 2018-11-16 00:17:08.101655 Vmare_28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SN=1438, FN=0, Flagspr,FC 397892 2018-11-16 00:17:08.10555 <td>397884 2018-11-16 00:17:08.099999 Vmmare_28:89:dd HedGloba_6a:69:11 002.11 162 dof Data, SN-1436, FM-0, FlagspTC 397886 2018-11-16 00:17:08.099999 HmdGloba_6a:69:11 Vmmare_28:89:dd 802.11 154 doS Data, SN-101, FM-0, FlagspTC 397887 2018-11-16 00:17:08.099095 (isco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T</td> <td></td> <td>397883 2018-11-16 00:17:08.098495</td> <td>HmdGloba_6a:69:11 (04:f1:28:6a:69:11)_</td> <td>Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (RA)</td> <td>802.11</td> <td>57 802.11 Block Ack, Flags=C</td>	397884 2018-11-16 00:17:08.099999 Vmmare_28:89:dd HedGloba_6a:69:11 002.11 162 dof Data, SN-1436, FM-0, FlagspTC 397886 2018-11-16 00:17:08.099999 HmdGloba_6a:69:11 Vmmare_28:89:dd 802.11 154 doS Data, SN-101, FM-0, FlagspTC 397887 2018-11-16 00:17:08.099095 (isco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T		397883 2018-11-16 00:17:08.098495	HmdGloba_6a:69:11 (04:f1:28:6a:69:11)_	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (RA)	802.11	57 802.11 Block Ack, Flags=C
397886 2018-11-16 00:17:08.099090 HmdGlobs_6s:09:11 Vmware_28:89:dd 802.11 154 QoS Data, SH=101, FH=0, Flags=.pTC 397887 2018-11-16 00:17:08.099060 HmdGlobs_6s:09:11 Vmware_28:89:dd 802.11 154 QoS Data, SH=102, FH=0, Flags=.pTC 397888 2018-11-16 00:17:08.099060 HmdGlobs_6s:09:11 Vmware_28:89:dd 802.11 154 QoS Data, SH=102, FH=0, Flags=.pTC 397889 2018-11-16 00:17:08.099065 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T HmdGlobs_6s:09:11 (04:f1:28:6e:09:11) (RA) 802.11 154 QoS Data, SH=103, FH=0, Flags=.pTC 397899 2018-11-16 00:17:08.101708 HmdGlobs_6s:09:11 Vmware_28:89:dd 802.11 154 QoS Data, SH=103, FH=0, Flags=.pTC 397892 2018-11-16 00:17:08.1080512 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T HmdGloba_6s:09:11) (RA) 802.11 57 802.11 Block Ack, Flags=.pTC 397892 2018-11-16 00:17:08.1080512 Vmware_28:89:dd HmdGloba_6s:09:11 802.11 57 802.11 Block Ack, Flags=.p,C 397892 2018-11-16 00:17:08.1080545 Vmware 28:89:dd HmdGloba_6s:09:11 802.11 57 802.11 Block Ack, Flags=.p,F.C 397892 2018-11-16 00:17:08.1080545 Vmware 28:89:dd HmdGloba_6s:09:11 802.11 55 QoS Data, SH=143, FN=0, Flags=.p,F.C 397892 2018-11-16 00:17:08.1080545 Vmware 28:89:dd HmdGloba_6s:09:11 802.11 154 QoS Data, SH=143, FN=0, Flags=.p,F.C	397886 2018-11-16 00:17:08.099090 Heddlobe_da:69:11 Vmmare_28:89:dd 802.11 154 QoS Data, SN=101, FN=0, Flags=, p,TC 397887 2018-11-16 00:17:08.099181 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_m HmdGlobe_Ga:69:11) (04:f1:28:6a:69:11) (RA) 802.11 57 007.11 Block Ack, Flags=, p,TC 397887 2018-11-16 00:17:08.09965 HmdGlobe_da:69:11 Vmmare_28:89:dd 802.11 57 007.11 Block Ack, Flags=, p,TC 397889 2018-11-16 00:17:08.09965 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_m HmdGlobe_Ga:69:11) (A4:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=, p,TC 397890 2018-11-16 00:17:08.101812 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_m HmdGlobe_Ga:69:11) (A4:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=, p,TC 397891 2018-11-16 00:17:08.101812 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_m HmdGlobe_Ga:69:11) (A4:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=, p,FC 397892 2018-11-16 00:17:08.106455 Vmmare_28:89:dd HmdGlobe_Ga:69:11 802.11 57 802.11 Block Ack, Flags=, p,FC 397894 2018-11-16 00:17:08.106455 Vmmare_28:89:dd HmdGlobe_Ga:69:11 802.11 57 802.11 Block Ack, Flags=, p,FC 397894 2018-11-16 00:17:08.106455 Vmmare_28:89:dd HmdGlobe_Ga:69:11 802.11 50 QoS Data, SN=143, FN=0, Flags=, p,FC 1		397884 2018-11-16 00:17:08.098999	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	162 QoS Data, SN-1436, FN-0, FlagspF.C
397887 2018-11-16 00:17:08.099181 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T	397887 2018-11-16 00:17:08.099181 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T		397886 2018-11-16 00:17:08.099099	HmdGloba_6a:69:11	Vmware_28:89:dd	802.11	154 QoS Data, SN=101, FN=0, Flags=.pTC
397888 2018-11-16 00:17:08.099665 HmdGloba_6a:69:11 Vmware_28:99:dd 802.11 154 QoS Data, SH=102, FH=0, Flags=.p,TC 397869 2018-11-16 00:17:08.099655 Cisco_b4:3i:e4 (00:a3:8e:b4:3d:e4) (T. HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 802.11 157 802.11 Block Ack, Flags=.p,TC 397891 2018-11-16 00:17:08.01072 HmdGloba_6a:69:11 Vmware_28:89:dd 802.11 57 802.11 Block Ack, Flags=.p,TC 397891 2018-11-16 00:17:08.01072 LmdGloba_6a:69:11 Vmware_28:89:dd 802.11 57 802.11 Block Ack, Flags=.p,TC 397892 2018-11-16 00:17:08.010852 Vmware_28:89:dd HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.p,TC 397894 2018-11-16 00:17:08.010855 Vmware_28:89:dd HmdGloba_6a:69:11 802.11 55 00 Data, Sh=132, FN=0, Flags=.p,F.C 397894 2018-11-16 00:17:08.010655 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, Sh=1438, FN=0, Flags=.p,F.C 397894 2018-11-16 00:17:08.010655 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, Sh=1438, FN=0, Flags=.p,F.C 397894 2018-11-16 00:17:08.010655 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, Sh=1438, FN=0, Flags=.p,F.C Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header V0, Length 48 802.11 154 QoS Data, Flags: .p,F.C	397888 2018-11-16 00:17:08.099666 Hedlolob_@a:69:11 Vmmare_28:89:dd 902.11 154 0x5 Data, SN=102, FN=0, Flags=,p,TC 397898 2018-11-16 00:17:08.099655 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (THmdGloba_Ga:69:11) (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.,p,TC 397891 2018-11-16 00:17:08.10172 HmdGloba_Ga:69:11 Vmmare_28:89:dd 802.11 57 802.11 Block Ack, Flags=.p,TC 397891 2018-11-16 00:17:08.10182 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (THmdGloba_Ga:69:11) (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.p,TC 397892 2018-11-16 00:17:08.10182 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (THmdGloba_Ga:69:11) (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.p,TC 397892 2018-11-16 00:17:08.10855 Vmmare_28:89:dd HmdGloba_Ga:69:11 802.11 57 802.11 Block Ack, Flags=.p,F.C 397894 2018-11-16 00:17:08.10856 Vmmare 28:89:dd HmdGloba_Ga:69:11 802.11 154 QoS Data, SN=1433, FN=0, Flags=.p,F.C Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radictap Header v0, Length 43 802.11 CoS Data, Flags: .p,TC Data (66 bytes) S7 802.11 Block Ack, Flags=.p,F.C		397887 2018-11-16 00:17:08.099181	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T.	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=
397889 2018-11-16 00:17:08.099655 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T MedGloba_6a:69:11) (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, FlagsC 397890 2018-11-16 00:17:08.10475 MedGloba_6a:69:11 Venare_23:89:40 802.11 57 802.11 Block Ack, FlagsC 397891 2018-11-16 00:17:08.10453 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T MedGloba_6a:69:11) (RA:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, FlagsC 397891 2018-11-16 00:17:08.104535 Venare_28:89:dd HmdGloba_6a:69:11 802.11 57 802.11 Block Ack, FlagsC 397892 2018-11-16 00:17:08.104555 Venare_28:89:dd HmdGloba_6a:69:11 802.11 57 802.11 Block Ack, FlagsC 397894 2018-11-16 00:17:08.104555 Venare_28:89:dd HmdGloba_6a:69:11 802.11 57 802.11 Block Ack, FlagsC 397894 2018-11-16 00:17:08.104555 Venare_28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SN=1438, FN=0, Flags,F.C Frame 397865: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) 154 bytes captured (1232 bits) 154 goS Data, Flags:TC Data (66 bytes) Life flags:TC Data (66 bytes) Life flags:TC	397889 2018-11-16 00:17:08.099655 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_ HmdGloba_a6:69:11) (04:f1:28:6a:69:11) (8A) 802.11 57 802.11 Block Ack, Flags=TC 397891 2018-11-16 00:17:08.1016812 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_ HmdGloba_a6:69:11) (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=C 397891 2018-11-16 00:17:08.1016812 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_ HmdGloba_a6:69:11) (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=C 397891 2018-11-16 00:17:08.106805 Vmware_28:89:dd HmdGloba_a6:69:11 802.11 57 802.11 Block Ack, Flags=C 397892 2018-11-16 00:17:08.106905 Vmware_28:89:dd HmdGloba_a6:69:11 802.11 57 802.11 Block Ack, Flags=C 7Fame 397894 2018-11-16 00:17:08.106905 Vmware_28:89:dd HmdGloba_a6:69:11 802.11 57 802.11 Block Ack, Flags=C 7Fame 397894 2018-11-16 00:17:08.106905 Vmware_28:89:dd HmdGloba_a6:69:11 802.11 57 802.11 Block Ack, Flags=C 7Fame 3978962 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) 154 bytes captu		397888 2018-11-16 00:17:08.099606	HmdGloba_6a:69:11	Vmware_28:89:dd	802.11	154 QoS Data, SN=102, FN=0, Flags=.pTC
397890 2018-11-16 00:17:08.101762 HmdGloba_63:69:11 Vmmare_23:89:dd 802.11 479 QoS Data, 5N=103, FN=0, Flags=.p,TC 397801 2018-11-16 00:17:08.101812 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T HmdGloba_6a:69:11) (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.p,FC 397802 2018-11-16 00:17:08.101812 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T HmdGloba_6a:69:11) (04:f1:28:6a:69:11) (RA) 802.11 55 QoS Data, 5N=1437, FN=0, Flags=.p,FC 397802 2018-11-16 00:17:08.106055 Vmmare_28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, 5N=1438, FN=0, Flags=.p,FC 397804 2018-11-16 00:17:08.106055 Vmmare 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, 5N=1438, FN=0, Flags=.p,F.C Frame 397806: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Its) Flags: p,FC Stags: p,FC Radiotap Header v0, Length 48 802.11 radio information Its Stags: p,FC Stags: p,FC Data (68 bytes) Data (68 bytes) Flags: .p,TC Stags: p,FC Stags: p,FC	397890 2018-11-16 00:17:08.101762 HmdGloba_6a:69:11 Vmware_28:89:dd 802.11 479 QoS Data, SN=103, FN=0, Flags=, p,C 397892 2018-11-16 00:17:08.10812 Cisco_b4:3d:e4 (060:33:88:b4:3d:e4) (T_H HmdGloba_6a:669:11) (04:f1:28:6a:69:11) (8A) 802.11 57 802.11 Block Ack, Flags=C 397892 2018-11-16 00:17:08.108205 Vmware_28:89:dd HmdGloba_6a:69:11 802.11 595 QoS Data, SN=1437, FN=0, Flags=.p,F.C 397892 2018-11-16 00:17:08.10805 Vmware_28:89:dd HmdGloba_6a:69:11 802.11 595 QoS Data, SN=1433, FN=0, Flags=.p,F.C 397892 2018-11-16 00:17:08.10805 Vmware_28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SN=1433, FN=0, Flags=.p,F.C		397889 2018-11-16 00:17:08.099655	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T.	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=C
397891 2018-11-16 00:17:08.101832 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T. HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=,F.C 397892 2018-11-16 00:17:08.108056 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 595 Qos Data, Sh=1437, FN=0, Flags=, pF.C 397894 2018-11-16 00:17:08.108056 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 Qos Data, Sh=1438, FN=0, Flags=, pF.C Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) 154 802.11 154 Qos Data, Sh=1438, FN=0, Flags=, pF.C Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) 154 802.11 154 Qos Data, Flags: .pF.C Data (68 bytes) Data (68 bytes) Flags: .pTC Data (68 bytes) Flags: .pTC	397891 2018-11-16 00:17:08.101812 Cisco_b4:30:e4 (40:33:8e:b4:3d:e4) (T HmdGloba_6a:69:11) (04:f1:28:6a:69:11) 802.11 597 802.11 Block Ack, Flags=		397890 2018-11-16 00:17:08.101762	HmdGloba_6a:69:11	Vmware_28:89:dd	802.11	479 QoS Data, SN=103, FN=0, Flags=.pTC
397892 2018-11-16 00:17:08.105955 Vmware_28:89:dd HmdGloba_6a:69:11 802.11 595 QoS Data, SN=1437, FN=0, Flags=.pF.C 397894 2018-11-16 00:17:08.106055 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SN=1438, FN=0, Flags=.pF.C	397892 2018-11-16 00:17:08.105958 Vmware_28:89:dd HmdGloba_6a:69:11 802.11 595 (oS Data, SN=1437, FN=0, Flags=, pF.C 397892 2018-11-16 00:17:08.106055 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 Upts (oS Data, SN=1438, FN=0, Flags=, pF.C Frame 397896: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header v0, Length 48 802.11 rds10 information IEEE 802.11 (oS Data, Flags: .pTC Data (68 bytes)		397891 2018-11-16 00:17:08.101812	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T.	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=C
397894 2018-11-16 00:17:08.1060955 Vmmare 20:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, 5N=1438, FN=0, Flags=.pF.C Frame 397806: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header v0, Length 48 802.11 radio information IEEE 802.11 (OS Data, Flags: .pTC Data (68 bytes)	397894 2018-11-16 00:17:08.106055 Vmware 28:80:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SN=1438, FN=0, Flags=.pF.C Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header v0, Length 48 802.11 radio information EEE 802.11 (9C Data, Flags: .pTC Data (68 bytes)		397892 2018-11-16 00:17:08.105958	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	595 QoS Data, SN=1437, FN=0, Flags=.pF.C
Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header V0, Length 48 802.11 radio information IEEE 802.11 QoS Data, Flags: .pTC Data (68 bytes)	Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header V0, Length 48 802.11 radio information IEEE 802.11 QoS Data, Flags: .pTC Data (68 bytes)		397894 2018-11-16 00:17:08.106056	Vmware 28:89:dd	HmdGloba_6a:69:11	802.11	154 QoS Data, SN=1438, FN=0, Flags=.pF.C
	00 00 00 00 30 00 6b 08 1c 00 6d F9 30 31 00 00 00 00 · 0 k·····················	00 00	00 30 00 65 08 1c 00 6d f9 30 31 00	00 00 00 -0 k - m 01			
00 00 00 30 00 65 08 1c 00 6d f9 30 31 00 00 00 00 ·····················	00 00 00 00 30 00 50 81 C 00 5d 19 30 31 00 00 00 00 00 -0 k. m 01 10 14 00 9e 09 30 04 d9 a4 00 00 00 30 60 04 01 00 10 9e 09 30 -2 31 f0 06 06 55 00 08 00 40 01 00 00	00 00 10 14 20 9=	00 30 00 65 08 1c 00 6d f9 30 31 00 00 9c 09 30 04 d9 a4 00 00 00 08 30 09 05 22 16 09 66 00 55 00 aa aa	90 90 90 0 k··· m·01···· 94 91 90			
00 00 00 60 64 f9 30 10 00 <td< td=""><td>00 00 00 00 00 00 00 00 00 10 00 10 00 0</td><td>00 00 10 14 20 9e 30 88</td><td>00 30 00 65 08 1c 00 6d f9 30 31 00 00 9c 09 50 04 d9 44 00 00 00 00 00 09 05 22 1f 00 06 00 55 00 00 00 4 1 30 00 00 03 36 c 54 36 c 40 4f 12 8</td><td>00 00 00 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td><td></td><td></td><td></td></td<>	00 00 00 00 00 00 00 00 00 10 00 10 00 0	00 00 10 14 20 9e 30 88	00 30 00 65 08 1c 00 6d f9 30 31 00 00 9c 09 50 04 d9 44 00 00 00 00 00 09 05 22 1f 00 06 00 55 00 00 00 4 1 30 00 00 03 36 c 54 36 c 4 0 4f 12 8	00 00 00 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0			
00 00 <td< td=""><td>00 <td< td=""><td>000 00 119 14 120 9e 330 88 340 00</td><td>00 30 00 65 06 1c 00 6d f9 30 31 00 00 9c 09 30 04 d9 44 00 00 00 00 80 90 b2 21 f0 00 60 00 55 00 00 00 44 11 30 00 00 a3 8c 54 3d e4 41 23 C 29 28 90 d5 00 60 00 00 c8 84 00</td><td>00 00 00 00 00 k m 01 04 01 00 00 00 00 c e c (j1 20 01 00) (P</td><td></td><td></td><td></td></td<></td></td<>	00 00 <td< td=""><td>000 00 119 14 120 9e 330 88 340 00</td><td>00 30 00 65 06 1c 00 6d f9 30 31 00 00 9c 09 30 04 d9 44 00 00 00 00 80 90 b2 21 f0 00 60 00 55 00 00 00 44 11 30 00 00 a3 8c 54 3d e4 41 23 C 29 28 90 d5 00 60 00 00 c8 84 00</td><td>00 00 00 00 00 k m 01 04 01 00 00 00 00 c e c (j1 20 01 00) (P</td><td></td><td></td><td></td></td<>	000 00 119 14 120 9e 330 88 340 00	00 30 00 65 06 1c 00 6d f9 30 31 00 00 9c 09 30 04 d9 44 00 00 00 00 80 90 b2 21 f0 00 60 00 55 00 00 00 44 11 30 00 00 a3 8c 54 3d e4 41 23 C 29 28 90 d5 00 60 00 00 c8 84 00	00 00 00 00 00 k m 01 04 01 00 00 00 00 c e c (j1 20 01 00) (P			
00 00 <td< td=""><td>00 <td< td=""><td>000 00 010 14 020 9e 030 88 040 00 050 00</td><td>00 30 00 65 08 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 a4 00 00 00 60 80 90 8b 22 16 00 60 00 55 09 00 00 44 41 30 00 00 a3 5e b4 3d e4 04 f1 28 0c 29 28 59 dd 50 66 00 00 c8 84 00 0a ff 4c 2 2f 90 d1 14 52 a5 8b 2e</td><td>00 00 00 · 0 k· · m·01···· 04 01 00 06 00 00 · · · · · · · · · · · · · · · ·</td><td></td><td></td><td></td></td<></td></td<>	00 00 <td< td=""><td>000 00 010 14 020 9e 030 88 040 00 050 00</td><td>00 30 00 65 08 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 a4 00 00 00 60 80 90 8b 22 16 00 60 00 55 09 00 00 44 41 30 00 00 a3 5e b4 3d e4 04 f1 28 0c 29 28 59 dd 50 66 00 00 c8 84 00 0a ff 4c 2 2f 90 d1 14 52 a5 8b 2e</td><td>00 00 00 · 0 k· · m·01···· 04 01 00 06 00 00 · · · · · · · · · · · · · · · ·</td><td></td><td></td><td></td></td<>	000 00 010 14 020 9e 030 88 040 00 050 00	00 30 00 65 08 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 a4 00 00 00 60 80 90 8b 22 16 00 60 00 55 09 00 00 44 41 30 00 00 a3 5e b4 3d e4 04 f1 28 0c 29 28 59 dd 50 66 00 00 c8 84 00 0a ff 4c 2 2f 90 d1 14 52 a5 8b 2e	00 00 00 · 0 k· · m·01···· 04 01 00 06 00 00 · · · · · · · · · · · · · · · ·			
00 00 <td< td=""><td>00 <td< td=""><td>00 00 10 14 20 9e 30 88 40 00 50 00 60 d8</td><td>00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9c 09 50 04 d9 40 00<!--</td--><td>00 00 00 · 0 · k · · m · 01 · · · · · · · · · · · · · · · · ·</td><td></td><td></td><td></td></td></td<></td></td<>	00 00 <td< td=""><td>00 00 10 14 20 9e 30 88 40 00 50 00 60 d8</td><td>00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9c 09 50 04 d9 40 00<!--</td--><td>00 00 00 · 0 · k · · m · 01 · · · · · · · · · · · · · · · · ·</td><td></td><td></td><td></td></td></td<>	00 00 10 14 20 9e 30 88 40 00 50 00 60 d8	00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9c 09 50 04 d9 40 00 </td <td>00 00 00 · 0 · k · · m · 01 · · · · · · · · · · · · · · · · ·</td> <td></td> <td></td> <td></td>	00 00 00 · 0 · k · · m · 01 · · · · · · · · · · · · · · · · ·			
00 00	00 00 <td< td=""><td>00 00 19 14 28 9e 38 88 48 00 59 00 66 d8 70 5c</td><td>00 30 00 65 08 1c 00 6d f9 30 31 00 00 90 20 21 00<!--</td--><td>60 00 00 00 00 k m 01 00 00 00 00 00 00 00 00 00 00 00 00</td><td></td><td></td><td></td></td></td<>	00 00 19 14 28 9e 38 88 48 00 59 00 66 d8 70 5c	00 30 00 65 08 1c 00 6d f9 30 31 00 00 90 20 21 00 </td <td>60 00 00 00 00 k m 01 00 00 00 00 00 00 00 00 00 00 00 00</td> <td></td> <td></td> <td></td>	60 00 00 00 00 k m 01 00 00 00 00 00 00 00 00 00 00 00 00			

Attention : Vous pouvez rencontrer un problème avec Wireshark lors du déchiffrement, et dans ce cas, même si le bon PMK est fourni (ou si PSK est utilisé, SSID et PSK sont fournis), Wireshark ne déchiffre pas la capture OTA. La solution de contournement consiste à désactiver Wireshark et à le désactiver plusieurs fois jusqu'à ce que des informations de couche supérieure puissent être obtenues et que les paquets 802.11 ne soient plus affichés comme des données QoS, ou à utiliser un autre PC/Mac sur lequel Wireshark est installé.

Conseil : Un code C++ appelé pmkXtract est joint dans le premier billet de la rubrique Informations connexes. Les tentatives de compilation ont été réussies et un fichier exécutable est obtenu, mais le programme exécutable ne semble pas effectuer le déchiffrement correctement pour certaines raisons inconnues. En outre, un script Python qui tente d'extraire PMK est publié dans la zone des commentaires sur le premier billet, qui peut être exploré plus avant si les lecteurs sont intéressés.

Informations connexes

- Effacer le lien faible d'EAP : retirer les PMK WiFi de RADIUS avec pmkXtract
- Comment décoder Radius MS-MPPE-Recv-Key
- Support et documentation techniques Cisco Systems