

## Monitorización del proceso de conexión mediante un analizador de protocolos 802.11

El proceso de conexión se puede dividir en cuatro etapas:

- Etapa de búsqueda "scanning".
- Etapa de autenticación.
- Etapa de asociación.
- Etapa de negociación de clave.

A continuación se muestra la captura realizada de una trama de sondeo o beacon 802.11 enviada por el punto de acceso. Se han desplegado todos los campos de la cabecera con objeto de mostrar toda la información que transporta este tipo de trama, especialmente la que se muestra sombreada. Posteriormente se muestra el proceso de conexión indicando únicamente los campos más relevantes.

### CAPTURA DEL UN BEACON: búsqueda pasiva

No.	Time	Source	Destination	Protocol Info	
1	0.000000000	Cisco-Li_de:77:8e	Broadcast	Beacon frame	SSID: "LABTLMAT"



Protocols in frame: wlan

IEEE 802.11

Data Rate: 1.0 Mb/s

Channel: 1

Type/Subtype: Beacon frame (8)

Frame Control: 0x0080 (Normal)

Version: 0

Type: Management frame (0)

Subtype: 8

Flags: 0x0

DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)

.... 0.. = More Fragments: This is the last fragment

.... 0... = Retry: Frame is not being retransmitted

...0 .... = PWR MGT: STA will stay up

..0. .... = More Data: No data buffered

.0.. .... = Protected flag: Data is not protected

0... .... = Order flag: Not strictly ordered

Duration: 0

Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

Source address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)

BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)

Fragment number: 0

Sequence number: 486

Frame check sequence: 0xf0cb4ece [correct]

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Timestamp: 0x000000CE6526F18A

Beacon Interval: 0,102400 [Seconds]

Capability Information: 0x0011

.... 1 = ESS capabilities: Transmitter is an AP

.... 0.. = IBSS status: Transmitter belongs to a BSS

.... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)

.... 1 .... = Privacy: AP/STA can support WEP

.... 0. .... = Short Preamble: Short preamble not allowed

.... 0.. .... = PBCC: PBCC modulation not allowed

.... 0... .... = Channel Agility: Channel agility not in use

.... 0 .... = Spectrum Management: dot11SpectrumManagementRequired FALSE

.... 0.. .... = Short Slot Time: Short slot time not in use

.... 0... .... = Automatic Power Save Delivery: apsd not implemented

..0. .... = DSSS-OFDM: DSSS-OFDM modulation not allowed

.0.. .... = Delayed Block Ack: delayed block ack not implemented

0... .. = Immediate Block Ack: immediate block ack not implented  
 Tagged parameters (59 bytes)  
 SSID parameter set: "LABTLMAT"  
 Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) → Las cuatro velocidades soportadas son además velocidades básicas.  
 DS Parameter set: Current Channel: 1  
 (TIM) Traffic Indication Map: DTIM 0 of 1 bitmap empty  
 Vendor Specific: WPA  
 Tag interpretation: WPA IE, type 1, version 1  
 Tag interpretation: Multicast cipher suite: TKIP  
 Tag interpretation: Unicast cipher suite 1: TKIP  
 Tag interpretation: auth key management suite 1: PSK

## CAPTURA DEL PROCESO DE CONEXIÓN.

### 1- ETAPA DE BÚSQUEDA: Búsqueda activa mediante intercambio Probe Request/Probe Response

No.	Time	Source	Destination	Protocol Info	SSID
628	27.553035736	Cisco-Li_bd:83:94	Broadcast	Probe Request	Broadcast

↓

Protocols in frame: wlan  
 IEEE 802.11  
 Data Rate: 1.0 Mb/s  
 Channel: 1  
 Type/Subtype: Probe Request (4)  
 Frame Control: 0x0040 (Normal)  
 Version: 0  
 Type: Management frame (0)  
 Subtype: 4  
 Flags: 0x0  
 DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0)  
 (0x00)  
 .... 0.. = More Fragments: This is the last fragment  
 .... 0.. = Retry: Frame is not being retransmitted  
 ...0 .... = PWR MGT: STA will stay up  
 ..0. .... = More Data: No data buffered  
 .0.. .... = Protected flag: Data is not protected  
 0... .... = Order flag: Not strictly ordered  
 Destination address: Broadcast (ff:ff:ff:ff:ff:ff)  
 Source address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)  
 BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)  
 IEEE 802.11 wireless LAN management frame  
 SSID parameter set: Broadcast  
 Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B)

No.	Time	Source	Destination	Protocol Info	SSID
629	27.554828644	Cisco-Li_de:77:8e	Cisco-Li_bd:83:94	Probe Response	"LABTLMAT"

↓

Protocols in frame: wlan  
 IEEE 802.11  
 Data Rate: 1.0 Mb/s  
 Channel: 1  
 Type/Subtype: Probe Response (5)  
 Frame Control: 0x0850 (Normal)  
 Destination address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)  
 Source address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 IEEE 802.11 wireless LAN management frame  
 Fixed parameters (12 bytes)  
 Timestamp: 0x000000CE66CB6FA5

El cliente inalámbrico envía una trama de gestión Probe Request buscando puntos de acceso.

El punto de acceso responde al cliente mediante una trama de gestión Probe Response indicando sus capacidades, que son las mismas que envió en sus beacons.

Beacon Interval: 0,102400 [Seconds]  
 Capability Information: 0x0011  
 SSID parameter set: "LABTLMAT"  
 Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B)  
 DS Parameter set: Current Channel: 1  
 Vendor Specific: WPA  
 Tag interpretation: WPA IE, type 1, version 1  
 Tag interpretation: Multicast cipher suite: TKIP  
 Tag interpretation: Unicast cipher suite 1: TKIP  
 Tag interpretation: auth key management suite 1: PSK

No.	Time	Source	Destination	Protocol Info
630	27.555133819		Cisco-Li_de:77:8e (RA)	Acknowledgement

Protocols in frame: wlan  
 IEEE 802.11  
 Data Rate: 1.0 Mb/s  
 Channel: 1  
 Type/Subtype: Acknowledgement (29)  
 Frame Control: 0x00D4 (Normal)  
 Receiver address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 Frame check sequence: 0xe7716888 [correct]

Primer reconocimiento 802.11 que envía el cliente al punto de acceso por ser la primera trama unicast

## 2- ETAPA DE AUTENTICACIÓN

No.	Time	Source	Destination	Protocol Info
706	30.513029099	Cisco-Li_bd:83:94	Cisco-Li_de:77:8e	Authentication

Protocols in frame: wlan  
 IEEE 802.11  
 Data Rate: 1.0 Mb/s  
 Channel: 1  
 Type/Subtype: Authentication (11)  
 Frame control: 0x00B0 (Normal)  
 Type: Management frame (0)  
 Destination address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 Source address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)  
 BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 Fragment number: 0  
 Sequence number: 117  
 Frame check sequence: 0xfbeab99d [correct]  
 IEEE 802.11 wireless LAN management frame  
 Authentication Algorithm: Open System (0)  
 Authentication SEQ: 0x0001  
 Status code: Successful (0x0000)

El cliente inalámbrico envía una solicitud de autenticación en código abierto al punto de acceso.

No.	Time	Source	Destination	Protocol Info
707	30.513334274		Cisco-Li_bd:83:94 (RA)	Acknowledgement

Receiver address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)

Reconocimiento 802.11 que envía el punto de acceso al cliente inalámbrico.

No.	Time	Source	Destination	Protocol Info
708	30.513921738	Cisco-Li_de:77:8e	Cisco-Li_bd:83:94	Authentication

Protocols in frame: wlan  
 IEEE 802.11

El punto de acceso responde confirmando la petición del punto de acceso

Data Rate: 1.0 Mb/s  
Channel: 1  
Type/Subtype: Authentication (11)  
Frame Control: 0x00B0 (Normal)  
Version: 0  
Type: Management frame (0)  
Subtype: 11  
Flags: 0x0  
.0.. .... = Protected flag: Data is not protected  
Destination address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)  
Source address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
IEEE 802.11 wireless LAN management frame  
Authentication Algorithm: Open System (0)  
Authentication SEQ: 0x0002  
Status code: Successful (0x0000)

No.	Time	Source	Destination	Protocol Info
709	30.514230728		Cisco-Li_de:77:8e (RA)	Acknowledgement



Reconocimiento 802.11  
que envía e cliente.

### 3- ETAPA DE ASOCIACIÓN

No.	Time	Source	Destination	Protocol Info
710	30.515144348	Cisco-Li_bd:83:94	Cisco-Li_de:77:8e	Association Request SSID: LABTLMAT"



Protocols in frame: wlan  
IEEE 802.11

Data Rate: 1.0 Mb/s  
Channel: 1  
Type/Subtype: Association Request (0)  
Frame Control: 0x0000 (Normal)  
Version: 0  
Type: Management frame (0)  
Subtype: 0  
Duration: 314  
Destination address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
Source address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)  
BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
IEEE 802.11 wireless LAN management frame  
Fixed parameters (4 bytes)  
Capability Information: 0x0011  
Tagged parameters (47 bytes)  
SSID parameter set: "LABTLMAT"  
Supported Rates: 1,0 2,0 5,5 11,0  
Vendor Specific: WPA  
Tag interpretation: WPA IE, type 1, version 1  
Tag interpretation: Multicast cipher suite: TKIP  
Tag interpretation: Unicast cipher suite 1: TKIP  
Tag interpretation: auth key management suite 1: PSK

El cliente inalámbrico envía  
una petición de asociación al  
punto de acceso.

No.	Time	Source	Destination	Protocol Info
711	30.515443802		Cisco-Li_bd:83:94 (RA)	Acknowledgement



Reconocimiento 802.11  
que envía el punto de  
acceso.

No.	Time	Source	Destination	Protocol Info
712	30.516561508	Cisco-Li_de:77:8e	Cisco-Li_bd:83:94	Association Response

Protocols in frame: wlan  
IEEE 802.11

Data Rate: 1.0 Mb/s

Channel: 1

Type/Subtype: Association Response (1)

Frame Control: 0x0010 (Normal)

Version: 0

Type: Management frame (0)

Subtype: 1

Flags: 0x0

DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0)  
(0x00)

.... 0.. = More Fragments: This is the last fragment

.... 0... = Retry: Frame is not being retransmitted

...0 .... = PWR MGT: STA will stay up

..0. .... = More Data: No data buffered

.0.. .... = Protected flag: Data is not protected

0... .... = Order flag: Not strictly ordered

Duration: 314

Destination address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)

Source address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)

BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)

Frame check sequence: 0x3ce9f17e [correct]

IEEE 802.11 wireless LAN management frame

Fixed parameters (6 bytes)

Capability Information: 0x0011

Status code: Successful (0x0000)

Association ID: 0x0004

El punto de acceso asigna el identificador 4 a esta asociación.

Tagged parameters (14 bytes)

Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B)

No.	Time	Source	Destination	Protocol Info
713	30.516883850		Cisco-Li_de:77:8e (RA)	Acknowledgement

Reconocimiento 802.11.

#### 4- ETAPA DE NEGOCIACIÓN DE CLAVE

No.	Time	Source	Destination	Protocol Info
714	30.517518997	Cisco-Li_de:77:8e	Cisco-Li_bd:83:94	EAPOL Key

Protocols in frame: wlan:llc:eapol  
IEEE 802.11

Data Rate: 11.0 Mb/s

Channel: 1

Type/Subtype: Data (32)

Frame Control: 0x0208 (Normal)

Version: 0

Type: Data frame (2)

Subtype: 0

Flags: 0x2

1ª primitiva del 4-Way Handshaking: el punto de acceso envía el "Nonce" al cliente en claro, utilizando un mensaje EAPOL.

Los mensajes EAPOL del protocolo 802.1X viajan en tramas 802.11 de datos. Por tanto la velocidad es de 11 Mbps.

DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x02)

.... 0.. = More Fragments: This is the last fragment

.... 0... = Retry: Frame is not being retransmitted

...0 .... = PWR MGT: STA will stay up

..0. .... = More Data: No data buffered

.0.. .... = Protected flag: Data is not protected

0... .... = Order flag: Not strictly ordered

Duration: 213

Destination address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)

BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)

Source address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)

Frame check sequence: 0x9d0af925 [correct]

Logical-Link Control

DSAP: SNAP (0xaa)

IG Bit: Individual

SSAP: SNAP (0xaa)

CR Bit: Command

Control field: U, func=UI (0x03)

000. 00.. = Command: Unnumbered Information (0x00)

.... ..11 = Frame type: Unnumbered frame (0x03)

Organization Code: Encapsulated Ethernet (0x000000)

Encapsulado RFC 1042

Type: 802.1X Authentication (0x888e)

802.1X Authentication

Version: 1

Type: Key (3)

Length: 95

Descriptor Type: EAPOL WPA key (254)

Key Information: 0x0089

.... .... 001 = Key Descriptor Version: HMAC-MD5 for MIC and RC4 for encryption (1)

.... .... 1... = Key Type: Pairwise key

.... .... 1... .... = Key Ack flag: Set

.... .... 0... .... = Key MIC flag: Not set

Petición de confirmación, devolviendo el Replay Counter recibido.

Key Length: 32

Replay Counter: 3

Nonce: 1F4C818CEA48F0BEDFEACF26ECCF0C3B23716FB4D348D213...

Key IV: 00000000000000000000000000000000

WPA Key RSC: 0000000000000000

WPA Key ID: 0000000000000000

WPA Key MIC: 00000000000000000000000000000000

WPA Key Data Length: 0

No.	Time	Source	Destination	Protocol Info
715	30.517707825		Cisco-Li_de:77:8e (RA)	Acknowledgement

Protocols in frame: wlan

IEEE 802.11

Data Rate: 11.0 Mb/s

Reconocimiento 802.11 que envía el cliente. Es el primer reconocimiento que se envía a 11 Mbps, máxima velocidad básica de datos.

No.	Time	Source	Destination	Protocol Info
716	30.527397156	Cisco-Li_bd:83:94	Cisco-Li_de:77:8e	EAPOL Start

Protocols in frame: wlan:llc:eapol:data

IEEE 802.11

Data Rate: 11.0 Mb/s

Channel: 1

Signal Strength: 48%

Type/Subtype: Data (32)

Primitiva opcional que envía el cliente para indicar el comienzo de la fase EAPOL

Frame Control: 0x0108 (Normal)  
 Version: 0  
 Type: Data frame (2)  
 Subtype: 0  
 BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 Source address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)  
 Destination address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 Frame check sequence: 0x01c9baa3 [correct]

Logical-Link Control  
 802.1X Authentication  
 Version: 1  
 Type: Start (1)

No.	Time	Source	Destination	Protocol Info
717	30.527584076		Cisco-Li_bd:83:94 (RA)	Acknowledgement



No.	Time	Source	Destination	Protocol Info
718	30.529592514	Cisco-Li_bd:83:94	Cisco-Li_de:77:8e	Reconocimiento 802.11 que envía el punto de acceso.



Protocols in frame: wlan:llc:eapol  
 IEEE 802.11

Data Rate: 11.0 Mb/s  
 Type/Subtype: Data (32)  
 Frame Control: 0x0108 (Normal)  
 Version: 0  
 Type: Data frame (2)  
 Subtype: 0  
 Flags: 0x1

DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x01)

.... 0.. = More Fragments: This is the last fragment

.... 0... = Retry: Frame is not being retransmitted

...0 .... = PWR MGT: STA will stay up

..0. .... = More Data: No data buffered

**..0. .... = Protected flag: Data is not protected**

0... .... = Order flag: Not strictly ordered

BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)

Source address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)

Destination address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)

Frame check sequence: 0x3a0aba3f [correct]

Logical-Link Control  
 802.1X Authentication

Version: 1  
 Type: Key (3)  
 Length: 121

Descriptor Type: EAPOL WPA key (254)

Key Information: 0x0109

.... .... 001 = Key Descriptor Version: HMAC-MD5 for MIC and RC4 for encryption (1)

.... .... 1... = Key Type: Pairwise key

.... .... 00 .... = Key Index: 0

.... .... 0.. .... = Install flag: Not set

.... .... 0... .... = Key Ack flag: Not set

.... .... 1 .... = Key MIC flag: Set

.... .... 0. .... = Secure flag: Not set

.... .... 0.. .... = Error flag: Not set

.... .... 0... .... = Request flag: Not set

.... .... 0 .... = Encrypted Key Data flag: Not set

Key Length: 0

Replay Counter: 3 →

Confirmación del cliente a la 1ª primitiva del handshake.

Nonce: 63F2C058501FE3C8E08DED5254598519FE58CB8C83F0B047...

Key IV: 00000000000000000000000000000000  
WPA Key RSC: 0000000000000000  
WPA Key ID: 0000000000000000  
WPA Key MIC: 9B0185C558DA1622471243FAFADA00B5  
WPA Key Data Length: 26  
WPA Key Data: DD180050F20101000050F20201000050F20201000050F202...

Envía la información que tiene el cliente a cerca de la seguridad que utiliza el punto de acceso.

No.	Time	Source	Destination	Protocol Info
719	30.529766083		Cisco-Li_bd:83:94 (RA)	Acknowledgement



Reconocimiento 802.11 que envía el punto de acceso.

No.	Time	Source	Destination	Protocol Info
720	30.531055451	Cisco-Li_de:77:8e	Cisco-Li_bd:83:94	EAPOL Key



Protocols in frame: wlan:llc:eapol  
IEEE 802.11

Data Rate: 11.0 Mb/s

Flags: 0x2

DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x02)

.... 0.. = More Fragments: This is the last fragment

.... 0... = Retry: Frame is not being retransmitted

...0 .... = PWR MGT: STA will stay up

..0. .... = More Data: No data buffered

.0.. .... = Protected flag: Data is not protected

0... .... = Order flag: Not strictly ordered

Destination address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)

BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)

Source address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)

Logical-Link Control

802.1X Authentication

Type: Key (3)

Descriptor Type: EAPOL WPA key (254)

Key Information: 0x01c9

.... .001 = Key Descriptor Version: HMAC-MD5 for MIC and RC4 for encryption (1)

.... .1... = Key Type: Pairwise key

.... .00 .... = Key Index: 0

.... .1.. .... = Install flag: Set

.... .1.... = Key Ack flag: Set

.... .1 .... = Key MIC flag: Set

.... .0. .... = Secure flag: Not set

.... .0.. .... = Error flag: Not set

.... 0... .... = Request flag: Not set

...0 .... .... = Encrypted Key Data flag: Not set

Key Length: 32

Replay Counter: 4

Nonce: 1F4C818CEA48F0BEDFEACF26ECCF0C3B23716FB4D348D213...

Key IV: 00000000000000000000000000000000

WPA Key RSC: 0000000000000000

WPA Key ID: 0000000000000000

WPA Key MIC: 319CCDC9167EDBBA99C4ECE92D11C15F

WPA Key Data Length: 26

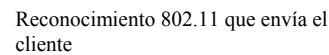
WPA Key Data: DD180050F20101000050F20201000050F20201000050F202...

Envía la información relativa a la seguridad que maneja el punto de acceso y coincide en la 2ª primitiva.

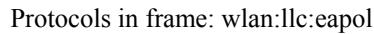


No.	Time	Source	Destination	Protocol Info
721	30.531158447		Cisco-Li_de:77:8e (RA)	Acknowledgement





No.	Time	Source	Destination	Protocol Info
722	30.532209396	Cisco-Li_bd:83:94	Cisco-Li_de:77:8e	EAPOL Key



IEEE 802.11

Flags: 0x1

DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x01)

.... 0.. = More Fragments: This is the last fragment

.... 0... = Retry: Frame is not being retransmitted

...0 .... = PWR MGT: STA will stay up

..0. .... = More Data: No data buffered

.0.. .... = Protected flag: Data is not protected

0... .... = Order flag: Not strictly ordered

BSS Id: Cisco-Li de:77:8e (00:14:bf:de:77:8e)

Source address: Cisco-Li bd:83:94 (00:12:17:bd:83:94)

Destination address: Cisco-Li de:77:8e (00:14:bf:de:77:8e)

Frame check sequence: 0xad269685 [correct]

## Logical-Link Control

## 802.1X Authentication

Type: Key (3)

Descriptor Type: EAPOL WPA key (254)

Key Information: 0x0109

Key Information: 0x0109

.....001 = Key Descriptor Version: HMAC-MD5 for MIC and RC4 for encryption (1)

.... 1... = Key Type: Pairwise key

.... ..00 .... = Key Index: 0

.....0..... = Install flag: Not set

.... 0... = Key Ack flag: Not set

.... 1 .... = Key MIC flag: Set

.....0..... = Secure flag: Not set

```
.....0..... = Error flag: Not set
```

.... 0... .... = Request flag: Not set

...0 .... = Encrypted Key Data flag: Not set

Key Length: 0

Replay Counter: 4 →

Confirmación del cliente a la 3ª primitiva del handshake.

Nonce: 0000000000000000000000000000000000000000000000000000000...

[illegible]

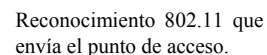
WPA Key RSC: 0000000000000000

WPA Key ID: 0000000000000000

WPA Key MIC: D0358DE415C8EACA1B7A164E94851247

WPA Key Data Length: 0

No.	Time	Source	Destination	Protocol Info
723	30.532396317		Cisco-Li bd:83:94 (RA)	Acknowledgement



No.	Time	Source	Destination	Protocol Info
724	30.533555985	Cisco-Li_de:77:8e	Cisco-Li_bd:83:94	Data



Protocols in frame: wlan:data  
 IEEE 802.11  
 Data Rate: 11.0 Mb/s  
 Type/Subtype: Data (32)  
 Frame Control: 0x4208 (Normal)  
 Version: 0  
 Type: Data frame (2)  
 Subtype: 0

**1ª primitiva del Group Key Handshaking:** el punto de acceso envía el mensaje EAPOL con la GTK encriptada con la clave de cifrado EAPOL, también envía el MIC. Es la primera trama 802.11 con los datos protegidos. Por eso, ya no se decodifica el LLC ni otros protocolos superiores.

Flags: 0x42  
 DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x02)  
 .... 0.. = More Fragments: This is the last fragment  
 .... 0... = Retry: Frame is not being retransmitted  
 ...0 .... = PWR MGT: STA will stay up  
 ..0. .... = More Data: No data buffered  
 .1.. .... = Protected flag: Data is protected  
 0... .... = Order flag: Not strictly ordered  
 Destination address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)  
 BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 Source address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 Frame check sequence: 0x94f11a17 [correct]  
 TKIP/CCMP parameters  
 TKIP Ext. Initialization Vector: 0x000000000001  
 Key Index: 0  
 Data (151 bytes)

No.	Time	Source	Destination	Protocol Info
725	30.533727646		Cisco-Li_de:77:8e (RA)	Acknowledgement



Reconocimiento 802.11

No.	Time	Source	Destination	Protocol Info
726	30.549957275	Cisco-Li_bd:83:94	Cisco-Li_de:77:8e	Data



Protocols in frame: wlan:data  
 IEEE 802.11  
 Data Rate: 11.0 Mb/s  
 Type/Subtype: Data (32)  
 Frame Control: 0x4108 (Normal)  
 Version: 0  
 Type: Data frame (2)  
 Subtype: 0  
 Flags: 0x41

**2ª primitiva del Group Key Handshaking:** el cliente finaliza el Group Key Handshaking con un mensaje EAPOL cifrado con la clave de encriptado EAPOL.

.1.. .... = Protected flag: Data is protected  
 BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 Source address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)  
 Destination address: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 Frame check sequence: 0xaa54a98d [correct]  
 TKIP/CCMP parameters  
 TKIP Ext. Initialization Vector: 0x000000000002  
 Key Index: 0  
 Data (119 bytes)

No.	Time	Source	Destination	Protocol Info
727	30.550119400		Cisco-Li_bd:83:94 (RA)	Acknowledgement



Reconocimiento 802.11

No.	Time	Source	Destination	Protocol Info
829	35.106718063	Cisco-Li_bd:83:94	Broadcast	Data

Protocols in frame: wlan:data  
 IEEE 802.11  
 Data Rate: 11.0 Mb/s  
 Type/Subtype: Data (32)  
 Frame Control: 0x4108 (Normal)

El cliente inalámbrico envía un mensaje DHCP para solicitar una dirección IP con una trama de broadcast. Irá encriptado con la clave de grupo que envía el AP. Por tanto, el tamaño de los datos será el tamaño del datagrama que transporta el DHCP Request (328 bytes) más los 20 bytes que añade en total el protocolo de seguridad.

Version: 0  
 Type: Data frame (2)  
 Subtype: 0  
 Flags: 0x41  
 DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x01)  
 ....0.. = More Fragments: This is the last fragment  
 ....0... = Retry: Frame is not being retransmitted  
 ...0 .... = PWR MGT: STA will stay up  
 ..0. .... = More Data: No data buffered  
 .1.. .... = Protected flag: Data is protected  
 0... .... = Order flag: Not strictly ordered

Duration: 213  
 BSS Id: Cisco-Li\_de:77:8e (00:14:bf:de:77:8e)  
 Source address: Cisco-Li\_bd:83:94 (00:12:17:bd:83:94)  
 Destination address: Broadcast (ff:ff:ff:ff:ff:ff)  
 Frame check sequence: 0x2889be4d [correct]  
 TKIP/CCMP parameters  
 TKIP Ext. Initialization Vector: 0x0000000000003  
 Key Index: 0  
 Data (348 bytes)

No.	Time	Source	Destination	Protocol Info
830	35.106866837		Cisco-Li_bd:83:94 (RA)	Acknowledgement



Reconocimiento 802.11 del punto de acceso.