Privacidad en WiFi mediante WEP

Privacidad en WiFi con WEP

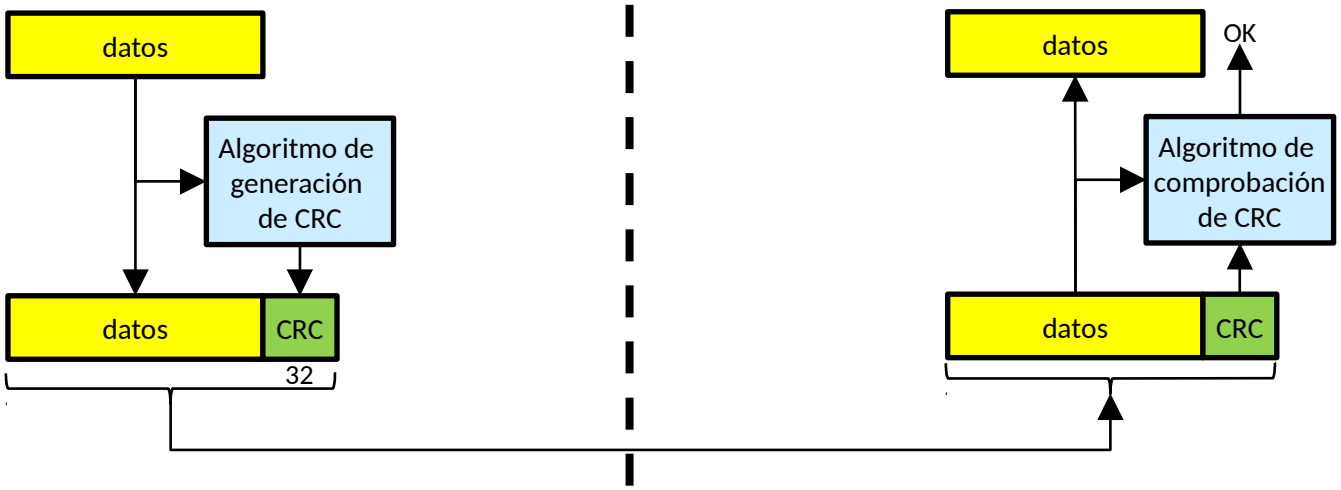
WEP (Wired Equivalent Privacy)

- Pretende proporcionar al enlace inalámbrico una seguridad equivalente a la de un enlace cableado

Privacidad en WiFi con WEP

Integridad de datos

- CRC lineal de 32 bits calculado sobre los datos
  - Es independiente de IV y clave
- Se descartan paquetes cuyo CRC no coincida



Privacidad en WiFi con WEP

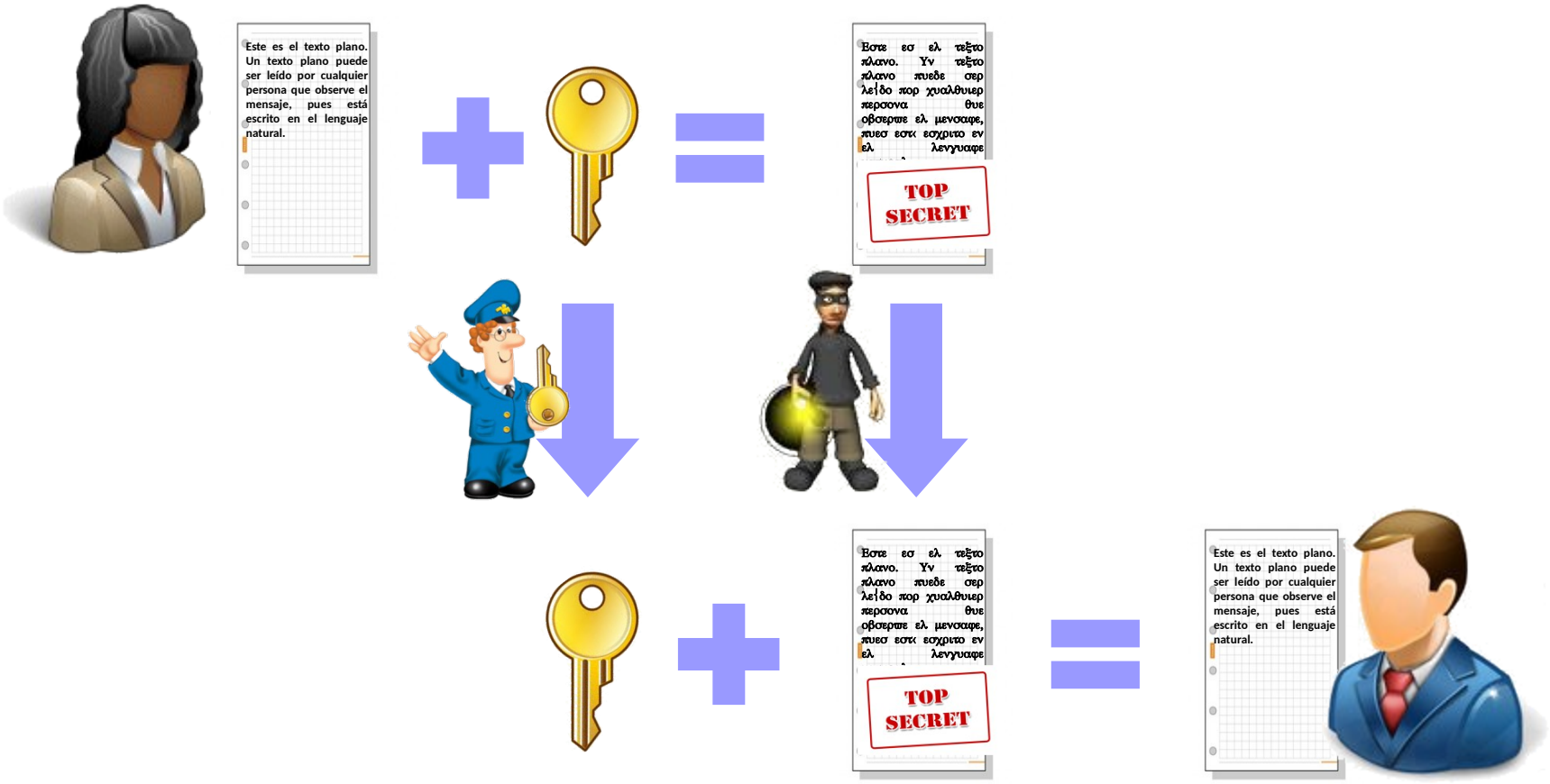
Integridad de datos

- CRC se diseñó para detectar errores fortuitos
- No incluye un control criptográfico de la integridad

- Se puede cambiar el destinatario

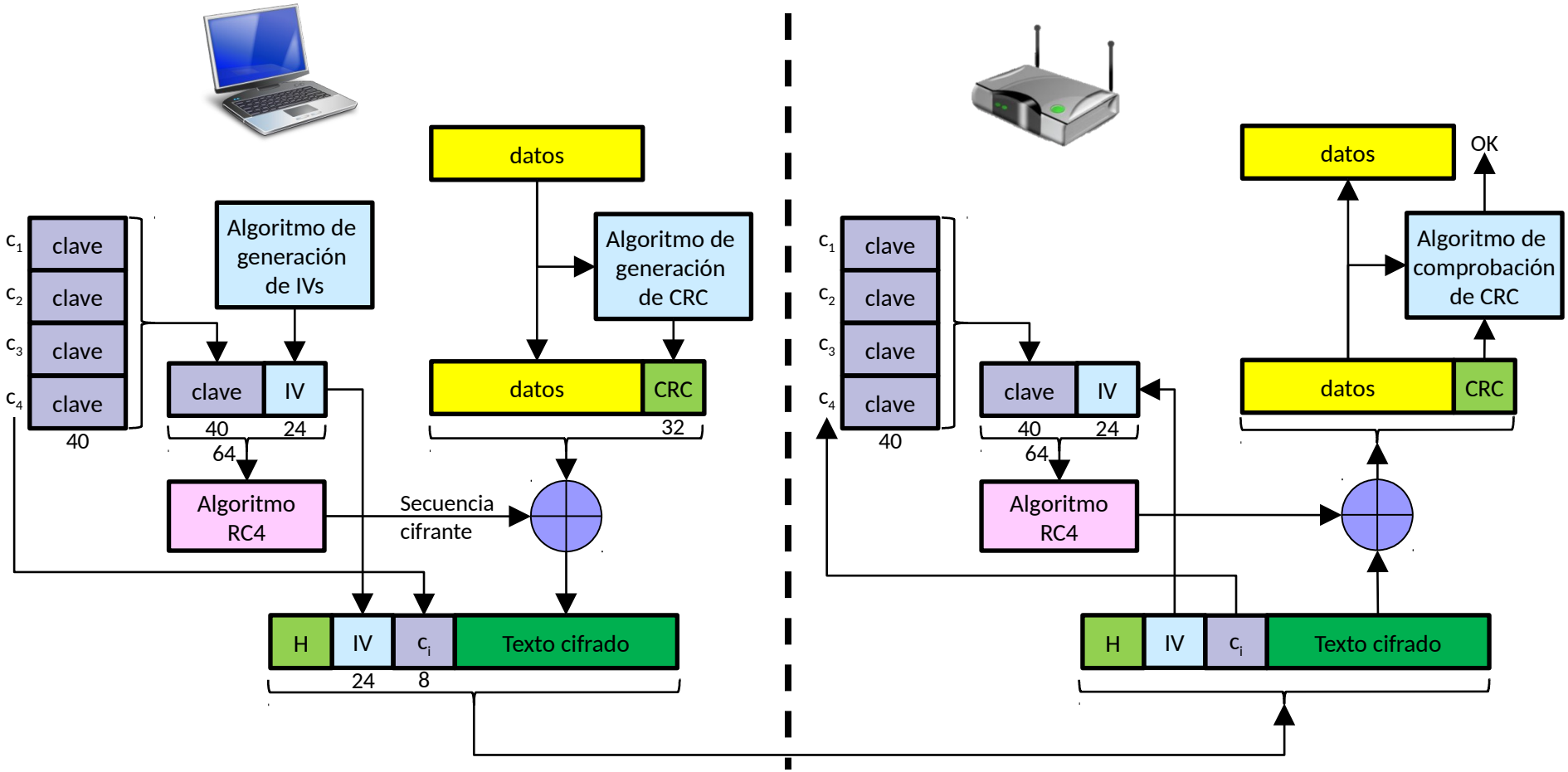
Privacidad en WiFi con WEP

Encriptación simétrica con clave compartida



Privacidad en WiFi con WEP

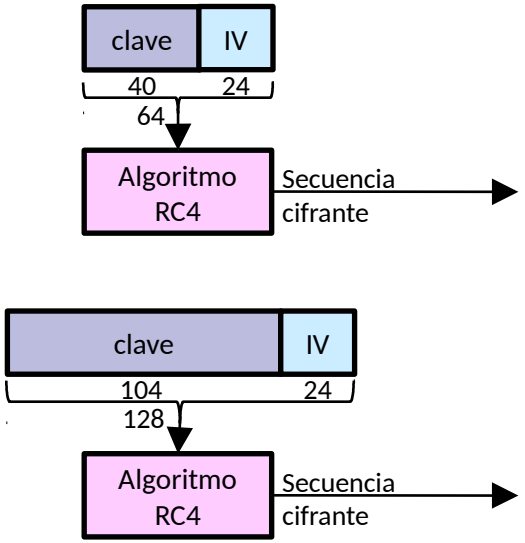
Encriptación / desencriptación WEP



Privacidad en WiFi con WEP

Encriptación de 64 / 128 bits

- Semilla de 64 bits
  - 24 bits: vector de inicialización (IV)
  - 40 bits: clave compartida
- Semilla de 128 bits
  - 24 bits: vector de inicialización (IV)
  - 104 bits: clave compartida

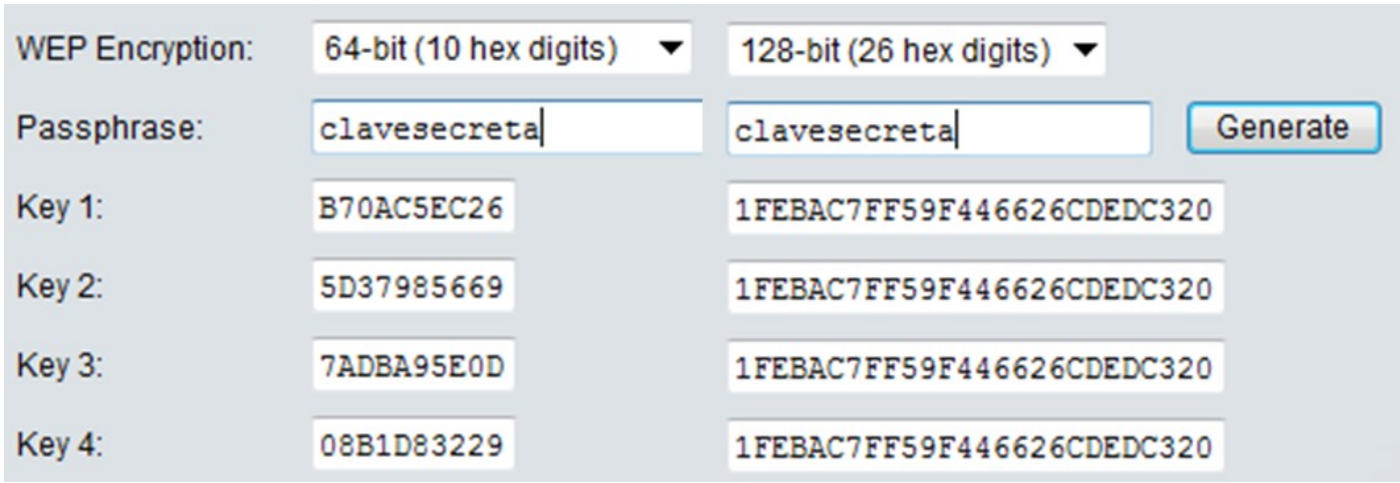


- La semilla se introduce al algoritmo RC4 para generar la secuencia cifrante

Privacidad en WiFi con WEP

Generadores automáticos de claves

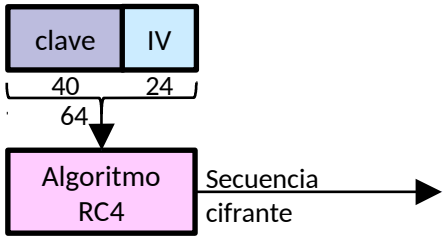
- A partir de una cadena de caracteres
  - Más fácil de recordar que una secuencia de bits (o dígitos hexadecimales)
- Amplio uso, aunque no forman parte del estándar

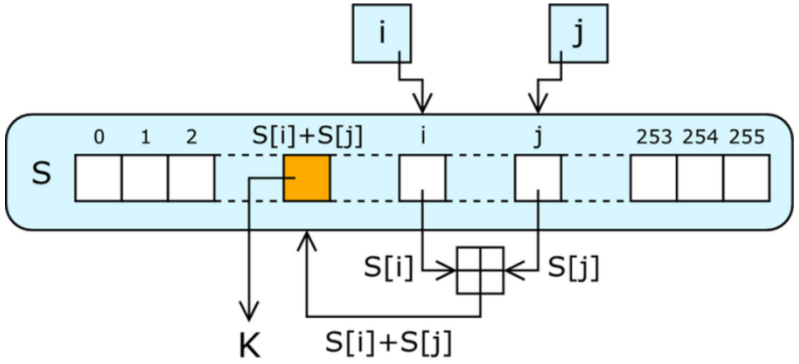


Privacidad en WiFi con WEP

Algoritmo RC4

- Desarrollado por RSA labs
- Síncrono
  - Genera una secuencia cifrante a partir de una semilla
  - La secuencia es independiente del texto claro a cifrar
- Fases del algoritmo
  - KSA (Key Scheduling Algorithm)
  - PRGA (Pseudo-Random Generation Algorithm)

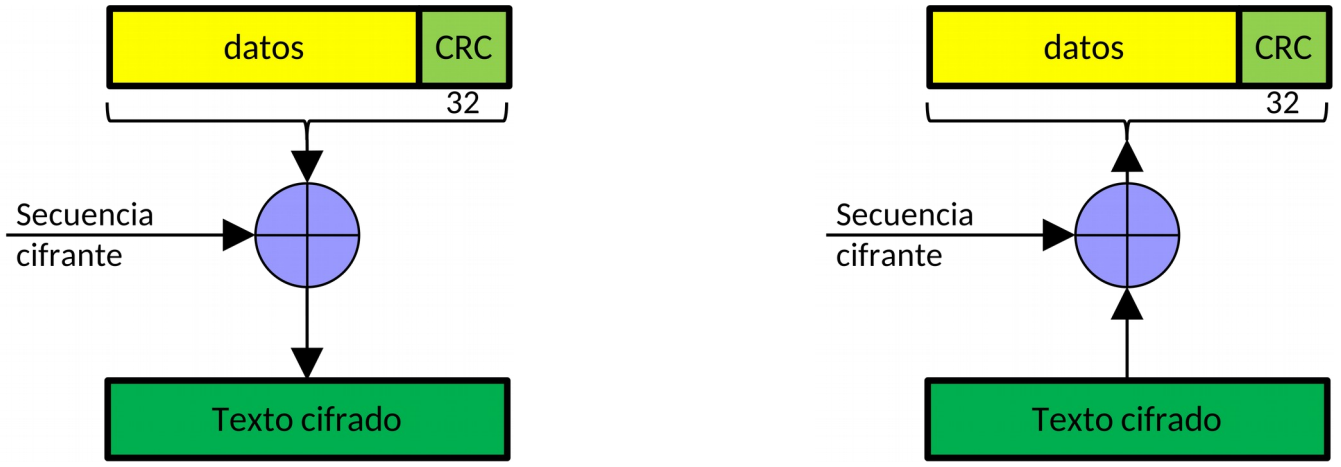




Privacidad en WiFi con WEP

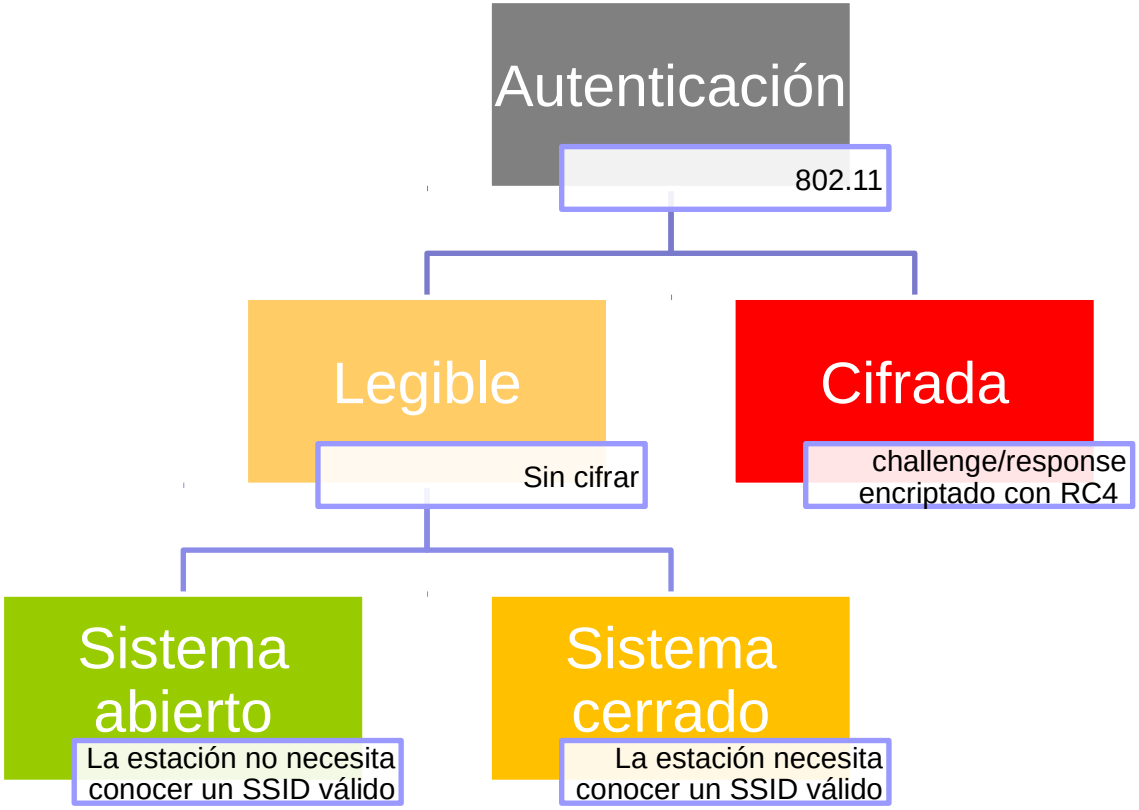
Cifrado de flujo

- Los datos se cifran/descrifran byte a byte haciendo un XOR con la secuencia cifrante



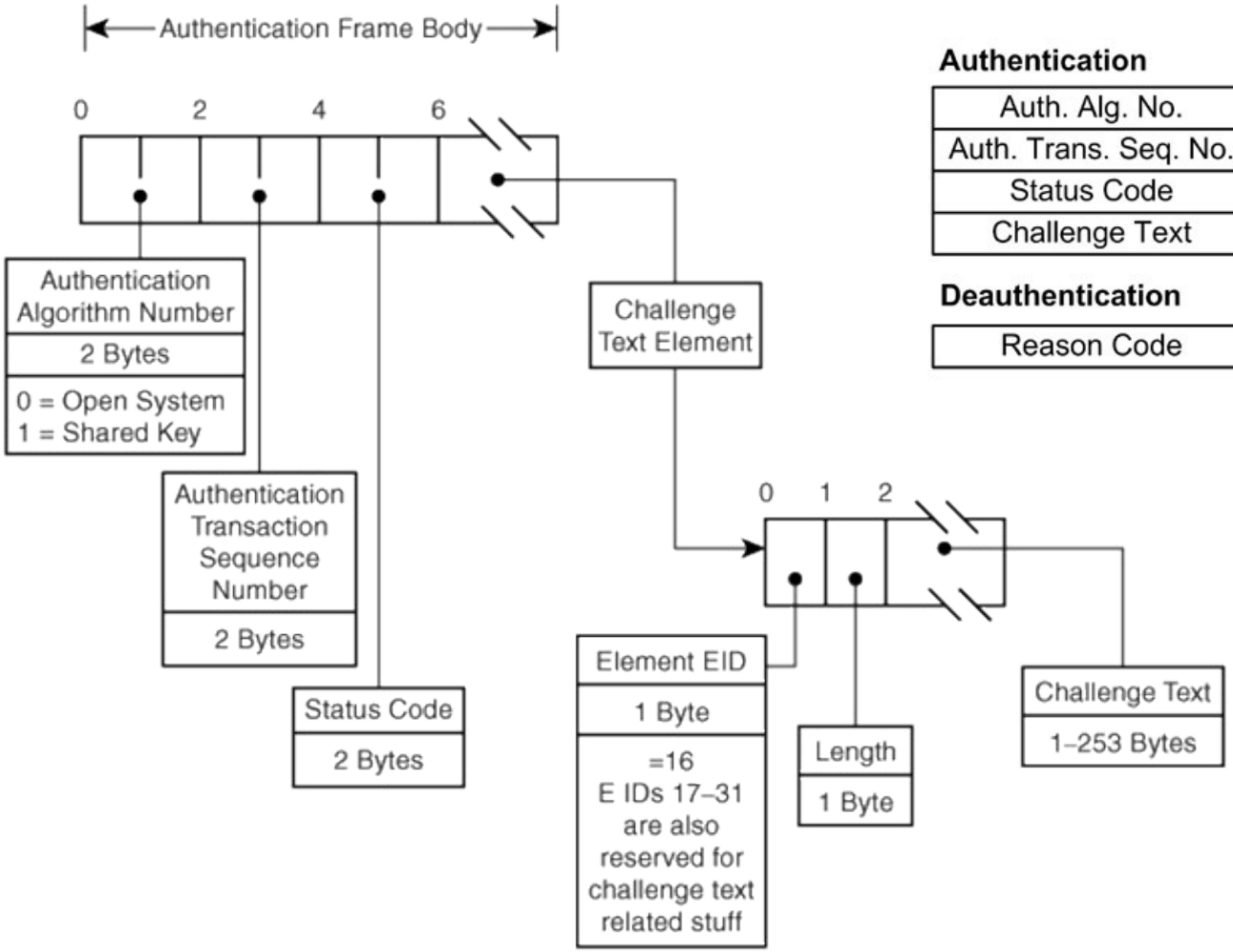
Privacidad en WiFi con WEP

Tipos de autenticación de estaciones



Privacidad en WiFi con WEP

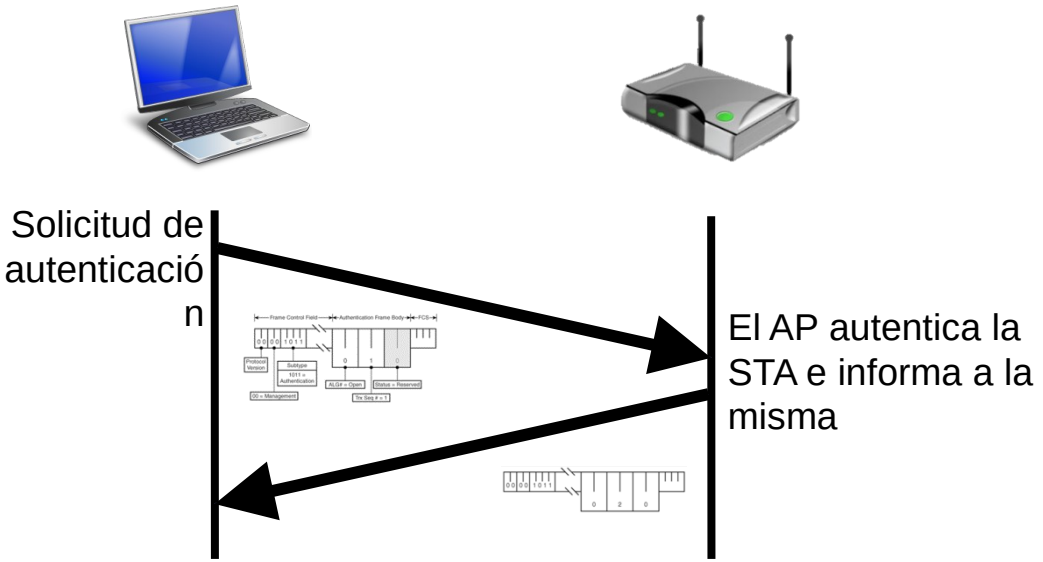
Tramas de autenticación



Privacidad en WiFi con WEP

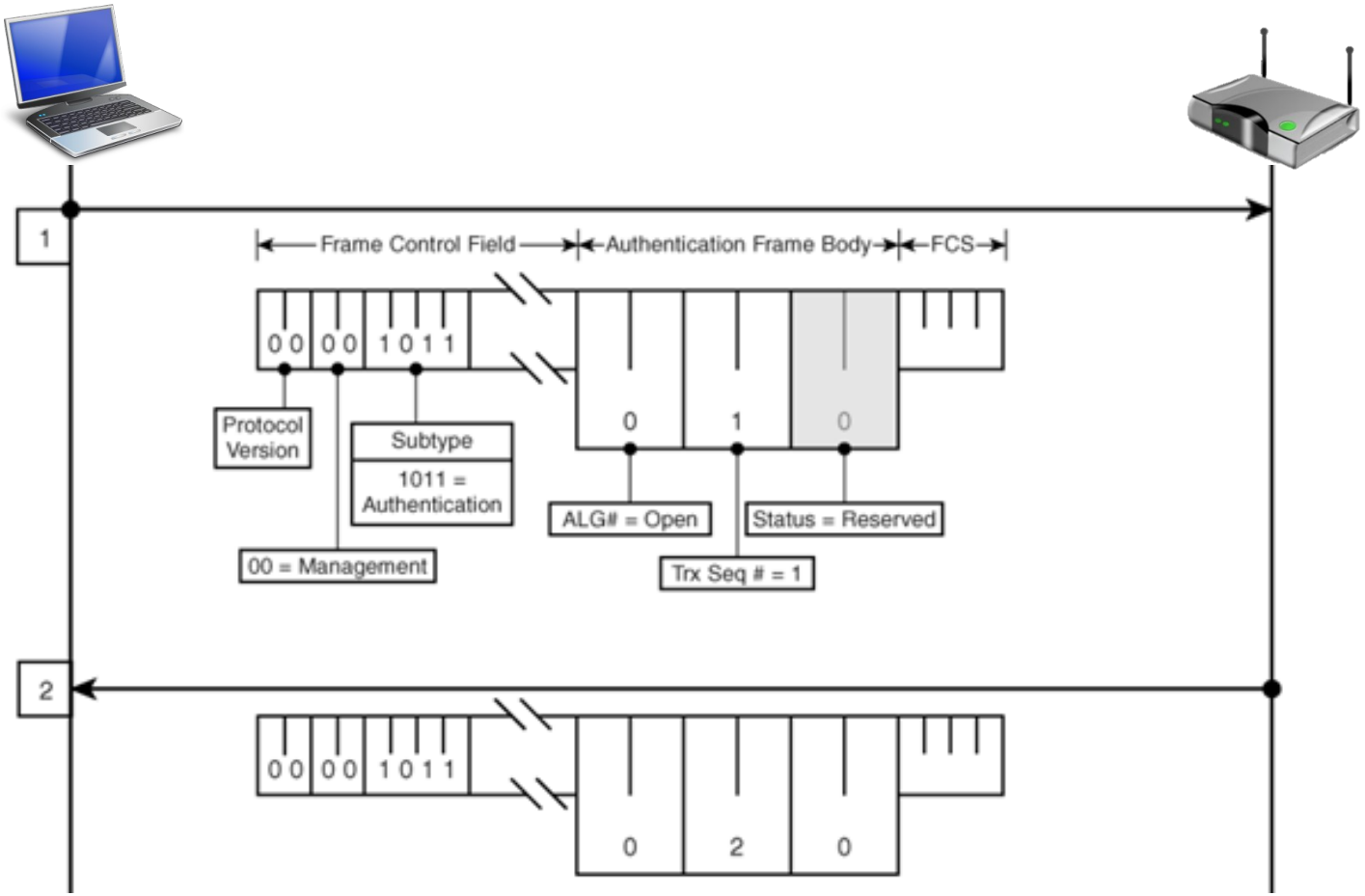
Autenticación de sistema abierto

- La estación se autentica con sólo solicitarlo



Privacidad en WiFi con WEP

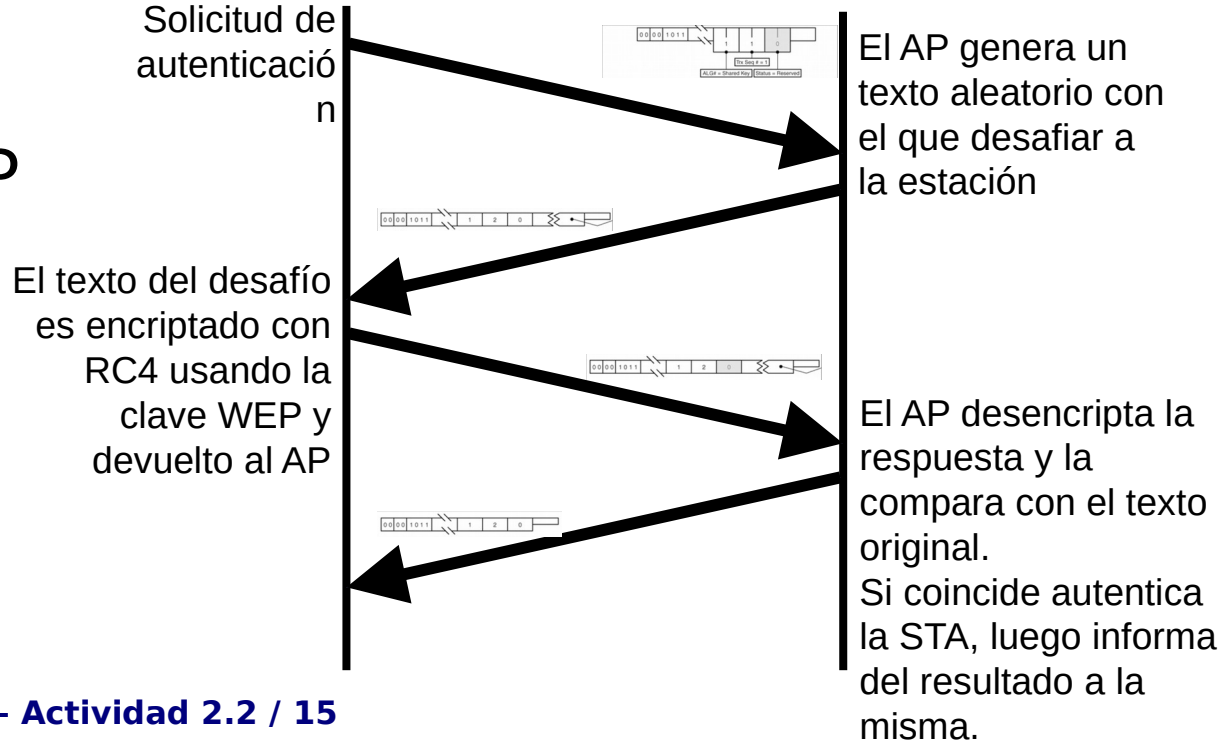
Autenticación de sistema abierto



Privacidad en WiFi con WEP

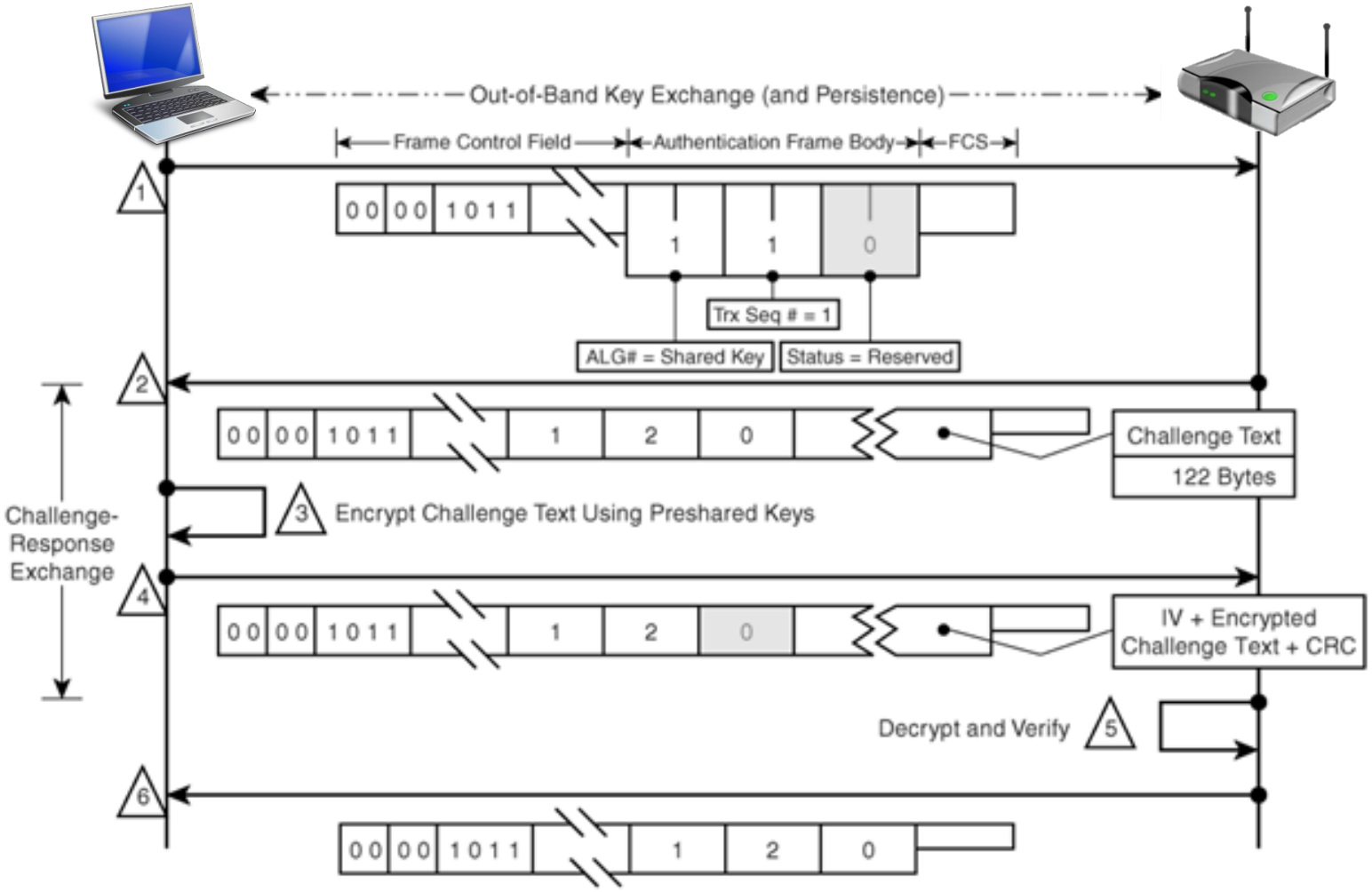
Autenticación por clave compartida

- El AP autentica la STA
- La STA no autentica al AP
  - Posibilidad de AP falso



Privacidad en WiFi con WEP

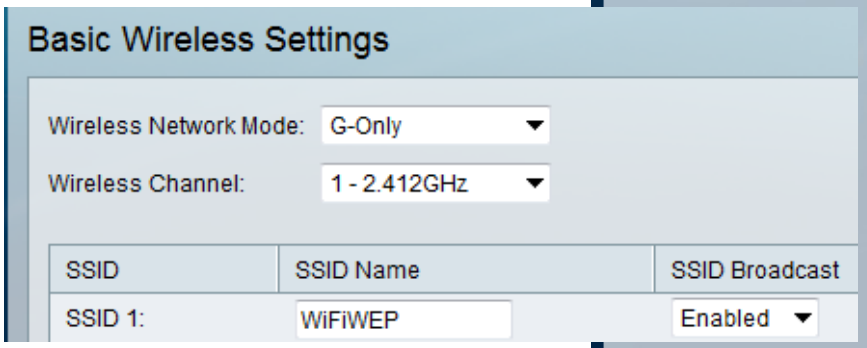
Autenticación por clave compartida

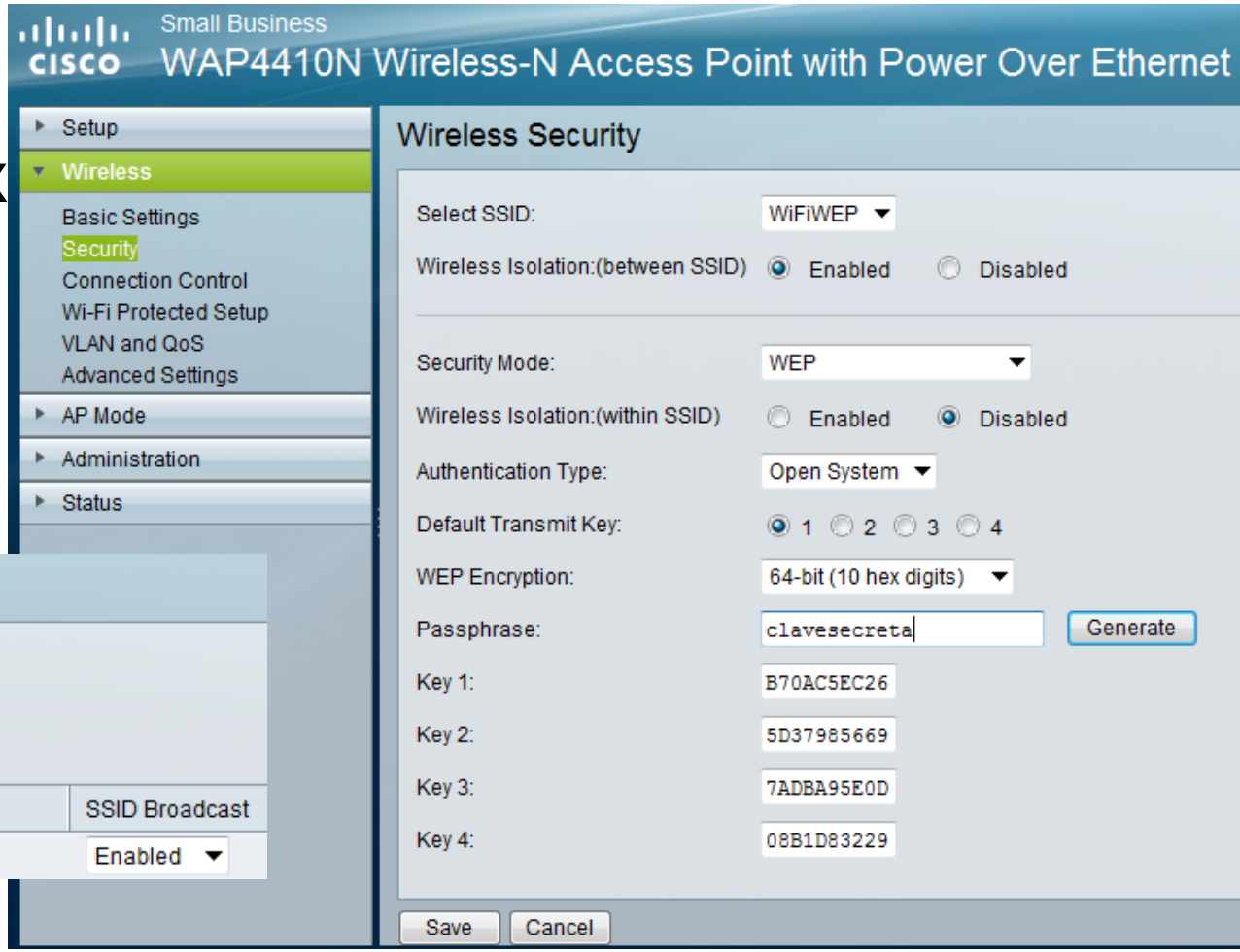


Privacidad en WiFi con WEP

Configuración de AP con cifrado WEP

- 64 bits
- 10 dígitos hex

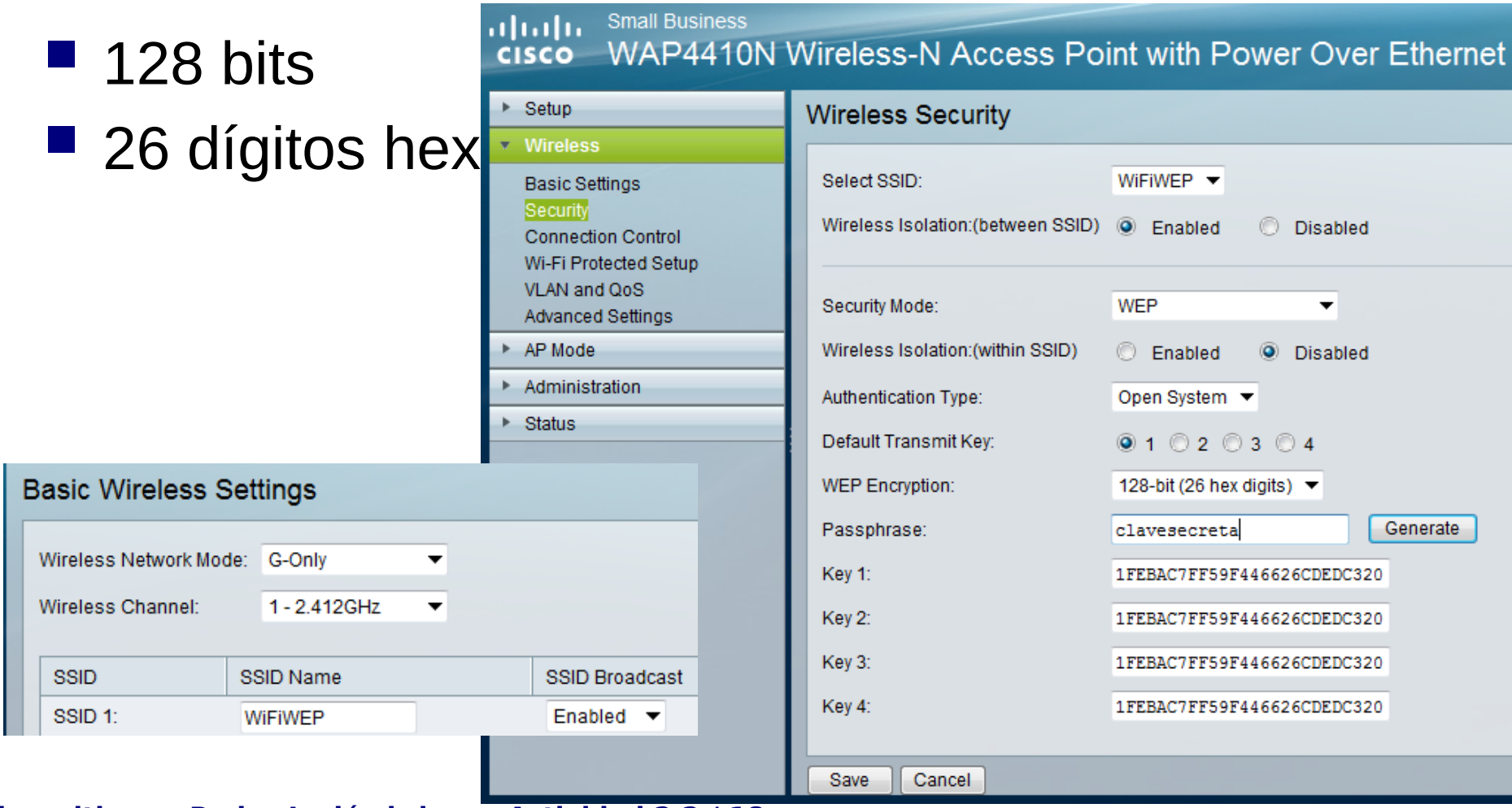




Privacidad en WiFi con WEP

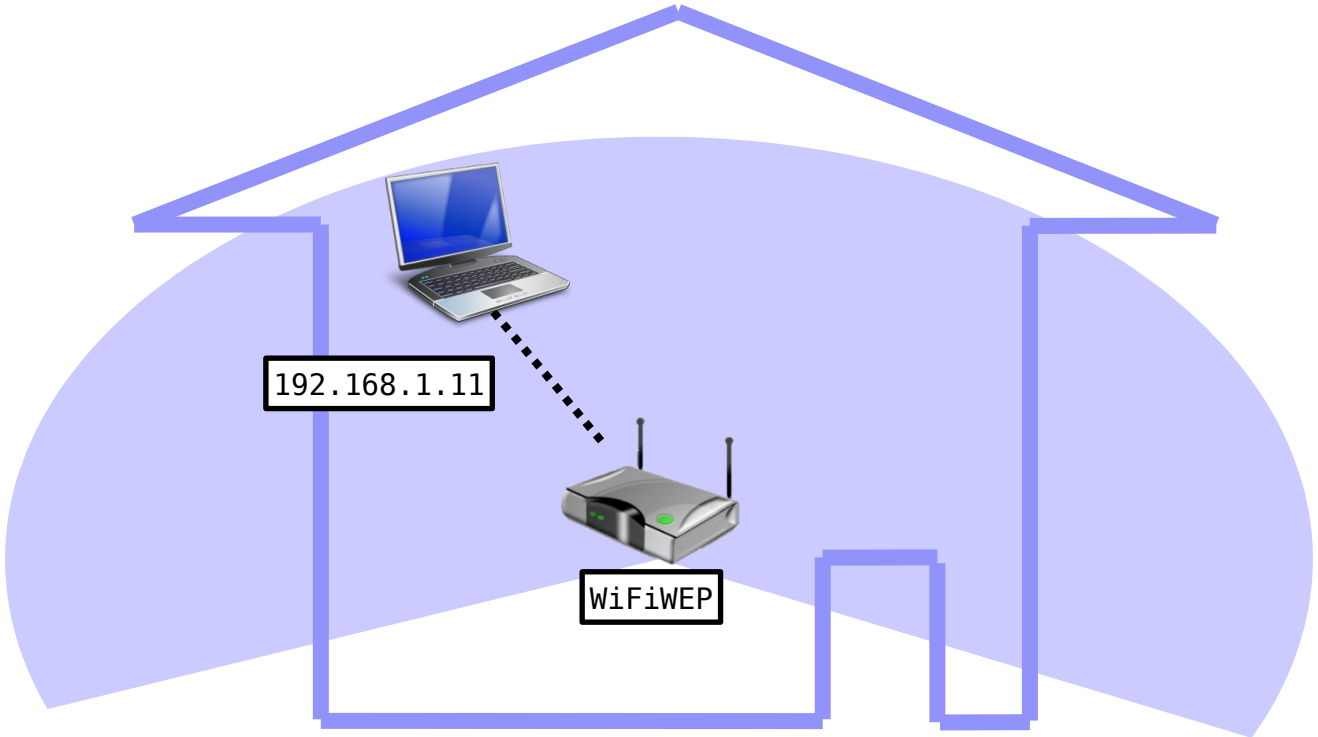
Configuración de AP con cifrado WEP

- 128 bits
- 26 dígitos hex



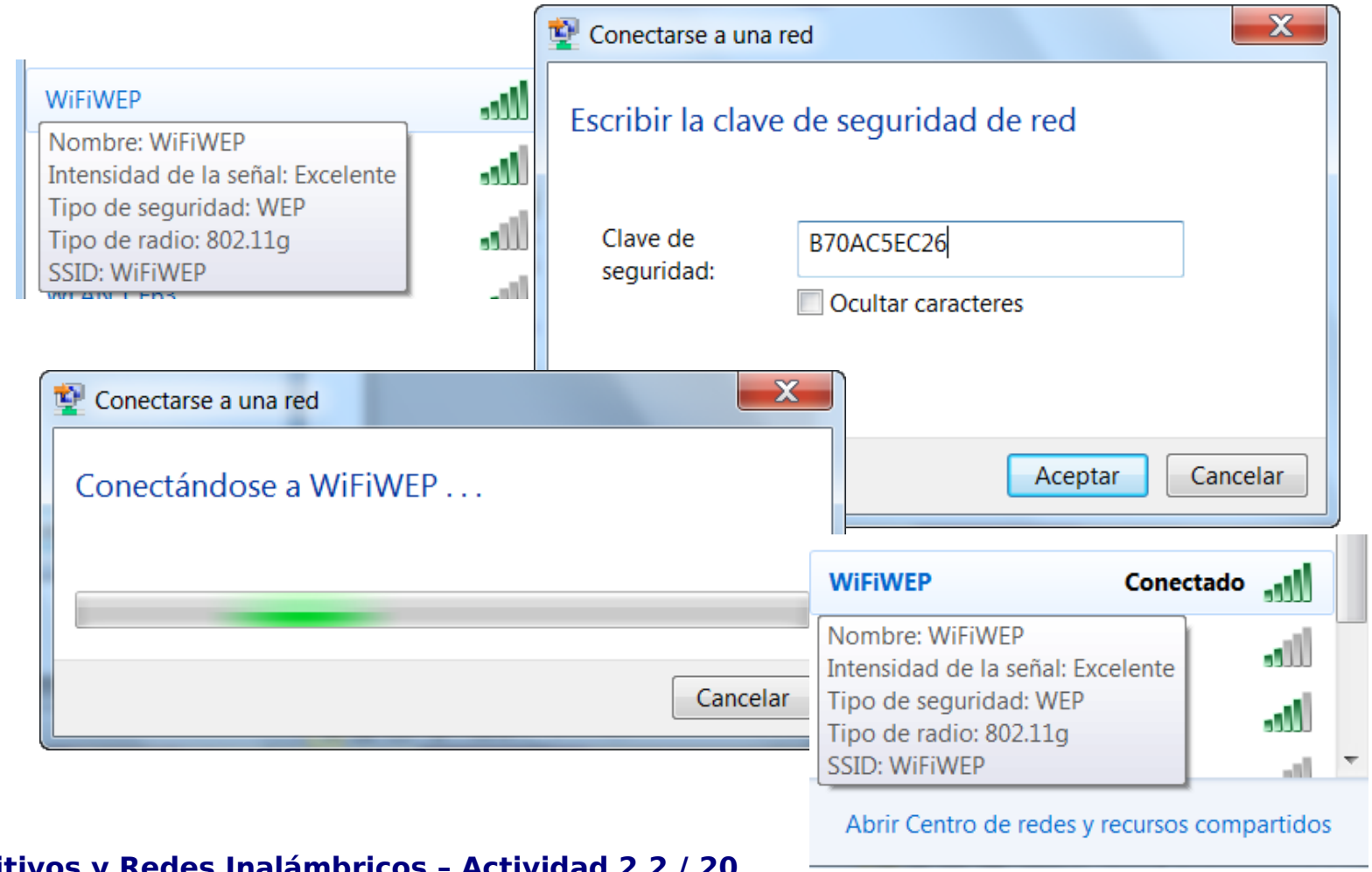
Privacidad en WiFi con WEP

Conexión desde Windows a AP con WEP



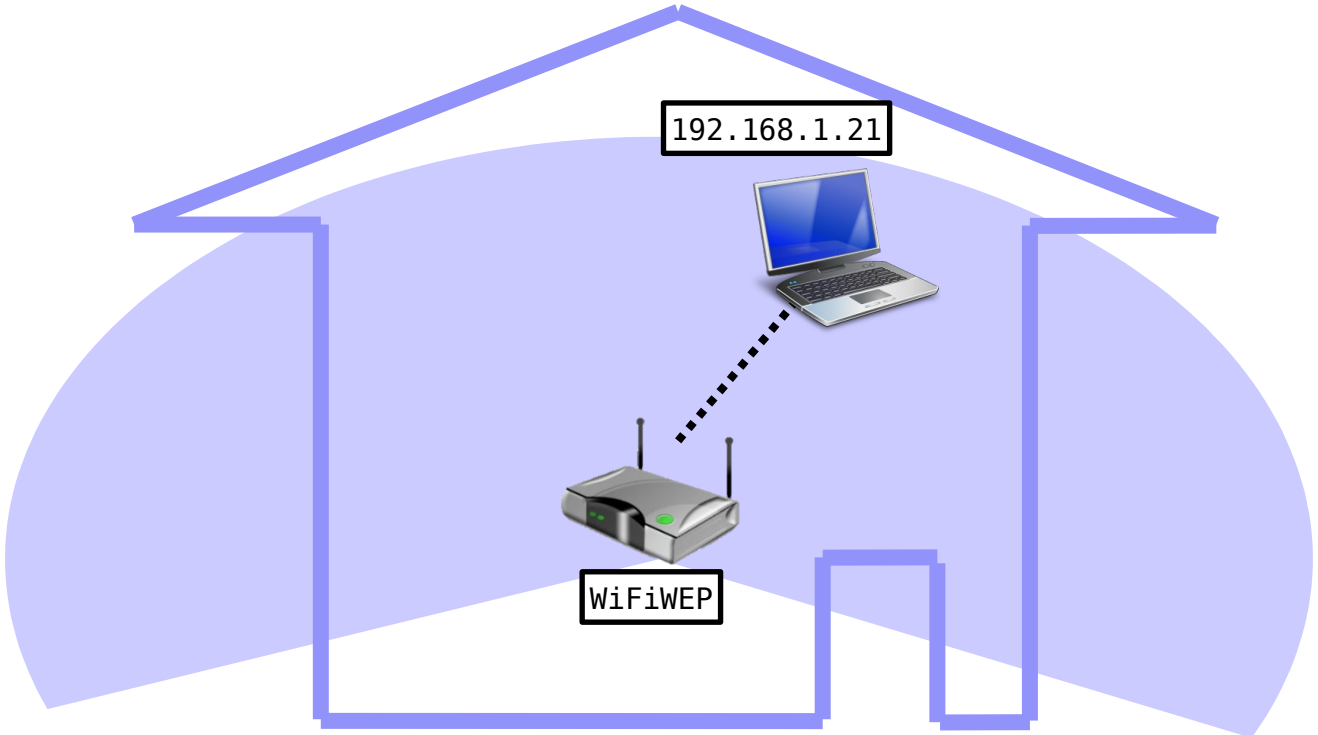
Privacidad en WiFi con WEP

Conexión desde Windows a AP con WEP



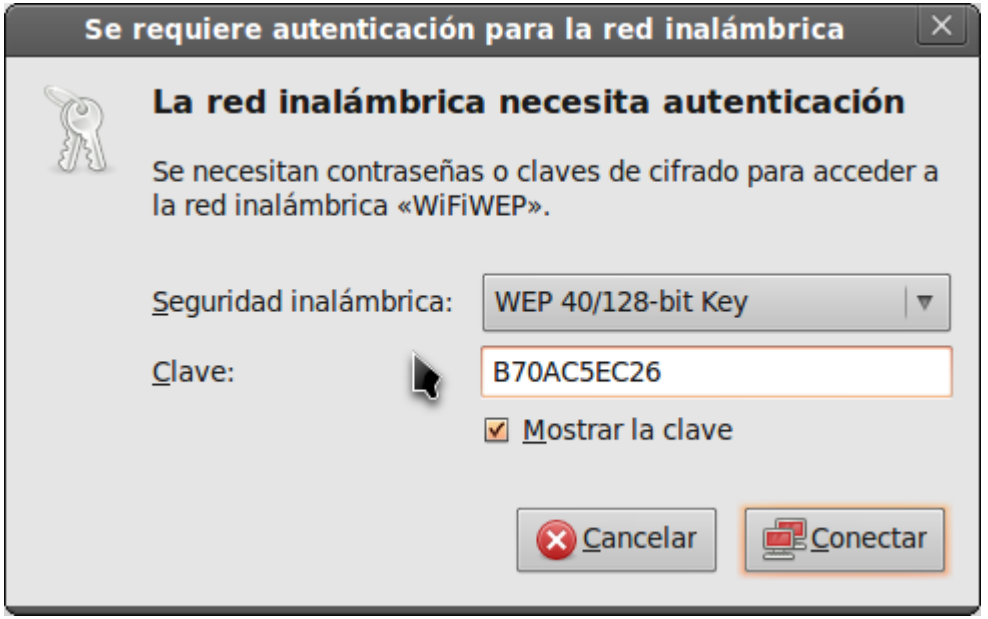
Privacidad en WiFi con WEP

Conexión desde Linux a AP con WEP



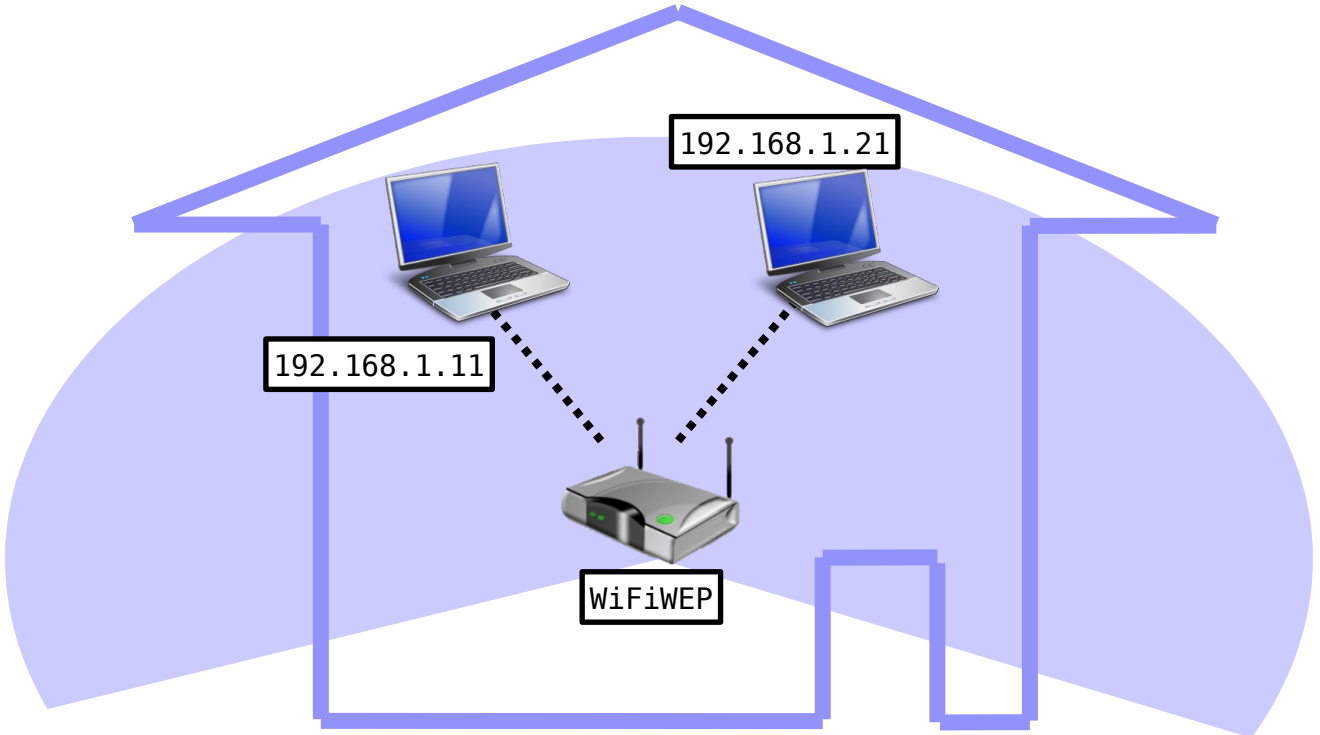
Privacidad en WiFi con WEP

Conexión desde Linux a AP con WEP



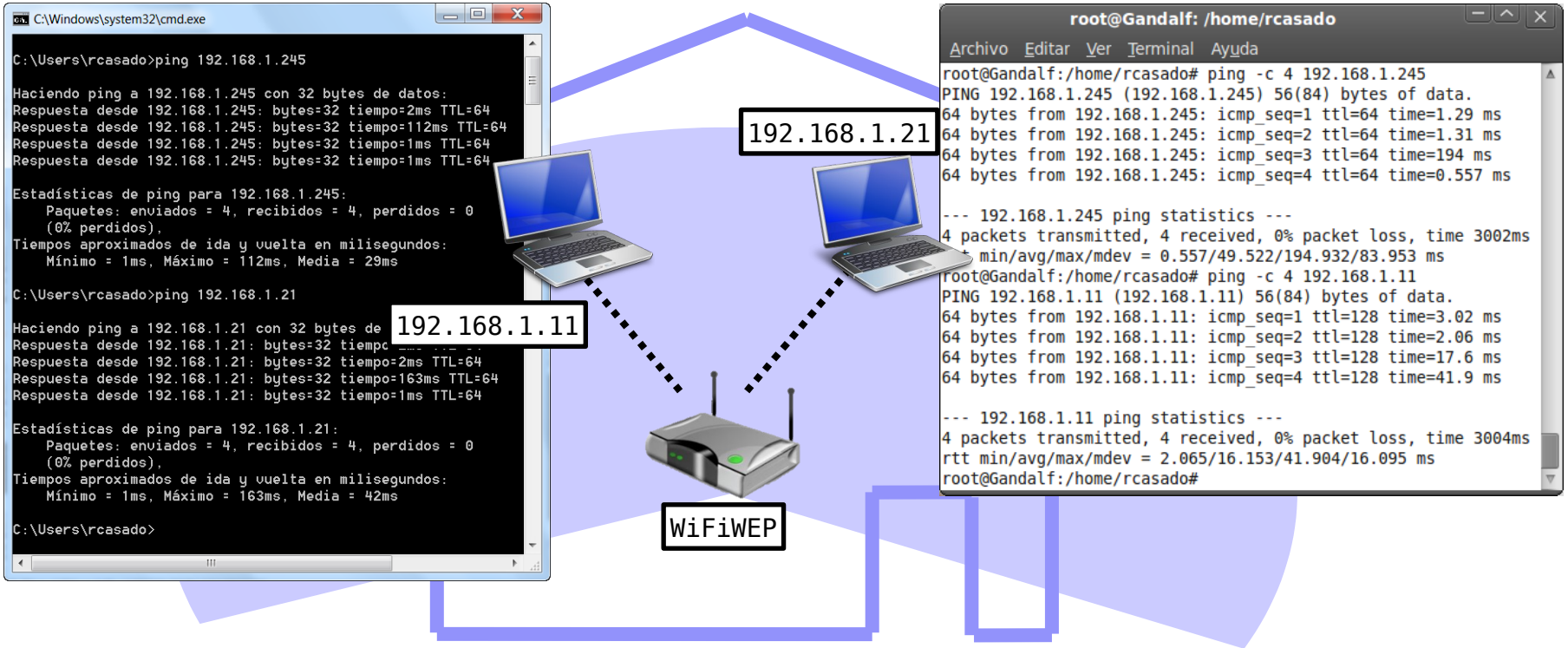
Privacidad en WiFi con WEP

Montaje a realizar



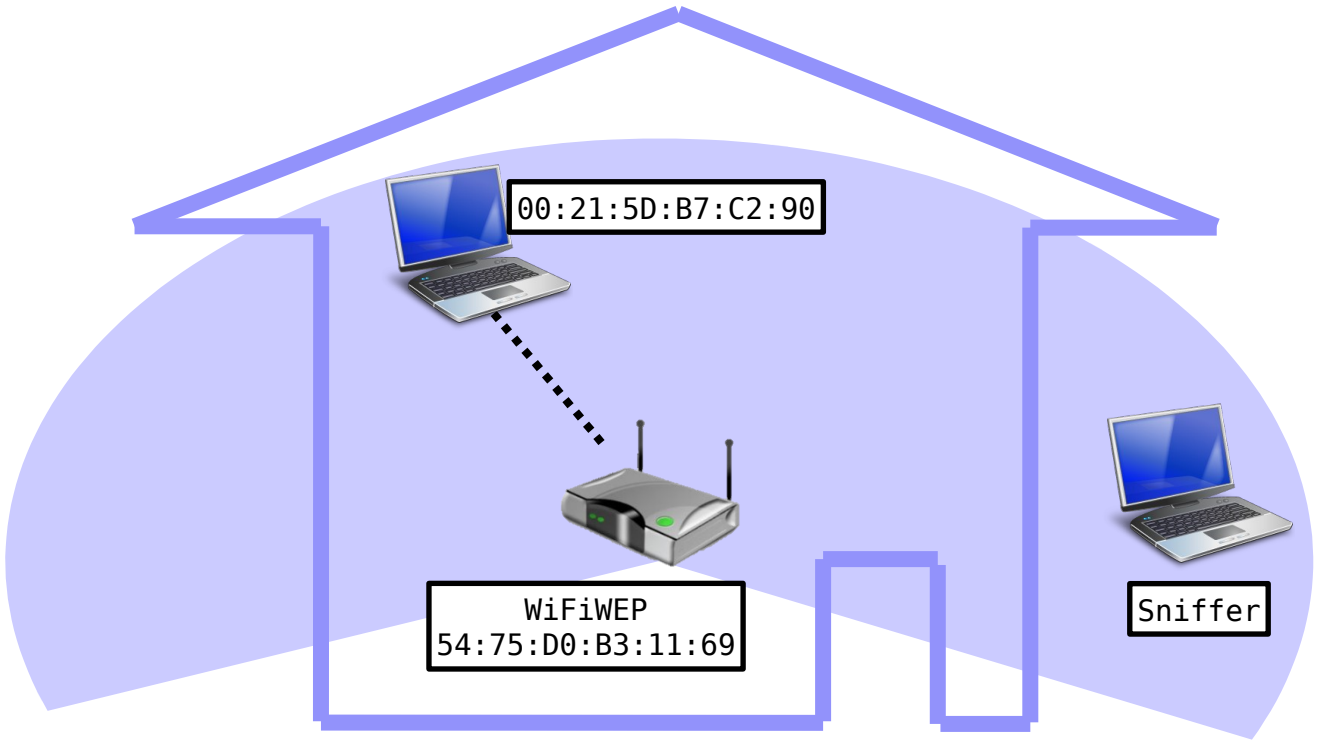
Privacidad en WiFi con WEP

Pruebas de conectividad



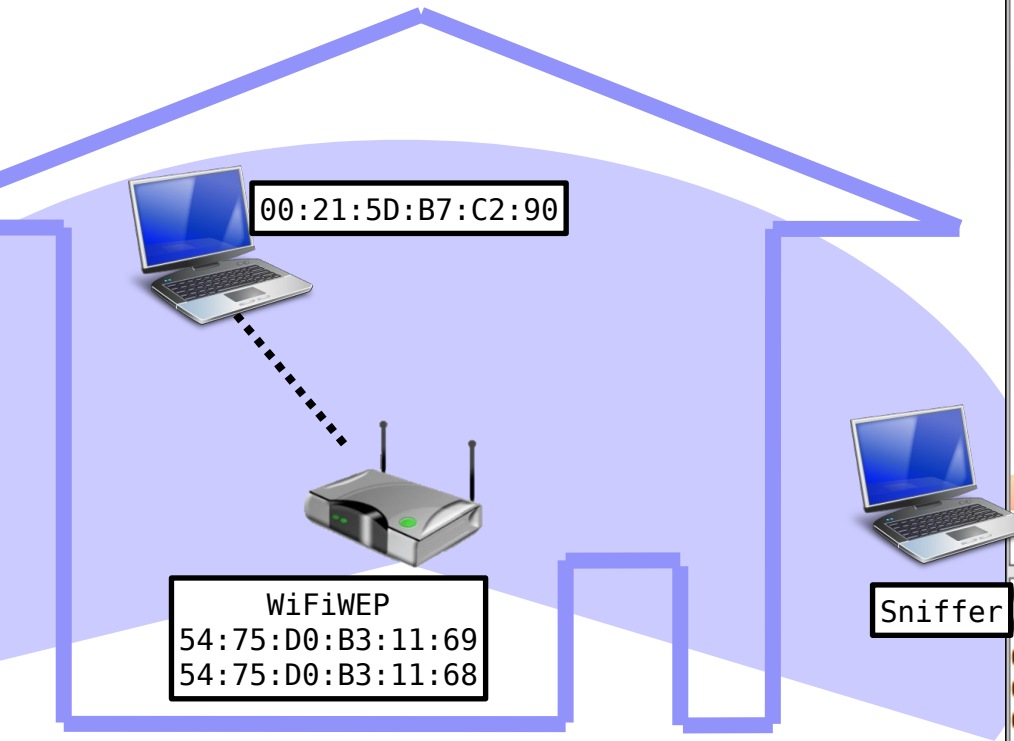
Privacidad en WiFi con WEP

Montaje a realizar



Privacidad en WiFi con WEP

Monitorización de IVs con WireShark

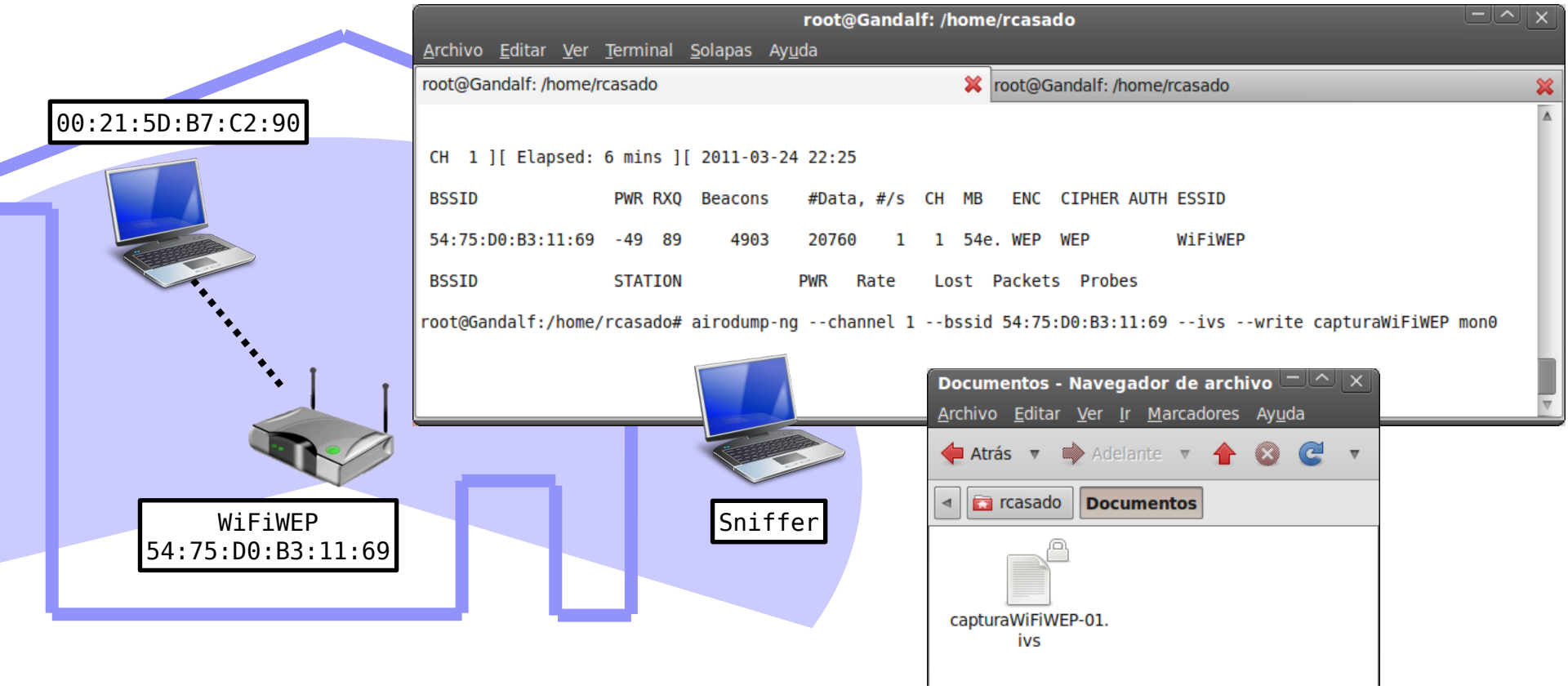



```
7 0.474452 IntelCor_b7:c2:90 Cisco_b3:11:68 IEEE 802.11 QoS Da
▷ Frame 7 (126 bytes on wire, 126 bytes captured)
▷ Radiotap Header v0, Length 24
▽ IEEE 802.11 QoS Data, Flags: .p.....T
    Type/Subtype: QoS Data (0x28)
  ▷ Frame Control: 0x4188 (Normal)
    Duration: 44
    BSS Id: Cisco_b3:11:69 (54:75:d0:b3:11:69)
    Source address: IntelCor_b7:c2:90 (00:21:5d:b7:c2:90)
    Destination address: Cisco_b3:11:68 (54:75:d0:b3:11:68)
    Fragment number: 0
    Sequence number: 682
  ▷ QoS Control
  ▽ WEP parameters
      Initialization Vector: 0xbb5877
      Key Index: 0
      WEP ICV: 0xdfafdf32 (not verified)
▽ Data (68 bytes)
    Data: 9248497AF33A1D6071F7470875C55B7975975F6C81949335..
    [Length: 68]

0000  00 00 18 00 6e 48 00 00  00 6c 6c 09 c0 00 d1 81   ....
0010  01 00 00 00 00 00 00 00  88 41 2c 00 54 75 d0 b3   ....
0020  11 69 00 21 5d b7 c2 90  54 75 d0 b3 11 68 a0 2a   .i.!
0030  00 00 bb 58 77 00 92 48  49 7a f3 3a 1d 60 71 f7   ...X
0040  47 08 75 c5 5b 79 75 97  5f 6c 81 94 93 35 64 6b   G.u.
0050  25 06 fb fd 90 e9 a6 13  48 ec d6 c5 71 45 a6 68   %...
0060  df 0f 17 80 46 9c e5 56  c1 75 ef 54 b7 06 de 6e   ....
0070  91 b5 82 39 8d 35 8e 2c  8f 54 df af df 32         ...9
```

Privacidad en WiFi con WEP

Captura de IVs con airodump-ng



Privacidad en WiFi con WEP

Extracción de clave con aircrack-ng


```
root@Gandalf: /home/rcasado/Documentos
Archivo  Editar  Ver  Terminal  Ayuda
root@Gandalf:/home/rcasado/Documentos# aircrack-ng capturaWiFiWEP-01

Opening capturaWiFiWEP-01.ivs
Read 20761 packets.

   #  BSSID              ESSID                     Encryption

   1  54:75:D0:B3:11:69  WiFiWEP                   WEP (20760 IVs)

Choosing first network as target.

Opening capturaWiFiWEP-01.ivs
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 20760 ivs.


                              Aircrack-ng 1.0


            [00:00:00] Tested 18 keys (got 20760 IVs)

   KB    depth   byte(vote)
    0    0/  2   B7(26228) 34(25460) 78(25228) 97(25104)
    1    1/  3   5E(25832) C1(25684) 89(25424) 73(25352)
    2    0/  1   C5(28876) 6E(26928) 1B(26604) C5(26560)
    3    0/  4   EC(25676) 87(24812) A7(24804) 57(24736)
    4    0/  1   26(30728) AD(26588) CA(25416) DD(25356)

                         KEY FOUND! [ B7:0A:C5:EC:26 ]
        Decrypted correctly: 100%
```