

Privacidad en WiFi mediante WPA-Empresarial



Privacidad WiFi con WPA/EAP

WPA-Empresarial

WPA2 Personal / Empresarial

Integridad
de datos

Encriptación de
comunicaciones

Autenticación
de usuarios

CBC/
MAC

CBC/
MAC

CCMP
(AES)

CCMP
(AES)

PSK

802.1x
EAP

Privacidad WiFi con WPA/EAP

WPA-Empresarial

WPA1/2 Empresarial

Integridad
de datos

Encriptación de
comunicaciones

Autenticación
de usuarios

MIC

CBC/
MAC

TKIP
(RC4)

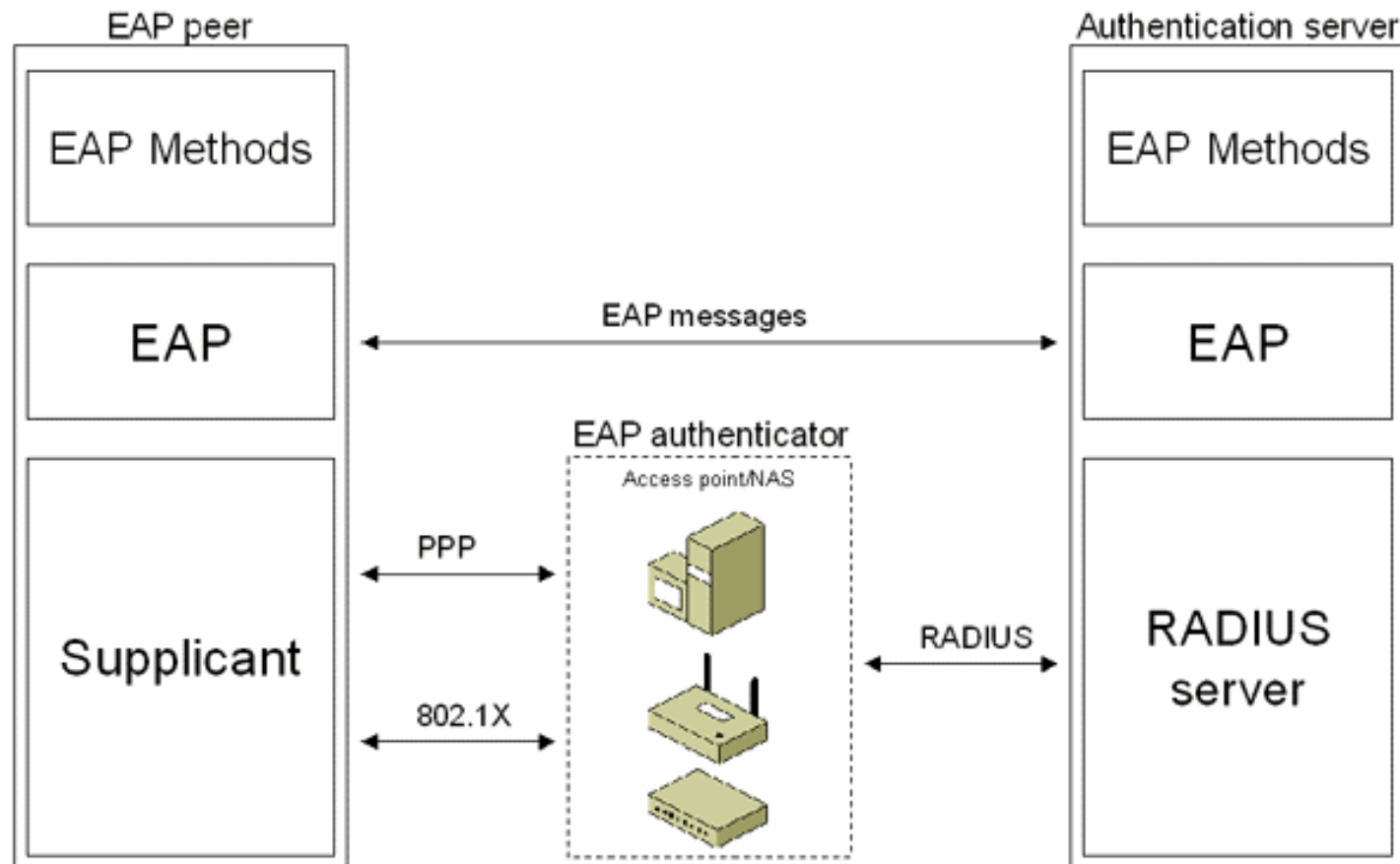
CCMP
(AES)

802.1x
EAP

802.1x
EAP

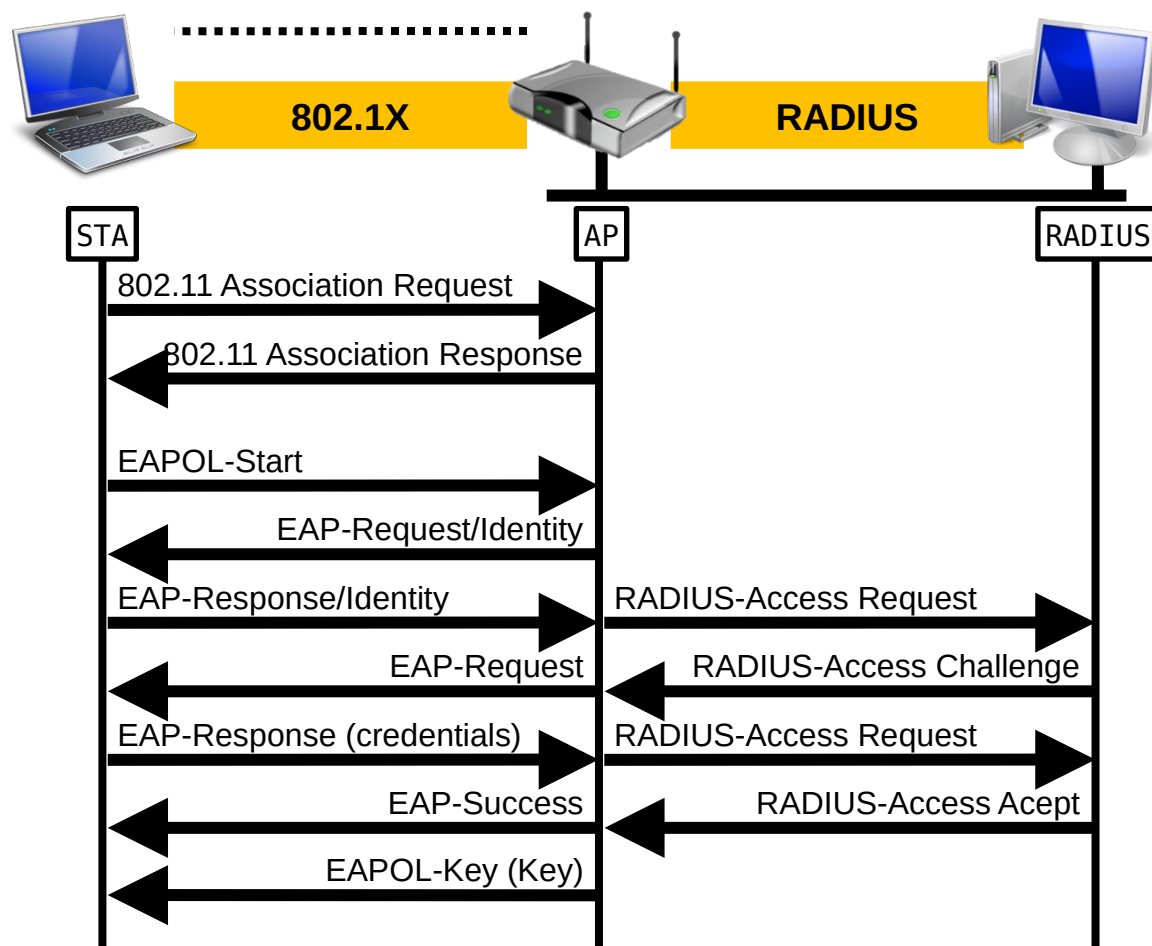
Privacidad WiFi con WPA/EAP

EAP – Extensible authentication Protocol



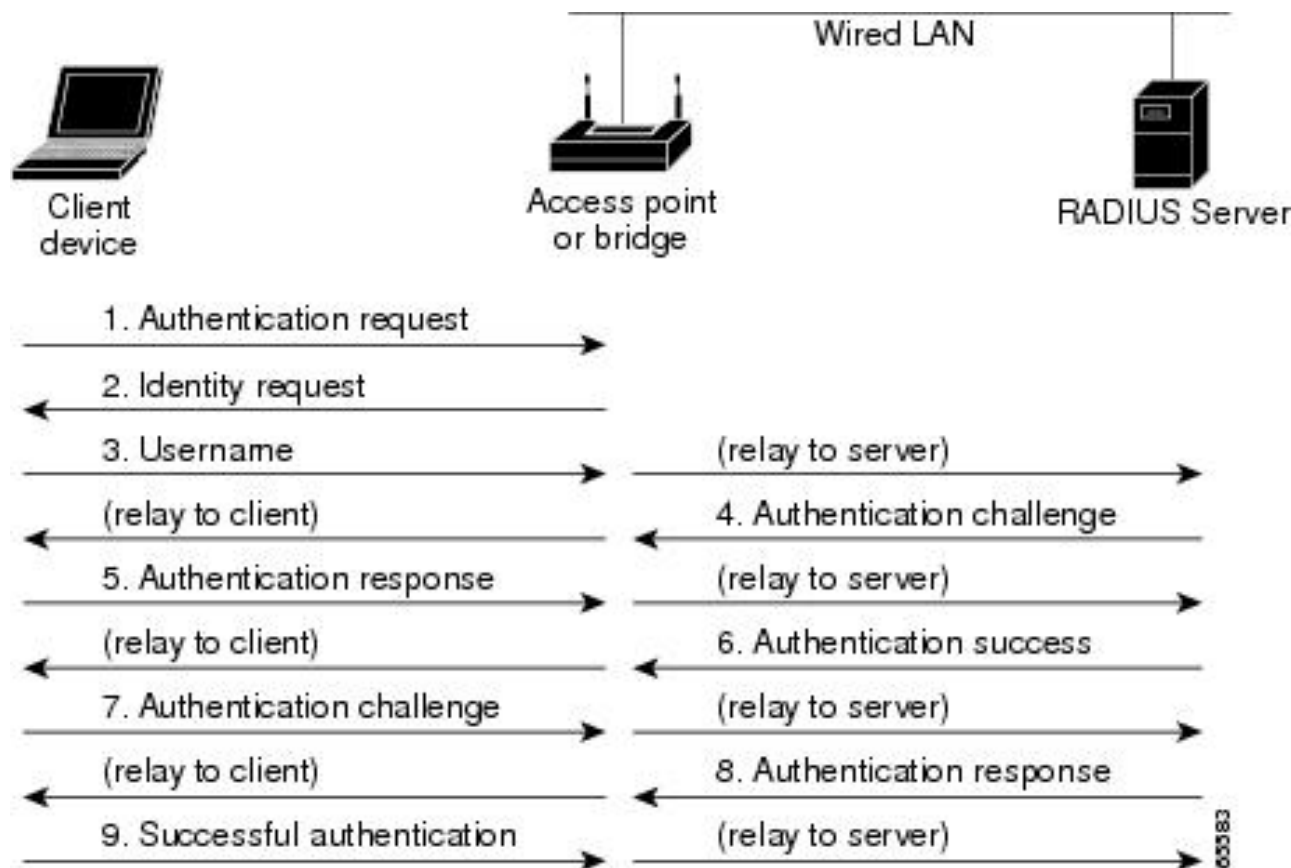
Privacidad WiFi con WPA/EAP

EAP – Extensible authentication Protocol



Privacidad WiFi con WPA/EAP

EAP – Extensible authentication Protocol

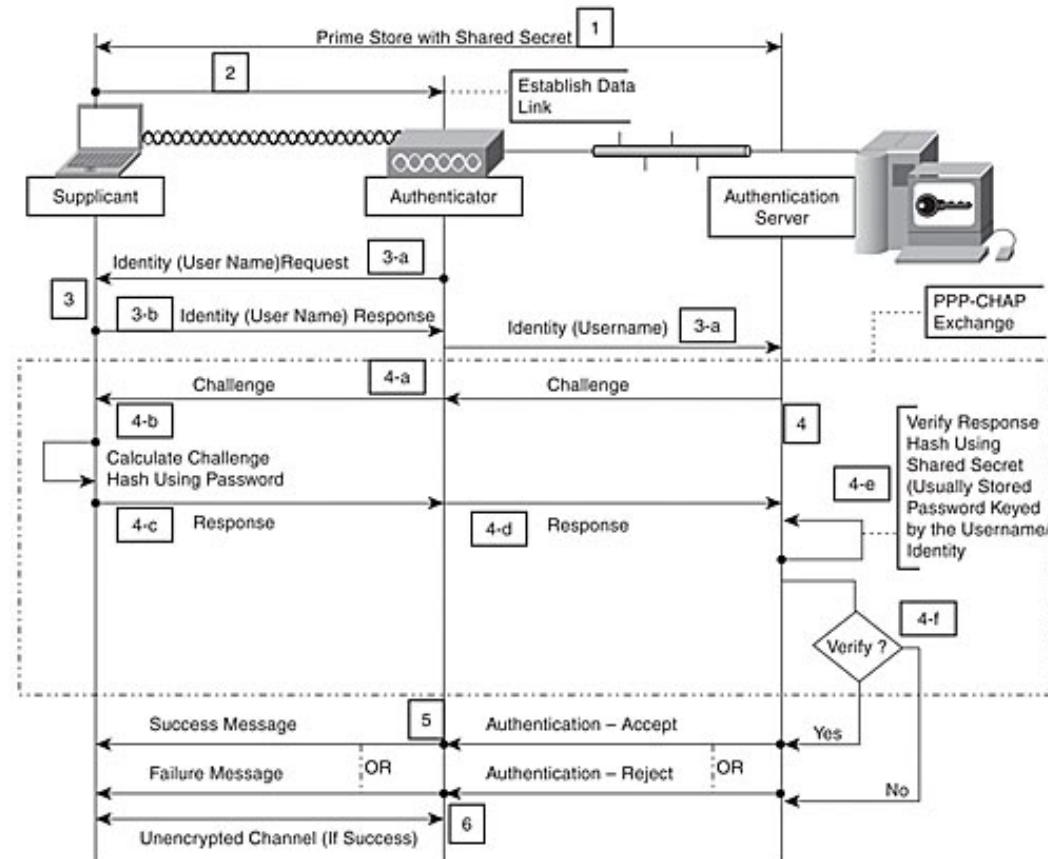


Privacidad WiFi con WPA/EAP

Métodos EAP

- EAP-MD5
(Message Digest)

- No soporta autenticación mutua de cliente y red

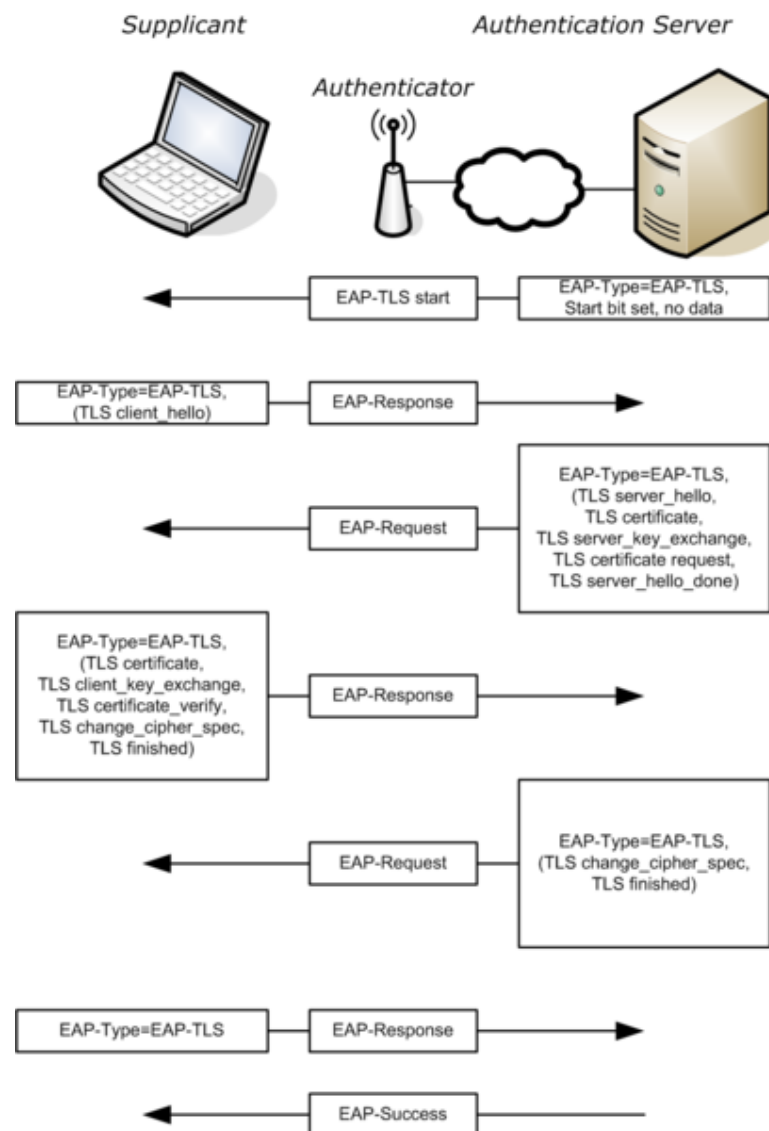


Privacidad WiFi con WPA/EAP

Métodos EAP

■ EAP-TLS (Transport Layer Security)

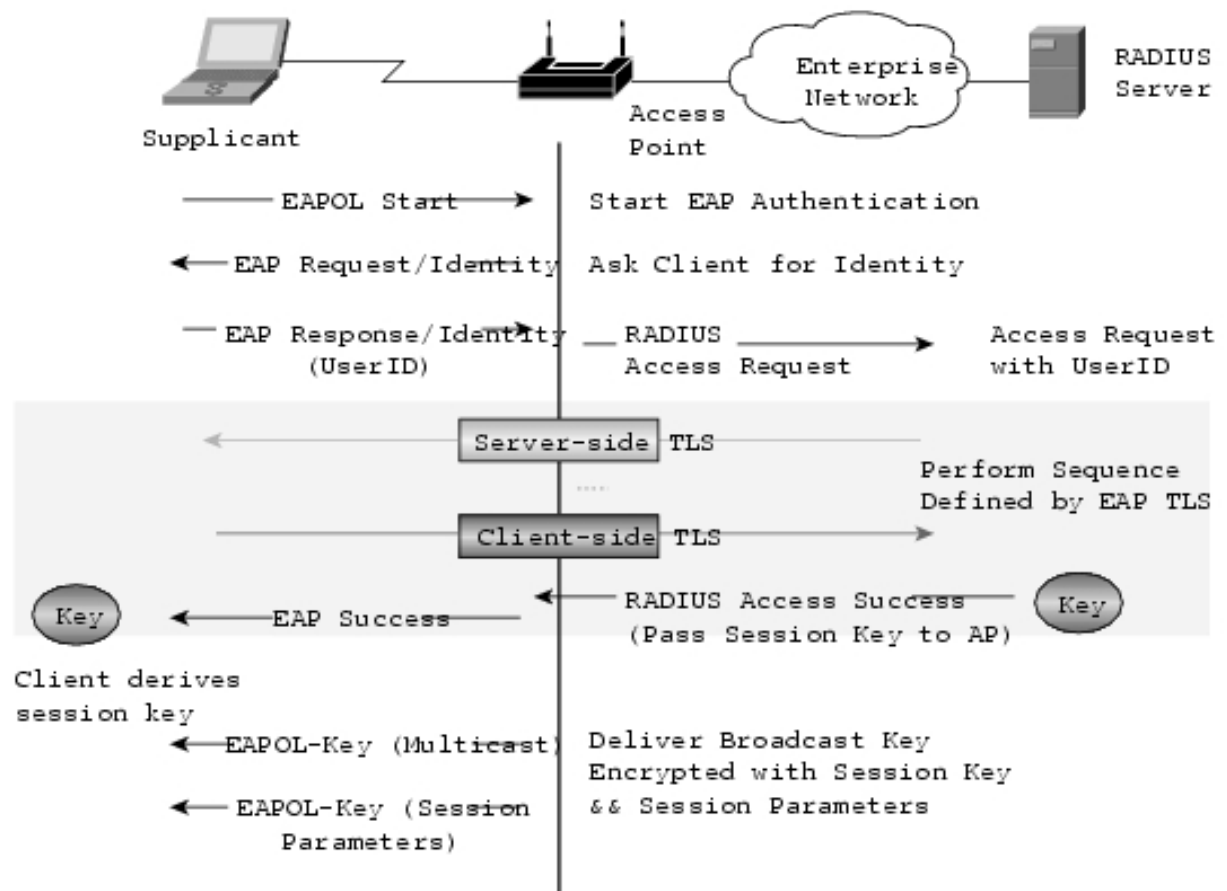
- Soporta autenticación mutua de cliente y red
- Certificados gestionados en cliente y servidor



Privacidad WiFi con WPA/EAP

Métodos EAP

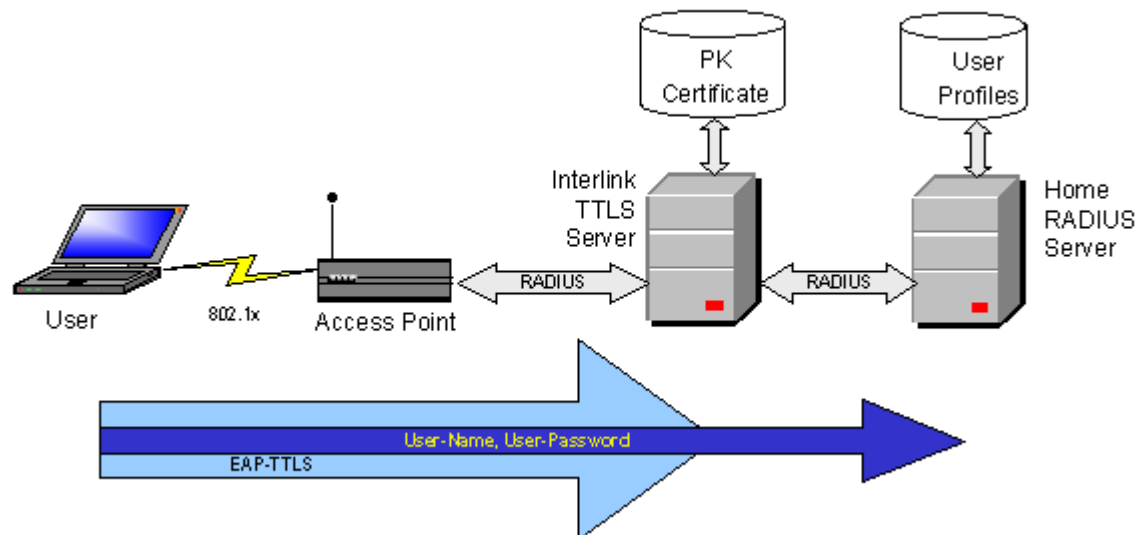
■ EAP-TLS



Privacidad WiFi con WPA/EAP

Métodos EAP

- EAP-TTLS (Tuneled Transport Layer Security)
 - Soporta autenticación mutua de cliente y red
 - Certificado gestionado en servidor





Privacidad WiFi con WPA/EAP

Métodos EAP

- LEAP (Lightweight EAP)
 - Utilizado en Cisco Aironet



Privacidad WiFi con WPA/EAP

Métodos EAP

- PEAP (Protected EAP)
 - Proporciona un método para transporte seguro de datos de autenticación, incluso para protocolos basados en contraseña.
 - Emplea tunelado PEAP entre cliente y servidor

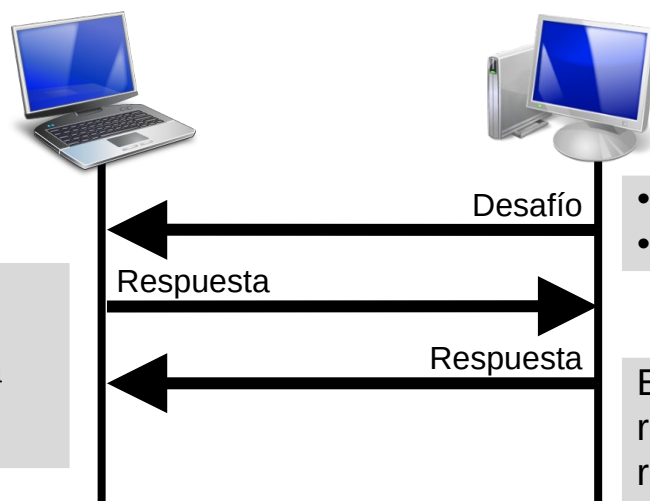
Privacidad WiFi con WPA/EAP

EAP – Extensible authentication Protocol

■ MS-CHAP

*MicroSoft
Challenge
Handshake
Authentication
Protocol*

- Nombre del usuario
- Codificación unidireccional
 - cadena de desafío recibida
 - identificador de sesión
 - contraseña del usuario



- Identificador de sesión
- Cadena de desafío arbitraria

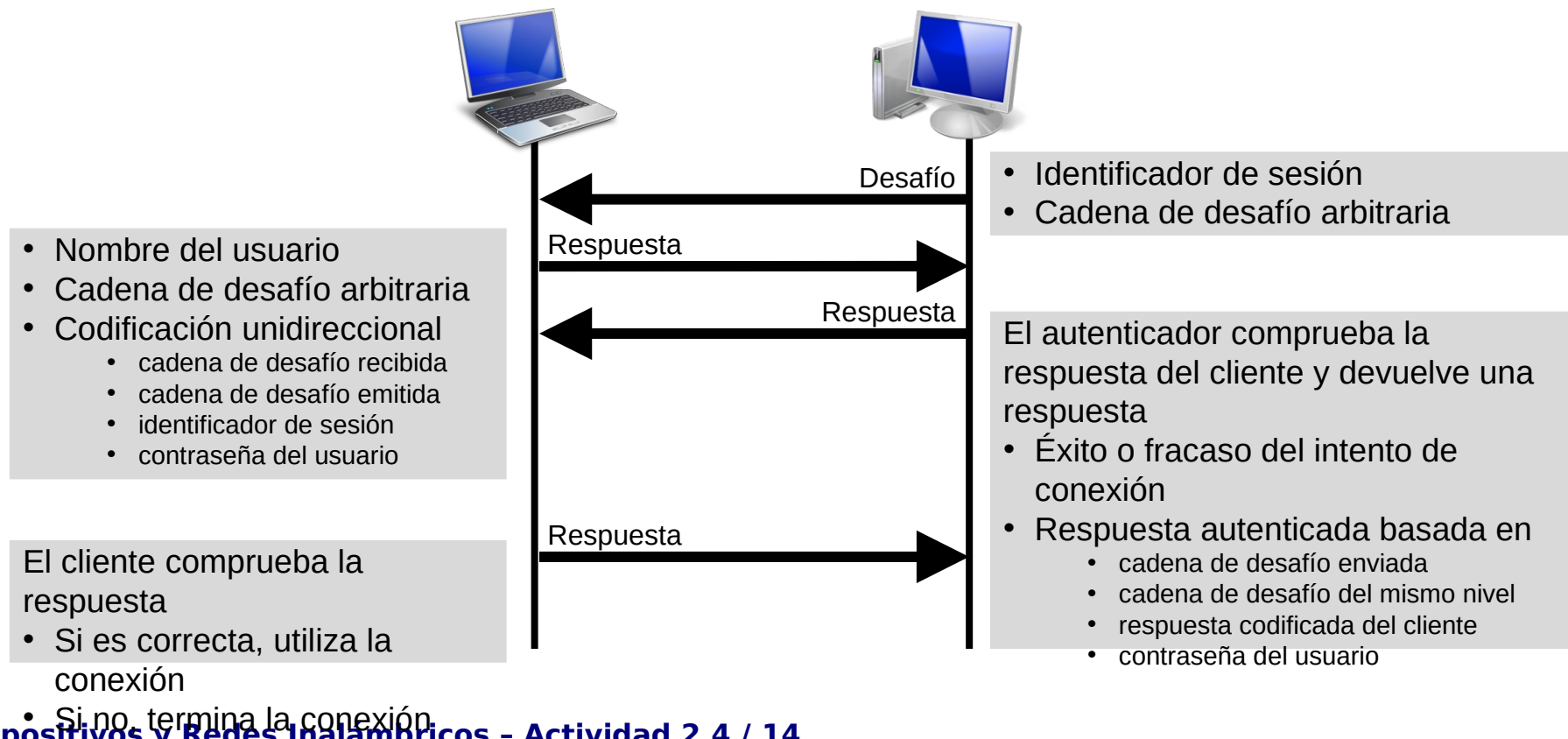
El autenticador comprueba la respuesta del cliente y devuelve una respuesta

- Éxito o fracaso del intento de conexión

Privacidad WiFi con WPA/EAP

EAP – Extensible authentication Protocol

■ MS-CHAPv2



Privacidad WiFi con WPA/EAP

Configuración de servidor *free***RADIUS**

■ Clientes



```
clients.conf (/etc/freeradius) - gedit
Archivo  Editar  Ver  Buscar  Herramientas  Documentos  Ayuda
★  📁  Abrir  📄  Guardar  🖨  🔄  Deshacer  📄  📄  📄
eap.conf ✖  clients.conf ✖  users ✖

client localhost {
    ipaddr = 127.0.0.1
    secret      = testingPC
    require_message_authenticator = no
    shortname   = localhost
    nastype     = other      # localhost isn't usually a NAS...
}

client 192.168.1.0/24 {
    ipaddr      = 192.168.1.245
    secret      = clavesecreta
    shortname   = private-WiFiRadius
}

Texto plano ▾  Ancho de la tabulación: 8 ▾  Ln 2, Col 1  INS
```

Privacidad WiFi con WPA/EAP

Configuración de servidor *free***RADIUS**

■ Usuarios

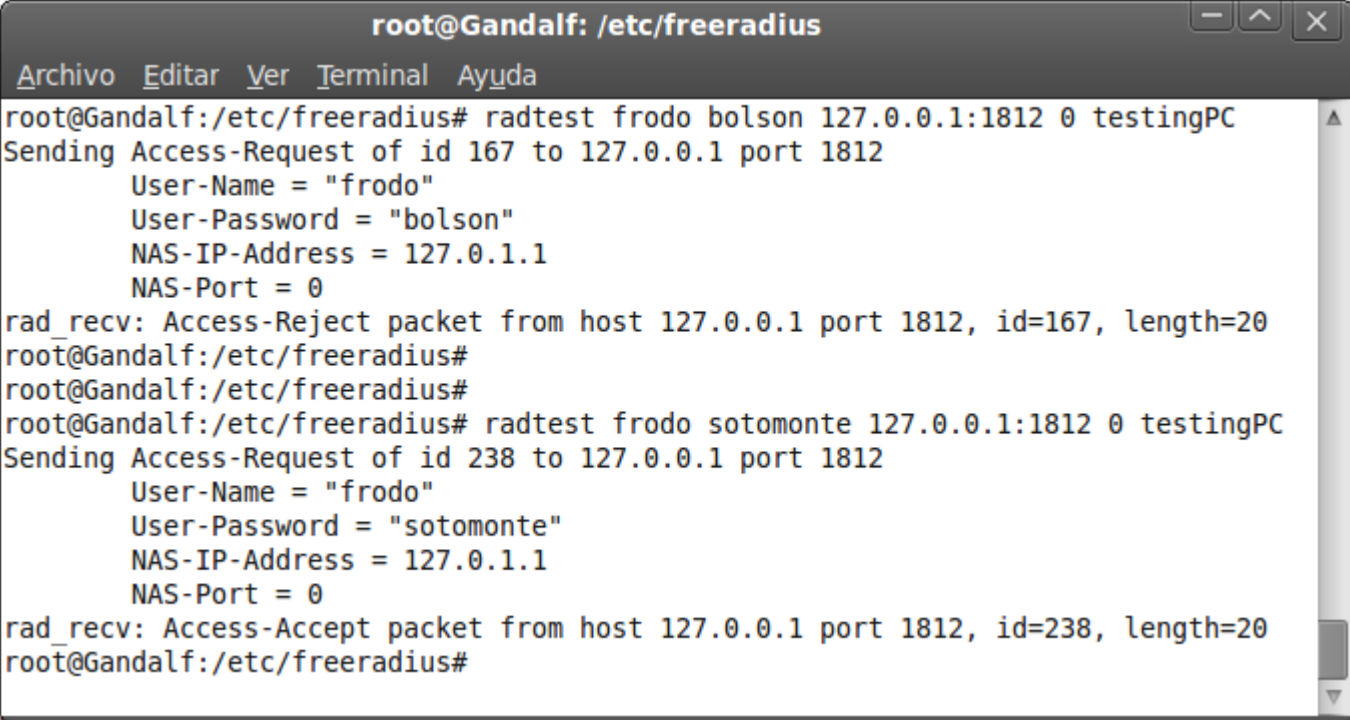
A screenshot of a gedit text editor window titled 'users (/etc/freeradius) - gedit'. The window shows a configuration file with several lines of text. The first line is 'testing' followed by 'Cleartext-Password := "password"'. The next five lines are 'bilbo', 'frodo', 'sam', 'merry', and 'gandalf', each followed by 'Cleartext-Password := "password"'. The status bar at the bottom indicates 'Texto plano', 'Ancho de la tabulación: 8', 'Ln 8, Col 1', and 'INS'.

```
users (/etc/freeradius) - gedit
Archivo  Editar  Ver  Buscar  Herramientas  Documentos  Ayuda
Abrir  Guardar  Deshacer
eap.conf  clients.conf  users
testing      Cleartext-Password := "password"
bilbo         Cleartext-Password := "bolson"
frodo         Cleartext-Password := "sotomonte"
sam           Cleartext-Password := "sagazgangi"
merry         Cleartext-Password := "brandigamo"
gandalf       Cleartext-Password := "elgris"
|
Texto plano  Ancho de la tabulación: 8  Ln 8, Col 1  INS
```


Privacidad WiFi con WPA/EAP

Configuración de servidor *free***RADIUS**

- Test de autenticación



```
root@Gandalf: /etc/freeradius
Archivo  Editar  Ver  Terminal  Ayuda
root@Gandalf:/etc/freeradius# radtest frodo bolson 127.0.0.1:1812 0 testingPC
Sending Access-Request of id 167 to 127.0.0.1 port 1812
    User-Name = "frodo"
    User-Password = "bolson"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 0
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=167, length=20
root@Gandalf:/etc/freeradius#
root@Gandalf:/etc/freeradius#
root@Gandalf:/etc/freeradius# radtest frodo sotomonte 127.0.0.1:1812 0 testingPC
Sending Access-Request of id 238 to 127.0.0.1 port 1812
    User-Name = "frodo"
    User-Password = "sotomonte"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=238, length=20
root@Gandalf:/etc/freeradius#
```

Privacidad WiFi con WPA/EAP

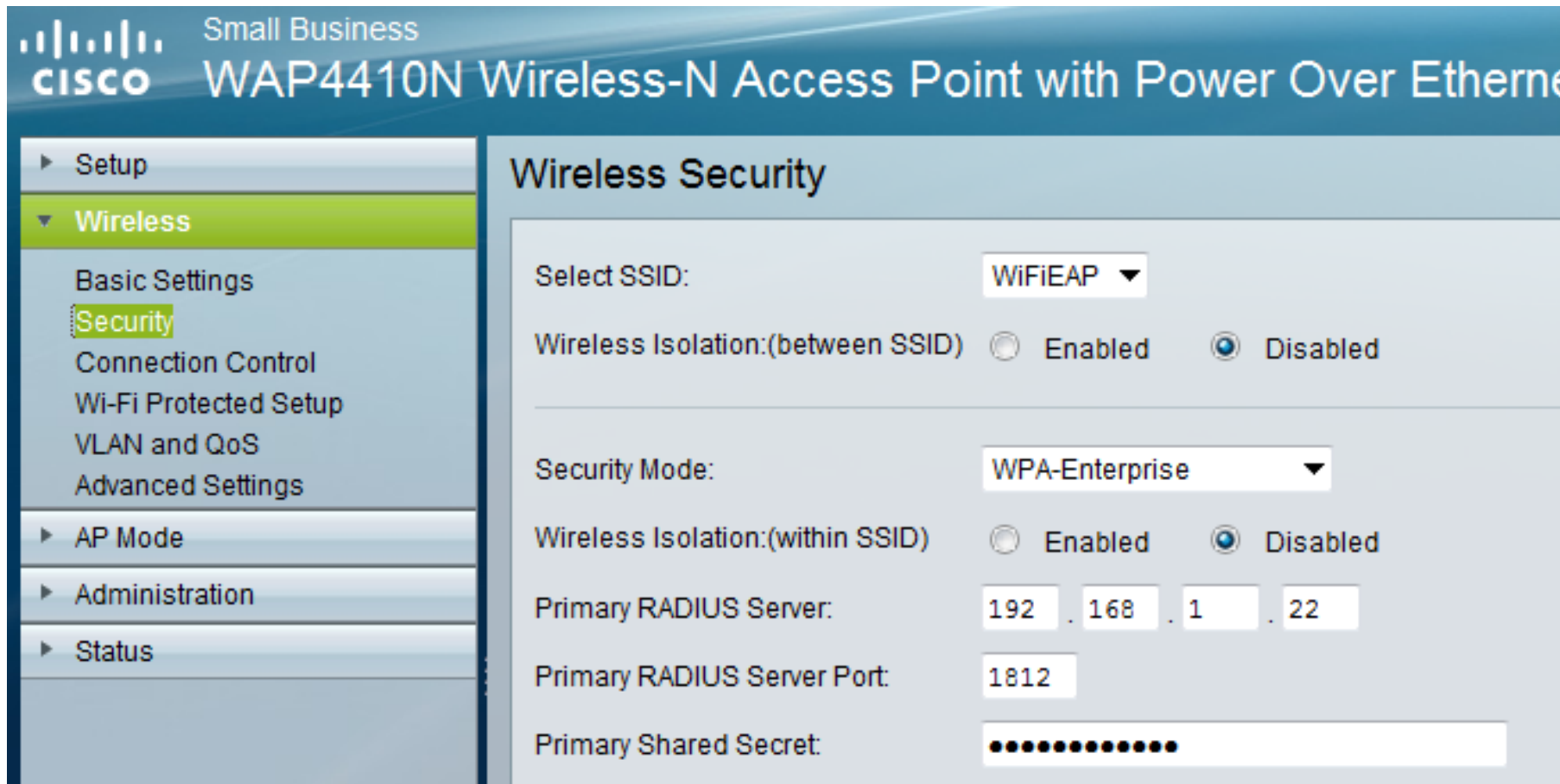
Configuración de servidor *free***RADIUS**

- Log de depuración del servidor

```
root@
Archivo Editar Ver Terminal Ayuda
[suffix] No such realm "NULL"
++[suffix] returns noop
[eap] EAP packet type response id 8 length 43
[eap] Continuing tunnel setup.
++[eap] returns ok
Found Auth-Type = EAP
+- entering group authenticate {...}
[eap] Request found, released from the list
[eap] EAP/peap
[eap] processing type peap
[peap] processing EAP-TLS
[peap] eaptls_verify returned 7
[peap] Done initial handshake
[peap] eaptls_process returned 7
[peap] EAPTLS_OK
[peap] Session established. Decoding tunneled attributes.
[peap] Received EAP-TLV response.
[peap] Success
[eap] Freeing handler
++[eap] returns ok
+- entering group post-auth {...}
++[exec] returns noop
Sending Access-Accept of id 128 to 192.168.1.245 port 2053
MS-MPPE-Recv-Key = 0x2708bc756ea2e56346a940570c60182ab8ed
MS-MPPE-Send-Key = 0xfb7711bb2b30dad5a4bd3d49cdf15dfa1924
EAP-Message = 0x03080004
Message-Authenticator = 0x00000000000000000000000000000000
User-Name = "bilbo"
Finished request 7.
Going to the next request
```

Privacidad WiFi con WPA/EAP

AP con seguridad WPA-Empresarial




The screenshot displays the configuration interface for a Cisco WAP4410N Wireless-N Access Point. The left sidebar shows the navigation menu with 'Wireless' selected, and 'Security' highlighted under the 'Basic Settings' section. The main content area is titled 'Wireless Security' and contains the following configuration options:

- Select SSID:** A dropdown menu set to 'WiFiEAP'.
- Wireless Isolation:(between SSID)** Two radio buttons: 'Enabled' (unselected) and 'Disabled' (selected).
- Security Mode:** A dropdown menu set to 'WPA-Enterprise'.
- Wireless Isolation:(within SSID)** Two radio buttons: 'Enabled' (unselected) and 'Disabled' (selected).
- Primary RADIUS Server:** Four input fields containing the IP address '192', '168', '1', and '22'.
- Primary RADIUS Server Port:** An input field containing the port number '1812'.
- Primary Shared Secret:** A password field represented by a series of dots.

Privacidad WiFi con WPA/EAP

AP con seguridad WPA2-Empresarial

 Small Business
WAP4410N Wireless-N Access Point with Power Over Ethernet

Setup

Wireless

- Basic Settings
- Security
- Connection Control
- Wi-Fi Protected Setup
- VLAN and QoS
- Advanced Settings

AP Mode

Administration

Status

Wireless Security

Select SSID: WiFiEAP ▼

Wireless Isolation:(between SSID) ☐ Enabled ☒ Disabled

Security Mode: WPA2-Enterprise ▼

Wireless Isolation:(within SSID) ☐ Enabled ☒ Disabled

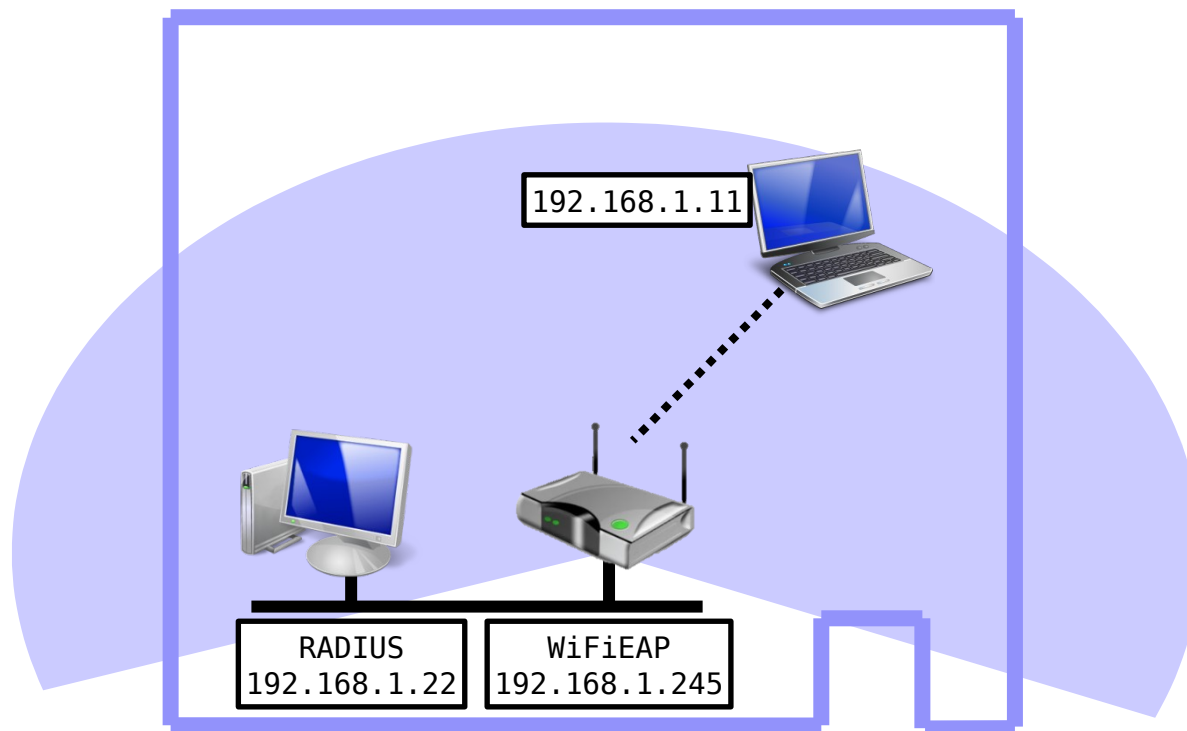
Primary RADIUS Server: 192 . 168 . 1 . 22

Primary RADIUS Server Port: 1812

Primary Shared Secret:

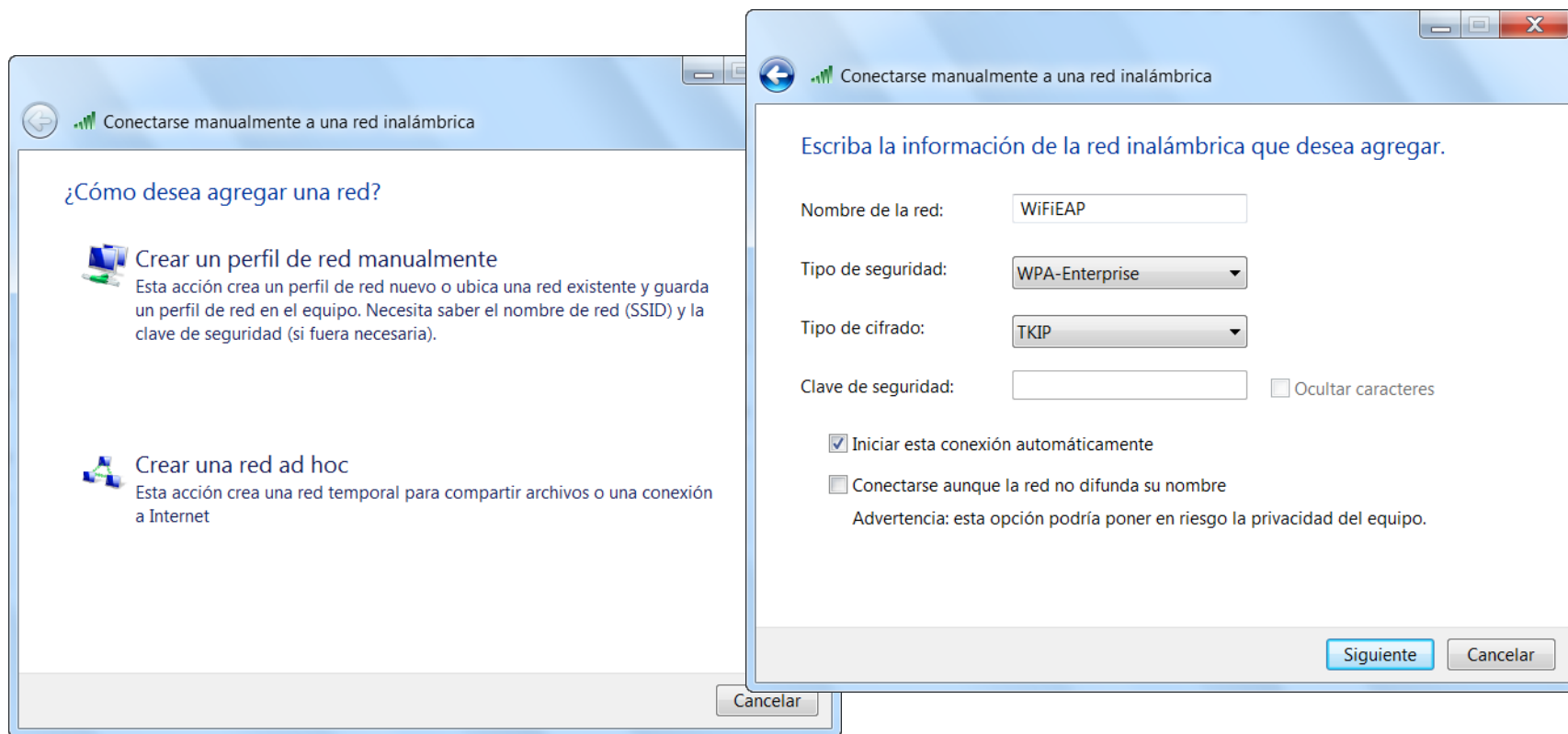
Privacidad WiFi con WPA/EAP

Conexión Windows a WPA-Empresarial



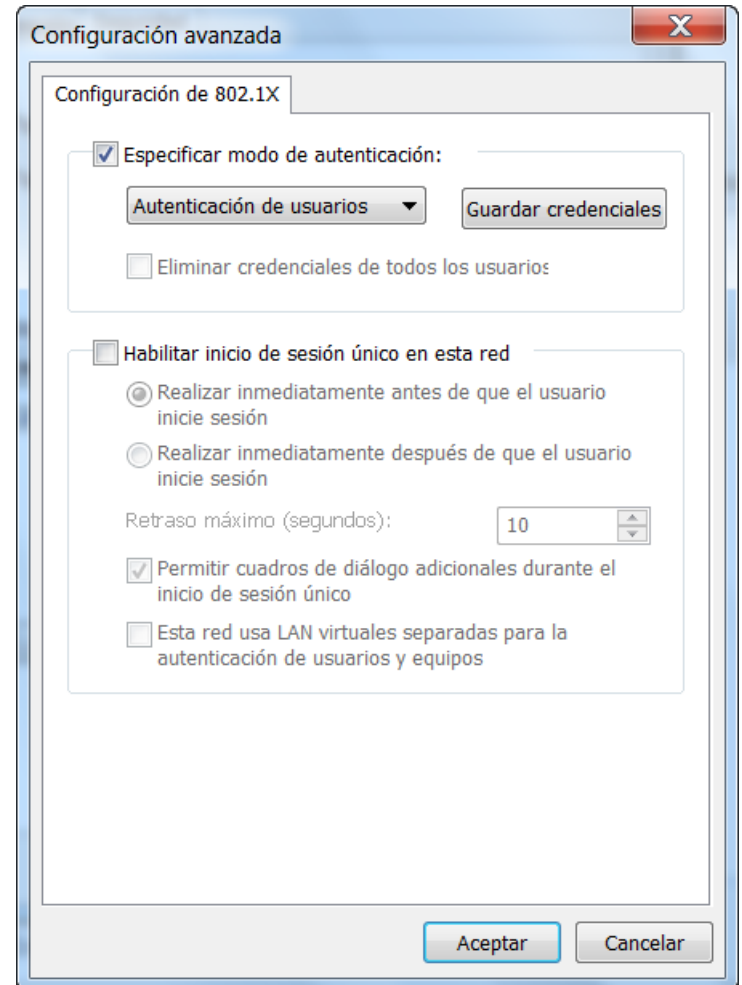
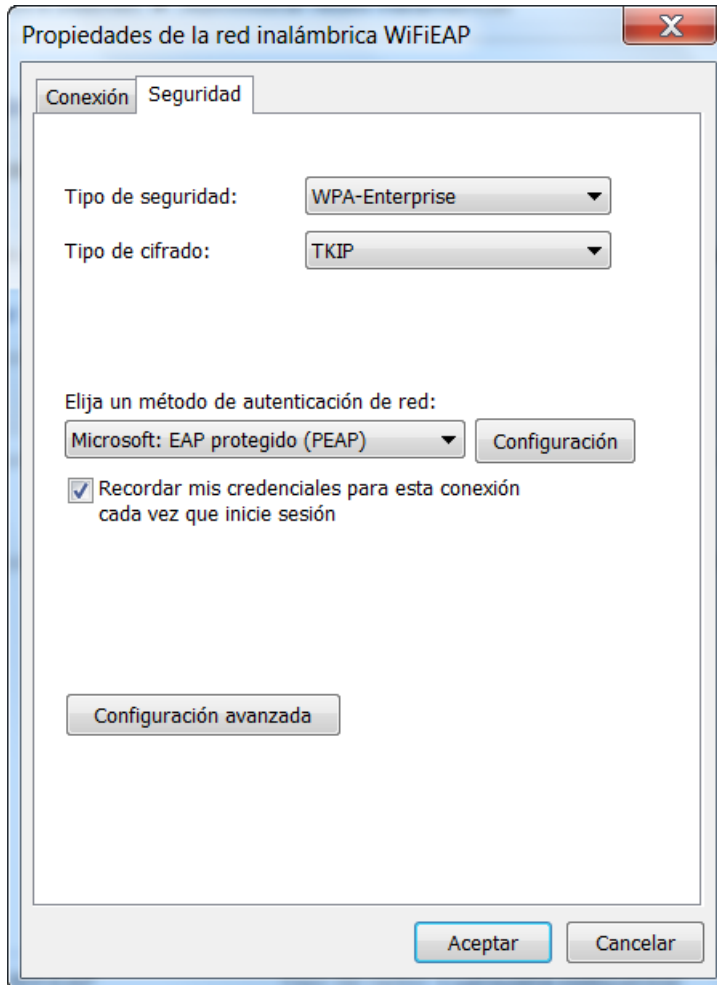
Privacidad WiFi con WPA/EAP

Conexión Windows a WPA-Empresarial



Privacidad WiFi con WPA/EAP

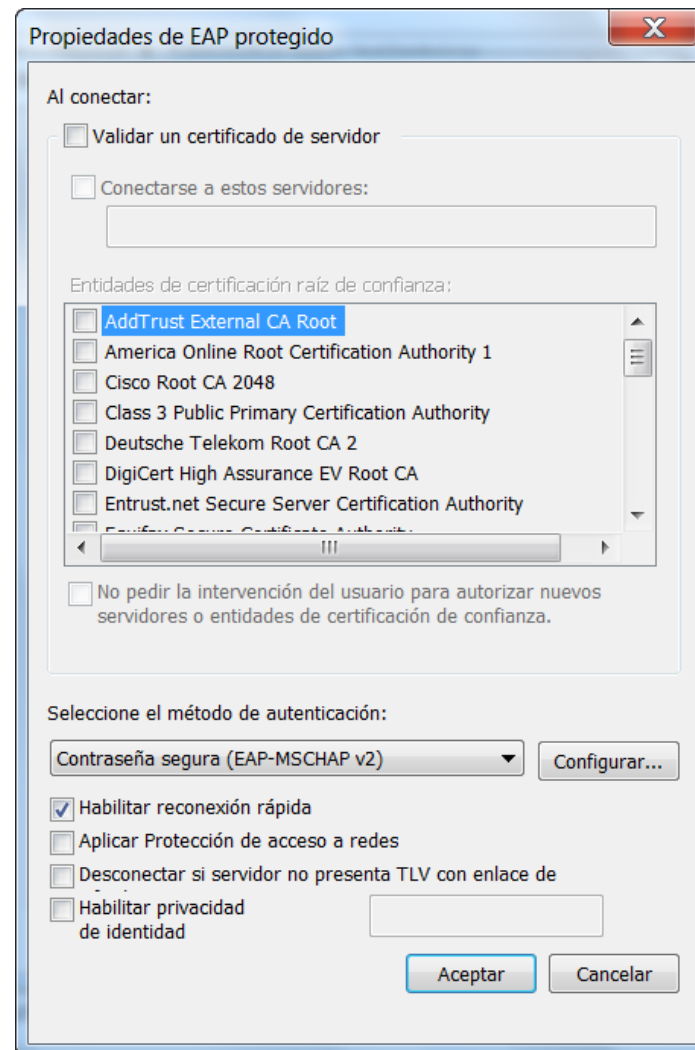
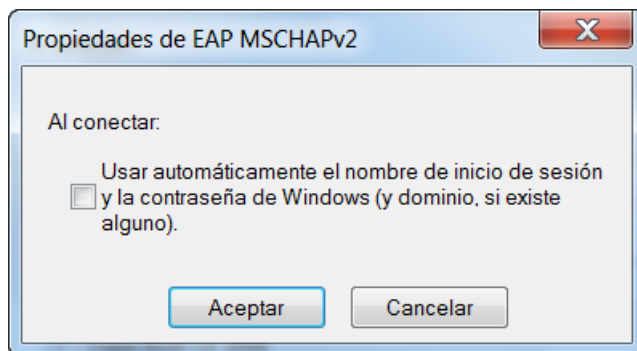
Conexión Windows a WPA-Empresarial



Privacidad WiFi con WPA/EAP

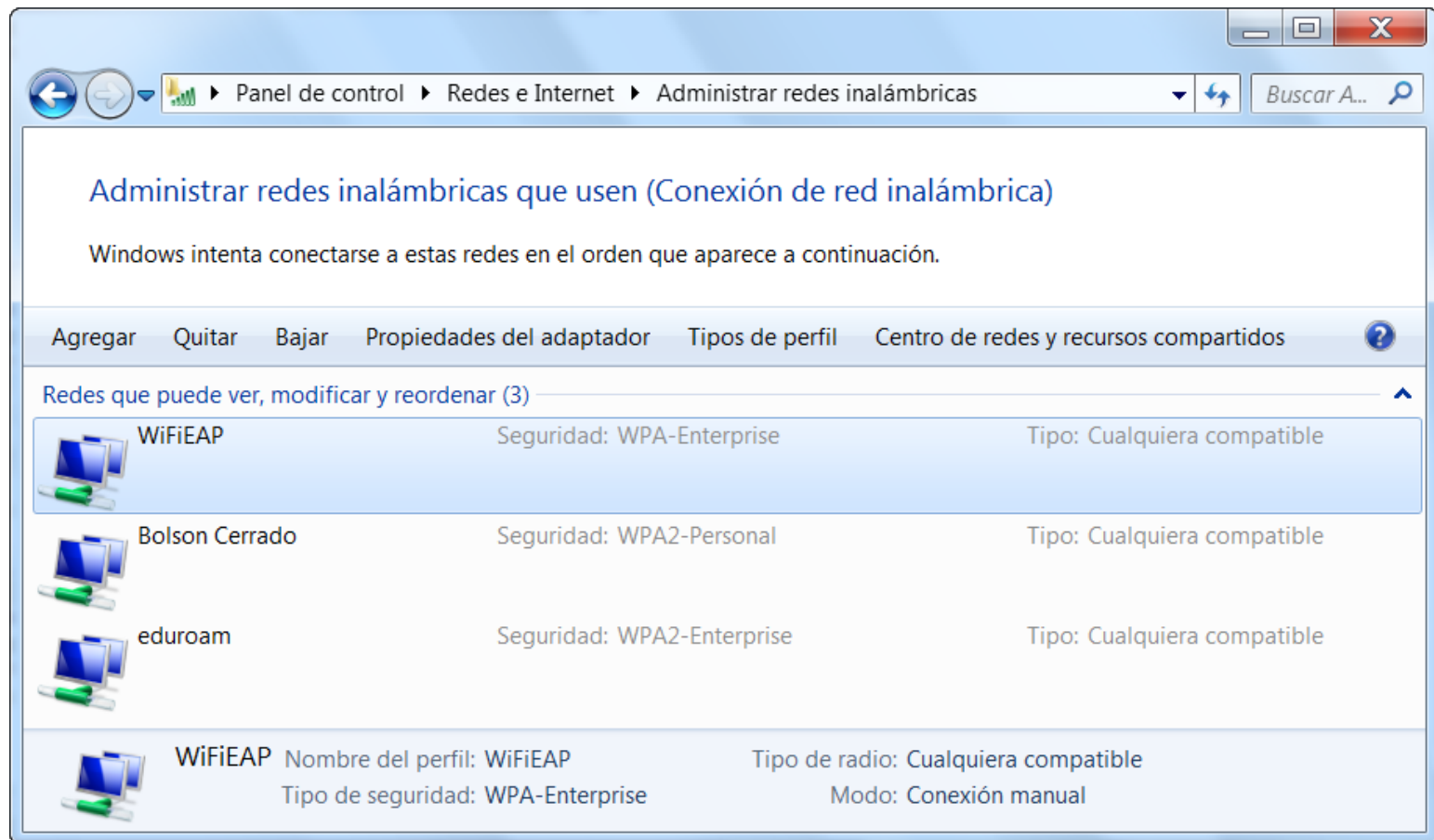
Conexión Windows a WPA-Empresarial

■ EAP MSCHAPv2



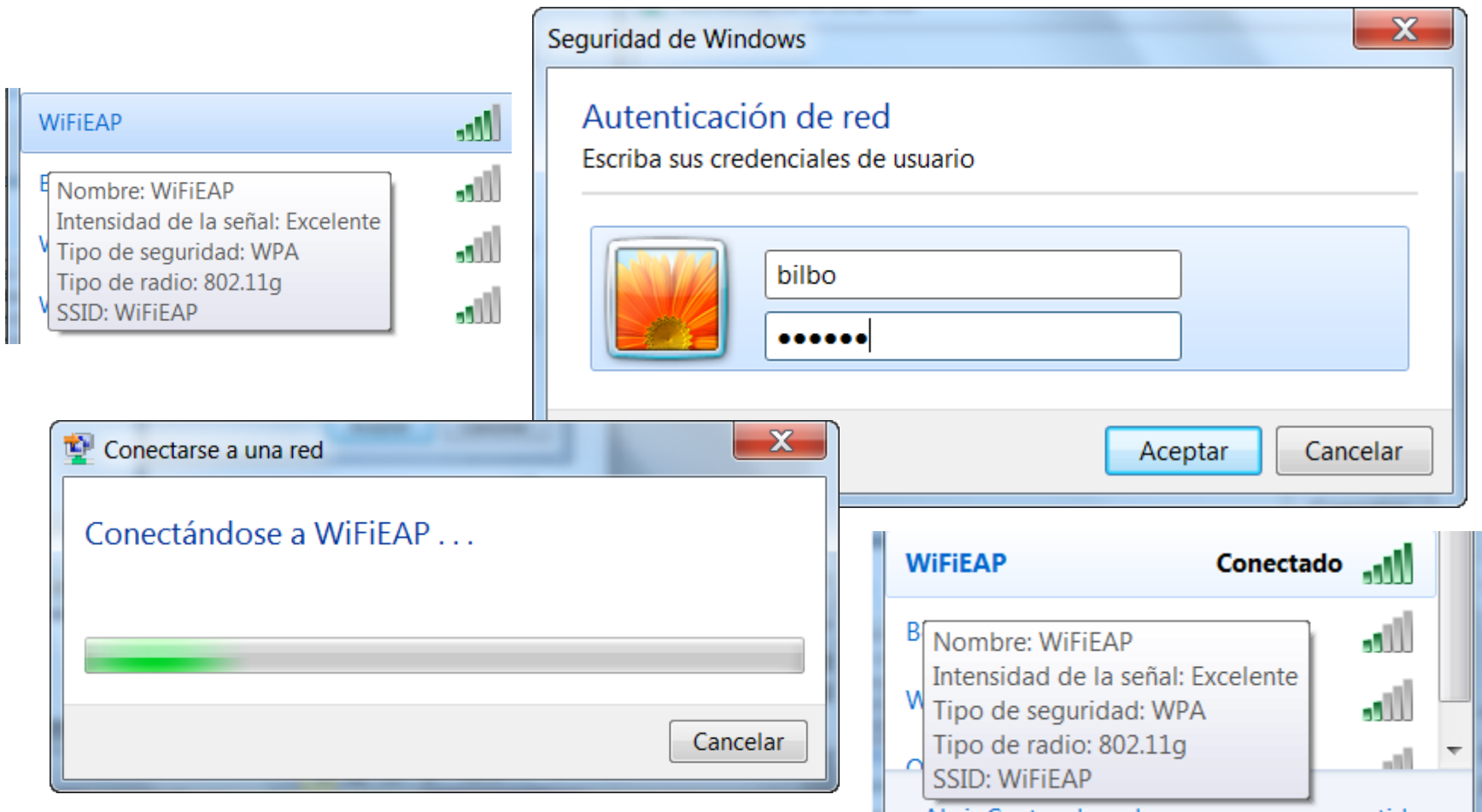
Privacidad WiFi con WPA/EAP

Conexión Windows a WPA-Empresarial



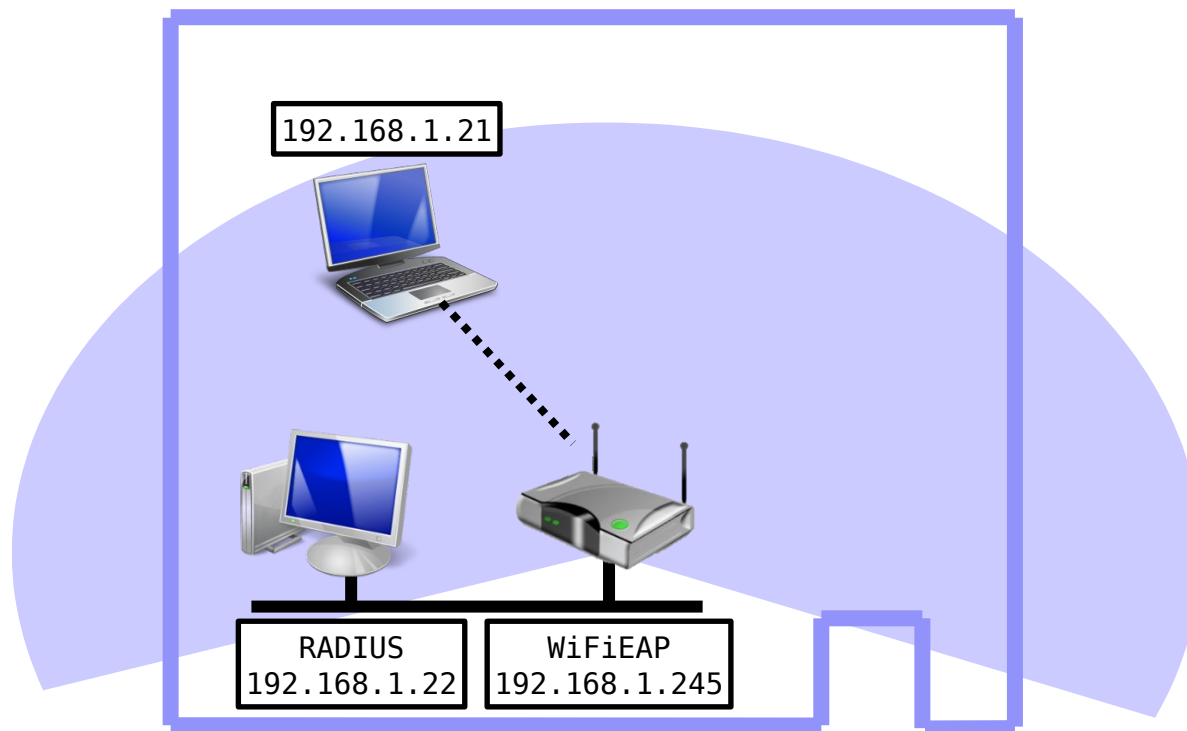
Privacidad WiFi con WPA/EAP

Conexión Windows a WPA-Empresarial



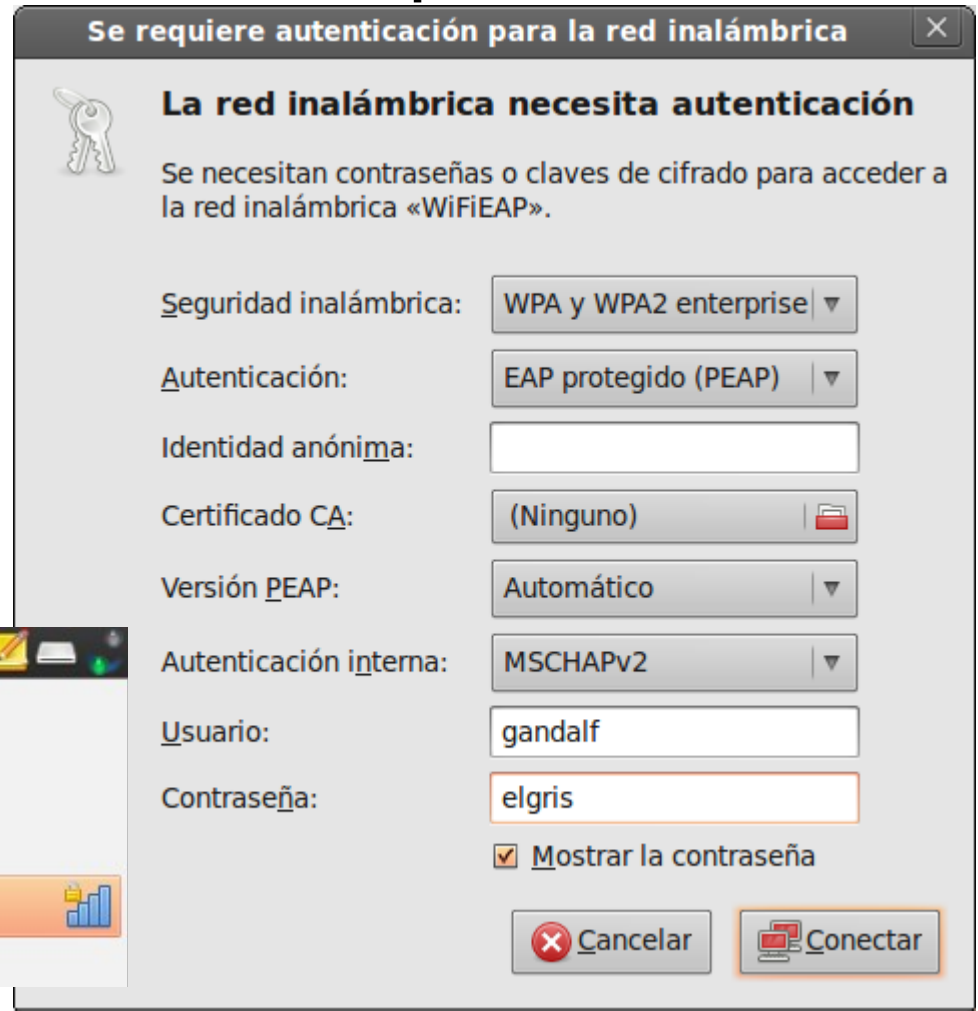
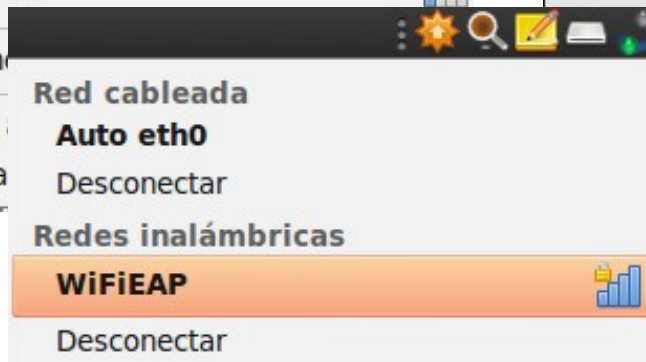
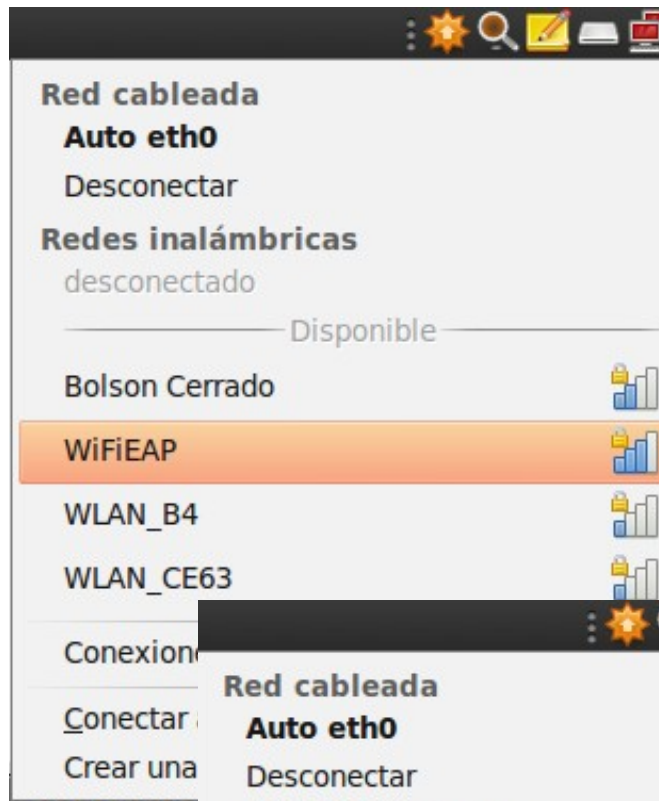
Privacidad WiFi con WPA/EAP

Conexión Linux a AP WPA-Empresarial



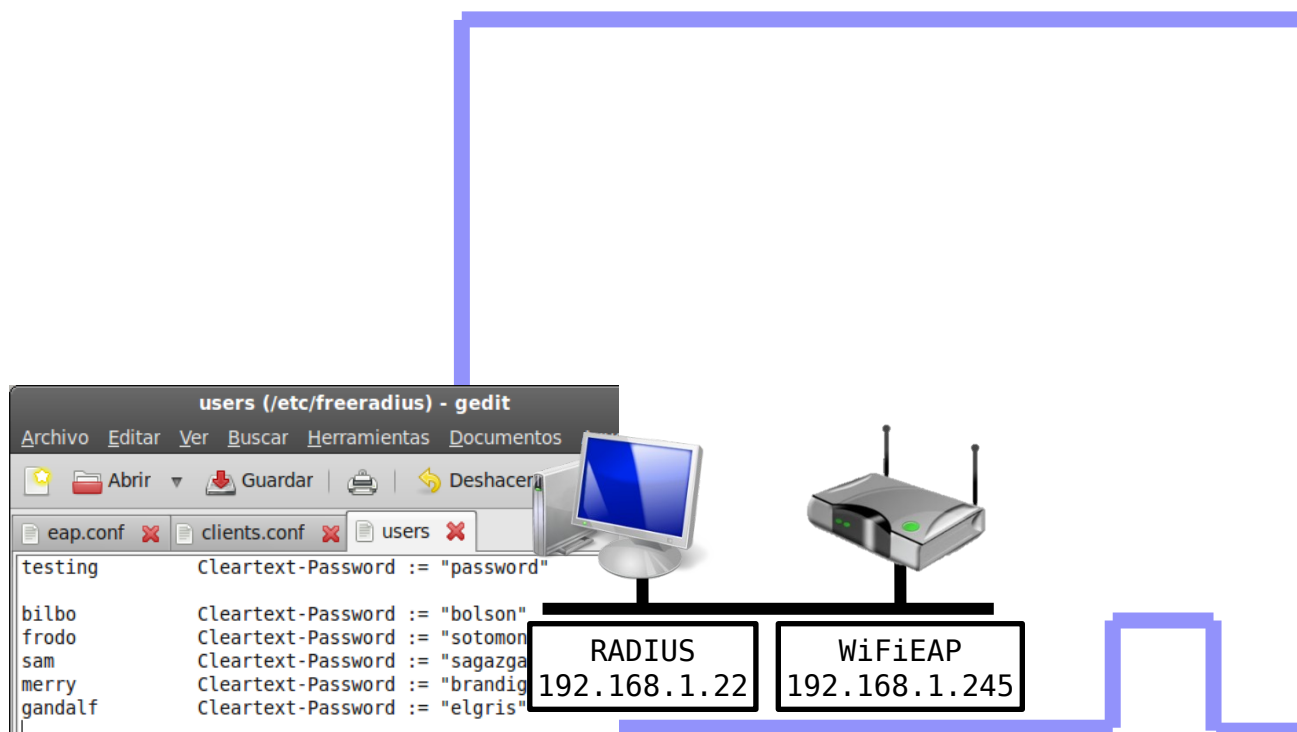
Privacidad WiFi con WPA/EAP

Conexión Linux a AP WPA-Empresarial



Privacidad WiFi con WPA/EAP

Montaje a realizar



Privacidad WiFi con WPA/EAP

Pruebas de conectividad

