Configuración básica de redes Wireless

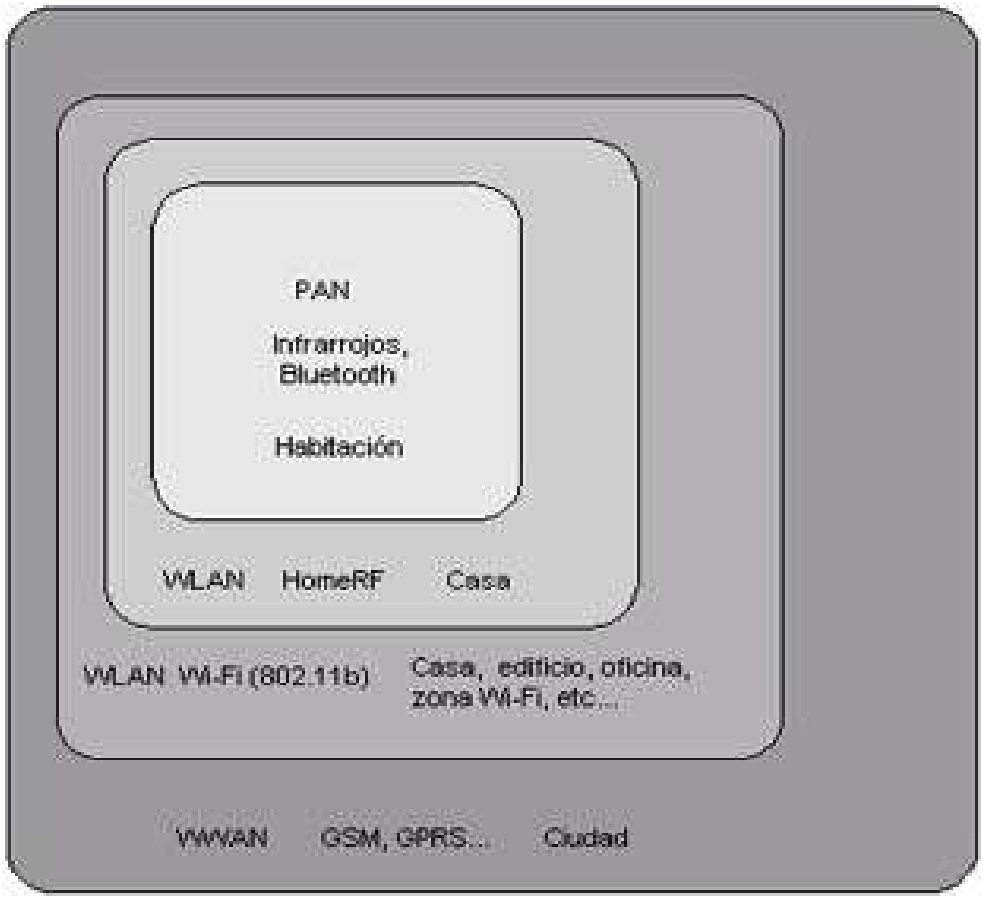
macada@gulo.org

Introducción

- Pasión por esta tecnología
- Las grandes Telycos están preocupadas por el gasto en licencias de UMTS
- Poco dinero -> Red WiFi con APs
- En pocos meses tendríamos todo funcionando-> backup
- Tenemos muchas comunidades wireless
  - Madrid Wireless, Baleares WiFi,....

¿Qué es Wireless?

- Comunicación sin cables



¿Qué es Wireless?

gULO
Grupo de Usuarios de Linux de Ourense

- **Tecnologías:**
  - 802.11a (Wi-Fi)
  - 802.11b (Wi-Fi)
  - 802.11g (Wi-Fi)
  - 802.11i (Security)
  - 802.16 (Wi-Max)
  - Bluetooth (802.15)
  - GSM (Global System for MobileCommunications)
  - 3GSM
  - GPRS (General Packet Radio Service)

Wi Fi™

¿Qué es Wireless?

GULO Grupo de Usuarios de Linux de Ourense

Tecnología	*Proposito*	*Frecuencia*	*Distancia*	*Velocidad*	*Dispositivos*	*Compatibilidad*
802.11a	Acceso Internet sin cables	5GHz	10 to 30 metros en interiores; puede depender de los materiales de construcción	Hasta 54 Mbps	Ordenadores portatiles, PDAs, telefonos móviles	No compatible con 802.11b, 802.11g

Wi Fi™

¿Qué es Wireless?

GULO Grupo de Usuarios de Linux de Ourense

Tecnología	*Proposito*	*Frecuencia*	*Distancia*	*Velocidad*	*Dispositivos*	*Compatibilidad*
802.11b	Acceso Internet sin cables	2.4GHz	90 metros en interiores; puede depender de los materiales de construcción	Hasta 11 Mbps	Ordenadores portatiles, PDAs, telefonos móviles	Compatible con otros dispositivos de frecuencia 2.4Ghz

Wi Fi™

¿Qué es Wireless?

GULO Grupo de Usuarios de Linux de Ourense

Tecnología	*Proposito*	*Frecuencia*	*Distancia*	*Velocidad*	*Dispositivos*	*Compatibilidad*
802.11g	Acceso Internet sin cables	2.4GHz	50 metros en interiores; puede depender de los materiales de construcción	Hasta 54 Mbps	Ordenadores portatiles, PDAs	Compatible con otros dispositivos de 802.11b

Wi Fi™

¿Qué es Wireless?

GULO Grupo de Usuarios de Linux de Ourense

Tecnología	*Proposito*	*Frecuencia*	*Distancia*	*Velocidad*	*Dispositivos*	*Compatibilidad*
802.16 (Wi-Max)	Acceso Internet sin cables en areas Metropolitanas	Entre 10 y 66 GHz	Distancias de Km	En evolución	En evolución	Según los fabricantes

Wi Fi™

¿Qué es Wireless?

Tecnología	*Proposito*	*Frecuencia*	*Distancia*	*Velocidad*	*Dispositivos*	*Compatibilidad*
Bluetooth	Conectar disp. móviles como PDA, camaras, impresoras	2.4Ghz	Hasta unos 10 m. Puede afectar los materiales de construcción	Hasta 720 Kbps	Impresoras, camaras, teléfonos móviles y otros dispositivos	Otros dispositivos bluetooth

¿Qué es Wireless?

GULO Grupo de Usuarios de Linux de Ourense

Tecnología	*Proposito*	*Frecuencia*	*Distancia*	*Velocidad*	*Dispositivos*	*Compatibilidad*
GSM (Sistema Global para Comunicaciones Móviles)	Sistema telefónico digital celular (sistema más usado en el mundo)	900MHz, 1,800MHz, 1,900MHz	Depende del terminal y el proveedor	Depende del proveedor	Teléfonos móviles, PDAs	Otros dispositivos GSM

Wi Fi™

¿Qué es Wireless?

Tecnología	*Proposito*	*Frecuencia*	*Distancia*	*Velocidad*	*Dispositivos*	*Compatibilidad*
3GSM	Red GSM de 3ª Generación	1,920-, 1,980Mhz and 2,110-2,170MHz	Depende del terminal y el proveedor	Hasta 2Mbps	Teléfonos móviles de 3GSM, PDAs	Otros dispositivos 3GSM

¿Qué es Wireless?

GULO Grupo de Usuarios de Linux de Ourense

Tecnología	*Proposito*	*Frecuencia*	*Distancia*	*Velocidad*	*Dispositivos*	*Compatibilidad*
GPRS	Aceso a Internet usando la misma red GSM	Depende del Proveedor	Depende del terminal y el proveedor	En teoría la velocidad máxima es 171Kbps; en la realidad 40-50 Kbps	Teléfonos móviles GSM, GPRS	Otros dispositivos compatibles con GSM

Wi Fi™

Wi-Fi Consortium

- Estándar 802.11 -> redes inalámbricas
- Subgrupos dentro de 802.11 (a, b, g, i, h). Son variantes
- En 1999 se aprobó 802.11b
- Wi-fi (Wireless Fidelity): grupo de fabricantes que certifica todos los productos compatibles entre sí dentro de la norma 802.11

Conceptos básicos

Tipos de Conectividad (formas de Trabajo)

- **802.11a** (5 Ghz)
- **802.11b** (2.4 Ghz)
- **802.11c** Define carateristicas de AP como bridges.
- **802.11d** Permite el uso de 802.11 en paises restringidos por el uso de las frecuencias.
- **802.11e** Define el uso de QoS.
- **802.11f** Define el enlace entre STA y AP. Roaming
- **802.11g** (2.4 Ghz a más velocidad que 802.11b)
- **802.11h** Superior al 802.11a permite asignación dinámica de canales (coexistencia con el
- HyperLAN). Regula la potencia en función de la distancia.
- **802.11i** Estándar que define la encriptación y la autentificación para complementar completar y mejorar el WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del WPA con su Temporal Key Integrity Protocol (TKIP).
- **802.11j** Estándar que permitirá la armonización entre el IEEE, el ETSI HyperLAN2, ARIB e HISWAN
- **802.11m** Propuesto para mantenimiento de redes inalámbricas.

Wi-Fi Consortium

GULO Grupo de Usuarios de Linux de Ourense

- **Ventajas:**
  - **Movilidad**
  - **Fácil instalación**
  - **Flexibilidad**
  - **Facilidad**, para incorporar redes en lugares históricos sin necesidad de extender cable
  - **Adaptabilidad**. Permite frecuentes cambios de la topología de la red y facilita su escalabilidad
  - Facilita la **ampliación** de nuevos usuarios a la red, sin la necesidad de extender un cable a su nuevo puesto de trabajo

Wi Fi™

Conceptos básicos

- **Punto de acceso (AP/PA)**: Se trata de un dispositivo que ejerce básicamente funciones de Puente entre una red Ethernet cableada con una red *WiFi* sin cables.

- **Clientes WiFi**: Equipos portatiles (PDAs, portatiles,..) con tarjetas WiFi (PCMCIA, USB o MINI-PCI) y equipos sobremesa con tarjetas WiFi (PCI, USB o internas en placa).

- **SSID *(Service Set Identification):*** Este identificador suele emplearse en las redes Wireless creadas con Infraestructura. Se trata de un conjunto de Servicios que agrupan todas las conexiones de los clientes en un sólo canal.

- **Roaming**: Propiedad de las redes WiFi por la los clientes pueden estar en movimiento a ir cambiando de punto de acceso de acuerdo a la potencia de la señal.

Conceptos básicos

Seguridad en Wireless

- Las redes inalámbricas requieren nuevos conceptos de seguridad que se obvian en las redes cableadas.
- Un intruso que busque acceso a una LAN cableada se enfrenta irremediablemente con el problema del acceso físico a la misma.

- En una WLAN el problema del intruso se torna etéreo. Es suficiente con permanecer en el área de cobertura, que puede ser muy extensa, para estar en contacto con la red local. Puede incluso estar en movimiento.

- Esta nueva situación obliga a la búsqueda de nuevas soluciones para garantizar la seguridad de los usuarios.

¿Qué es seguridad?

- Autenticidad: El usuario es quien dice ser.
- Privacidad: La información no es legible por terceros.
- Integridad: La información no puede ser alterada en tránsito.

Conceptos básicos

Seguridad en Wireless - WEP

WEP (Wired Equivalent Privacy)

- Privacidad equivalente a red cableada.
- Con este estándar el usuario debía introducir un juego de claves, que podían ser de 40 o de 104 bits, coincidente con las configuradas en el punto de acceso.
- Un sistema de clave compartida (PSK, Pre-Shared Key).

- **PROBLEMAS:**
  - Todos los usuarios deben usar las mismas claves.
  - Un atacante puede sin demasiada dificultad determinar por fuerza bruta el WEP y desencriptar el tráfico o inyectar paquetes válidos en la red.

- NUNCA CONFIGURAR UNA WIFI SIN ENCRIPTACION WEP

Conceptos básicos

Seguridad en Wireless - WEP

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version: v3.03.1

Wireless-G Broadband Router hotspot.macada.net

Wireless

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Wireless Security

Security Mode: WEP

Default Transmit Key: 1 2 3 4

WEP Encryption: 64 bits 10 hex digits

Passphrase: gulo Generate

Key 1: 450D2B1F49

Key 2: EB141B7450

Key 3: 719E579BF7

Key 4: 1DECED0EEE

Security Mode: You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate.
More...

Cisco Systems

Save Settings Cancel Changes

Conceptos básicos

Seguridad en Wireless - WPA

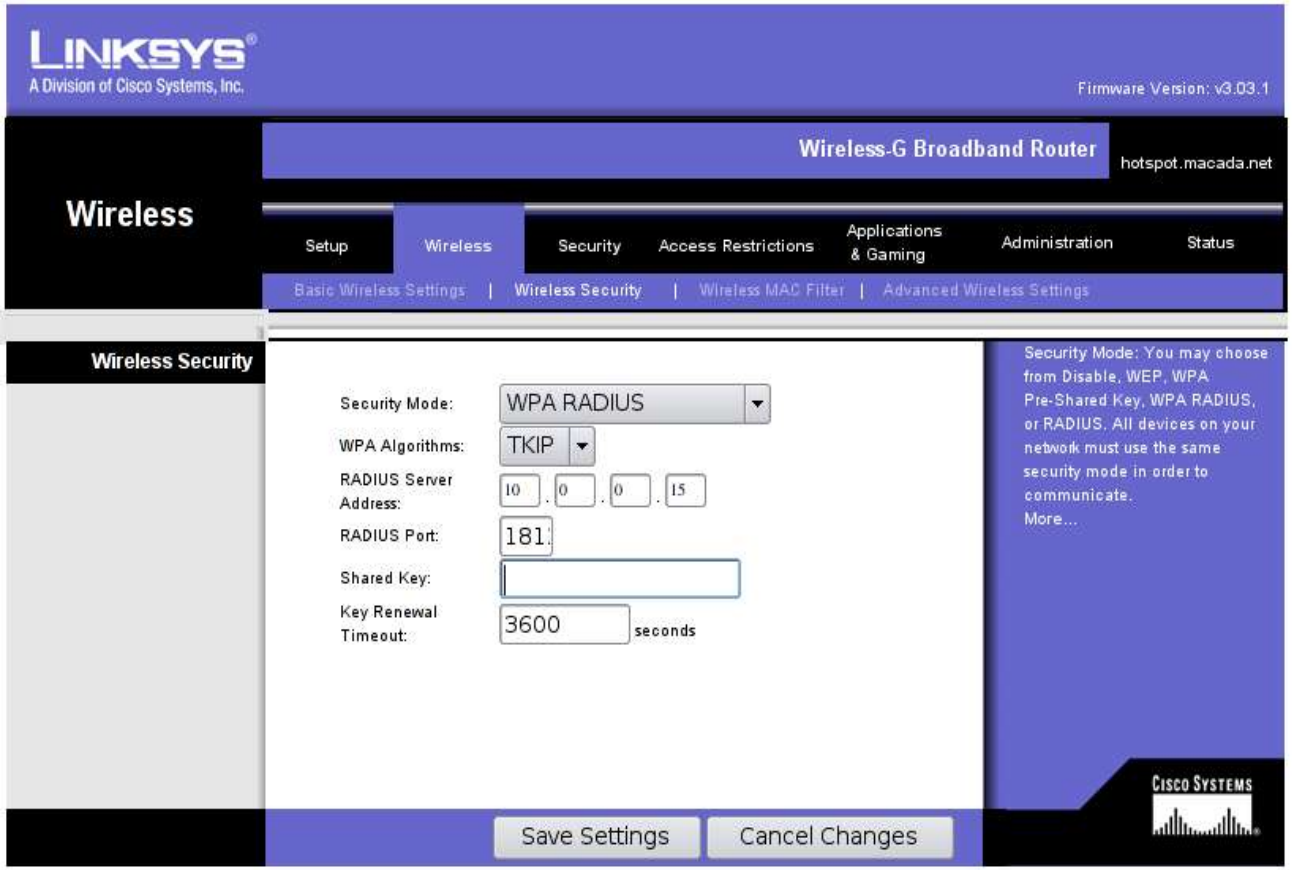
WPA (Wi-Fi Protected Access)

- Este estándar desarrollado por la Wi-Fi alliance trata de ser el sustituto de WEP.
- A la hora de diseñarlo se trató de que fuera compatible con la mayor cantidad de dispositivos ya presentes en el mercado.
- WPA puede ser incorporado en muchos sistemas diseñados para WEP sin más que una actualización de firmware.

- TKIP (Temporal Key Integrity Protocol)
  - Al contrario que WEP, utiliza claves de sesión dinámicas de 128 bits, para cada usuario, cada sesión y cada paquete.
  - Los usuarios deben acceder a través de un servidor de autentificación, típicamente un RADIUS.
  - Una vez autentificados mutuamente el servidor genera una clave "master" que transmite de manera segura al cliente y que será utilizada para enviar el resto de claves auxiliares que serán utilizadas durante esa sesión.
- MIC (Message Integrity Check)
  - Se trata de un sistema que garantiza que un paquete no ha sido modificado en tránsito.

Conceptos básicos

Seguridad en Wireless - WPA



Conceptos básicos

Autenticación en Wireless

Sistema abierto

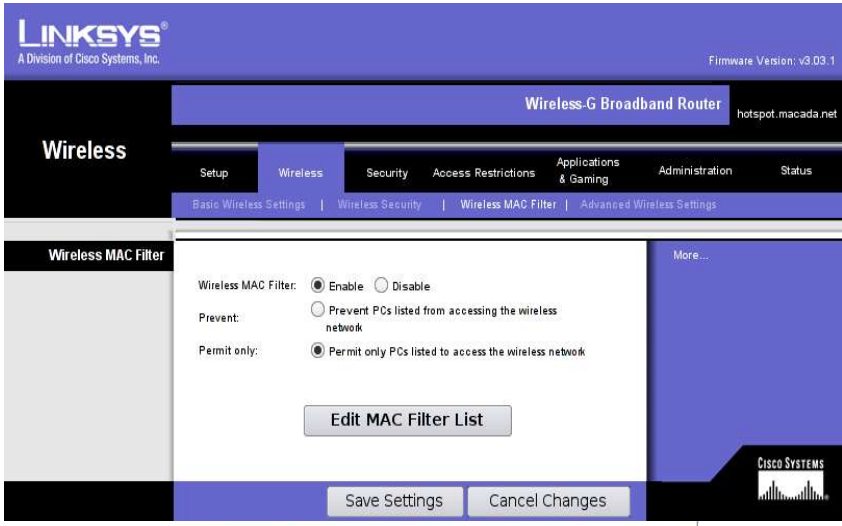
- Cualquier cliente puede asociarse a la red sin autentificarse.
- En este caso podría establecerse un filtro que confinara el tráfico a la red del GUI.
- El tráfico va sin encriptar.

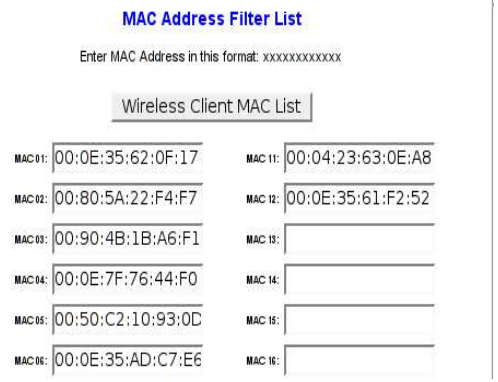
Conceptos básicos

Autenticación en Wireless

Autentificación por MAC

- El AP comprueba la MAC del cliente antes de permitir el acceso.
- Las MAC se introducen en el AP.





PROBLEMAS

- La dirección MAC de un cliente legítimo puede ser capturada por un atacante.
- Con este sistema se podría establecer un filtro que obligase a utilizar encriptación en SSL o a nivel de aplicación (pop3s, imaps, SSH, HTTPS).

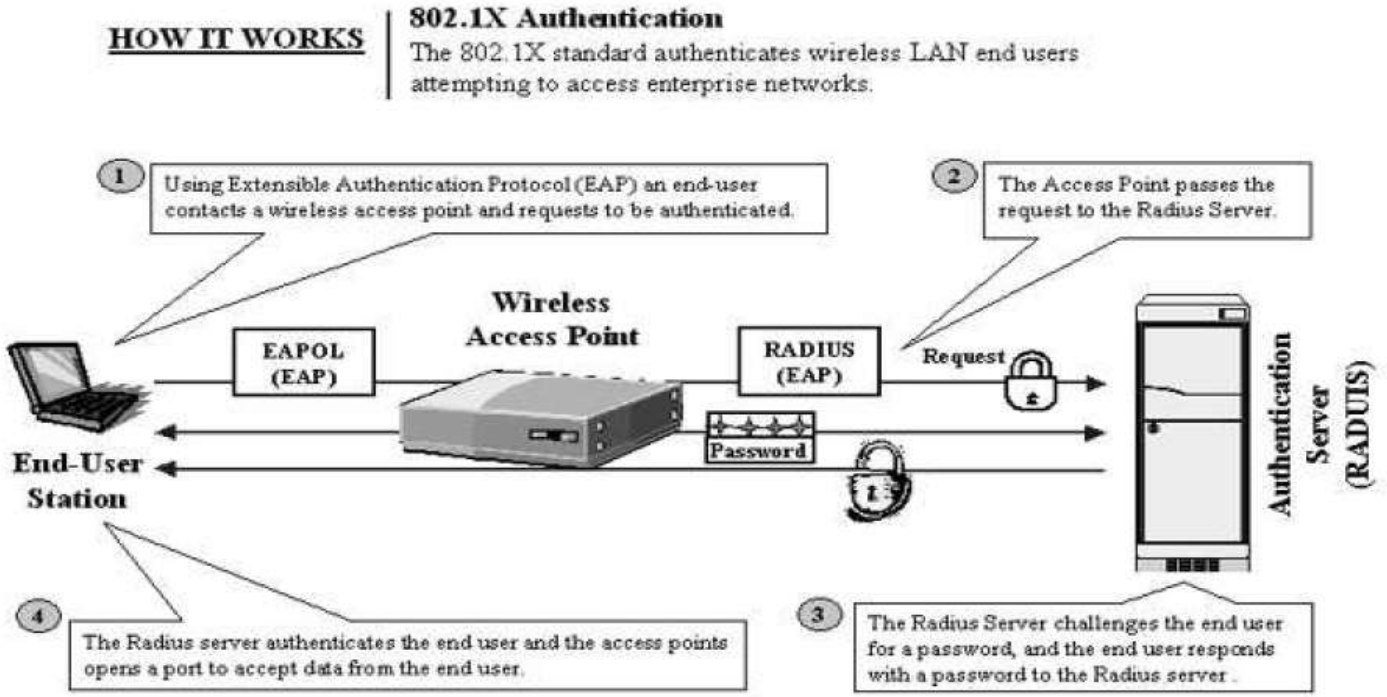
SOLUCIÓN

http://nocat.net/ (NocatNet)

Conceptos básicos

Autenticación en Wireless - EAP

- Protocolo extensible de autentificación.
- Es un protocolo que sirve para adaptar a las redes inalámbricas protocolos ya establecidos y otros nuevos.
- Este sistema requiere siempre un Servidor de Autenticación
- EAP utiliza dos WEP comos claves de sesión que las partes implicadas acuerdan durante la autentificación y que se cambia con una frecuencia que determina el administrador del AP.
- Un WEP es para el tráfico broadcast y otro se establece para cada cliente de manera que los clientes no pueden escucharse mutuamente.



Conceptos básicos

Variantes de EAP (Extensible Authentication Protocol):

- EAP-TLS (EAP – Transport Level Security)
- Autenticación mutua, cifrada y depende de certificados de una CA. Soportado
- por hostapd.

- EAP-TTLS (EAP Tuneled TLS)
- No necesita ambos certificados, solo el de el servidor para crear un tunel.
- Usado en redes wireless.

- EAP-MD5
- El servidor envia un mensaje desafío al cliente y este contesta con otro
- mensaje MD5 o no autentica. Fácil de implementar pero menos fiable.

- LEAP (Lightweigth EAP)
- Implementacion de Cisco, autenticación mutua, permite el uso dinámico de
- WEP.

- PEAP (Protected EAP): desarrollado por M$, Cisco y RSA, similar a EAPTTLS

Topologías

Tipos de Conectividad (formas de Trabajo)

- **Ad–hoc**: Son redes creadas punto a punto entre clientes WiFi.
  - En estas redes todos reciben los paquetes de todos y envían sus propios paquetes a todos los ordenadores de la red.
  - Para esto no se necesita nada especial, sólo definir una red con un nombre (SSID)
  - Consejo:
    - Encriptar a 128 bits (con WEP)
    - No tener demasiados ordenadores en la misma red.

.

- **Managed**: Este tipo de redes son las mas extendidas ya que es la configuración más estándar en la tecnología WiFi.
  - El Access Point (o Base Station en terminología comercial de Apple) envía las tramas 802.11 a los destinatarios finales.
  - Cuando un ordenador o tarjeta está conectado a la red a través de un AP, se dice que está en modo *managed*.
  - Características de un AP:
    - Soportan la propiedad de roaming.
    - Bridging de paquetes IP y además manipulan los bits de 802.11 a bajo nivel, normalmente en la propia tarjeta.
    - Enrutado IP, servidor DHCP

.

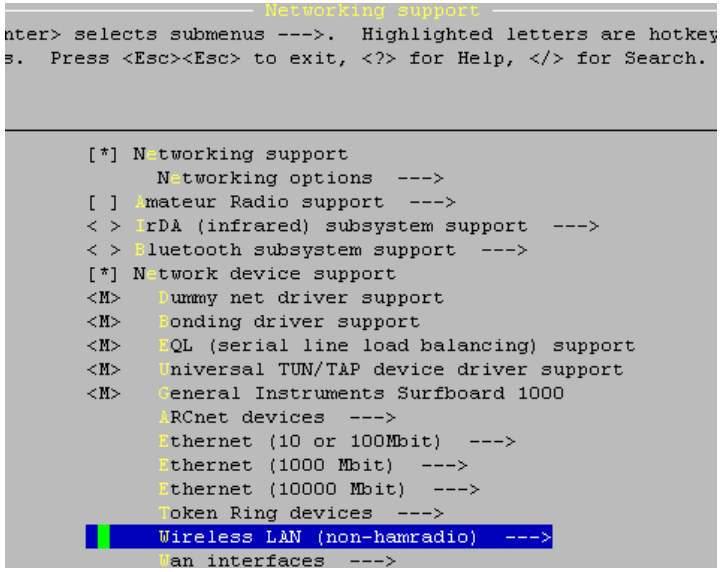
- **Master**: es el modo en que trabajan los AP. Algunos drivers en Linux pueden trabajar en modo *master*

Drivers - Controladores

GULO Grupo de Usuarios de Linux de Ourense

Configuración de drivers del núcleo

- Dentro del menu `Devices Drivers`, está el submenu `Networking support`.
- Entrar en el submenu
  - `Wireless LAN(non-hamradio).`



Marcas - ChipSets

Wavelan Orinoco - Hermes

- Fabricante: Lucent, AT&T y NCR
- Puede Funcionar en modo “master” gracias al proyecto: http://hunz.org/hermesap.html
- Driver: Está en el kernel
- Primera revisión:
  - PCMCIA (wavelan_cs.o)

```
AT&T/Lucent old WaveLAN Pcmcia wireless support
```

```
Hermes PCMCIA card support
```

  - Segunda revisión: (wvlan_cs.o)T

Marcas - ChipSets

Wavelan IEEE/Orinoco, PrismII and Symbol cards

- Fabricante: Lucent, Intersil y Symbol.
- El mismo controlador MAC (mismo driver)
- Driver: Está en el kernel

```
Hermes chipset 802.11b support (Orinoco/Prism2/Symbol)
```

- Tarjetas soportadas:
  - La mayoría de PCMCIA 802.11b (excepto Cisco/Aironet).
  - PCI: Apple Airport (no PCMCIA), WavelanIEEE/Orinoco, Cabletron/EnteraSys Roamabout, ELSA AirLancer, MELCO Buffalo, Avaya, IBM High Rate Wireless, Farralon Syyline, Samsung MagicLAN, Netgear MA401, LinkSys WPC-11, D-Link DWL-650, 3Com AirConnect, Intel PRO/Wireless y Symbol Spectrum24.

Marcas - ChipSets

Intersil PrismII (puro)

- Fabricante: Samsung and Compaq.
- Marcas: D-Link, LinkSys, NetGear, SMC, ZoomAir, Nokia y GemTek
- Driver:
  - `Intersil Prism GT/Duette/Indigo PCI/Cardbus`
  - `Prism 2.5 PCI 802.11b adaptor support`
  - http://www.linux-wlan.com/linux-wlan
- Puede Funcionar en modo “master” gracias al driver de Jouni Malinen : http://hostap.epitest.fi/

Drivers Win-Ndiswrapper

gULO Grupo de Usuarios de Linux de Ourense

Introducción

- Pues como su nombre indica es un sistema que nos va a permitir usar los drivers para Window$ de nuestra tarjeta wifi "envolviendolos" para que puedan funcionar en un kernel linux.

Configuración de Ndiswrapper

- Ndiswrapper está compuesto por un módulo del kernel (que usaremos como si fuese el módulo de la tarjeta) y unas utilidades.
- El módulo viene ya incluido en muchos kernels de las ultimas distribuciones:
  - apt-get install ndiswrapper-source (compilarlo como módulo en debian)
- Sino estamos en debian, nos bajamos los fuentes de sourceforge y las descomprimimos y hacemos un make install como root.
- NOTA: Se necesitan las fuentes del kernel.

Wi Fi™

Drivers Win-Ndiswrapper

GULO Grupo de Usuarios de Linux de Ourense

Configuración de Ndiswrapper (Drivers XP/W2000 de la tarjeta)

- Según la documentación de ndiswrapper hay que usar los drivers de XP. Estos drivers suelen constar de un archivo con extensión .inf y otro con extensión .sys

Instalando los drivers

- En el directorio donde se encuentren los archivos con los drivers de XP y hacemos como root:

```
ndiswrapper -i driver.inf
```

- La -i de es install. Lo que hará ndiswrapper es copiar el archivo .sys y crear una configuración para el. Se encuentra en `/etc/ndiswrapper`.
- Ahora se puede empezar a probar. Si se ejecuta `ndiswrapper -l`, esto lista los drivers que hay instalados con ndiswrapper y si su hardware está presente o no.
- Se procede a insertar la tarjeta (PCMCIA o PCI).
  - Ejecutar `ndiswrapper -l` para comprobar que la reconoce bien.
  - Seguidamente se carga el módulo ndiswrapper propiamente dicho (modprobe ndiswrapper).
  - Mirando los logs del sistema se observa como ndiswrapper reconoce la tarjeta.

Drivers Win-Ndiswrapper

Configuración de Ndiswrapper (Drivers XP/W2000 de la tarjeta)

```
# cat /var/log/messages |grep ndiswrapper
localhost kernel: ndiswrapper version 0.10 loaded (preempt=yes,smp=no)
localhost kernel: ndiswrapper: using irq 11
localhost kernel: wlan0: ndiswrapper ethernet device 00:50:C2:10:93:0D using
     driver conrt.sys
localhost kernel: ndiswrapper device wlan0 supports WPA with AES/CCMP and TKIP
     ciphers
localhost kernel: ndiswrapper: driver conrt.sys (Conceptronic,23/04/2005,
     2.02.02.0000) added
```

- Por último ejecutar `ndiswrapper -m` para crear el alias wlan0 ndiswrapper en `/etc/modprobe.d/ndiswrapper`.
- Esto hará que cada vez que se use la interfaz wlan0, se cargue el módulo ndiswrapper.
- La interfaz se puede levantar normalmente con `ifconfig wlan0 up`.

Configuración WiFi

- La configuración de las tarjetas se hace de forma similar a las ethernet con el comando ifconfig pero esta vez ayudado con un nuevo comando, el iwconfig.
- **iwconfig** permite cambiar losparámetros específicos de las redes inalámbricas. Por ejemplo:
  - Identificador de red (**essid**)
  - Frecuencia o canal (**freq/channel**)
  - Modo (**mode**: *master*|*managed*|*ad-hoc*)
  - Velocidad (**rate**)
  - Clave de encriptación (**key/enc**)
  - Potencia de transmisión (**txpower**)
  - etc.
- En pocas palabras, con **iwconfig** configuramos los parámetros especiales de wireless y con el **ifconfig** configuramos los parámetros normales de la red IP

Configuración WiFi

Encriptación

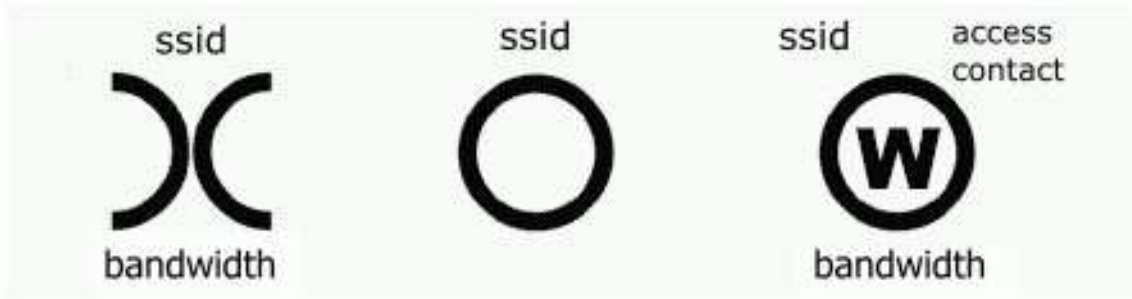
- Si especificamos una clave (key) en el iwconfig, las transmisiones están encriptadas con el protocolo WEP.
- En Linux has dos formas de especificarlas:
  - Con passphrase: `iwconfig interface key "s:mi_clave"`. La clave debe ser de 5 caracteres para encriptación de 64 bits (40 + 24 bits) y de 13 para 128 bits (en realidad de clave de 104 + 64 bits).
  - Con clave en hexadecimal: `iwconfig interface key "mi_clave_en_hexa"`. En este casose introduce la clave directamente con 5 o 13 caracteres especificados enhexadecimal.
- Para mayor seguridad se recomienda que los caracteres que forman la clave sean aleatorios.

Configuración WiFi

- La configuración de las tarjetas se hace de forma similar a las ethernet con el comando ifconfig pero esta vez ayudado con un nuevo comando, el iwconfig.
- **iwconfig** permite cambiar losparámetros específicos de las redes inalámbricas. Por ejemplo:
  - Identificador de red (**essid**)
  - Frecuencia o canal (**freq/channel**)
  - Modo (**mode**: *master*|*managed*|*ad-hoc*)
  - Velocidad (**rate**)
  - Clave de encriptación (**key/enc**)
  - Potencia de transmisión (**txpower**)
  - etc.
- En pocas palabras, con **iwconfig** configuramos los parámetros especiales de wireless y con el **ifconfig** configuramos los parámetros normales de la red IP

WarChalking

- Es un lenguaje de símbolos normalmente escritos con tiza en las paredes que informa a los posibles interesados de la existencia de una red inalámbrica en ese punto.
- Inspirado en el lenguaje de símbolos que utilizan los vagabundos, su sencillez ha sido uno de los factores que han hecho posible su proliferación por las grandes ciudades.
- Los símbolos más usados son:



Redes SoHo

GULO Grupo de Usuarios de Linux de Ourense

Introducción a las Redes SoHo

- Wi-Fi nos conecta a otros equipos y a Internet sin tener que utilizar cables ni conexiones fijas.
- Wi-Fi puede hacer todo esto, mejor que otras tecnologías usadas para configurar redes SOHO (Small Office- Home Office).

- Ninguna otra tecnología utilizada para configurar una red SOHO nos brinda la conveniencia y movilidad que nos ofrece Wi-Fi, ya que cualquier otro método utilizado implica la utilización de cable de algún tipo.

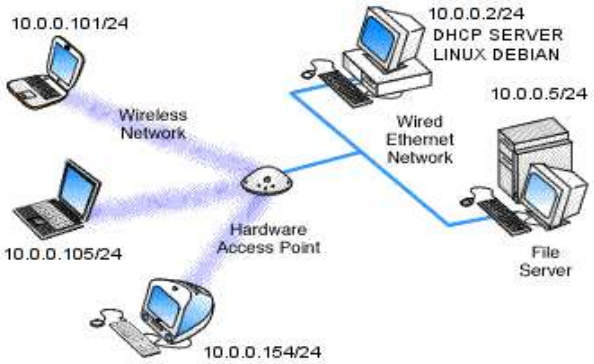
- Ninguna de las tecnologías de cable, nos permiten tomar nuestro portatil, o PDA, y movernos libremente en nuestra casa u oficina, y empezar o continuar el trabajo en otra ubicación sin perder el contacto con la red.

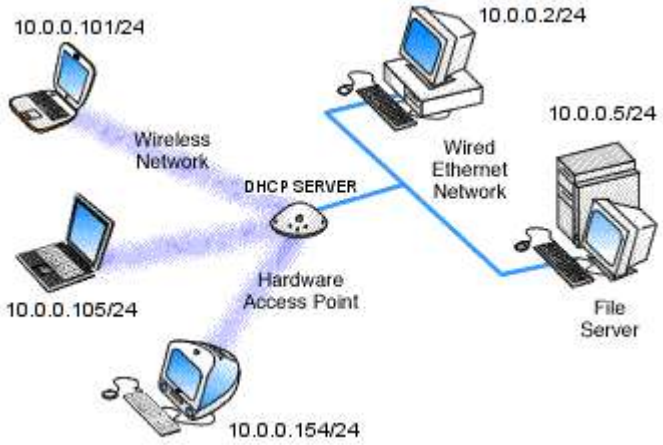
Wi Fi™

Redes SoHo

Convivencia redes Cableadas con redes WiFi

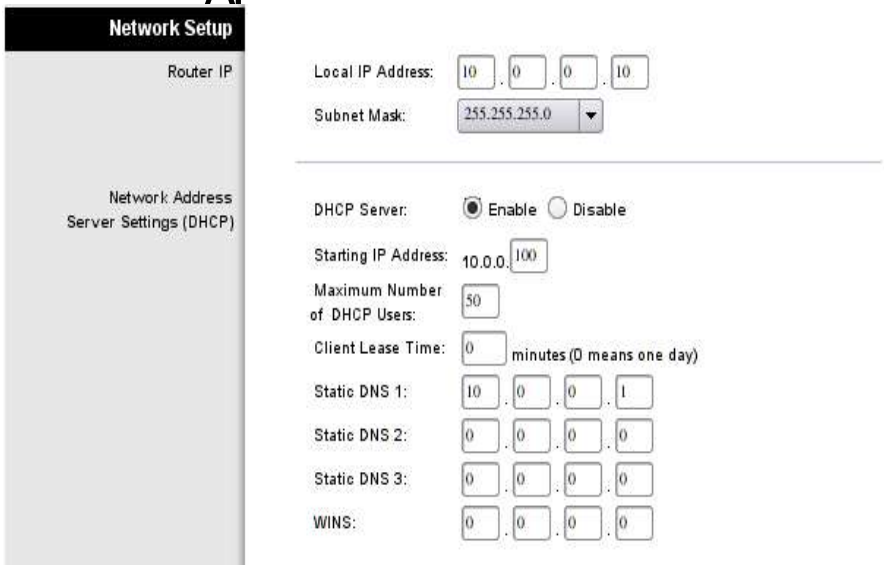
AP en modo Bridge





Asignación IPs???

- Manualmente en cada host
- DHCP:
  - Cualquier host de la red.
  - AP

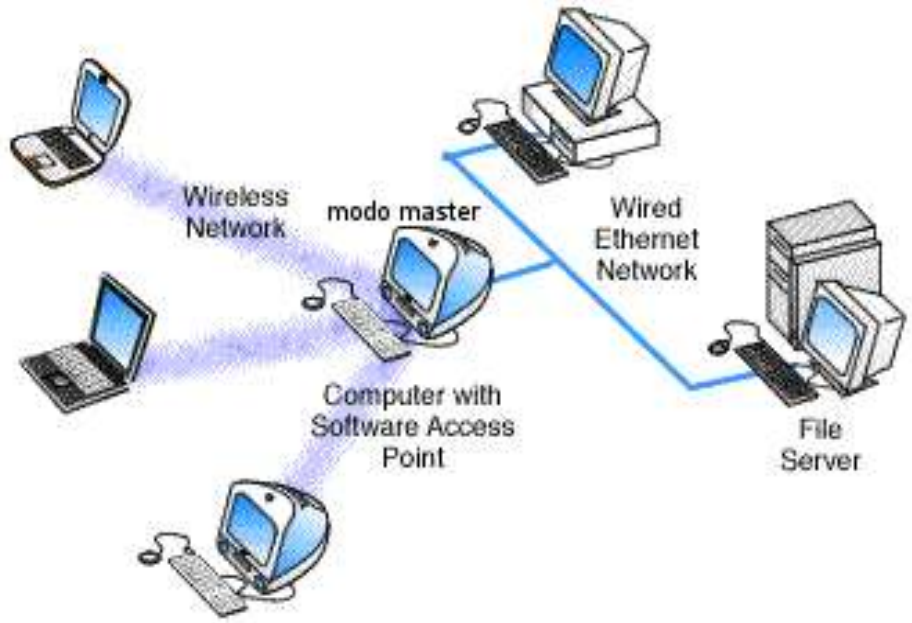


Redes SoHo

Convivencia redes Cableadas con redes WiFi

AP en modo Bridge por Software.

Configuración de la Ethernet WiFi en modo master



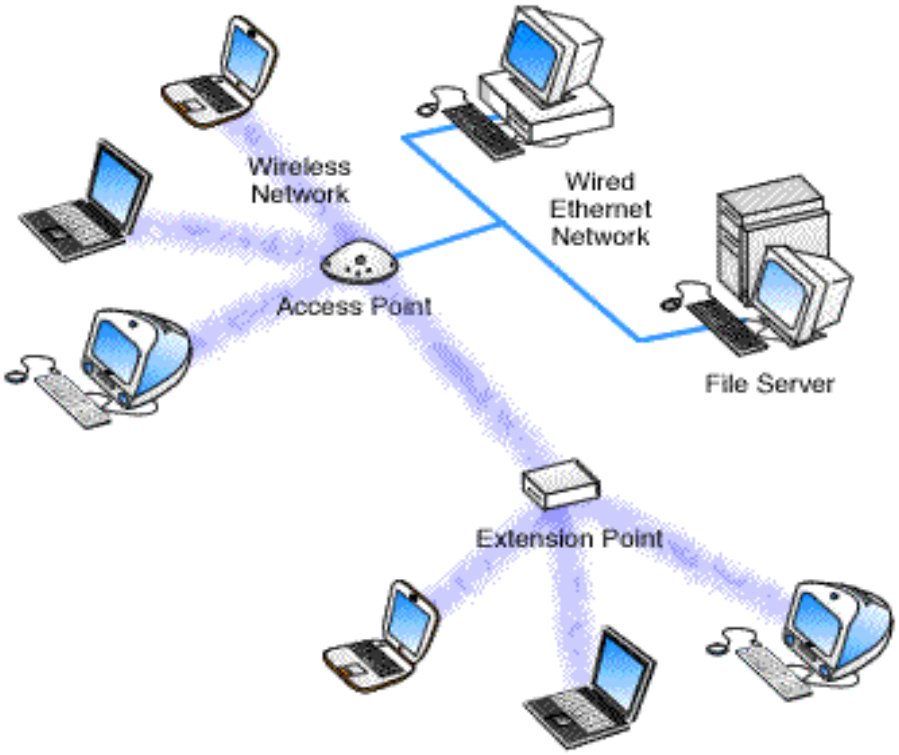
Ejemplo:

Ricardo Galli (Bulma)

Redes SoHo

Convivencia redes Cableadas con redes WiFi

Extendiendo un SSID. Inicio de Xwireless (comunidades wireless)



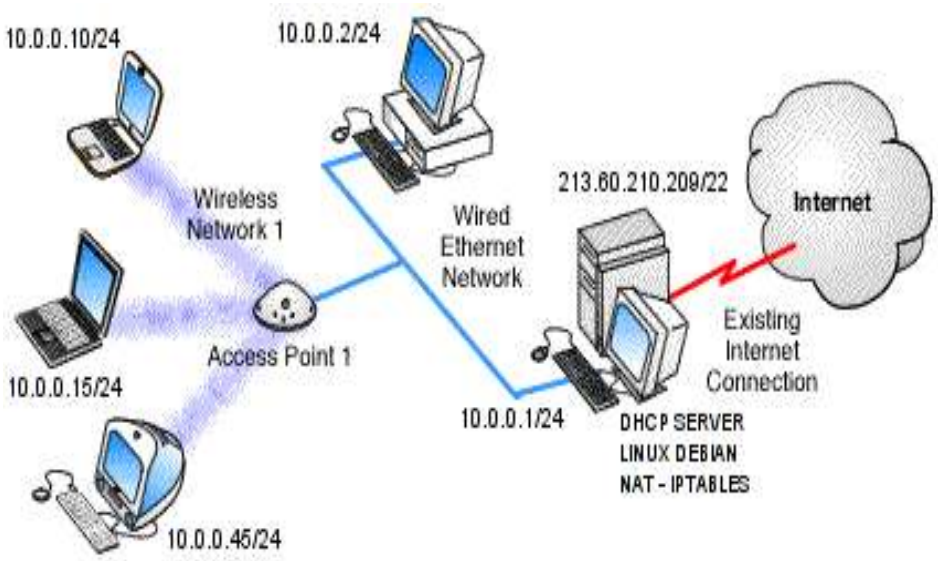
Modo de los AP???

- Para que exista conectividad, uno de ellos tiene que ser Cliente AP y el otro AP (modo master).
- Repeating mode

Redes SoHo

Convivencia redes Cableadas con redes WiFi

AP en modo Bridge con Pasarela definida (puerta de enlace)



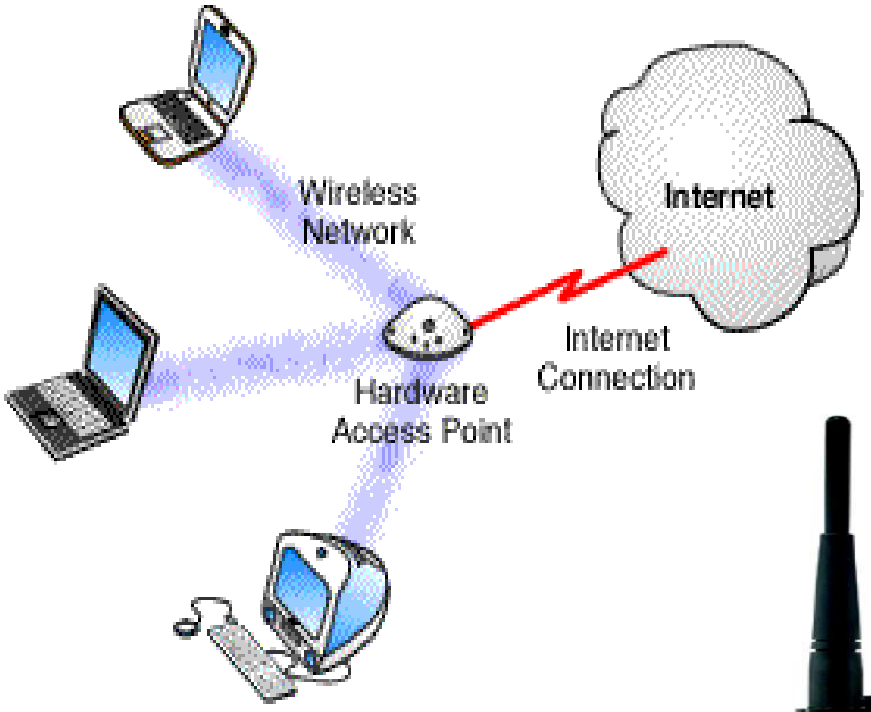
DHCP???

- address 10.0.0.10 – 50
- netmask: 255.255.255.0
- broadcast: 10.0.0.255
- network: 10.0.0.0
- gateway: 10.0.0.1
- DNS1: 193.147.87.2
- DNS2: 193.146.32.68
- DNS3: 10.0.0.1

Redes SoHo

Convivencia redes Cableadas con redes WiFi

Soluciones Comerciales de las Telycos: Ya.com, Telefónica, ...



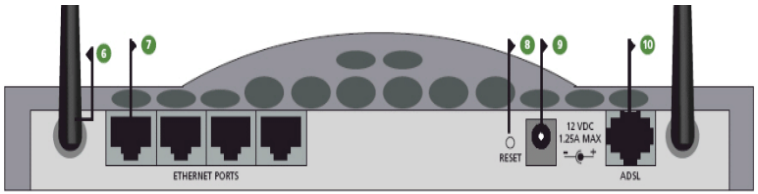
Características del AP

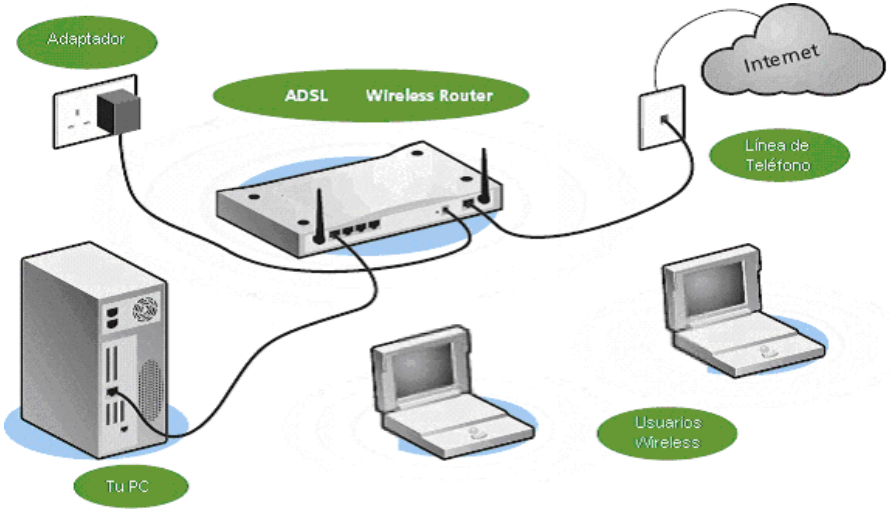
- Sin clave WEP
- Sin autenticación MAC
- Con servidor DHCP activado

Redes SoHo

Convivencia redes Cableadas con redes WiFi

Soluciones Comerciales de las Telycos: Ya.com, Telefónica, ...





Service Area Name/SSID es SMC o 3Com dependiendo del router 3Com SMC

Canal 11

Cifrado WEP deshabilitado