



asociación navarra  
**ingenieros de telecomunicación**  
anit - navarra

---

## :: CONCEPTOS BÁSICOS DE WIFI Y WIMAX ::

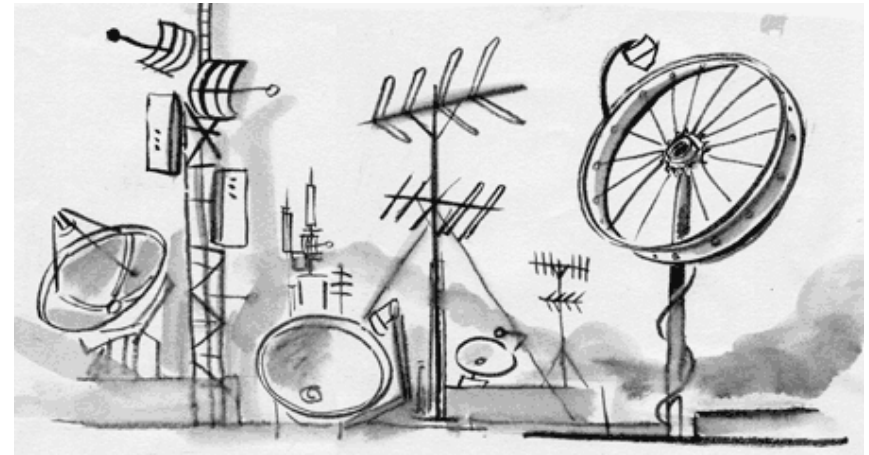
---

• <b>Fecha:</b>	5 de Octubre
• <b>Horario:</b>	19:30
• <b>Lugar:</b>	Centro de Encuentros Profesionales (Avda. Baja Navarra, 47)
• <b>Ponente:</b>	Eduardo Zariquiegui



# Objetivos de la presentación

- Comprender los fundamentos básicos de la tecnología wireless
- Conocer los parámetros fundamentales de configuración
- Hacernos una idea del nivel de seguridad alcanzable con las soluciones actuales
- Orientar hacia la mejor solución dependiendo del entorno en el que se está
- Introducir los fundamentos básicos de Wimax
- Ruegos y preguntas. Intercambio de experiencias.







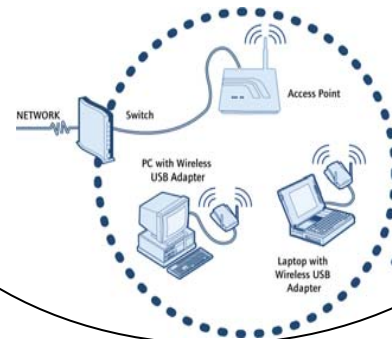
# Fundamentos Wireless. Concepto

LAN  
=  
Local Area Network

Wired LAN =  
LAN cableada (convencional)

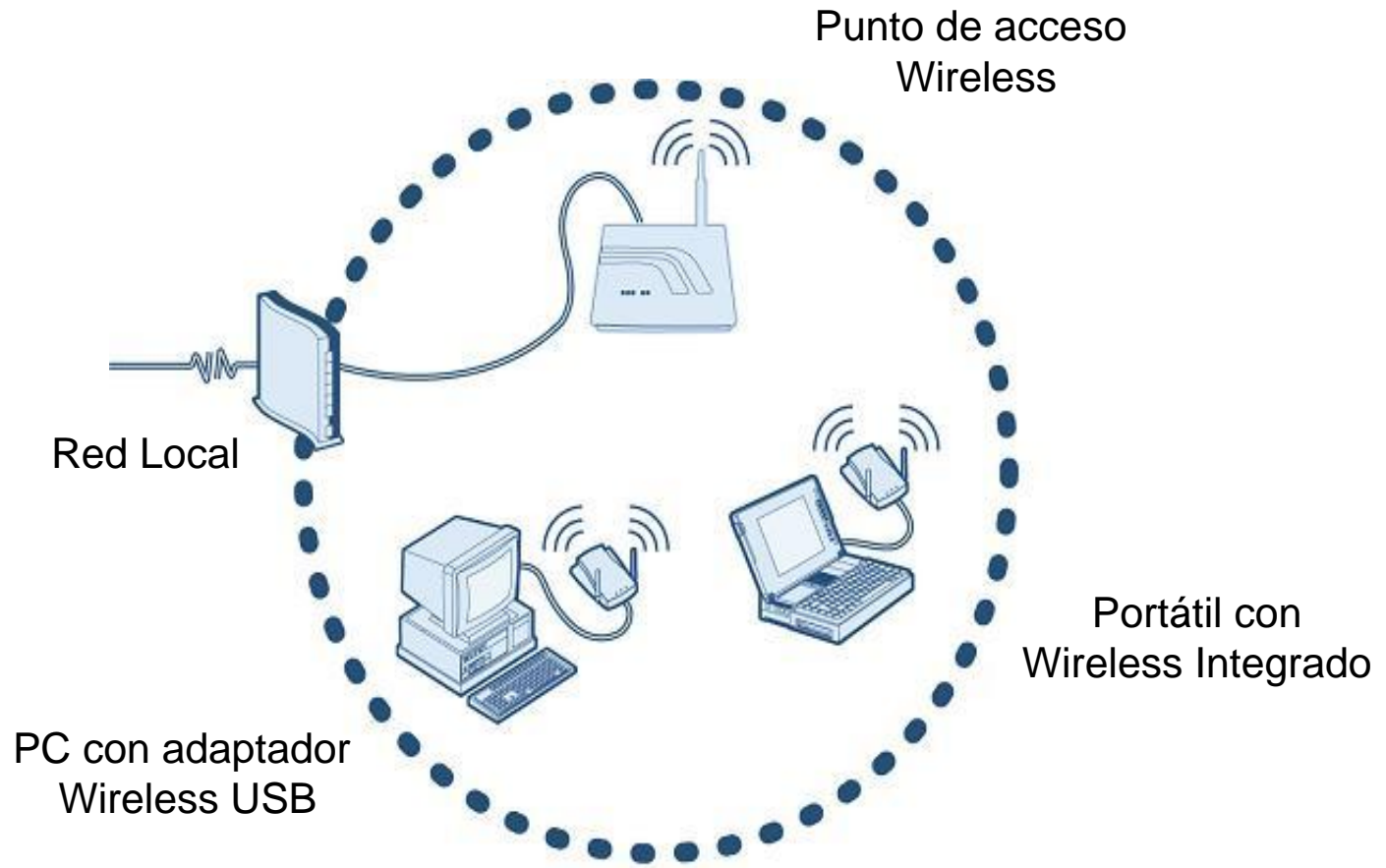


Wireless LAN =  
LAN inalámbrica



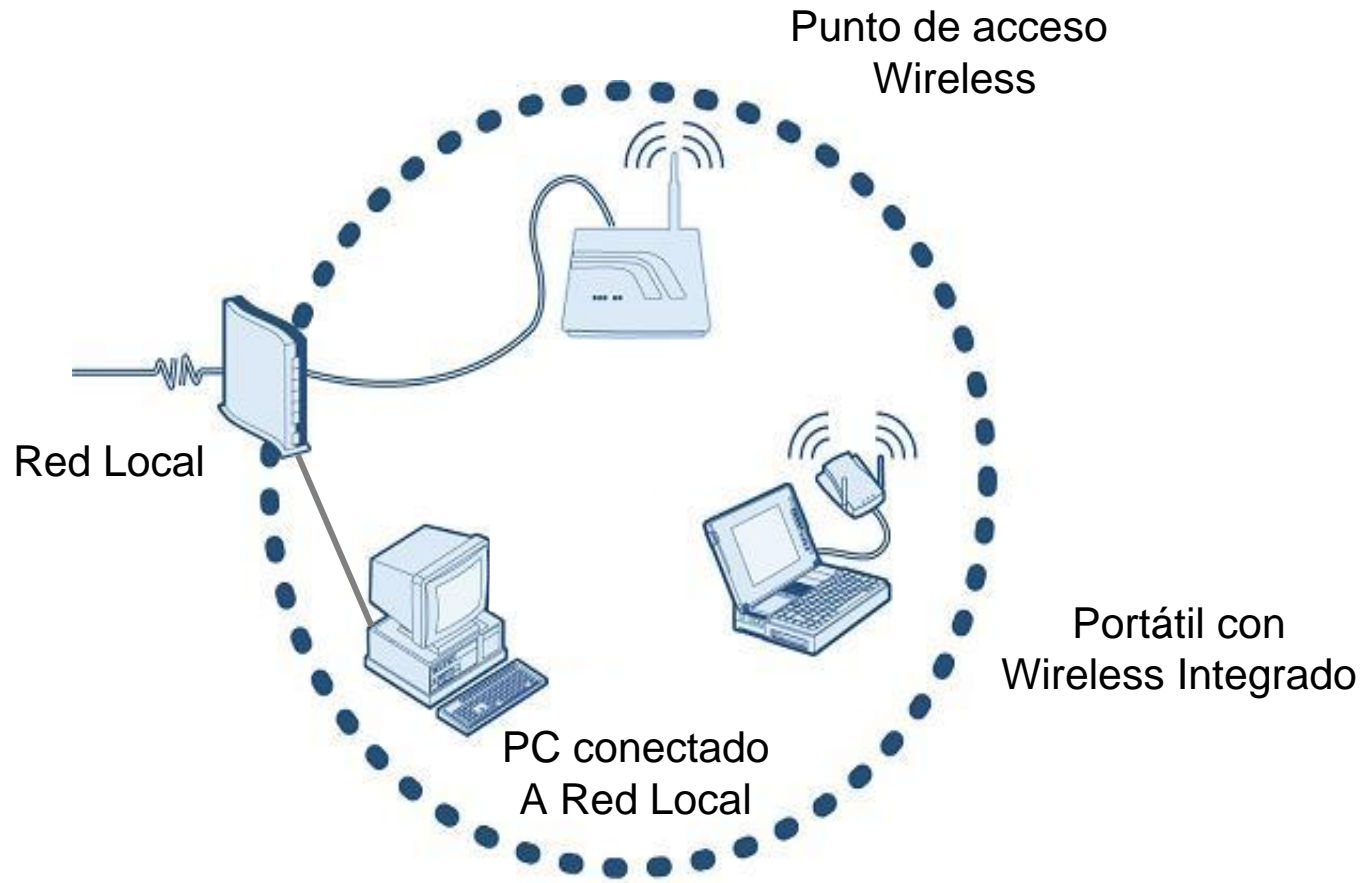


# Topología todo wireless





# Topología mixta





# Ejemplo de producto doméstico (I)



SMC2304WBR-AG EU

EZ-Stream™ Router de banda ancha Universal Wireless



# Ejemplo de producto doméstico (II)

## Features

- Universal Wireless Support: Compatible with 802.11a, 802.11b, and 802.11g.
- High-Speed Wireless Data rates up to 108Mbps – Supports both Turbo A and Super G modes
- Built-in Auto-Sensing 4-Port 10/100 Switch to support wired clients – No Need for Crossover Cables or Uplink Port
- Wireless Security features with 64-/128-bit WEP Encryption, Disable SSID Broadcast, and WPA support.
- Advanced Feature set including, Access Rules, Client Application Filtering, MAC Address Filtering, and support for 8 DMZ Hosts,
- Fully Configurable Stateful Packet Inspection (SPI) Firewall.
- Easily Connect to your Corporate Network using Virtual Private Networking (VPN) – Supports VPN Pass-Through
- Configurable your Barricade Router using a standard a Web Browser, both from your network and remotely over the Internet
- Built in DHCP Server to support up to 253 clients.
- Integrated DDNS feature for automatic updating of your WAN IP.
- Full Universal Plug and Play Support
- Get alerted when an attempt is made to access your network with the built-in email alert system.

## Benefits

- Up to 108Mbps of throughput, ideal for bandwidth intensive applications.
- Universal Wireless Connectivity with Dual-band, tri-standard Access Points that can communicate with 802.11a, 802.11g, and 802.11b wireless clients
- Future-proof your network for tomorrow's home entertainment wireless networking technologies.
- Advanced NAT feature securely shares your high-speed Internet connection and protect your personal network information.
- Quality of Service (QoS) support for Multimedia based applications and content
- Hacker Attack logging and email alerts keeps you aware of any attempts to access your network without your permission.

## Compatibility

- Platform independent - works with PC, Mac, and Linux.
- IEEE 802.3, 802.3u
- IEEE 802.11a, 802.11g, and 802.11b compliant



# Ejemplo de producto gama media (I)



## OVERVIEW

The EliteConnect™ Universal 2.4GHz/5GHz Wireless Access Point (SMC2555W-AG2) provides a secure and high-performance enterprise class wireless LAN supporting up to 64 users. The reliability, security, and manageability of the SMC2555W-AG2 make it an ideal solution for any organization looking to satisfy its workforce's mobile computing needs

New features included in the new SMC2555W-AG2 include Multiple SSID support, Wireless Distribution System (WDS), VLAN tagging, and Wireless Multimedia (WMM) support. Multiple SSID's allow you to create virtual access points with one physical unit. You can set different encryption schemes and VLAN ID's per SSID which allows for segmentation of user groups and policies. WDS support enables repeating functionality between other SMC enterprise access points or bridges. Wireless repeating is an alternative to extending your wireless coverage without the need to run Ethernet cables.

Wireless LAN security is a main concern in enterprise deployment. The EliteConnect™ Universal 2.4GHz/5GHz Wireless Access Point provides enterprise level advanced authentication and encryption security features. Security features include the new Wi-Fi Protected Access (WPA and WPA2), up to 152-bit WEP encryption, AES, 802.1x authentication access control with key rotation (MD5, EAP-TLS per user per session key, EAP-TTLS per user per session key, session key and broadcast key rotation, and PEAP), support for FUNK Odyssey and Microsoft RADIUS Server, up to 1024 MAC address authentication, disabled SSID broadcast, and up to 64 virtual LANs (VLANs) through 802.1x.

The new SMC2555W-AG2 also has flexible management features. Web-based network management tools make configuration and remote management of the network simple. IT professionals can also use Command Line Interface (CLI) to quickly and easily manage the device, along with telnet and SSH. In addition, SMC Networks EliteView Management Software and SNMP (v1, 2c, 3) support in SMC2555W-AG2 allows easy integration of your wireless LAN with your wired infrastructure. Other management features include Syslog and Event Logging.

If extended range is required, users can choose among the wide selection of SMC 2.4GHz/5GHz High Gain Antennas. SMC2555W-AG2 comes with detachable antennas with R-SMA connectors for optional 2.4GHz and 5GHz High Gain Antennas for extended range and coverage. The new enterprise level 802.11a/b/g Wireless Access Point supports Power over Ethernet that adheres to 802.3af standard. Power over Ethernet support reduces installation cost by using standard Category 5 cable to provide power to the Access Point. In addition, SMC2555W-AG2 provides an anti-theft mechanism by integrating a Kensington security slot on the device. All of the above make SMC2555W-AG2 a perfect solution with unparalleled flexibility and investment protection for your wireless LAN deployment.



# Ejemplo de producto gama media (II)

FEATURES	BENEFITS
IEEE802.11a, 802.11b, and 802.11g compliant	Simultaneous support of IEEE802.11a, 802.11b, and 802.11g wireless clients. IEEE802.11a/b/g compliance allows for seamless interoperation among multiple vendors
Flexible management features	Flexible network management through CLI, Web, Telnet, SSH, TFTP, SNMP make it simple and easy to monitor, troubleshoot, and view event logging
Detachable antennas	Optional use of SMC's 2.4GHz/5GHz High Gain Antenna for extended range and coverage
Enterprise level of authentication and encryption security	Enterprise class security features including the new WPA2, up to 152-bit WEP encryption, AES, 802.1x authentication and dynamic key management, ACLs, up to 1024 MAC address authentication, and disabled SSID broadcast
Quality of Service Support	The access point implements QoS using the Wi-Fi Multimedia (WMM) standard. WMM employs techniques that are a subset of the developing IEEE 802.11e QoS standard.
Power over Ethernet support	PoE Reduces installation cost by using standard Cat. 5 cable to provide power and data to the Access Point



# Ejemplo de otros usos

**El teléfono Wi-Fi para Skype** de SMC Networks - WSKP100 es un teléfono inalámbrico que te permite hacer llamadas **Skype** sin usar el ordenador.



El teléfono le permite usar su cuenta de **Skype** con la movilidad completa: a diferencia de otros dispositivos que deben conectarse con un ordenador, el WSKP100 trabajará en todas partes donde usted puede encontrar conexiones a Internet inalámbricas, como: en casa, trabajo o el campus, sin la molestia de conectar el ordenador.





# Fundamentos Wireless. Estándares



LAN (802.x) ∈ Estándar IEEE para Redes Locales



WLAN (802.11x) ∈ Estándar IEEE para LANs inalámbricas



Otros estándares (no IEEE):

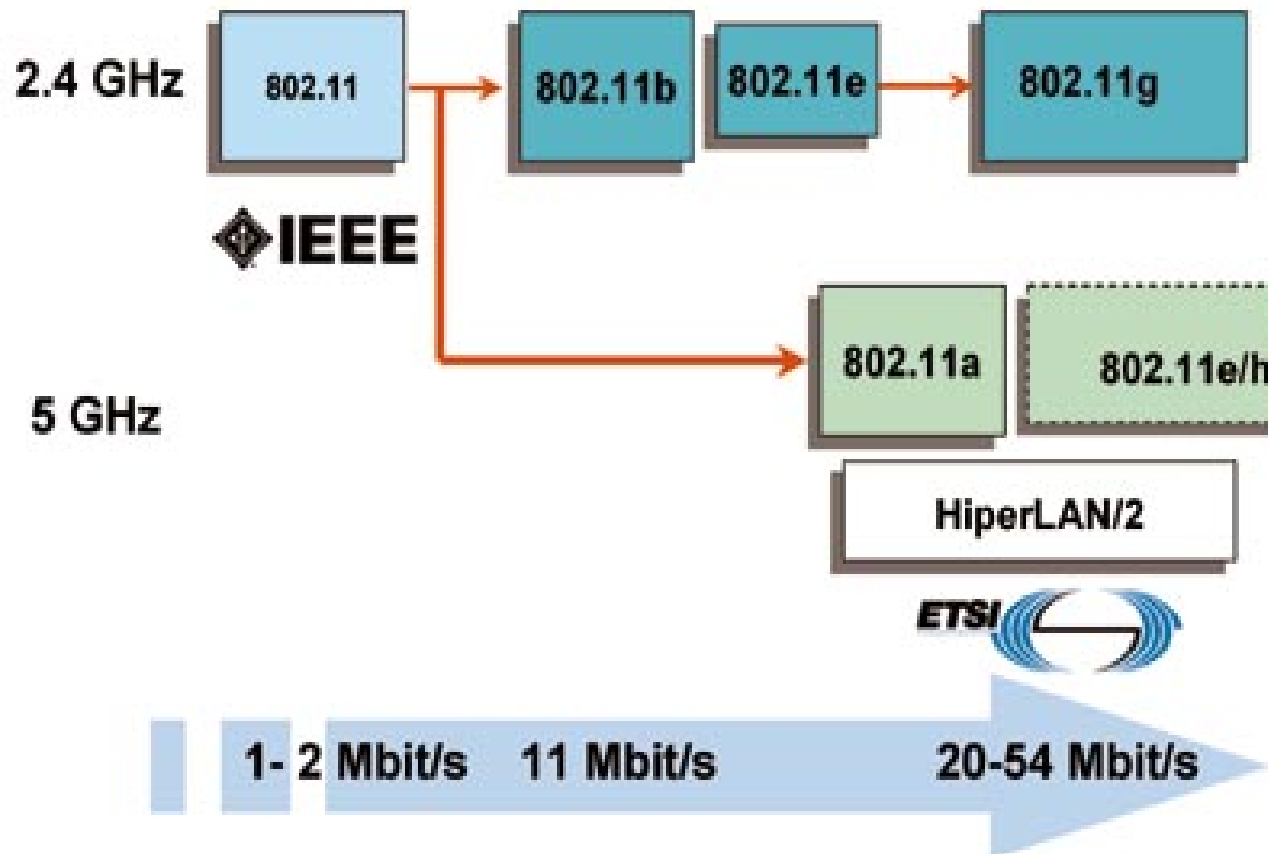
- Bluetooth
- HyperLAN ∈ ETSI
- HomeRF





# Fundamentos Wireless. Estándares

## ESTÁNDARES PARA WLAN

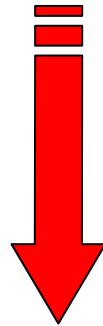




# Fundamentos Wireless. Estándares (II)

---

Estándar presente/pasado: 802.11 b .



Estándar presente/futuro: 802.11g. Compatible hacia atrás.



# Fundamentos Wireless. Estándares (III)

## Otros estándares

Norma	Ampliación
802.11d	Aspectos reglamentarios en países sin normativa vigente sobre 802.11
802.11e	Define niveles de Calidad de Servicio (QoS)
802.11f	IAPP (Inter Access Point Protocol)
802.11 h	Mejora de 11a en potencia y selección de canal de radio
802.11i	Mecanismos de seguridad-AES (Advanced Encryption Standar)
802.11j	Resuelve la adición del canal 4.9GHz al de 5GHz para 11a en Japón



# Fundamentos Wireless. Estándares futuros

## 802.11 Super G. **Propietario**

Hoy en día el estándar 802.11 Super G, con una banda de 2.4 Ghz y 5 Ghz, alcanza una velocidad de transferencia de 108 Mbps

## 802.11n

En enero de 2004, la [IEEE](#) anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. la velocidad real de transmisión podría llegar a los **500 Mbps** (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el **alcance** de operación de las redes sea **mayor** con este nuevo estándar. Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar que debía ser completado hacia finales de 2006, **se implante hacia 2008**, puesto que no es hasta principios de 2007 que no se acabe el segundo boceto.



# Fundamentos Wireless. Resumen tecnología

- ▶ Wireless es una **tecnología madura**, normalizada por el IEEE que permite montar redes locales inalámbricas utilizando frecuencias “desnormalizadas” legalmente.
- ▶ Wireless emplea **tecnologías de modulación avanzadas** basadas en técnicas de espectro expandido (**CCK**, Complementary Code Keying, para 802.11b y **OFDM**, orthogonal frequency division multiplexing, para 802.11g) que son muy **robustas ante interferencias**
- ▶ **Rendimiento:**
  - ▶ Con el estandar **802.11**) pueden conseguirse unos **5 Mbps** reales (11 teóricos) por punto de acceso.
  - ▶ Con el estandar **802.11g** pueden conseguirse unos **25 Mbps** reales (54 teóricos) por punto de acceso.
  - ▶ Conforme aumenta el número de usuarios el rendimiento decae casi “exponencialmente”. El comportamiento de un punto de acceso Wireless se asemeja al de un Hub más que al de un Switch.



# Fundamentos Wireless. Resumen tecnología (II)

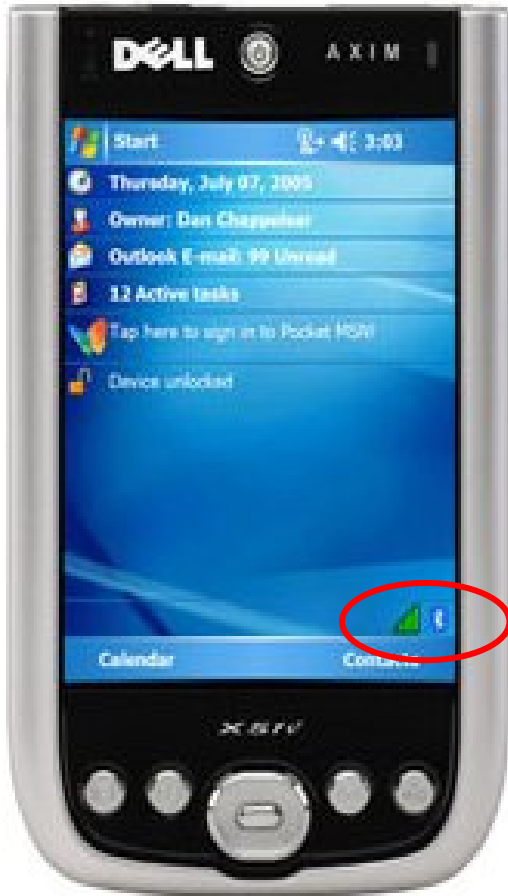
## ► **Alcance.** Resumen teórico de velocidades y alcances

Protocol	Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)
Legacy	1997	2.4 -2.5 GHz	1 Mbit/s	2 Mbit/s	?
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	25 Mbit/s	54 Mbit/s	~30 meters (~100 feet)
802.11b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s	~30 meters (~100 feet)
802.11g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s	~30 meters (~100 feet)
802.11n	2008 (projected)	2.4 GHz or 5 GHz bands	200 Mbit/s	540 Mbit/s	~50 meters (~160 ft)

► Actualmente wireless opera a 2,4 GHz por lo que a la hora de diseñar redes wireless conviene tener en cuenta todos los **principios aplicables al diseño de redes de microondas** (visión directa, calculo de balances de potencia, etc). El problema es cuando el diseño se hace **en interiores** ya que resulta imposible hacer un cálculo matemático y si queremos tener garantías de rendimiento hay que hacer un **estudio de campo** de cobertura.



# Fundamentos Wireless. Resumen tecnología (III)



<http://www.netstumbler.com/>



# Fundamentos Wireless. Resumen tecnología (IV)

Network Stumbler - [20061003224506]

File Edit View Device Window Help

Channels

- SSIDs
  - datil10
    - 0015F2EB33E7**
  - ICS-Wireless
  - oyenppna
  - SMC
  - UPN
  - WLAN\_00
    - 0060B3A56A3E
  - WLAN\_0F
    - 0060B3D2D63C
  - WLAN\_1C
  - WLAN\_74
  - WLAN\_C5
- Filters
  - Encryption Off
  - Encryption On
  - ESS (AP)
  - IBSS (Peer)
  - CF Pollable
  - Short Preamble
  - PBCC
  - Short Slot Time (11g)
  - Default SSID

MAC	SSID	Chan	Speed	Vendor	Type	Encryption	SNR	Signal+	Noise-	SNR+
0060B3D57BB1	WLAN_74	4	54 Mbps	Z-Com	AP	WEP		-87	-100	13
00120E2DEBA3	UPN	11	54 Mbps	(Fake)	AP	WEP		-82	-100	18
00805A31A889	ICS-Wireless	6	54 Mbps		AP	WEP		-84	-100	16
0060B3F24BDE	WLAN_C5	9	54 Mbps	Z-Com	AP	WEP	18	-74	-100	26
0060B3509EB8	WLAN_1C	4	54 Mbps	Z-Com	AP	WEP		-84	-100	16
00013850CC6A	oyenppna	1	54 Mbps		AP	WEP	17	-78	-100	22
0060B3D2D63C	WLAN_0F	9	54 Mbps	Z-Com	AP	WEP		-74	-100	26
0013F701EC01	SMC	6	54 Mbps	(Fake)	AP	WEP		-82	-100	18
000F66EDAA1A		11	54 Mbps	Linksys	AP	WEP		-70	-100	30
0060B3A56A3E	WLAN_00	11	54 Mbps	Z-Com	AP	WEP		-68	-100	32



# Fundamentos Wireless. Compatibilidad

Para indicar la compatibilidad entre

- Dispositivos inalámbricos
- Tarjetas de red
- Puntos de acceso

de **cualquier fabricante**, se les incorpora el logo Wi-Fi (estándar de fidelidad/compatibilidad inalámbrica desarrollado por la WECA)



<http://www.wi-fi.org/>



# Fundamentos Wireless. Configuración

---

- ▶ Parámetros fundamentales:
  - ▶ Modo de operación
  - ▶ Velocidad
  - ▶ SSID/ESSID
  - ▶ Canal (zona)
  - ▶ Opciones de seguridad
    - ▶ Filtrado MAC
    - ▶ Broadcast SSID
    - ▶ Login/Password del equipo
    - ▶ Encriptación
    - ▶ .....



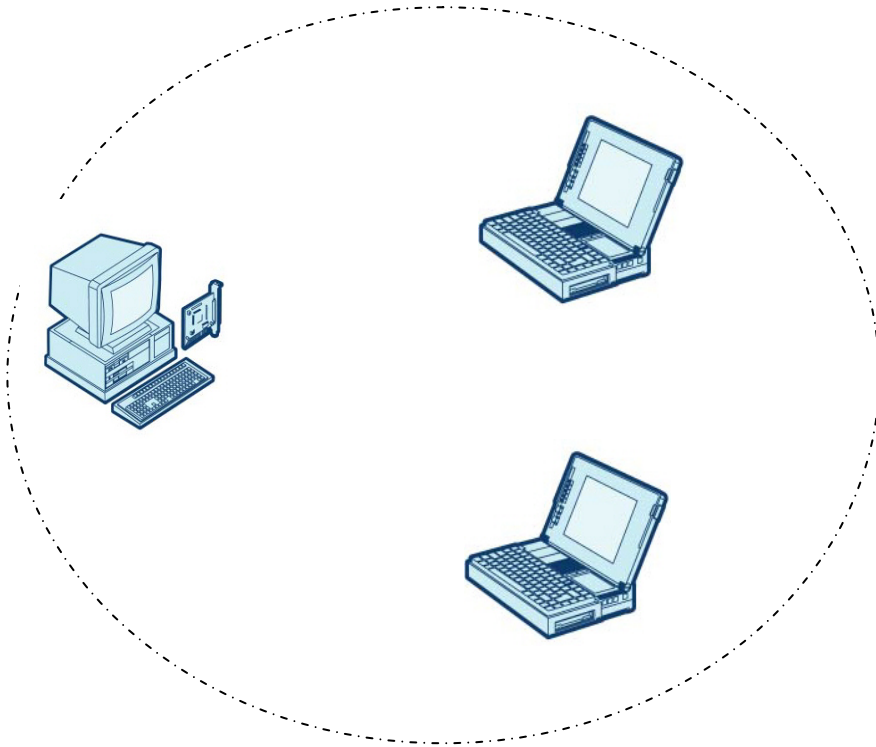
# Fundamentos Wireless. Modo de operación

---

- ▶ 2 modos:
  - ▶ punto a punto (o ad hoc)
  - ▶ con punto de acceso (infraestructura)



# Fundamentos Wireless. Modo punto a punto



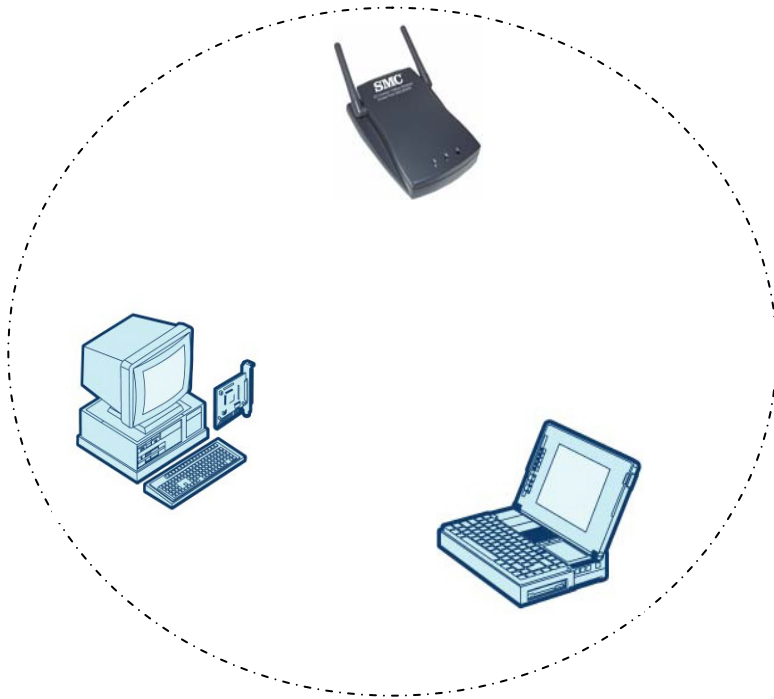
Consiste en un grupo de ordenadores cada uno equipado con una tarjeta LAN inalámbrica.

Equivale a un cable cruzado inalámbrico.

**Mal rendimiento.** No escala.



# Fundamentos Wireless. Modo infraestructura



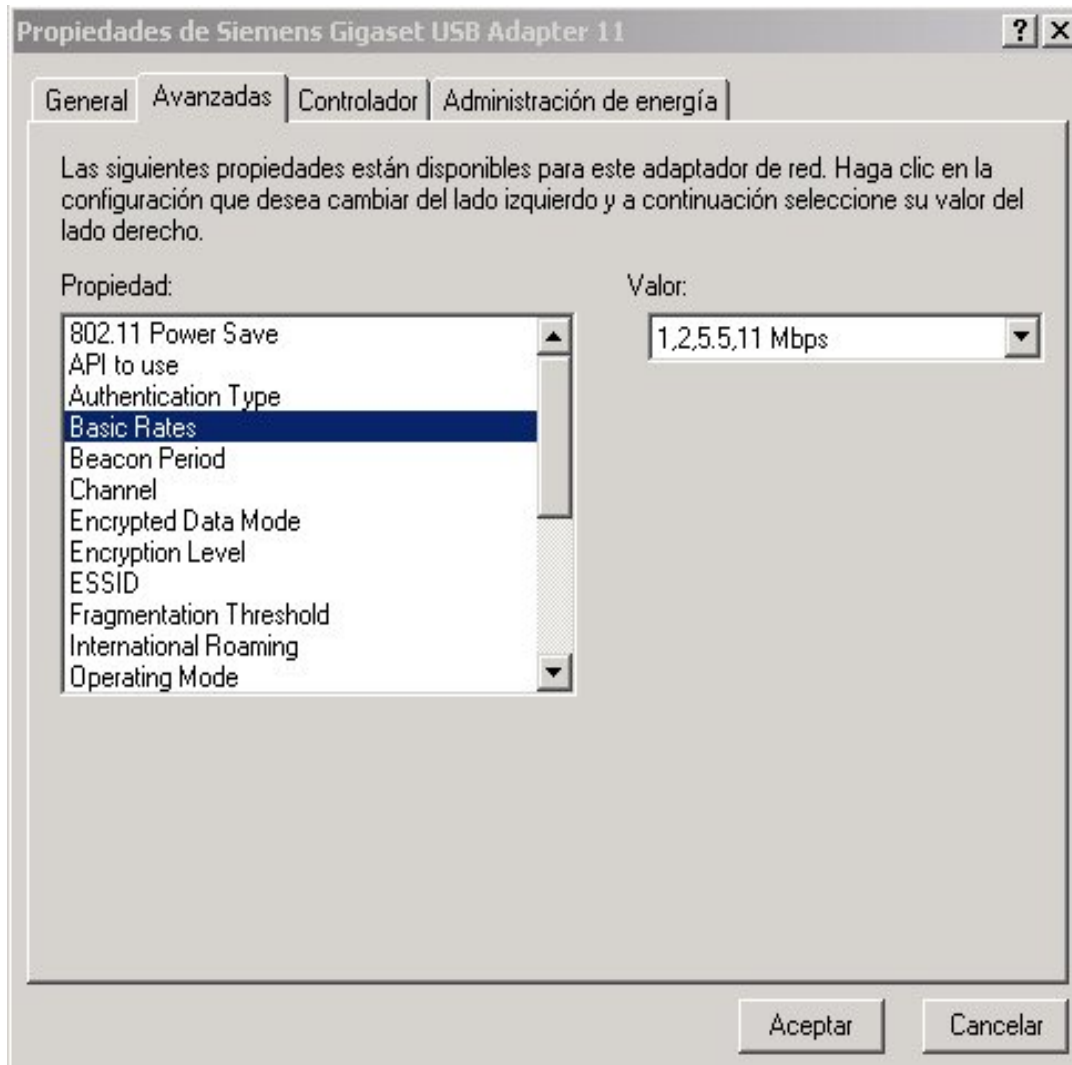
El punto de acceso equivale al conmutador LAN.

Cada PC necesita una tarjeta wireless (USB; PCI, PCMCIA, etc.)

**Configuración habitual**




# Fundamentos Wireless. Configuración velocidad



Regla base: a  
más velocidad  
menos  
distancia y  
viceversa



# Fundamentos Wireless. Configuración SSID/ESSID



**SIEMENS** Gigaset SE105 dsl/cable - Instalación avanzada

[Inicio](#) | [Estado](#) | [Instalación básica](#) | [Instalación avanzada](#) | [Cierre de sesión](#)

- ▶ Sistema
- ▶ WAN
- ▶ LAN
- ▶ Comunicación inalámbrica
  - ▶ Canal y SSID
  - ▶ Encriptación
- ▶ NAT
- ▶ Cortafuegos
- ▶ Herramientas

## Canal y SSID

Esta página permite definir la SSID, la velocidad de transmisión, la velocidad básica y la ID de canal para una conexión inalámbrica. En el entorno de comunicación inalámbrica, este router puede actuar como un punto de acceso inalámbrico. Estos parámetros se utilizan para que las estaciones móviles se conecten con este punto de acceso.


SSID :	<input type="text" value="ConnectionPoint"/>
Canal :	<input type="text" value="10"/>
SSID visible :	<input checked="" type="radio"/> Activar <input type="radio"/> Desactivar

[AYUDA](#) [APLICAR](#) [CANCELAR](#)

© Siemens AG 2002, 2003 [arriba](#) ↗



# Fundamentos Wireless. Configuración Canal



**SIEMENS** Gigaset SE105 dsl/cable - Instalación avanzada

[Inicio](#) | [Estado](#) | [Instalación básica](#) | [Instalación avanzada](#) | [Cierre de sesión](#) |

- ▶ Sistema
- ▶ WAN
- ▶ LAN
- ▶ Comunicación inalámbrica
  - ▶ Canal y SSID
  - ▶ Encriptación
- ▶ NAT
- ▶ Cortafuegos
- ▶ Herramientas

## Canal y SSID

Esta página permite definir la SSID, la velocidad de transmisión, la velocidad básica y la ID de canal para una conexión inalámbrica. En el entorno de comunicación inalámbrica, este router puede actuar como un punto de acceso inalámbrico. Estos parámetros se utilizan para que las estaciones móviles se conecten con este punto de acceso.


SSID :	<input type="text" value="ConnectionPoint"/>
Canal :	<input type="text" value="10"/>
SSID visible :	<input checked="" type="radio"/> Activar <input type="radio"/> Desactivar

[AYUDA](#) [APLICAR](#) [CANCELAR](#)

© Siemens AG 2002, 2003 [arriba](#) ↗



# Fundamentos Wireless. Configuración SSID



**SIEMENS** Gigaset SE105 dsl/cable - Instalación avanzada

[Inicio](#) | [Estado](#) | [Instalación básica](#) | [Instalación avanzada](#) | [Cierre de sesión](#)

- ▶ Sistema
- ▶ WAN
- ▶ LAN
- ▶ Comunicación inalámbrica
  - ▶ Canal y SSID
  - ▶ Encriptación
- ▶ NAT
- ▶ Cortafuegos
- ▶ Herramientas

## Canal y SSID

Esta página permite definir la SSID, la velocidad de transmisión, la velocidad básica y la ID de canal para una conexión inalámbrica. En el entorno de comunicación inalámbrica, este router puede actuar como un punto de acceso inalámbrico. Estos parámetros se utilizan para que las estaciones móviles se conecten con este punto de acceso.

SSID :	<input type="text" value="ConnectionPoint"/>
Canal :	<input type="text" value="10"/>
SSID visible :	<input checked="" type="radio"/> Activar <input type="radio"/> Desactivar

[AYUDA](#) [APLICAR](#) [CANCELAR](#)

© Siemens AG 2002, 2003 [arriba](#) ↗



# Fundamentos Wireless. Filtrado MAC

**MAC Address Filter** [X]

Set MAC addresses which are allowed to associate with AP. Other wireless stations will be rejected to link with the AP.

No.	MAC Address
-----	-------------

Filtering:

<< Add

Delete Save

Delete All Cancel

Add from File... Help

**MAC Address Filter** [X]

Set MAC addresses which are allowed to associate with AP. Other wireless stations will be rejected to link with the AP.

No.	MAC Address
1	00-04-E2-36-72-12
2	00-78-D4-F5-B2-11
3	AA-00-77-BB-44-CC
4	B2-67-D2-D4-D1-D1

Filtering:

<< Add

Delete Save

Delete All Cancel

Add from File... Help



# Fundamentos Wireless. Login/Password

**CONTRASEÑA DE USUARIO PARA EL REGISTRO**

**Pantalla de registro**

**Contraseña:**

Por favor, introduzca la contraseña. Gracias.



# Fundamentos Wireless. Configuración WEP

WIRELESS CONFIGURATION

DEVICE INFORMATION | DEVICE STATUS | SETUP WIZARD | ADVANCED SETTINGS | SYSTEM TOOLS | HELP

Main menu

DHCP SERVER SETTING

CABLE/xDSL ISP SETTINGS

ISP ADDITIONAL SETTINGS

**WIRELESS SETTINGS**


SAVE & RESTART

## WIRELESS SETTINGS

ESSID:

Domain:

Channel:

 Selecting your location incorrectly may invalidate the product certification and result in illegal operation.

Key Format:

No Encryption

40(64) Bit

Default Key:

Key 1:	<input type="text" value="11"/>	<input type="text" value="00"/>	<input type="text" value="11"/>	<input type="text" value="00"/>	<input type="text" value="11"/>
Key 2:	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>
Key 3:	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>
Key 4:	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>

128 Bit

<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>
<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>
<input type="text" value="00"/>	<input type="text" value="00"/>	<input type="text" value="00"/>		



# Fundamentos Wireless. WEP (I)

---

El protocolo WEP es un sistema de encriptación estándar propuesto por el comité 802.11 implementado en la capa MAC y soportado por la mayoría de productos para soluciones inalámbricas. Se diseña con el objetivo de proteger los datos transmitidos.



# Fundamentos Wireless. WEP (II)

## **Problema**

A pesar de que la clave compartida puede ser de hasta 128 bits, lo que debería ser suficiente, **WEP** tiene importantes **debilidades**:

- Insuficiencia de tamaño en el vector de inicialización.
  - En pocas horas se repite dicho vector
- Claves compartidas estáticas.
  - Susceptibles de ser atacadas sin límite de tiempo
- WEP no ofrece servicio de autenticación.
  - Una vez conseguida la clave el acceso a la red es inmediato



# Fundamentos Wireless. WEP (III)

Herramientas WEP:

- ▶ WepCrack
- ▶ AirSnort
- ▶ AirCrack





# Fundamentos Wireless. WEP (IV)

---

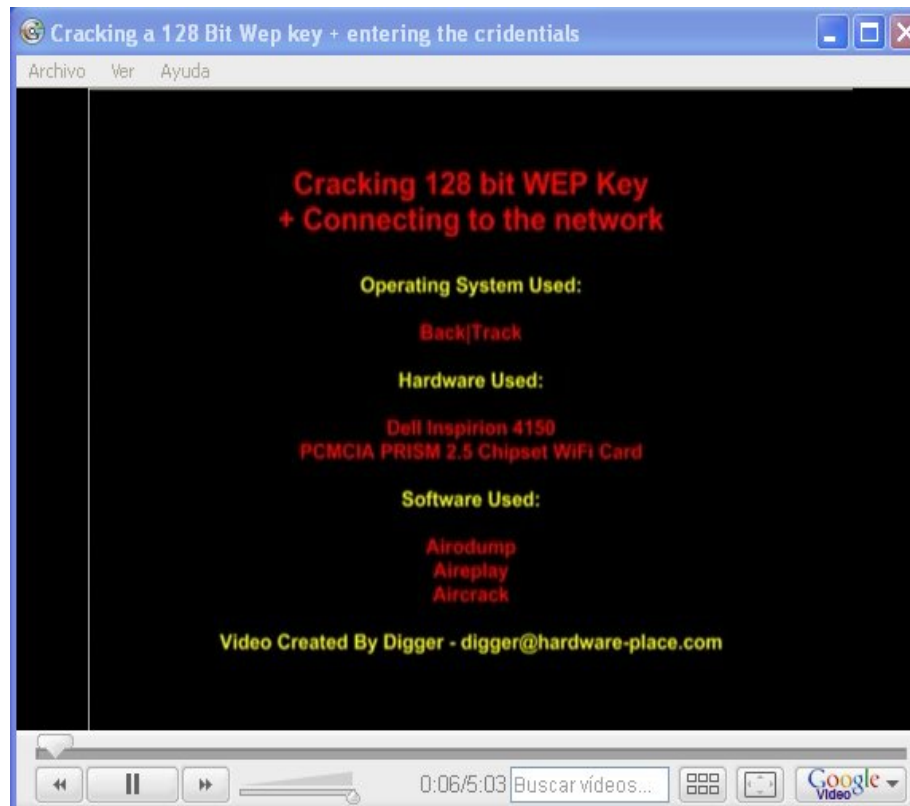
Conclusiones:

- **WEP no es seguro.**
- El principio de proporcionalidad podría hacernos pensar que para ciertas situaciones (redes domésticas) WEP es válido.
- La mejora funcional de los dispositivos Wireless de gama baja hace que hoy en día no se justifique su uso.



# Fundamentos Wireless. WEP (V)

Ejemplo de ataque a una red protegida con WEP



<http://video.google.com/videoplay?docid=-5967855731391344698>



# Fundamentos Wireless. WPA

WPA es el estándar de transición hacia 802.11i y reemplaza WEP por un algoritmo más robusto. Sin embargo tiene un sistema de intercambio de creación de claves muy fácil de romper por lo que en modalidad PSK mal configurada puede ser incluso más fácil de romper que WEP.

**According to the Wi-Fi Alliance, an industry body, WPA has never been broken. However, some security pros say it can be broken. They say the trick is a password of less than 21 characters. So, if you have WPA, err on the side of caution and use a really long password.**



# Fundamentos Wireless. WPA2

---

WPA2 es una certificación de producto que otorga Wi-Fi Alliance y certifica que los equipos inalámbricos son compatibles con el estándar 802.11i.

Con WPA2, el cifrado se realiza mediante AES (estándar de cifrado avanzado).

**WPA2 es el protocolo wifi más robusto.**

El problema es que no todos los equipos soportan WPA 2 por lo que dependiendo de la antigüedad de nuestras infraestructuras muchas veces nos veremos obligados o bien a cambiar de HW y/o Sw o bien emplear protocolos wireless menos seguros



# Fundamentos Wireless. WPA y WPA2

---

## Conclusiones:

- tanto WPA como WPA2 se consideran suficientemente seguros si bien con WPA existe el riesgo de hacer una mala configuración y dejar la red expuesta.
- si nuestra infraestructura lo soporta emplearemos WPA2. Si empleamos WPA debemos de ser especialmente cuidadosos con la configuración.
- en ambos casos el punto débil de la solución no está en la robustez de la criptografía sino es posibles ataque de DoS, Rogue AP, etc.

Más información sobre WPA y WPA2:

<http://blogs.zdnet.com/Ou/?p=67>



# Fundamentos Wireless. 802.11 i (I)

- **WPA2.** para confidencialidad e integridad
- **802.11 x** para autenticación basada en arquitectura cliente-servidor sobre protocolo Radius.





# Fundamentos Wireless. 802.11 i (II)

---

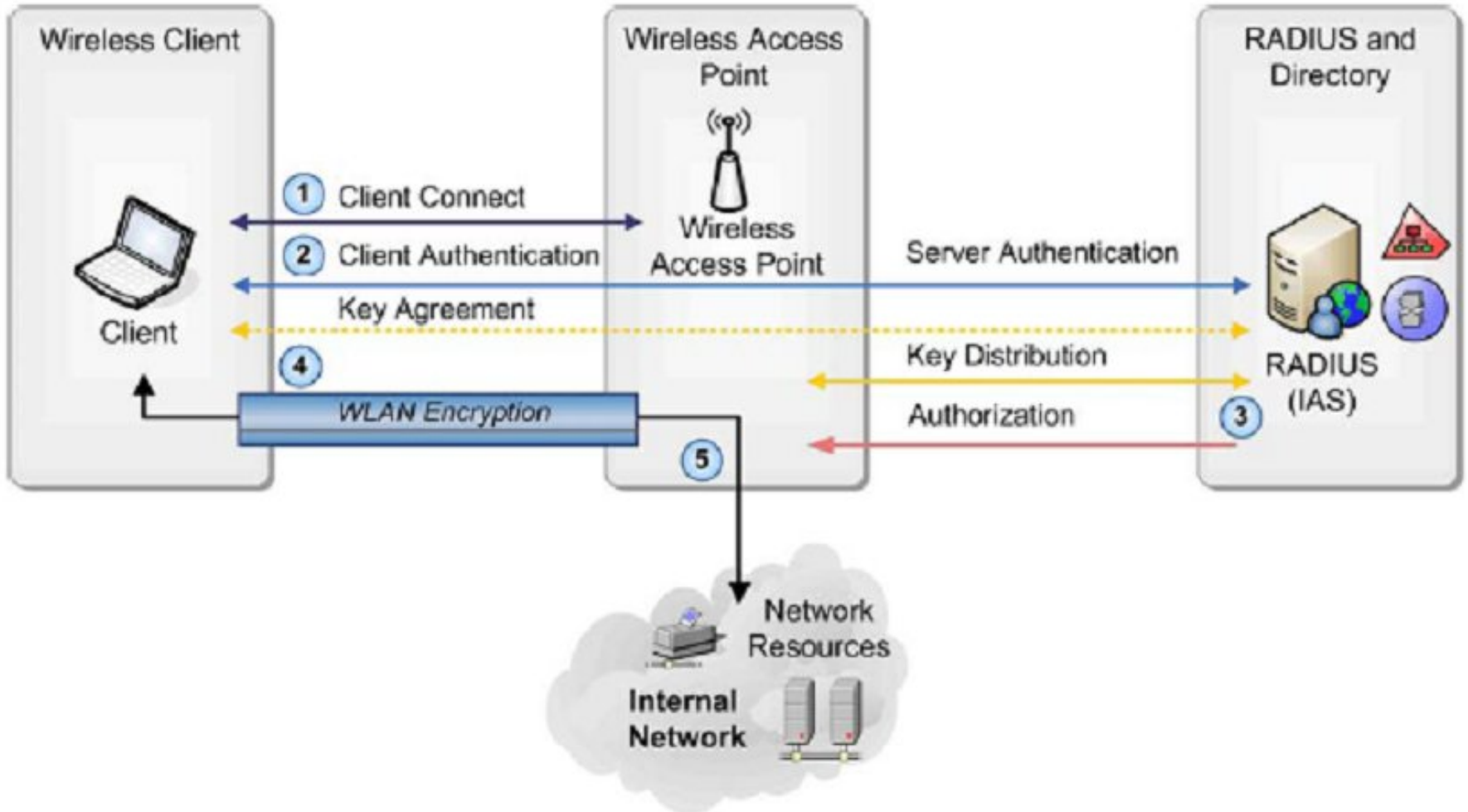
La comunicación entre el servidor Radius y el punto de acceso puede realizarse de diferentes maneras:

- EAP MD5.
- EAP-Tunneled TLS (EAP-TTLS)
- Lightweight EAP (LEAP)
- Protected EAP (PEAP).

La RFC 2284 deja abierto el mecanismo de autenticación de EAP y habrá que elegirlo en función de las posibilidades que nos ofrezcan los dispositivos HW y SW que empleemos.



# Fundamentos Wireless. 802.11 i (III)





# Fundamentos Wireless. VPN Inalámbrica (I)

---

▶ Si todavía necesitamos un nivel de seguridad mayor la opción que nos queda es la de **integrar nuestra red Wireless en una arquitectura VPN**. Las opciones son muy variadas:

- Puntos de acceso con IPSEC Integrado.
- Dejar el nivel de transporte sin protección y utilizar VPN cliente-servidor integrada en el sistema operativo de los Hosts.
- Etc.



# Fundamentos Wireless. VPN Inalámbrica (II)

## OUR SOLUTION

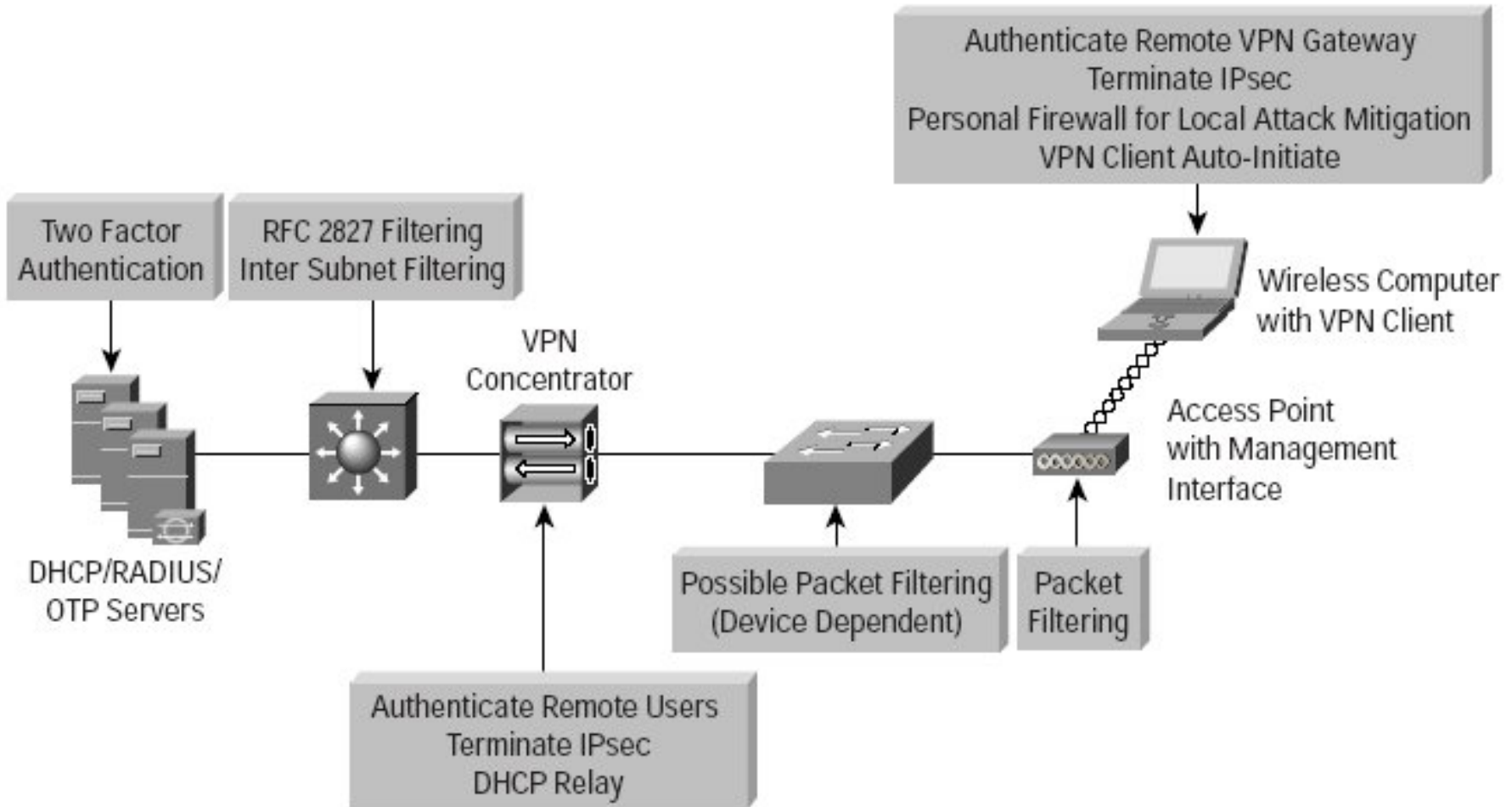
VPN-1® UTM™ Edge™ Wireless (W) security appliances deliver the same security found in VPN-1 UTM Edge appliances and add the highest levels of security for wireless networks. VPN-1 UTM Edge W appliances support multiple security protocols, including 802.1x, IPsec over WLAN, RADIUS, WPA2, and WEP authentication. They also have dedicated WLAN interfaces from which administrators can set specific security rules for WLAN segments. This protects wireless interfaces by granting access only to authorized users, preventing hackers from attacking corporate resources and applications.



[http://www.checkpoint.com/products/vpn-1\\_edge/index\\_wireless.html](http://www.checkpoint.com/products/vpn-1_edge/index_wireless.html)



# Fundamentos Wireless. VPN Inalámbrica (III)





# Fundamentos Wireless. Seguridad

---

## **CONCLUSIÓN:**

Las inseguridad de las redes inalámbricas, en la práctica, se debe a que no se utilizan correctamente los medios que están a nuestro alcance.





# Introducción (I)

**WiMAX** (del inglés *Worldwide Interoperability for Microwave Access*) es un estándar de transmisión inalámbrica de datos (**802.16x**).

- Diseñado para ser utilizado en el área metropolitana (MAN).
- En condiciones óptimas presenta un **gran alcance**: hasta 50-60 kilómetros de radio.
- **Gran ancho de banda**: velocidades de hasta 70 Mbps.





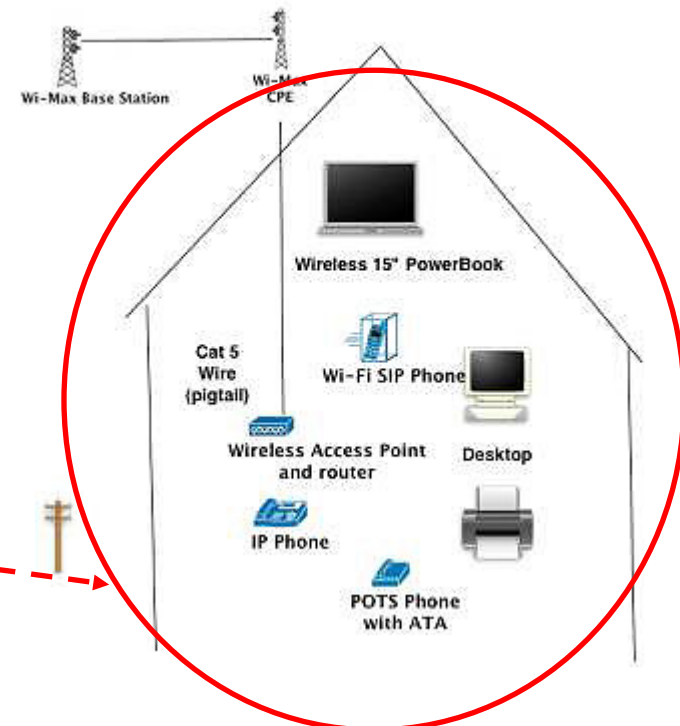
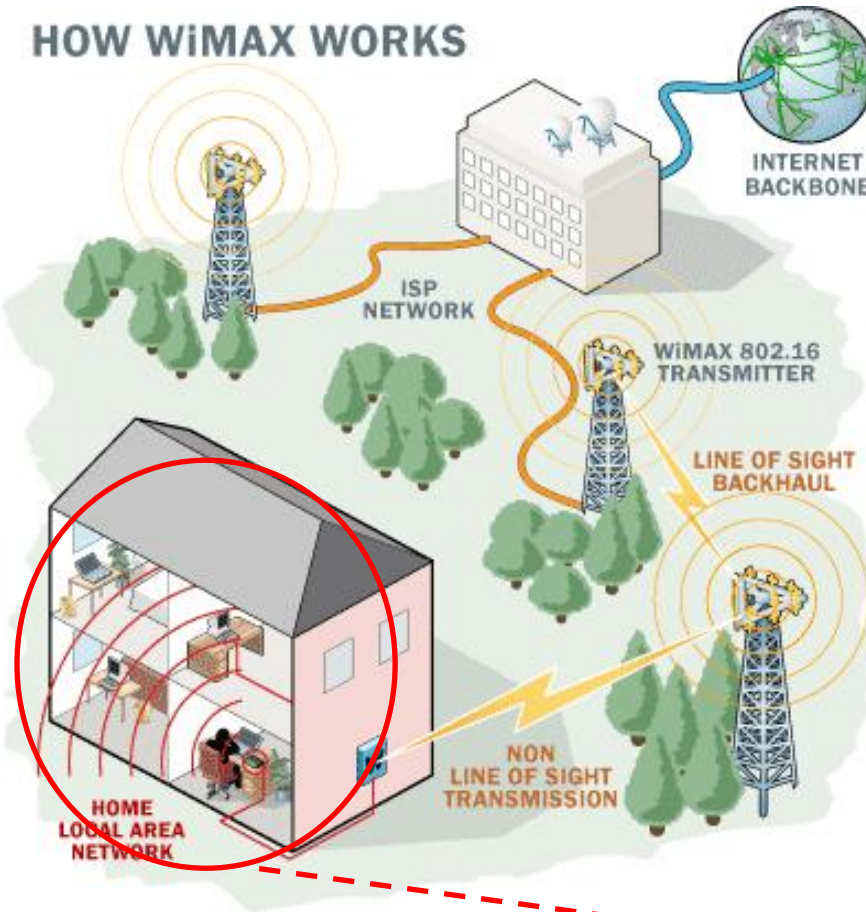
# Introducción (II)

- WiMAX está basado en la norma 802.16. Esta norma fue diseñada específicamente como una **solución de Última Milla**, y enfocada en los requerimientos para prestar servicio a nivel comercial.
  - Es **independiente del protocolo** IP, Ethernet, ATM...).
  - **Soporta servicios paquetizados** como IP y voz sobre IP (VoIP), como también **servicios conmutados** (TDM), E1/T1 y voz tradicional; también soporta interconexiones de ATM y Frame Relay.
  - Facilita varios **niveles de servicio** para poder dar diferentes velocidades de datos dependiendo del contrato con el suscriptor.
  - **Opera** en condiciones **donde no hay línea de visión** (N-LOS) a distancias de varios kilómetros.
  - Es **seguro** ya que el estándar se ha definido con cuestiones de seguridad “en mente”.



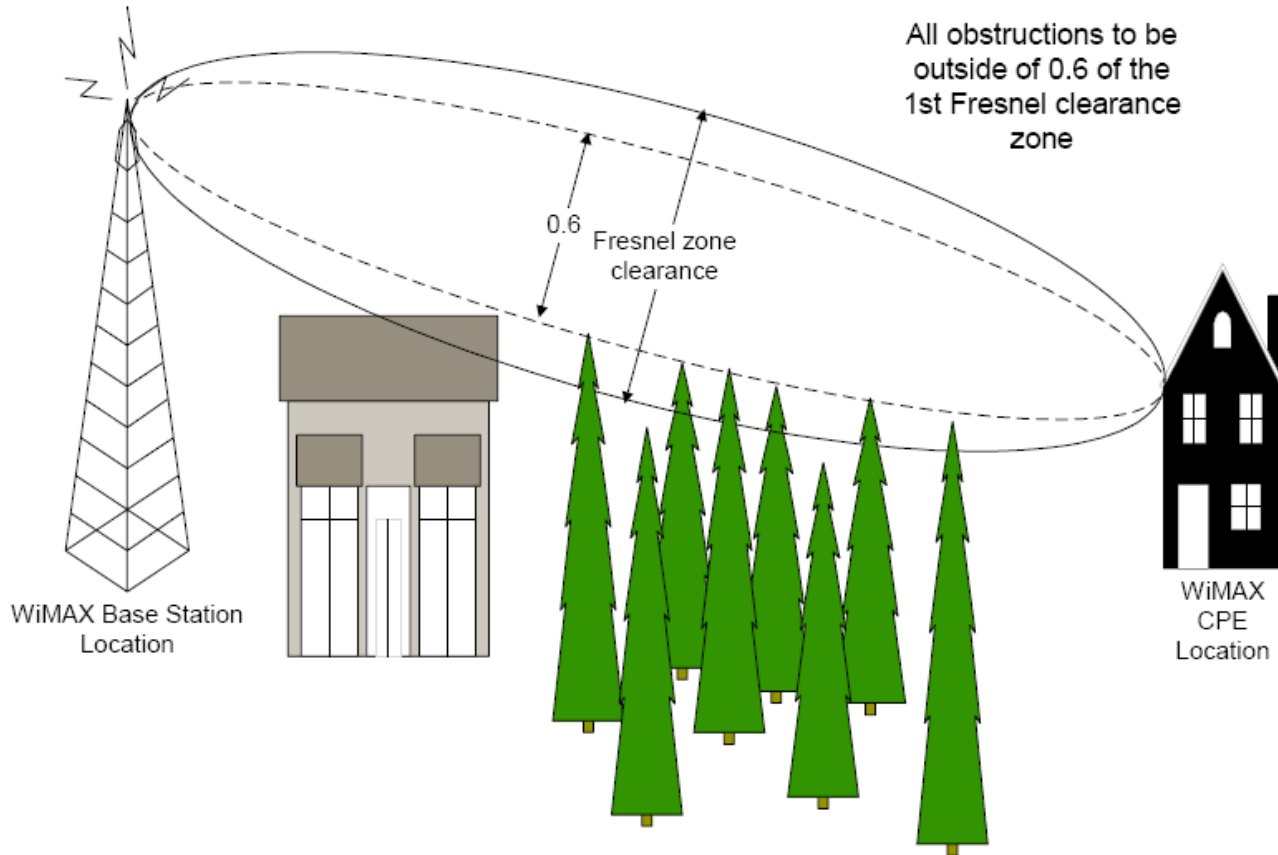
# Introducción (III)

## HOW WiMAX WORKS





# Non Line Of Sight - NLOS





# Non Line Of Sight - NLOS (I)

---

- La tecnología WiMAX ha sido optimizada para proveer cobertura sin línea de visión (Non line of sight – NLOS).
- WiMAX resuelve los problemas que resultan de condiciones NLOS utilizando diferentes técnicas:
  - Tecnología OFDM.
  - Sub-Canalización.
  - Antenas direccionales.
  - Diversidad de transmisión y recepción.
  - Modulación adaptativa.
  - Técnicas de corrección de error.
  - Control de potencia.

Sin embargo el rendimiento real no es tan bueno...



# Non Line Of Sight - NLOS (II)

- Ejemplo de prestaciones para dos estaciones base diferentes en un mismo sistema:

Assumptions	Frequency: 3.5 GHz Bandwidth: 3.5 MHz Per 60 <sup>o</sup> sector	Full featured		Standard	
		From	To	From	To
Cell radius (km)	LOS	30	50	10	16
	NLOS(Erceg-Flat)	4	9	1	2
	Indoor self-install CPE	1	2	0.3	0.5
Maximum throughput per sector (Mbps)	Downlink	11.3	8	11.3	8
	Uplink	11.3	8	11.3	8
Maximum throughput per CPE at cell edge (Mbps)	Downlink	11.3	2.8	11.3	2.8
	Uplink	0.7	0.175*	11.3	2.8
Maximum number of subscribers		More		Less	



# Seguridad

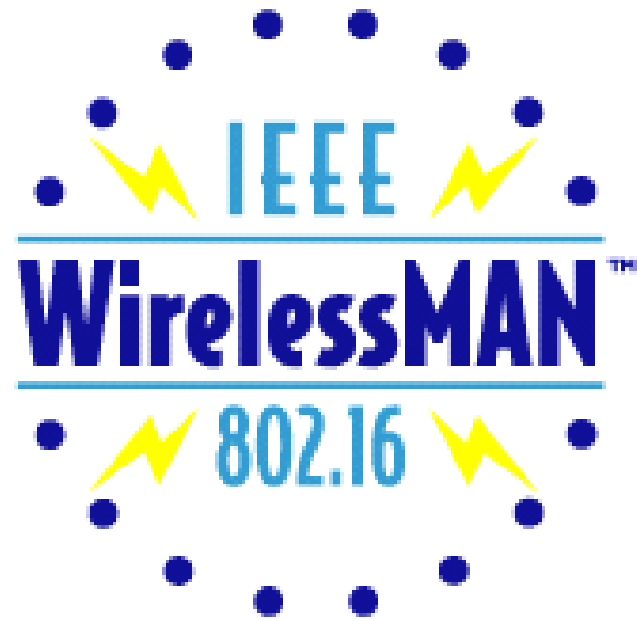
Al contrario que las anteriores soluciones WLAN, WiMAX nace con una solución robusta en materia de seguridad.

- **Autenticación de usuario:** protocolo EAP (*Extensible Authentication Protocol*).
- **Autenticación del terminal:** intercambio de certificados digitales que impiden la conexión de terminales no autorizados.
- **Cifrado de las comunicaciones:** se utilizan algoritmos como el DES (*Data Encryption Standard*) o el AES (*Advanced Encryption Standard*), mucho más robustos que el WEP (*Wireless Equivalent Privacy*), utilizado inicialmente en las WLAN. Adicionalmente, cada servicio es cifrado con la asociación específica de clave pública/clave privada.





# Estándares





## Comparativa entre estándares (I)

WiMAX engloba cuatro versiones del estándar IEEE 802.16:

- **IEEE 802.16 (1988):**
  - Sin movilidad. Conexiones punto-multipunto.
  - Antenas fijas y direccionales.
  - Bandas 10-60 GHz.
  
- **IEEE 802.16a (Enero 2003):**
  - Banda de 2 a 11GHz.
  - En esta banda hay frecuencias no licenciadas, que permiten utilizar antenas no direccionales, de interior y autoinstalables.
  
- **IEEE 802.16d (Julio 2004):**
  - NLOS
  
- **IEEE 802.16e (diciembre 2005):**
  - Movilidad



## Comparativa entre estándares (III)

- Tabla comparativa de las características de los estándares:

	802.11	802.16	802.16a	802.16e	802.20
Status	Complete	Dec 2001	Jan. 2003	January. 2004	ETA '05-06
Target App.	LAN	MAN	MAN	MAN	WAN
Range	Up to 300 ft. optimized for indoor LAN	Up to 5 miles Average Cell Radius 1-3 mi	Up to 25 miles Average Cell Radius 4-8 mi	Average Cell Radius 1-3 mi	
Channel Conditions	LOS when outdoors	LOS	nLOS	nLOS	nLOS
Spectrum	2.4 GHz & 5 GHz – Unlicensed	10-66 GHz Licensed	2-11 GHz Licensed and Unlicensed	2-8 GHz Licensed and Unlicensed	<3.5 GHz Licensed
Mobility Support	Portable – Local Roaming	Fixed	Fixed	Pedestrian Mobility – Regional Roaming	Vehicular Mobility – Global Roaming
Channelization	20 MHz	Scalable 1.5-20 MHz	Scalable 1.5-20 MHz	Scalable 1.5-5 MHz w/ sub-channels	1.25 or 5 MHz
Spectral Efficiency	< 2.7 bps/Hz	< 4.8 bps/Hz	< 3.75 bps/Hz	< 3 bps/Hz	< 1.25 bps/Hz
Bit Rate	54 Mbps (20 MHz BW)	< 134 Mbps (20 MHz BW)	< 75 Mbps (20 MHz BW)	15 Mbps (5 MHz BW)	< 6 Mbps (5 MHz BW)



# *Wimax Forum (I)*

- Es una corporación dirigida a la industria, sin ánimo de lucro, formada para **promocionar y certificar la conformidad e interoperabilidad de los productos de Acceso Inalámbrico** a Banda ancha que utilizan las especificaciones IEEE 802.16 y ETSI HiperMAN wireless MAN.
- Los esfuerzos del WiMAX Forum han servido para tener una tecnología que se basa en estándares.
- WiMAX Forum definirá y realizará tests de ajuste e interoperabilidad para asegurar que sistemas de diferentes vendedores trabajan de manera similar con los demás.
  - Aquellos que pasen el test recibirán la designación de “WiMAX Forum Certified”.
- Cetecom labs, con base en Málaga (España) fue elegida para realizar los tests de interoperabilidad de los productos WiMAX.



## *Wimax Forum (II)*

- Se fundó en abril de 2001 pero fue en 2.003 cuando comenzó a cobrar importancia.
- Actualmente, el WiMAX Forum tiene **más de 310 miembros**.
  - Se incluyen proveedores de servicio de banda ancha, vendedores de equipos, fabricantes de silicio, vendedores de software, integradores y medios de comunicación.
- El número de miembros crece continuamente.



<http://www.wimaxforum.org/home/>



# Segmentos de mercado Wimax

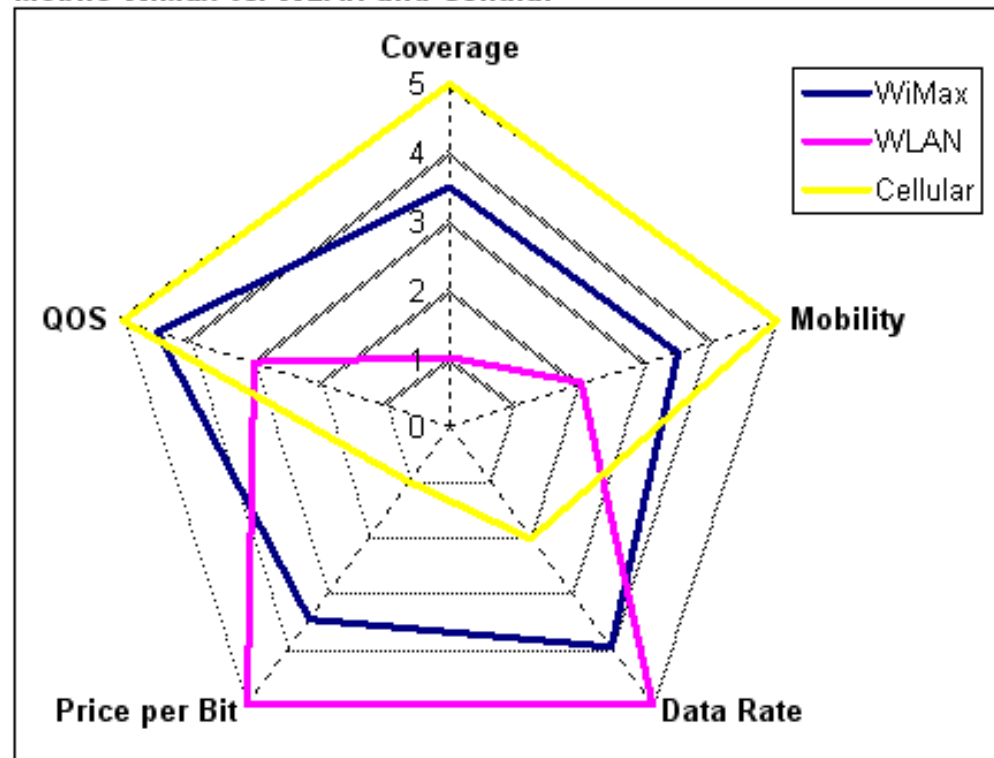
---

- La tecnología WiMAX fue visionada **en un principio** como una forma de proveer acceso inalámbrico de banda ancha en la “**última milla**” en las redes metropolitanas.
  - Accesos a Internet de alta velocidad residenciales y SOHO (Small Office/ Home Office).
  - Pequeñas y medianas empresas.
  - WiFi Hot Spot Backhaul.
- **Potencial adicional**
  - Backhaul celular.
  - Servicios públicos de seguridad y redes privadas.



# WiMAX - WiFi - Celular

Mobile WiMax vs. WLAN and Cellular



Source: Samsung and Unstrung Insider



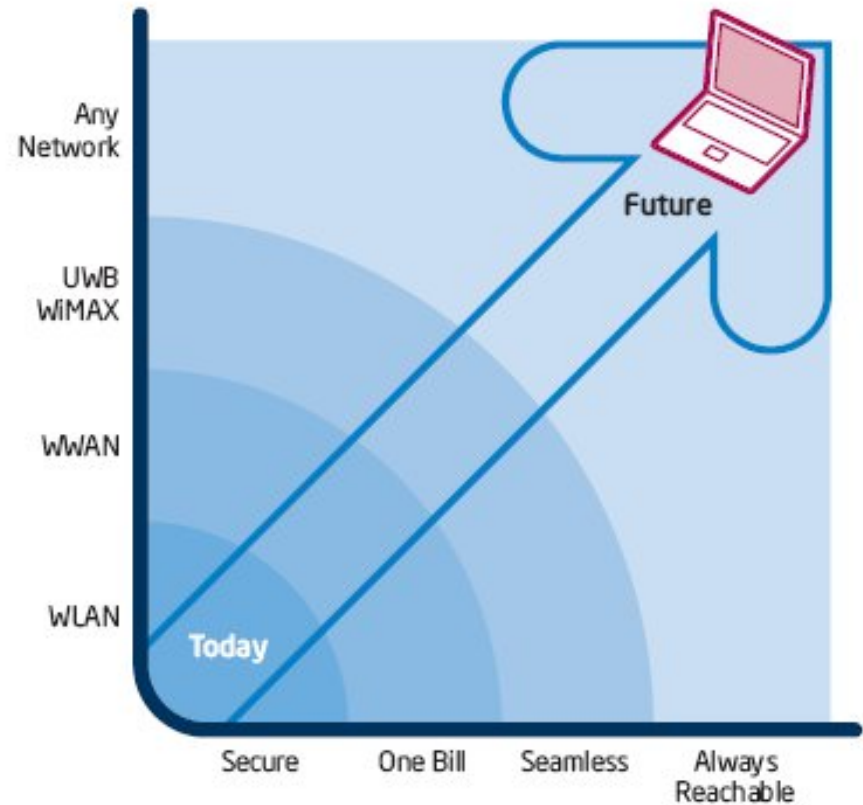
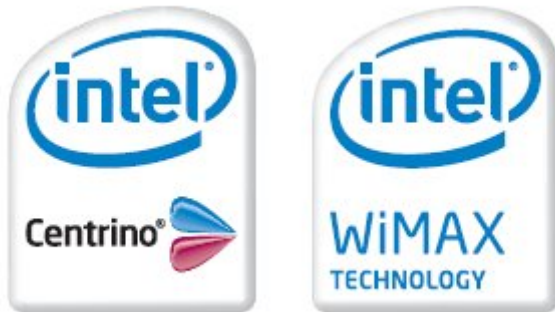
# Fabricantes

---

- **Intel**
- **Nokia**
- **Motorola**
- Flarion
- Fujitsu Microelectronics.
- Gen-Wan Technology
- Alvarion
- Aperto Networks
- Etc, etc...



# Fabricantes



<http://www.intel.com/netcomms/technologies/wimax/313900.pdf>



# Preguntas



¿?