

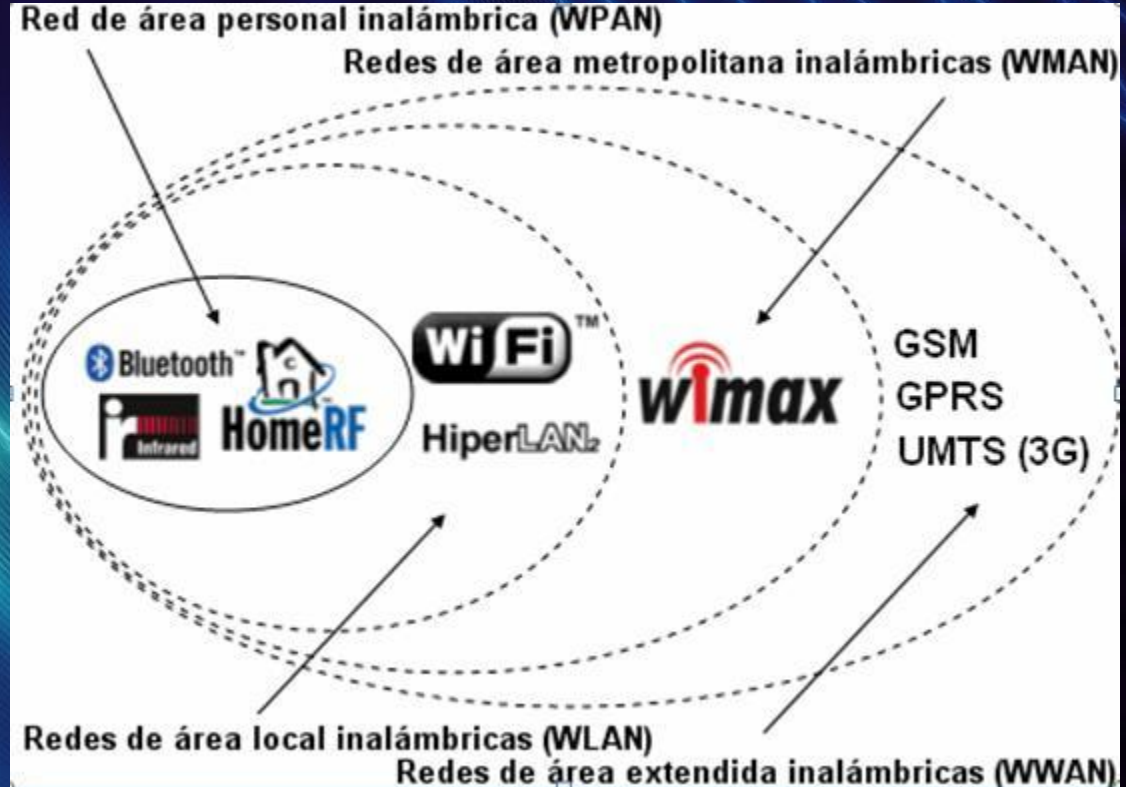
Redes Inalambricas

Patricio Tella Arena
Adrian Juri
Juan Pablo Moraes



Redes Inalambricas

- ❑ **WPAN**
(Bluetooth)
- ❑ **WLAN**
(Wi-Fi)
- ❑ **WMAN**
(Wi-Max)
- ❑ **WWAN**
(Telefonia Movil)



Espectros o Bandas de Frecuencia

- ❑ Regulados por la CNC (Argentina)
- ❑ Frecuencias:
 - ❑ Licenciadas
 - ❑ Reservadas
 - ❑ De uso gubernamental
 - ❑ Libres:
 - ❑ 900 MHz: 902-928 MHz
 - ❑ 2.4 GHz: 2403-2483 MHz
 - ❑ 5 GHz: 5725-5850 MHz, 5150-5250 MHz, 5250-5350 MHz, 5725-5825 MHz

WI-FI

- ❑ Wi-Fi es una abreviatura de Wireless Fidelity (Fidelidad inalámbrica)
- ❑ Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.
- ❑ Los dispositivos habilitados con Wi-Fi, tales como una PC, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a internet a través de un punto de acceso de red inalámbrica.
- ❑ Dicho punto de acceso (o hotspot) tiene un alcance de unos 20 metros en interiores y al aire libre una distancia mayor que pueden cubrir grandes áreas la superposición de múltiples hotspot.



Historia

- ❑ Esta nueva tecnología surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuese compatible entre distintos dispositivos.
- ❑ 1999 : 3Com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies crean la Wireless Ethernet Compatibility Alliance, o WECA, actualmente llamada Wi-Fi Alliance. El objetivo designar una marca para fomentar la tecnología inalámbrica y asegurar compatibilidad de equipos.
- ❑ 2000 : WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11b, bajo la marca Wi-Fi. (Wi-Fi en Alliance - Certified Products.)



Historia

- ❑ 2002 : WECA estaba formada ya por casi 150 miembros en su totalidad. La familia de estándares 802.11 ha ido evolucionando, mejorando el rango y velocidad de la transferencia de información, su seguridad, entre otras cosas.
- ❑ La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet).
- ❑ Una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet).

Seguridad y fiabilidad

❑ Problemas:

- ❑ Saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros) que están expuestas a un excesivo riesgo de interferencias.
- ❑ Instalaciones inseguras, redes abiertas (o completamente vulnerables ante el intento de acceder a ellas por terceras personas), sin proteger la información que por ellas circulan. La configuración por defecto de muchos dispositivos Wi-Fi es muy insegura (routers, por ejemplo) a partir del identificador del dispositivo se puede conocer la clave de éste y acceder y controlar el dispositivo se puede conseguir en sólo unos segundos.
- ❑ El acceso no autorizado a un dispositivo Wi-Fi es muy peligroso para el propietario, accediendo al Wi-Fi se puede monitorizar y registrar toda la información que se transmite a través de él (incluyendo información personal, contraseñas, etc.)

La forma de hacerlo seguro es seguir algunos consejos:

- ❑ Cambios frecuentes de la contraseña de acceso, utilizando diversos caracteres, minúsculas, mayúsculas y números.
- ❑ Se debe modificar el SSID que viene predeterminado.
- ❑ Realizar la desactivación del broadcasting SSID y DHCP.
- ❑ Configurar los dispositivos conectados con su IP (indicar específicamente qué dispositivos están autorizados para conectarse).
- ❑ Utilización de cifrado: WPA2.
- ❑ Filtrar los dispositivos conectados mediante la MAC address.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos.

- ❑ WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Cifrados de 64 y 128 bits codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire.
- ❑ WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.
- ❑ IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.
- ❑ Filtrado de MAC, de manera que solo se permite acceso a la red a aquellos dispositivos autorizados.
- ❑ Ocultar punto de acceso (Router) de manera que sea invisible a otros usuarios.
- ❑ El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. Es el protocolo de seguridad más seguro para Wi-Fi en este momento. Requieren hardware y software compatibles
- ❑ Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

Estandares

Existen diversos tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11 certificado

❑ **Wi-Fi A**

Conocido como Wi-Fi 5, ya que trabaja en 5GHz

Velocidades hasta 54Mbps

Menor alcance que en 2,4GHz



Estandares

❑ **Wi-Fi B**

Trabaja en 2.4GHz

Velocidades de hasta 11Mbps

Ya casi no es utilizado

Alcance de 300mts a campo abierto

3 canales de radio disponibles

Estandares

❑ **Wi-Fi G**

Retrocompatible con Wi-Fi B

Velocidades de hasta 54Mbps

Trabaja en 2.4GHz

❑ **Wi-Fi N**

Velocidades de hasta 150/300Mbps

Retrocompatible con Wi-Fi B y Wi-Fi G

Admite tecnología MiMo (Multiple Input Multiple Output)

Trabaja en 2.4GHz

Ventajas

Las redes Wi-Fi poseen una serie de ventajas, entre las cuales podemos destacar:

- ❑ Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un espacio lo bastante amplio.
- ❑ Una vez configuradas, las redes Wi-Fi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, ni gran cantidad de cables.
- ❑ La Wi-Fi Alliance asegura que la compatibilidad entre dispositivos con la marca Wi-Fi es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología Wi-Fi con una compatibilidad absoluta.

Desventajas

La tecnología Wi-Fi presenta los problemas intrínsecos de cualquier tecnología inalámbrica :

- ❑ Menor velocidad en comparación a una conexión cableada, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear.
- ❑ **SEGURIDAD.** Programas capaces de capturar paquetes, que pueden calcular la contraseña de la red y de esta forma acceder a ella. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad. De todos modos, muchas compañías no permiten a sus empleados utilizar una red inalámbrica. Este problema se agrava si consideramos que no se puede controlar el área de cobertura de una conexión, de manera que un receptor se puede conectar desde fuera de la zona de recepción prevista
- ❑ Esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc.
- ❑ La potencia de la conexión del Wi-Fi se verá afectada por los agente físicos que se encuentran a nuestro alrededor, tales como: árboles, paredes, arroyos, una montaña, etc. Dichos factores afectan la potencia de compartimiento de la conexión Wi-Fi con otros dispositivos.



Dispositivos

Existen varios dispositivos Wi-Fi, los cuales se pueden dividir en dos grupos: Dispositivos de Distribución o Red, entre los que destacan los routers, puntos de acceso y Repetidores; y Dispositivos Terminales que en general son las tarjetas receptoras para conectar a la computadora personal, ya sean internas (tarjetas PCI) o bien USB.

Dispositivos de Distribución o Red:

- ❑ Los puntos de acceso son dispositivos que generan un "set de servicio", que permiten conectar dispositivos en forma inalámbrica a una red existente.
- ❑ Los repetidores inalámbricos son equipos que se utilizan para extender la cobertura de una red inalámbrica.
- ❑ Los router inalámbricos son dispositivos compuestos, que incluyen, un Router, un punto de acceso y generalmente un switch que permite conectar algunos equipos vía cable (Ethernet y USB). Su tarea es tomar la conexión a internet, y brindar a través de ella acceso a todos los equipos que conectemos, sea por cable o en forma inalámbrica.



Dispositivos

Los dispositivos terminales abarcan tres tipos mayoritarios: tarjetas PCI, tarjetas PCMCIA y tarjetas USB:

- ❑ Las tarjetas PCI para Wi-Fi. Hoy en día están perdiendo terreno debido a las tarjetas USB. Dentro de este grupo también pueden agregarse las tarjetas MiniPCI que vienen integradas notebooks.
- ❑ Las tarjetas PCMCIA son un modelo que se utilizó mucho en las primeras notebooks. La mayor parte de estas tarjetas solo son capaces de llegar hasta la tecnología B de Wi-Fi.
- ❑ Las tarjetas USB para Wi-Fi son el tipo de tarjeta más común que existe en el mercado y más sencillo de conectar a una pc, haciendo uso de todas las ventajas que tiene la tecnología USB. Hoy en día puede encontrarse tarjetas USB con el estándar 802.11N (Wireless-N) que es el último estándar liberado para redes inalámbricas.
- ❑ También existen impresoras, cámaras Web y otros periféricos que funcionan con la tecnología Wi-Fi, permitiendo un ahorro de mucho cableado en las instalaciones de redes y especialmente, gran movilidad.



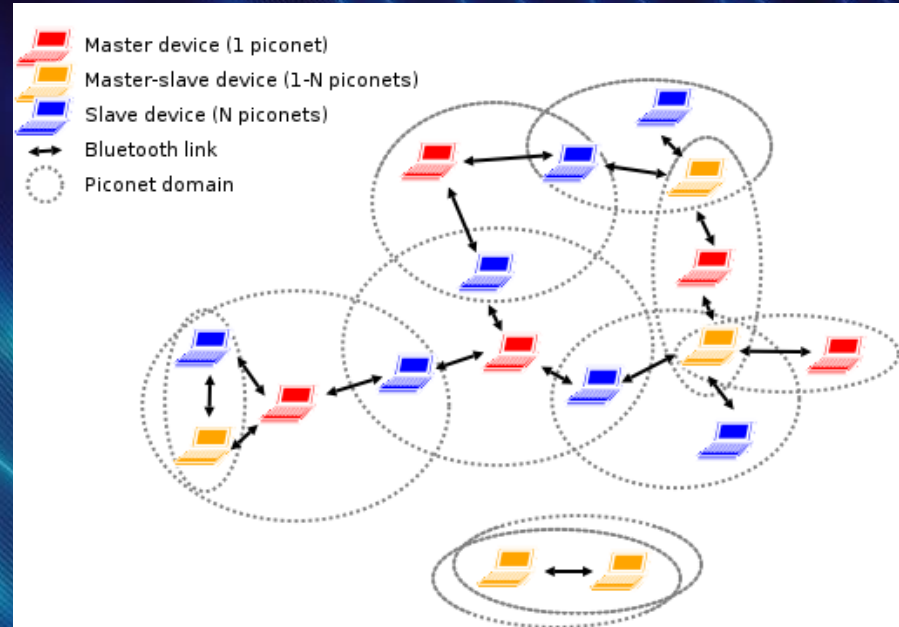
Bluetooth

- ❑ Es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN)
- ❑ Posibilita la transmisión de voz y datos entre diferentes dispositivos
- ❑ Utiliza un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz
- ❑ El nombre procede del rey Harald Blatand (Harald Bluetooth en inglés)

Piconets

Es la topología de red utilizada, donde cada enlace bluetooth une dos o más dispositivos por medio de un canal físico.

Permite que un dispositivo maestro se interconecte con 7 dispositivos esclavos activos.



Usos del Bluetooth

Es un protocolo de comunicaciones diseñado para dispositivos de:

- ❑ Bajo consumo
- ❑ Que requieren corto alcance de emisión
- ❑ Basados en transceptores de bajo costo

Los dispositivos pueden comunicarse entre ellos cuando se encuentran dentro de su alcance.

Las comunicaciones se realizan por radiofrecuencia:

- ❑ Los dispositivos no tienen que estar alineados
- ❑ Pueden incluso estar en habitaciones separadas



Lista de aplicaciones

- ❑ Conexiones sin cables via OBEX
- ❑ Transferencia de fichas de contactos y citas entre dispositivos via OBEX
- ❑ Controles remotos (tradicionalmente dominado por el infrarrojo)
- ❑ Algunos joysticks desde la séptima generacion
- ❑ Enlace inalámbrico entre sistemas de audio y altavoces.

Bluetooth versiones

v1.0 y v1.0b

- ❑ El anonimato era imposible, en la transmisión se incluía la dirección del dispositivo

v1.1(2002)

- ❑ Ratificado como estándar IEEE 802.15.1-2002
- ❑ Se corrigieron muchos errores en las especificaciones 1.0b
- ❑ Se añadió soporte para canales no cifrados
- ❑ Indicador de señal recibida

Bluetooth versiones

v1.2(2003):

- ❑ Compatibilidad con USB 1.1
- ❑ Conexión más rápida y Discovery (detección de otros dispositivos)
- ❑ Mayor velocidad de transmisión en la práctica
- ❑ Conexiones Sincrónicas extendidas (ESCO)
- ❑ Ratificado como estándar IEEE 802.15.1-2005

Bluetooth versiones

v2.0 + EDR(2004):

- ❑ EDR (Enhanced Data Rate) para acelerar la transferencia de datos

v2.1 + EDR(2007):

- ❑ SSP mejor la experiencia de emparejamiento
- ❑ Aumenta el uso y la fuerza de seguridad
- ❑ EIR que proporciona más información para permitir un mejor filtrado
- ❑ Oler Subrating, que reduce el consumo de energía



Bluetooth versiones

v3.0 + hs(2009)

- ❑ Soporta velocidades teóricas de hasta 24 Mbit/s
 - ❑ Negociación y establecimiento por conexión bluetooth
 - ❑ Transferencia de datos mediante un enlace 802.11
- ❑ AMP (Alternate MAC/PHY) es la adición de 802.11 como transporte de alta velocidad

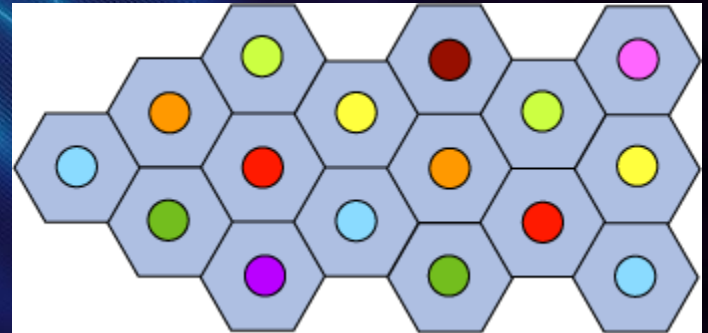
Bluetooth versiones

v4.0(2010):

- ❑ Incluye al Bluetooth clásico, al de alta velocidad, y los protocolos de bajo consumo.
- ❑ BLE (Bluetooth Low Energy) es la version 4.0 con protocolos nuevos para desarrollar rápidamente enlaces sencillos.

Telefonia Celular

- ❑ Surgió a fines de los '70 y principios de los '80
- ❑ Compuesta por terminales fijas (estaciones) y terminales móviles (celulares)
- ❑ Cada estación, está rodeada por otras 6, funcionando en frecuencias distintas, generando un Area de Cobertura



Telefonia Celular

1G

- ❑ La primera red celular a nivel mundial
- ❑ Totalmente analogica
- ❑ Comunicaciones no seguras
- ❑ Utilizaba la banda de frecuencia de 900MHz
- ❑ Estandares utilizados: AMPS, TACS, ETACS



Telefonia Celular

2G

- ❑ Totalmente Digital
- ❑ Transmite voz y datos digitales (ej: SMS, MMS)
- ❑ Permite navegación en internet a baja velocidad
- ❑ Estándares Utilizados: GSM, CDMA, TDMA, GPRS, EDGE

Telefonia Celular

CDMA

“Acceso Multiple Por Division de Codigo”

- ❑ Transmite señales a través de rangos de frecuencia amplios

TDMA

“Acceso Multiple Por Division de Tiempo”

- ❑ Aumenta volumen de datos transmitidos en simultáneo

Telefonia Celular

RED GSM

“Sistema Global de Comunicaciones Móviles”

- ❑ Usa bandas de 900, 1800 y 1900 MHz dependiendo el país
- ❑ Introduce tarjetas SIM para la identificación de usuarios dentro de la red
- ❑ Admite el concepto de Roaming

Telefonia Celular

GPRS

“Servicio General de Paquetes de Radio”

- ❑ Llamado “2.5G”
- ❑ Utiliza protocolo IP sobre redes GSM
- ❑ Transmisión de datos a 40Kbps
- ❑ Las transmisiones solo utilizan la red cuando es necesario
- ❑ Integra QoS

Telefonia Celular

EDGE

“Tasas de datos Mejoradas para la Evolución de GSM”

- ❑ Llamado “2.75G”
- ❑ Utiliza redes GSM
- ❑ Cuadriplica el ancho de banda de GPRS
- ❑ Ofrece menor area de cobertura
- ❑ Paso previo a la telefonia 3G

Telefonia Celular

3G

- ❑ Altas velocidades de transferencia de datos
- ❑ Compatibilidad Mundial
- ❑ Uso de aplicaciones multimedia
- ❑ Retrocompatibilidad con redes 2G
- ❑ Utiliza bandas de 1885 a 2025 MHz y 2110 a 2200 MHz
- ❑ Estándares Utilizados: UMTS, W-CDMA, HSPDA

Telefonia Celular

RED UMTS

“Sistema Universal de Telecomunicaciones Móviles”

- ❑ Servicios de voz de alta calidad
- ❑ Altas velocidades de ancho de banda

W-CDMA

- ❑ “Acceso Múltiple por División de Código de Ancho de Banda”

Telefonia Celular

HSPDA

“High Speed Downlink Packet Access”

- ❑ Llamada “3.5G”
- ❑ Velocidades de transferencia de hasta 14Mbps
- ❑ Basado en la tecnologia W-CDMA
- ❑ Disminuye la latencia en el envio de paquetes
- ❑ Programación de Paquetes rápidos
- ❑ Paso previo a las redes 4G

Telefonia Celular

4G

- ❑ Basada totalmente en el protocolo IP
- ❑ Mejora el área de cobertura
- ❑ Tasas de transferencia de hasta 1Gbps
- ❑ QoS garantizada de Punta a Punta
- ❑ Utiliza tecnología MiMo
- ❑ Utiliza la frecuencia de 800MHz
- ❑ Estándares Utilizados: LTE

Telefonia Celular

LTE

“Long Term Evolution”

- ❑ Bajos costos de implementación
- ❑ Solo transmite datos a través del protocolo IP
- ❑ Logra altísimas tasas de transferencia
- ❑ Transmite voz a través de IP

Wi-MAX

“Interoperabilidad Mundial
para acceso por Microondas”

Standard IEEE 802.16



Wi-MAX

- ❑ Tecnología de “Ultima Milla”
- ❑ Ofrece conexión a internet en lugares remotos
- ❑ Alcance de 80Kms
- ❑ Utiliza Espectros con o sin licencia
- ❑ Sirve como Backhaul de telefonía movil