



UNCUYO
UNIVERSIDAD
NACIONAL DE CUYO



**FACULTAD
DE INGENIERÍA**

**Licenciatura en Ciencias de la
Computación**

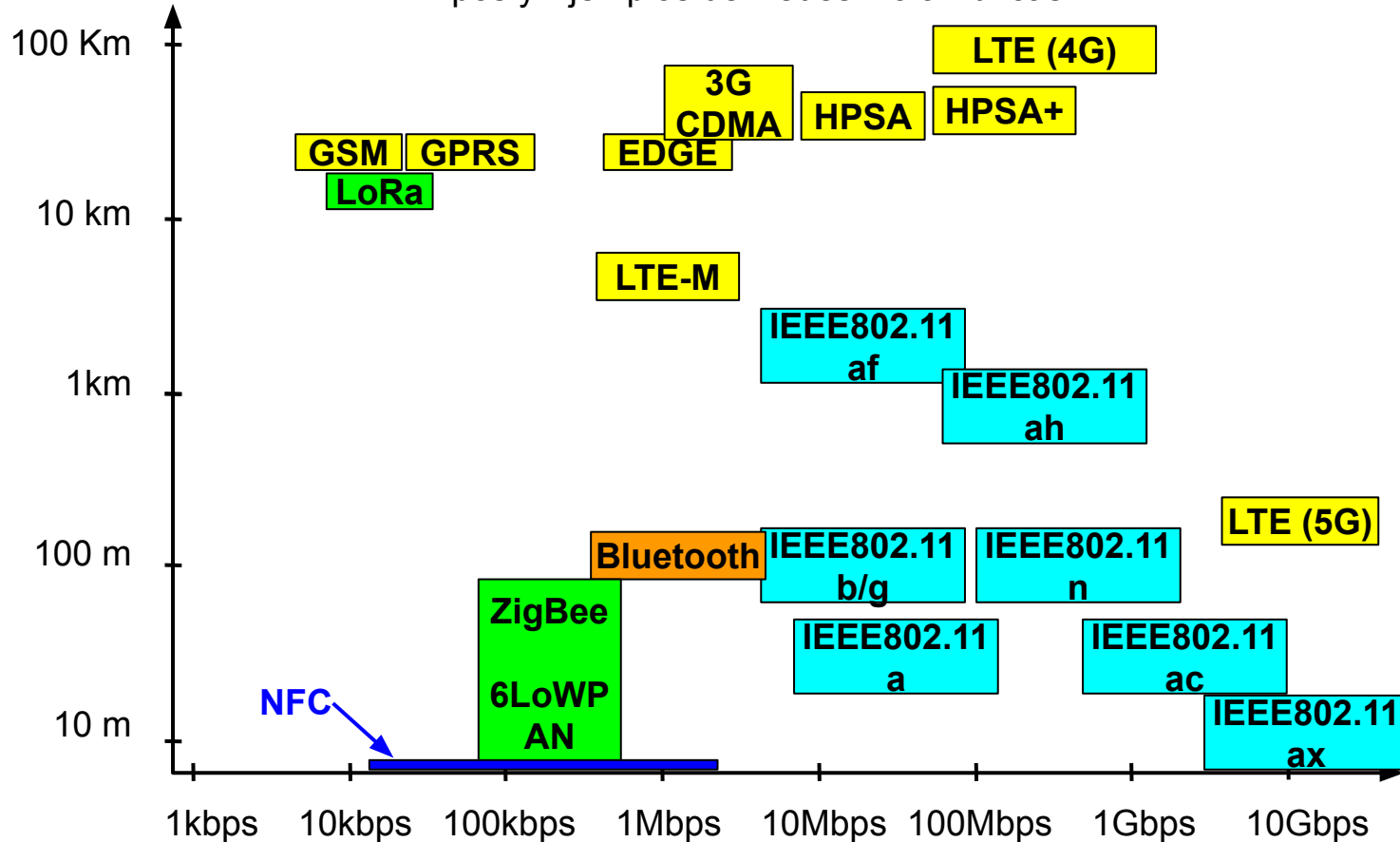
Redes de Computadoras

Unidad 7

Redes especiales y conceptos avanzados



Tipos y Ejemplos de Redes Inalámbricas





Redes Inalámbricas: Ventajas

1) Movilidad.

2) Menores costos.

Ventajas que han sido suficientes para motivar la investigación y desarrollo en el campo de las redes inalámbricas

Redes inalámbricas - desventajas:

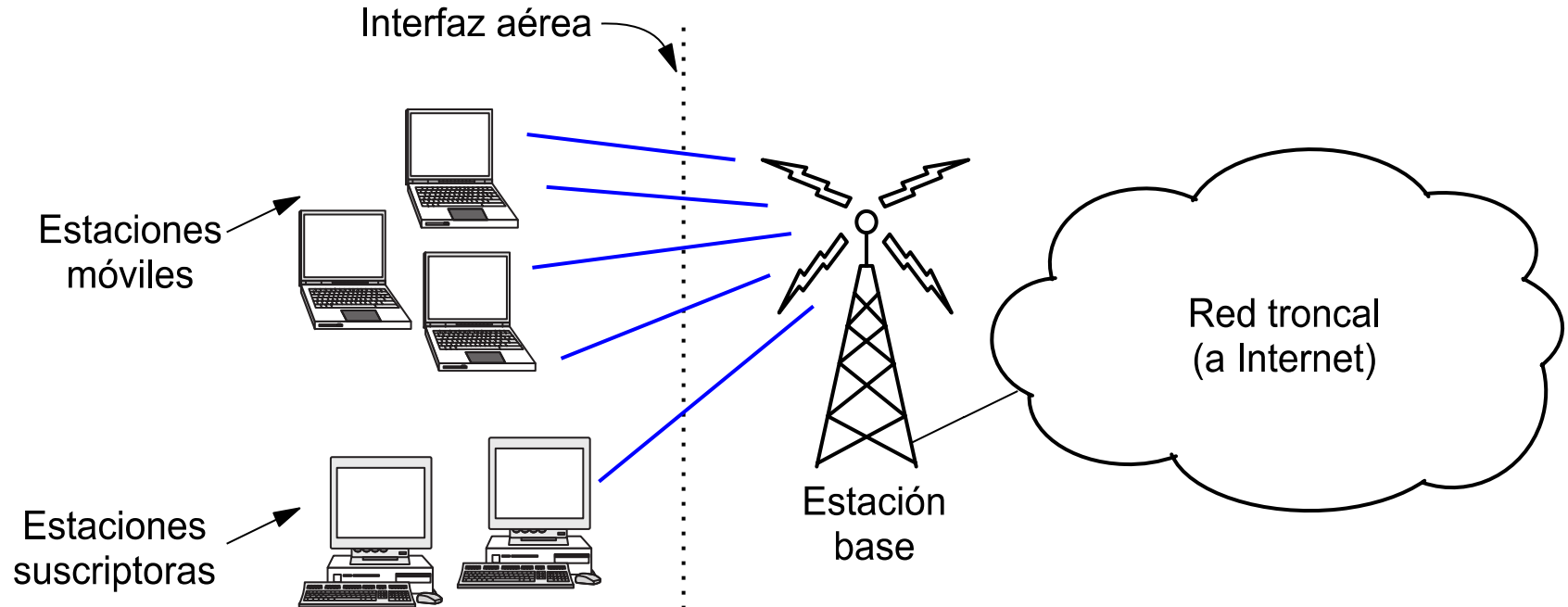
- 1) Multipath.
- 2) Colisiones agravado por el rango limitado:
- 3) Medio común que debe ser **compartido por muchas redes**, sobre todo la banda ISM.
- 4) Seguridad: Todos dentro del alcance de la red pueden **escuchar** la señal y acceder, ver datos, etc.
- 5) Atenuación: La intensidad (Potencia/Área) **Disminuye con $1/r^2$ o $1/r^3$**
- 6) Las ondas electromagnéticas son **absorbidas** por la lluvia, la humedad, obstáculos, etc. (sobre todo de alta frecuencia)
- 7) Interferencia: Otras fuentes de ondas electromagnéticas, motores, campos magnéticos o eléctricos variables, etc. pueden **interferir y degradar** la señal transmitida.
- 8) **Topología cambiante** por movilidad (especialmente en redes de telefonía)



Redes WAN inalámbricas: IEEE 802.16 (WiMAX) y LTE

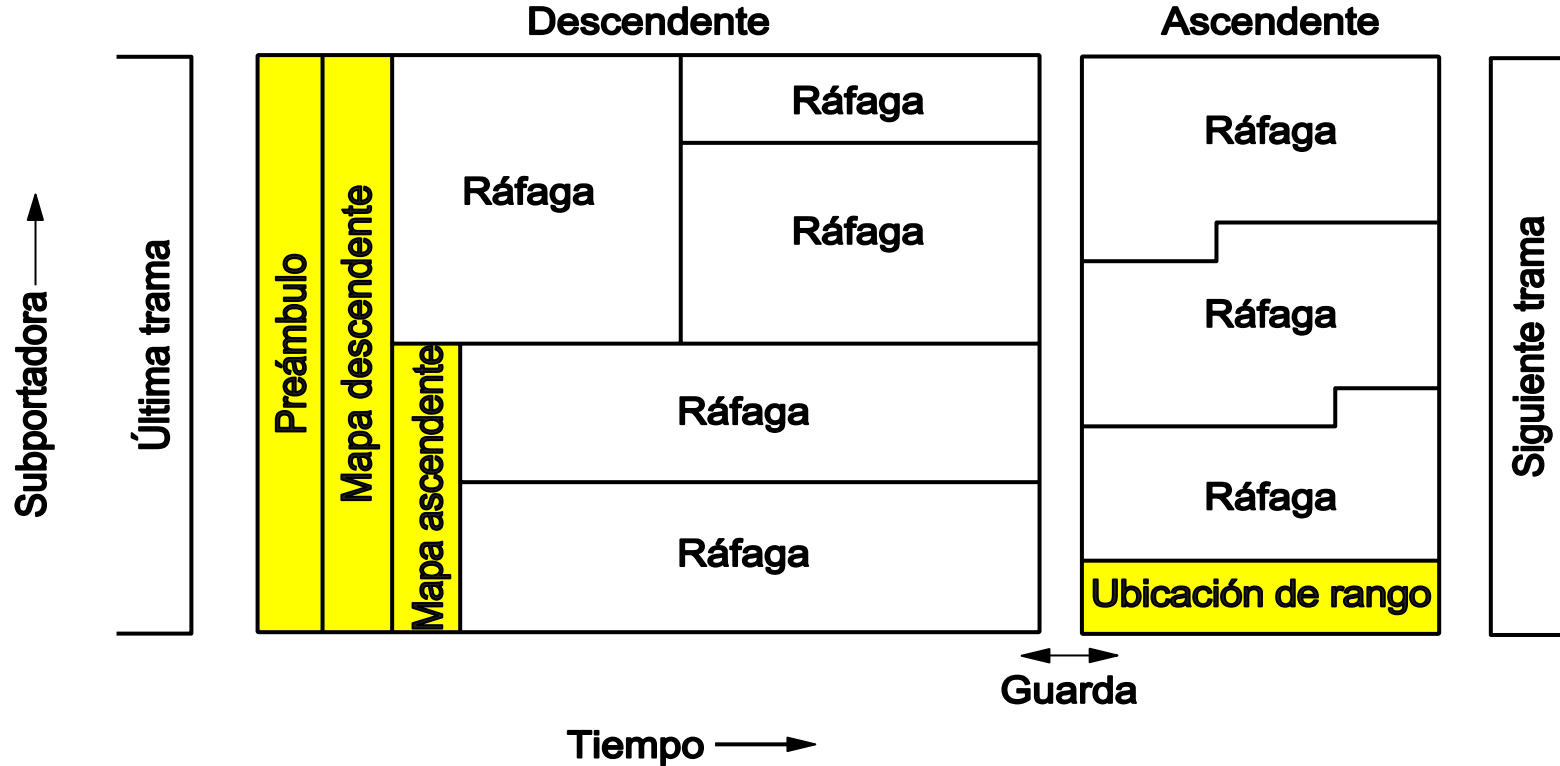
- WiMAX: Worldwide Interoperability for Microwave Access (ISPs inalámbricos)
- LTE: Long Term Evolution (ISPs inalámbricos, G4 y G5).
- Estándares para redes WAN inalámbricas.
 - Definen una capa física y una capa de enlace que trabajan bajo IP.
- Modulación: OFDM y antenas MIMO.
 - Antenas MIMO: varios flujos de datos entre varias antenas.
- Espectro licenciado (2 a 11 GHz).
- Topología punto-multipunto.
- Orientado a conexión (a nivel capa de enlace).
- Necesidad de mecanismos de seguridad muy robustos.

IEEE 802.16 (WiMAX) y LTE





Capa física WiMAX - OFDMA



802.16 WiMAX - Trama Capa Física

- **Preámbulo:** Para sincronizar estaciones (misma función del preámbulo de Ethernet y IEEE802.11)
- **Mapa descendente:** Mapa de subportadoras OFDMA descendentes asignadas a las estaciones clientes.
- **Mapa ascendente:** Mapa de subportadoras OFDMA ascendentes asignadas a las estaciones clientes.
- **Guarda:** Tiempo necesario para que las estaciones conmuten.
- **Ubicación de rango:** Portadoras ascendentes que se dejan libres para que nuevas estaciones “avisen” su presencia la estación base.
 - Los clientes compiten por ancho de banda.
 - Se les asigna ancho de banda según calidad de servicio.

WAN inalámbricas: LTE (Long Term Evolution)

- Desarrollado por 3GPP (consorcio varias empresas e instituciones: ISM forum, IPv6 Forum, etc.).
- Bajada de datos:
 - OFDM + TDM en cada portadora, formando una grilla de “bloques”.
 - QPSK, 16QAM, 64QAM dentro de cada bloque.
- Subida de datos:
 - SC-FDMA: (Single Carrier Frequency Division Multiple Access)
 - Menor consumo que OFDMA para los equipos de usuario.
- Estándar adoptado en 4G y 5G.

Telefonía celular

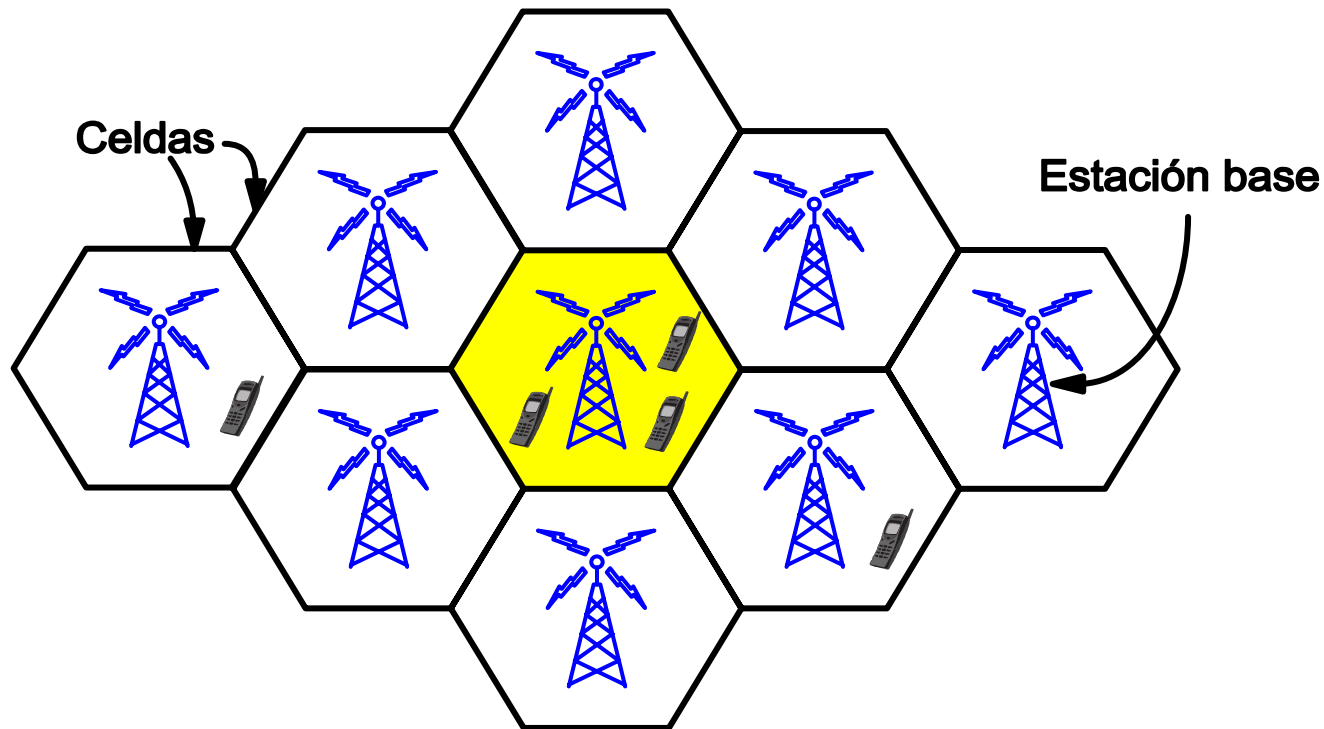
3 partes:

- Dispositivo Móvil
- Interfaz aérea inalámbrica entre dispositivo móvil - Red telefonía móvil.
- Red telefonía móvil





Red celular



Telefonía celular - 1G

- Precursores: varios sistemas propietarios no estandarizados:
 - Sistemas policiales (1924 policía Australia)
 - Sistemas militares.
- **1G** nace en 1982 con el protocolo AMPS (Advanced Mobile Phone System). Después se suman otros.
 - Desarrollado en los laboratorios Bell
 - **Transmisión analógica**: Se modula la voz directamente.
 - Muy sensible al ruido.
 - Introduce el concepto de celda ¹
 - **FDMA**: A cada usuario se le asigna un canal, que consiste en una frecuencia.



DynaTAC Motorola

¹ De aquí el nombre de teléfono celular

Telefonía celular - 2G

- 1991
- **Transmisión digital**
 - La voz primero se digitaliza (ceros y unos) y se modula una señal digital.
 - Mayor inmunidad al ruido.
 - Transmisión cifrada.
 - Posibilidad de transmitir datos.
- Protocolos más importantes:
 - GSM (Global System for Mobile communications) para voz.
 - GPRS (General Packet Radio Service)
 - Datos. 56–114 kbps
 - EDGE
 - Datos. 1 Mbit/s



Nokia 1100



Telefonía celular - 3G

- **Dispositivos más potentes que necesitan mayor velocidad.**
- Protocolos más importantes:
 - UMTS (Universal Mobile Telecommunications System)
 - 14 Mbps enlace de bajada
 - 6 Mbps enlace de subida
 - HSPA (High Speed Packet Access)
 - 337 Mbit/s.
 - HSPA+:



Iphone 3G
(Apple)

Telefonía móvil - 4G

- **Toda transmisión (voz y datos) basada en conmutación de paquetes IP:** “all-Internet Protocol (IP) packet-switched”.
 - Antes de 4G, la red de telefonía móvil era diferente y separada de la Internet.
- Algunos requisitos impuestos por la ITU:
 - Interface aerea: OFDMA
 - Antenas MIMO.
 - 100 Mbit/s para móviles en movimiento y 1 Gbit/s para móviles quietos.
- Protocolo: LTE (Long-Term Evolution)

Telefonía móvil - 5G

- Requisitos exigidos por el estándar (ITU): Capacidad de área (datos por unidad de área) 1000 veces superior a 4G.
 - Velocidad pico: 20 Gbps, Latencia: 1 ms
 - Movilidad: 500 km/h.
 - Densidad: 10^6 usuarios/km².
 - 99.999% availability
 - 90% de reducción de energía utilizada.
- Estándar: **LTE**. Interface aerea: **OFDMA**
- Celdas de menor tamaño:
 - **Picocells**: menos de 100 metros.
 - **Femtocells**: pocas decenas de metros.
- Se preve usar SDN (Software-Defined Networking) y NFV (Network Functions Virtualization).
- ¿Competencia del futuro: 5G vs WiFi?



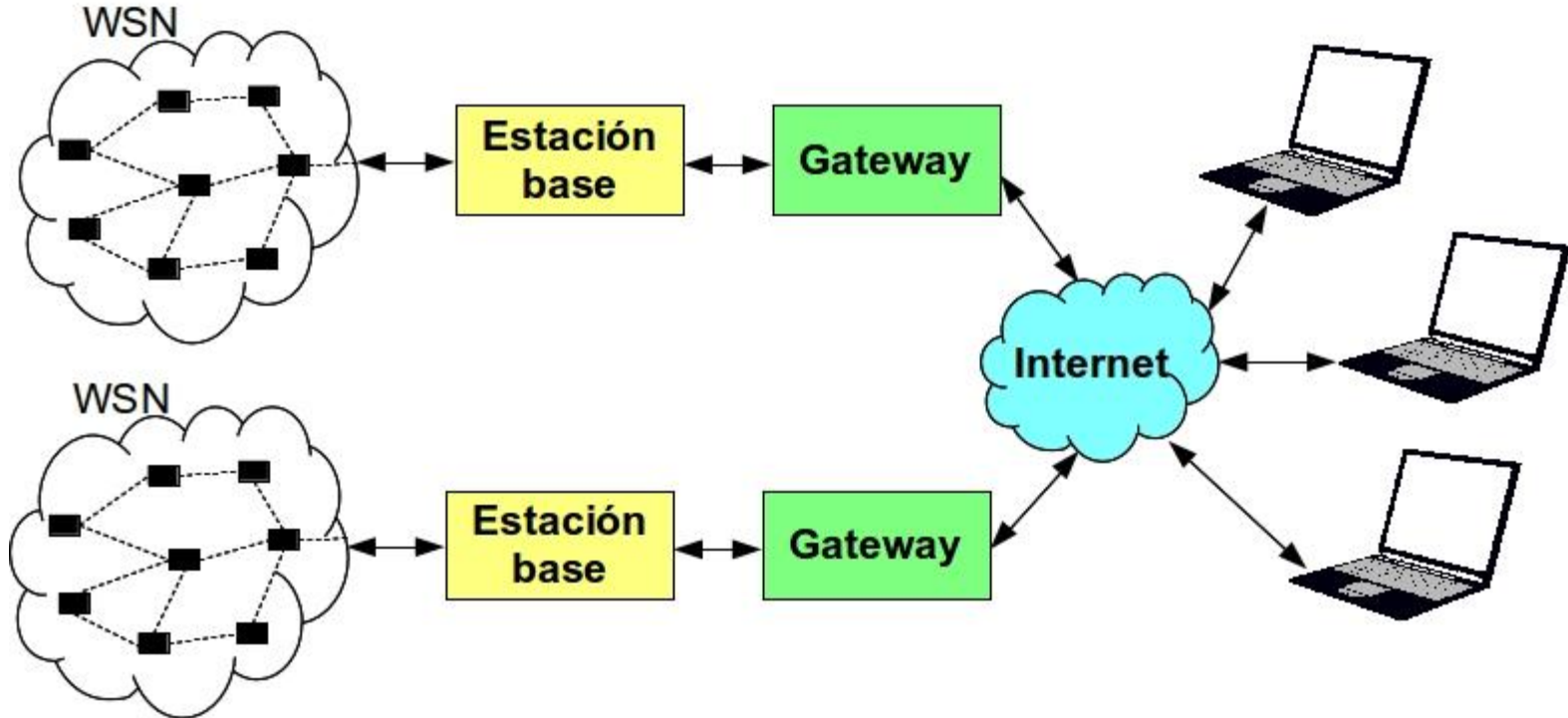
	Año	Tecnolog.	Comuta.	Veloc.	Modulac.	Protoco.	Estado
1G	1984	Analóg.	Circuitos	-		-	Obsoleta
2G	1990	Digital	Circuitos	100Kbs	TDMA-FDMA	GSM GPRS EDGE	En uso
3G	2008	Digital	Circuitos	80 Mbs	CDMA modificado	UMTS HSPA+ WCDMA	En uso
4G	2014	Digital	Paquetes	1Gbs	OFDMA	LTE	Expansión
5G	2018	Digital	Paquetes	20Gbs	OFDMA	LTE	Desarrollo

* AMPS fue dada de baja formalmente en 2008

Redes inalámbricas de baja velocidad

- Objetivo: **Muy bajo consumo de energía** (cuando el consumo es el parámetro fundamental).
- Aplicaciones:
 - Medición de variables ambientales (IoT):
 - Redes de sensores inalámbricos.
 - Smart cities.
 - Domótica.
- Características:
 - Tramas de datos de tamaño pequeño.

Redes inalámbricas de baja velocidad (WSN)

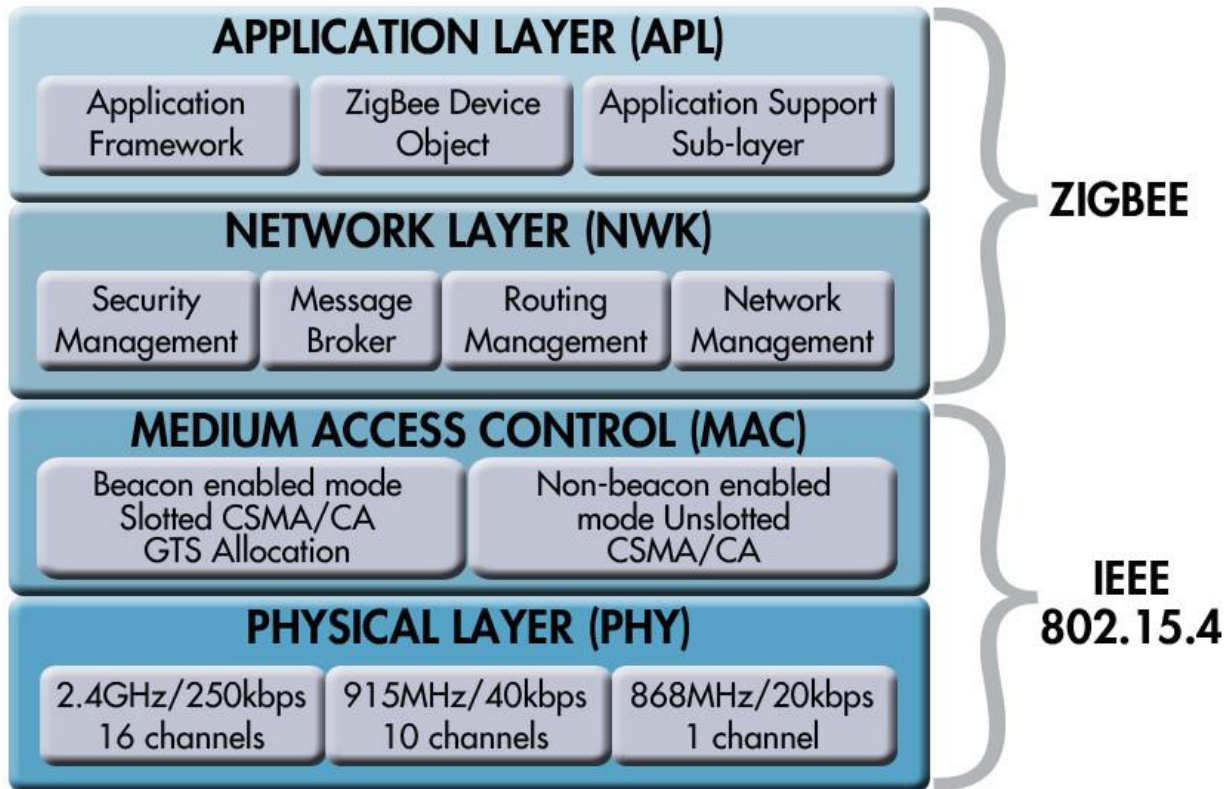


Redes inalámbricas de baja velocidad: IEEE-802.15.4

- Comunicación WPAN o WLAN de baja velocidad y **bajo consumo**.
- Estándar impuesto por el mercado. Define capas **Física** y **MAC** de redes inalámbricas de baja velocidad, estandarizado por **IEEE - 802.15.4**.
- Utilizados por varios protocolos de ruteo de datos: **ZigBee**, **6LowPAN**.
- Frecuencias de operación ISM.
- Baja velocidad (250 kbps).
- Tamaño máximo trama: 127 Bytes.
- Dos dispositivos:
 - RFD (Reduced Function Device)
 - FFD (Full Function Device): Pueden rutear datos.

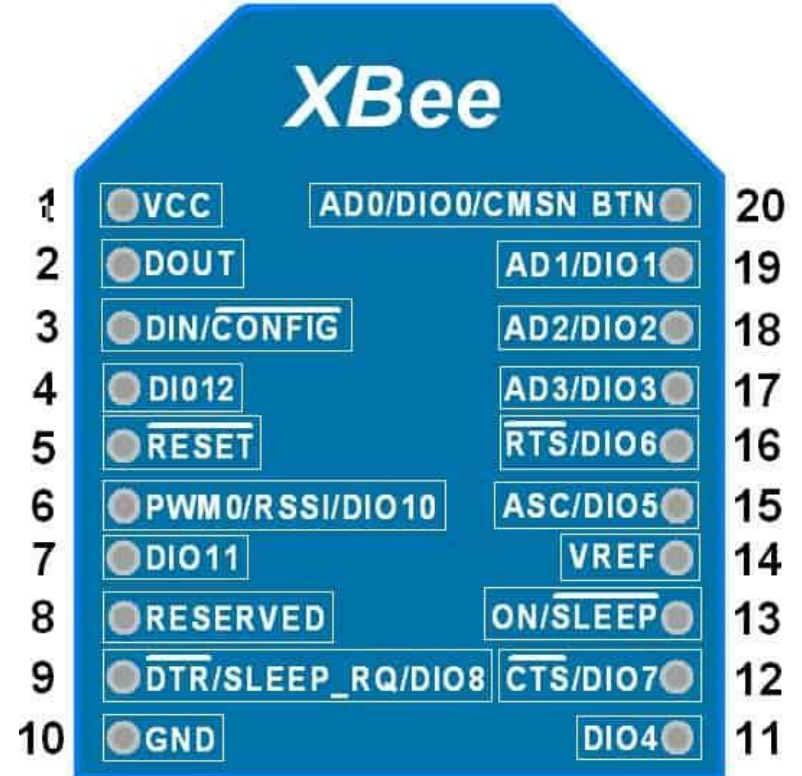
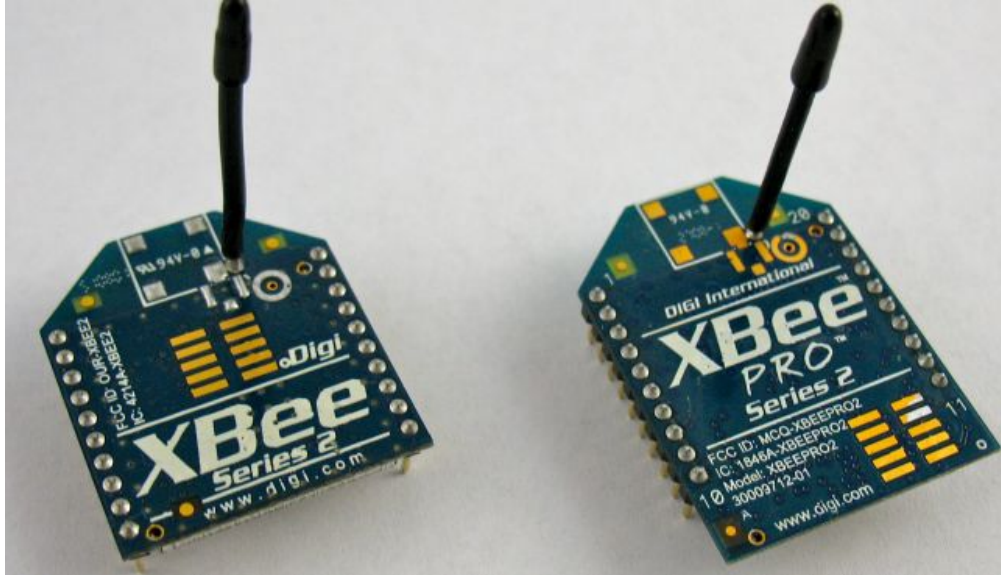


ZigBee 802.15.4





Ejemplo: Digi XBee

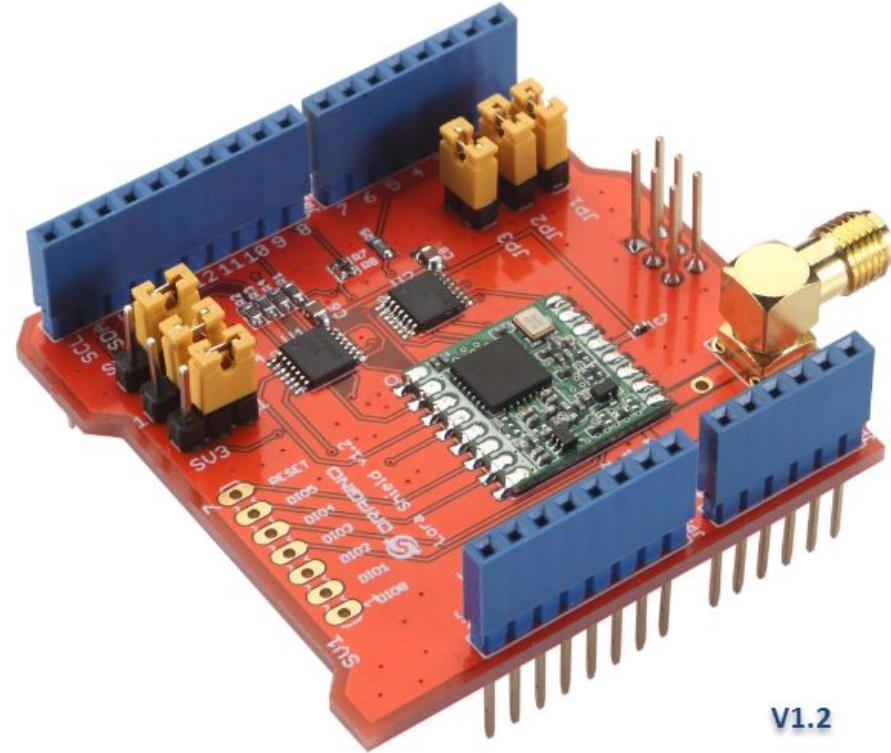


LoRa

- LoRa: Long Range (Lora Alliance).
- Modulación: Tecnología patentada por Semtech.
 - 915 MHZ/868 MHZ/433 MHZ.
- Consumo: TX: hasta 120 mA. RX: hasta 12 mA.
- Tramas de hasta 256 bytes con CRC.
- Dispositivos:
 - End devices.
 - Gateways.
- Topologías:
 - Estrella. Requiere Gateway
 - Punto a punto. End device + Gateway o dos End Devices.
- Encriptación AES.
- Distancias según hoja de datos: 200 km.
 - Según foros: 40 km con línea de visión.
 - 4 km sin línea de visión.

LoRa

- Placas Lora Shield: Placas preparadas para trabajar con Arduino.
- Gran cantidad de librerías y ejemplos disponibles en Internet.
- Comunicación SPI.



V1.2

RFID y NFC

RFID (Radio-frequency identification) y NFC (Near-Field Communication)

- Permiten identificar y seguir dispositivos llamados “etiquetas” que se adjuntan a objetos. Las etiquetas son leídas por “lectores”.
- Las etiquetas pueden:
 - Ser solo un dispositivo de identificación (memoria ROM).
 - Poseer memoria que puede ser escrita y leída.
- Etiquetas pueden ser:
 - Activas: Poseen fuente de alimentación.
 - Pasivas: No poseen fuente de alimentación. Obtienen la energía de las señales electromagnéticas emitidas por el lector.
- RFID: distancias entre 1 m y 200 m según frecuencia.
- NFC: distancias máximas de 10 cm, típicas de 4 cm.

RFID

- RFID: Radio Frequency IDentification
- 9600 bps, 115,2 kbps
- Nace en el MIT 1999
- Objetivo: Reemplazar el código de barra (lectura a 10 m)
- Comercializados por EPCglobal (Electronic Product Code).
- Dos componentes:
 - Etiquetas:
 - código de 96 bits
 - Pequeña memoria que puede ser leída o escrita.
 - Extraen energía de las señales generadas por el lector
 - Lector:
 - Detecta etiquetas presentes en el vecindario.
 - Soluciona problemas de múltiple acceso.



Frecuencias de RFID y NFC

Band	Range	Data Speed	Tags
Low frequency (LF): 125–134.2 kHz	10 m	low	passive
High frequency (HF): 13.56 MHz	10 cm–1 m	low to moderate	passive
Ultra high frequency (UHF): 433 MHz	1–100 m	moderate	passive or active
Ultra high frequency (UHF): 856 MHz–960 MHz	1–12 m	moderate to high	passive or active
Microwave: 2.45–5.8 GHz	1–2 m	high	active
Microwave: 3.1–10 GHz	<200 m	high	active

Frecuencia
NFC





RFID - Productos RFID



Etiquetas RFID





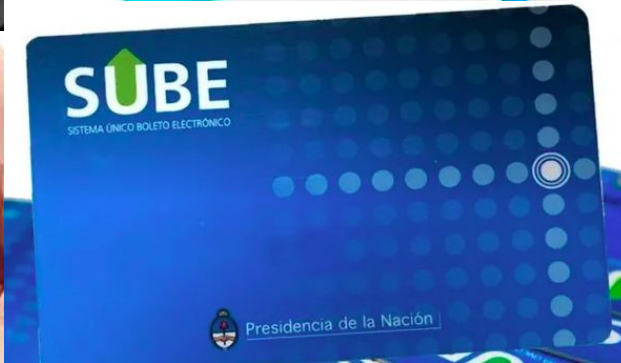
UNCUYO
UNIVERSIDAD
NACIONAL DE CUYO



**FACULTAD
DE INGENIERÍA**

**Licenciatura en Ciencias de la
Computación**

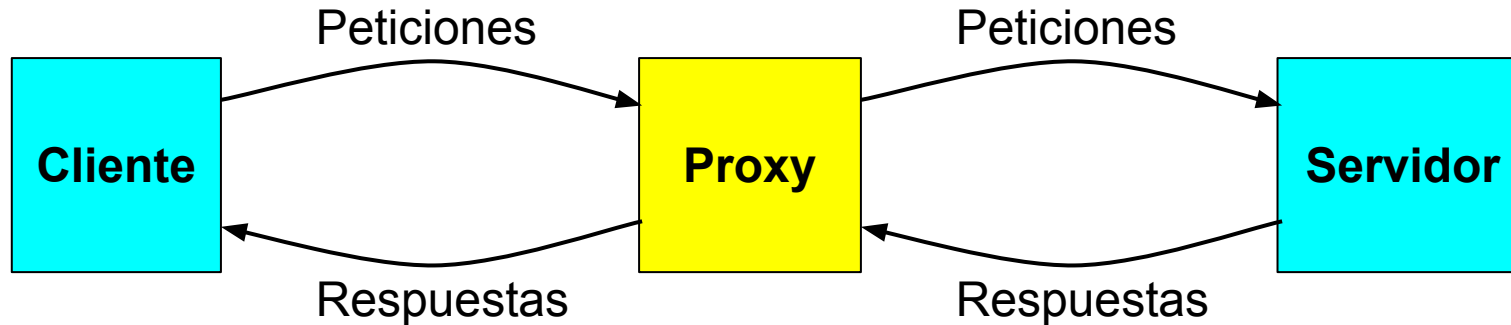
NFC



Servidores Proxy

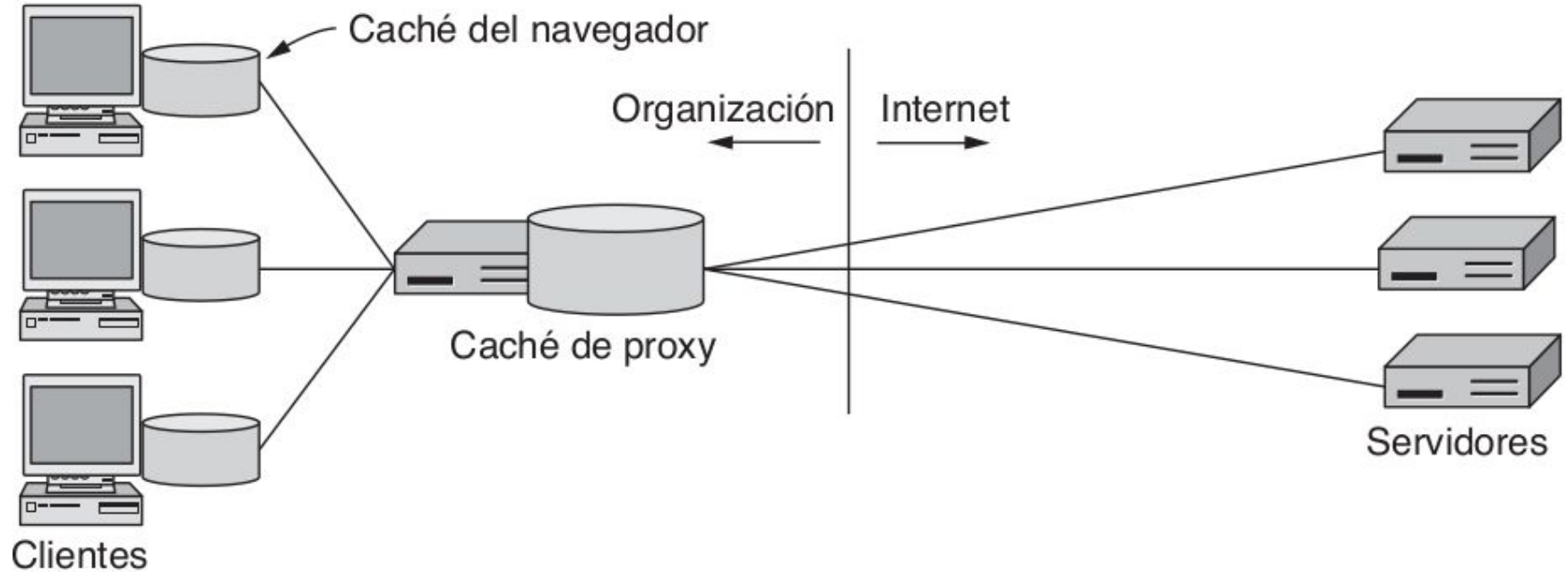
Intermediario entre un cliente y un servidor.

- Actúa en nombre del cliente.
 - Recibe y reenvía peticiones de los clientes hacia los servidores.
 - Recibe y reenvía respuestas de los servidores hacia los clientes.



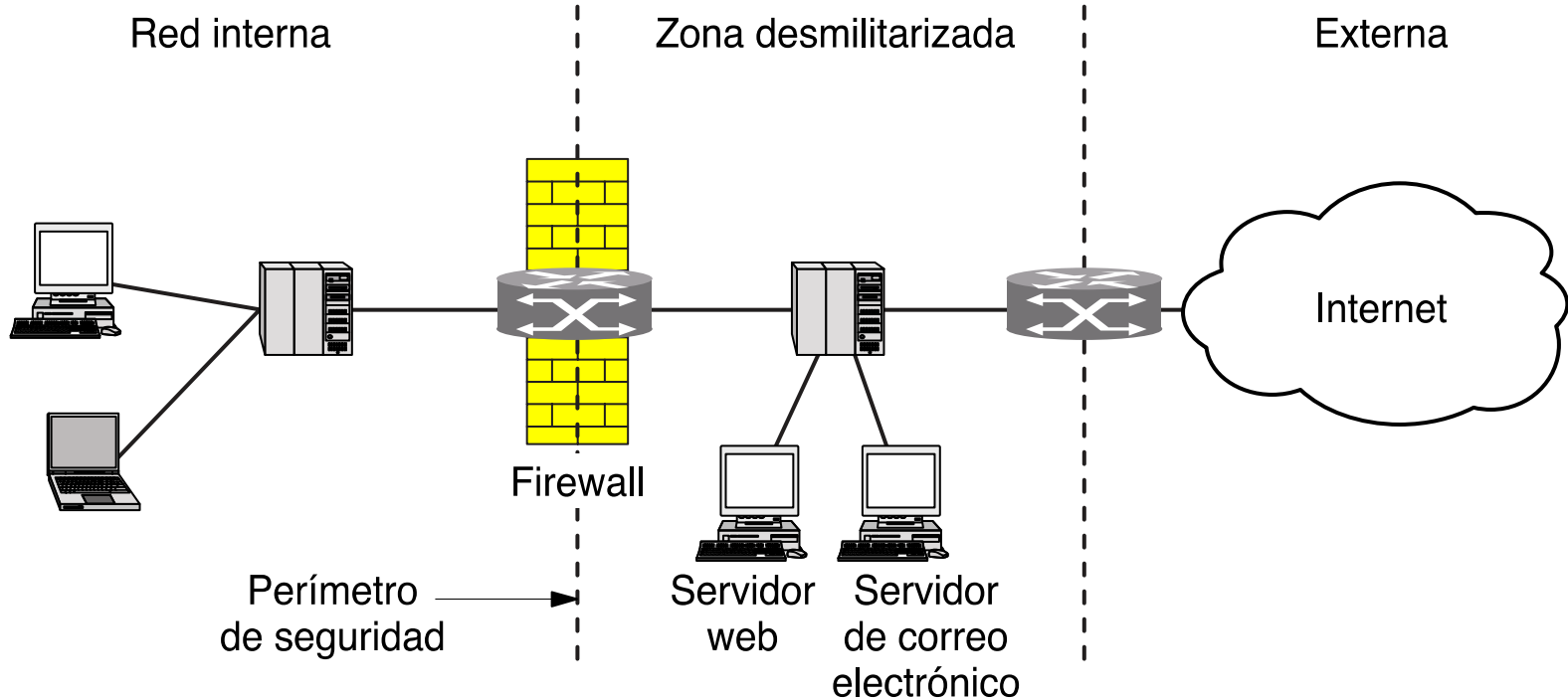
Servidores Proxy

Ejemplos: Caché web



Servidores Proxy

Ejemplos: Firewall.



Servidores Proxy

Ejemplos: Caché web

- Proxy HTTP: captura peticiones HTTP (HTTPS, FTP, etc.) y las reenvía al servidor solicitado. Captura las respuestas y las envía a los clientes.
- Proxy ARP. Responde solicitudes ARP en nombre de otra máquina, enviando su propia MAC. Permite que dos máquinas en distintas redes se comuniquen como si estuvieran en la misma LAN.
- Proxy NAT.

Otras funcionalidades que provee un servidor Proxy:

- **Control de acceso.** Restringir los usuarios que pueden acceder a ciertos recursos.
- **Anonimato.** Ocultar la IP de los clientes.
- **Registro de tráfico.**
- **Modificar el contenido** del tráfico: eliminar código Javascript peligroso, bloquear cookies.

Ejemplo: Configuración del Proxy HTTP de Linux

- Captura y reenvía peticiones HTTP y HTTPS. Usualmente también FTP (se deben configurar puertos).



Proxy de la red

Automático
 Manual
 Desactivado

Proxy para HTTP 8080 - +

Proxy para HTTPS 0 - +

Proxy para FTP 0 - +

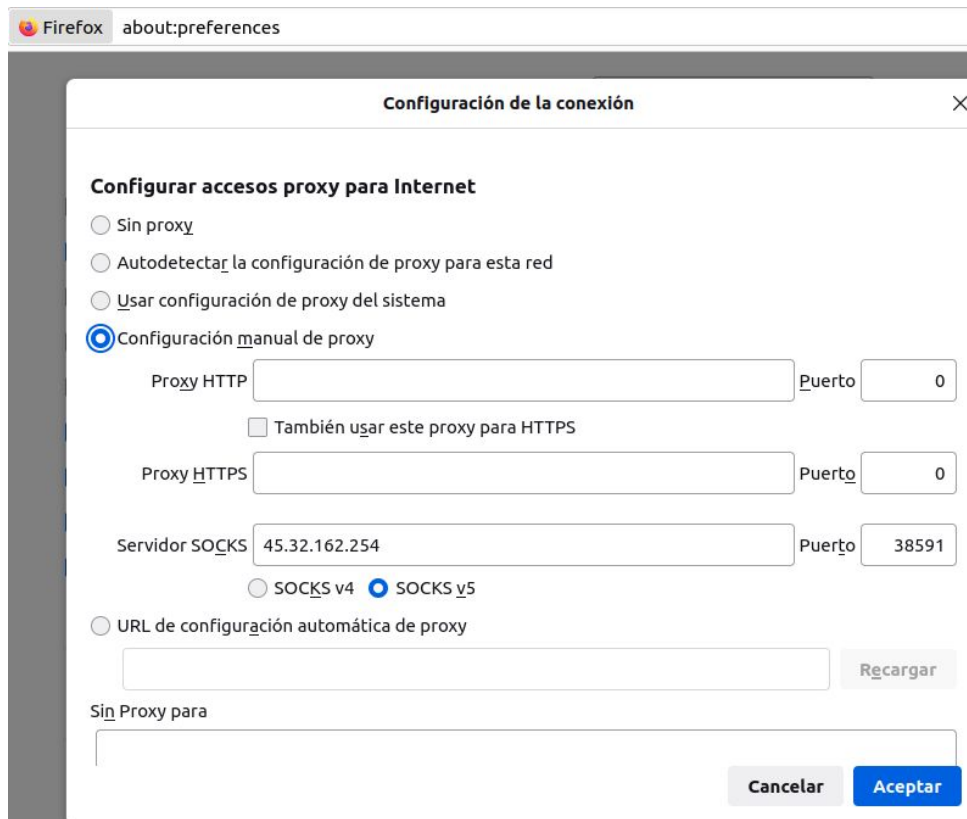
Servidor socks 0 - +

Ignorar anfitriones

Ejemplo: Configuración del Proxy HTTP de Firefox

- Captura y reenvía peticiones HTTP y HTTPS. Usualmente también FTP (se deben configurar puertos).

Pantalla captura configuración Proxy de Firefox (preferencias -> Configuración de red).



Firefox about:preferences

Configuración de la conexión

Configurar accesos proxy para Internet

Sin proxy

Autodetectar la configuración de proxy para esta red

Usar configuración de proxy del sistema

Configuración manual de proxy

Proxy HTTP Puerto

También usar este proxy para HTTPS

Proxy HTTPS Puerto

Servidor SOCKS Puerto

SOCKS v4 SOCKS v5

URL de configuración automática de proxy

Sin Proxy para

Servidores Proxy

Proxy SOCKS (SOCKetS).

- Utiliza un protocolo llamado SOCK en lugar de HTTP.
- Implementado como una capa entre la de transporte y la de aplicación en el modelo OSI.
- Utiliza una conexión TCP o paquetes UDP.
- Diferentes versiones. Versión actual: Sock5 (RFC 1928):
 - Autenticación (usuario y contraseña, Kerberos, SSL, etc.)
 - DNS en el servidor.
 - TCP, UDP, IPv6.
- Aplicaciones:
 - Lidar con el agotamiento de las IPs (Reemplazado por los NAT).
 - Evadir Firewalls, bloqueos de proxys, restricciones del país de origen (actual más importante).

Algunos servidores Proxy SOCKS 5 gratis: <https://spys.one/en/socks-proxy-list/>

No usar con datos privados

Ejemplo con servidor proxy SOCKS5 con IP 45.32.162.254 y puerto 38591.

No.	Time	Source	Destination	Protocol	Length	Source port	Dest Port	Information
1159	104.774655683	45.32.162.254	192.168.100.2	Socks	76	38591	35980	Version: 5
1160	104.775042107	192.168.100.2	45.32.162.254	HTTP	664	1080	38591	GET / HTTP/1.1
1162	105.304260555	45.32.162.254	192.168.100.2	Socks	1494	1080	35980	Version: 5 [TCP se
1163	105.304306657	45.32.162.254	192.168.100.2	TCP	1494	1080	35980	Version: 5 [TCP se
1168	105.325276454	192.168.100.2	45.32.162.254	TLSv1.2	217	1080	38591	Application Data
1169	105.325434392	192.168.100.2	45.32.162.254	TCP	716	1080	38591	Version: 5 [TCP se
1196	105.618537390	45.32.162.254	192.168.100.2	TLSv1.2	234	1080	46172	Application Data,

▶ Frame 1160: 664 bytes on wire (5312 bits), 664 bytes captured (5312 bits) on interface wlo1, id 0

▶ Ethernet II, Src: LiteonTe_59:47:93 (24:fd:52:59:47:93), Dst: Tp-LinkT_a6:8b:34 (ac:84:c6:a6:8b:34)

▶ Internet Protocol Version 4, Src: 192.168.100.2, Dst: 45.32.162.254

▶ Transmission Control Protocol, Src Port: 35980, Dst Port: 38591, Seq: 14, Ack: 13, Len: 598

▼ Socks Protocol

- [Version: 5]
- [Command: Connect (1)]
- [Remote Address: 179.0.132.58]
- [Remote Port: 80]
- TCP payload (598 bytes)

▼ Hypertext Transfer Protocol

- ▶ GET / HTTP/1.1\r\n
- Host: ingenieria.uncuyo.edu.ar\r\n
- User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0\r\n
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n

Nota: Para capturar paquetes SOCKS con wireshark se debe configurar el puerto utilizado para la comunicación con el servidor Proxy (Edición -> Preferencias -> Protocolos -> Socks).

Ejemplo con servidor proxy SOCKS5 con IP 45.32.162.254 y puerto 38591.

No.	Time	Source	Destination	Protocol	Length	Source port	Dest Port	Information
• 1261	108.044795968	45.32.162.254	192.168.100.2	TCP	1494	1080	35980	Version: 5 [TCP s
• 1266	108.429768484	45.32.162.254	192.168.100.2	HTTP	158	1080	35980	HTTP/1.1 200 OK
1268	108.430442696	192.168.100.2	45.32.162.254	HTTP	664	1080	38591	GET / HTTP/1.1
1288	108.858272101	192.168.100.2	45.32.162.254	Socks	69	58128	38591	Version: 5 Connec
1290	109.011947703	45.32.162.254	192.168.100.2	Socks	1494	1080	35980	Version: 5 [TCP s
1291	109.011948017	45.32.162.254	192.168.100.2	TCP	86	1080	35980	Version: 5 [TCP s
1296	109.088019433	45.32.162.254	192.168.100.2	TCP	1494	1080	35980	Version: 5 [TCP s
1300	109.088019433	45.32.162.254	192.168.100.2	TCP	1494	1080	35980	Version: 5 [TCP s

▶ Frame 1266: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface wlo1, id 0

▶ Ethernet II, Src: Tp-LinkT_a6:8b:34 (ac:84:c6:a6:8b:34), Dst: LiteonTe_59:47:93 (24:fd:52:59:47:93)

▶ Internet Protocol Version 4, Src: 45.32.162.254, Dst: 192.168.100.2

▶ Transmission Control Protocol, Src Port: 38591, Dst Port: 35980, Seq: 15564, Ack: 612, Len: 92

▼ Socks Protocol

- [Version: 5]
- [Command: Connect (1)]
- [Remote Address: 179.0.132.58]
- [Remote Port: 80]
- TCP payload (92 bytes)
- TCP segment data (92 bytes)

▶ [12 Reassembled TCP Segments (15643 bytes): #1162(1428), #1163(1428), #1206(1271), #1209(1428), #1211(

▼ Hypertext Transfer Protocol

- ▶ HTTP/1.1 200 OK\r\n
- Server: openresty\r\n
- Date: Sat, 03 Jun 2023 21:13:52 GMT\r\n
- Content-Type: text/html; charset=UTF-8\r\n



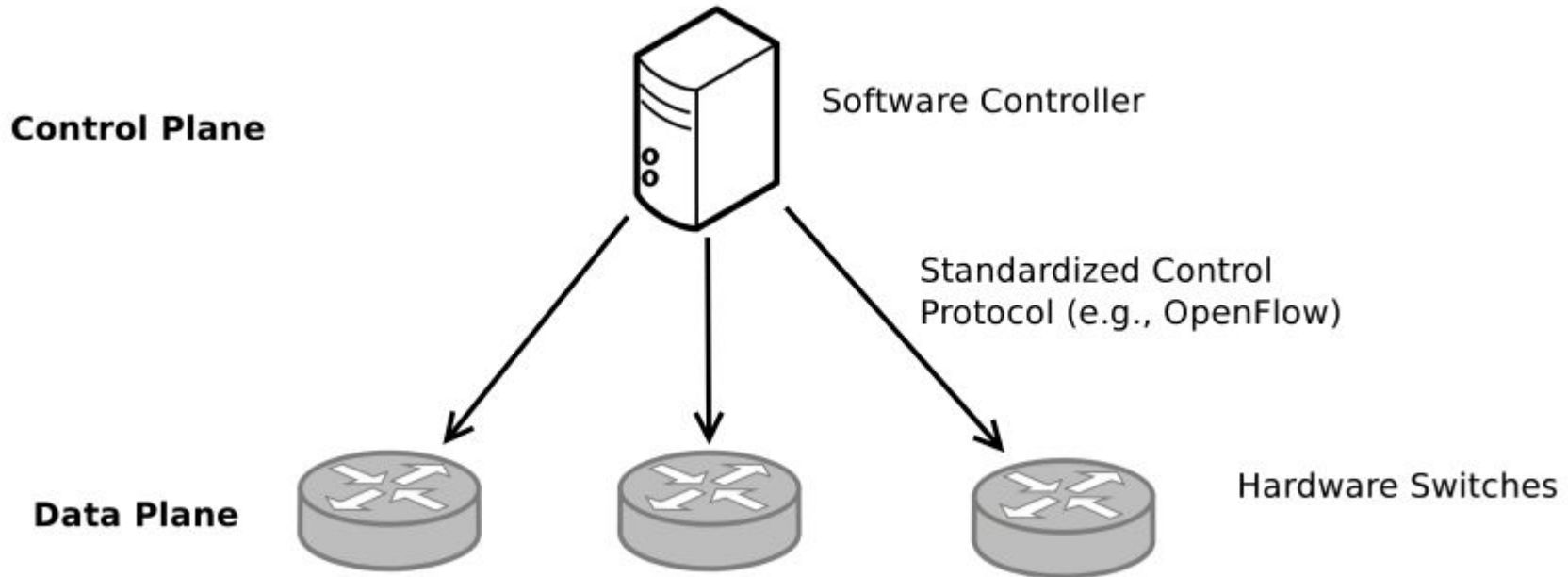
SDN (Software Defined Networking) en redes WAN

- **Necesidades** que surge con el avance de las redes y su uso comercial:
 - Proveedores necesitan proveer **calidad de servicio**.
 - Diferentes tipos de datos requieren diferente calidad de servicio.
 - Diferentes **servicios** con diferentes **tarifas**.
 - Diferentes rutas con diferentes velocidades.
 - **Interconexión con diferentes ISPs según costo y calidad de servicio.**
 - Las **variables de performance** que definen las rutas **cambian continuamente**.
 - Las rutas cambian todo el tiempo.
 - rebalanceo de tráfico.
 - cambios en el ruteo en la red propia como entre redes.
 - **La interacción entre redes y el comportamiento de la red propia es casi imposible de predecir.**

SDN (Software Defined Networking) en redes WAN

- SDN: concepto clave:
 - El **plano de control** y el **plano de datos** pueden operar de forma **totalmente separada**:
 - Plano de control: algoritmos que crean y seleccionan rutas (tarea de los algoritmos de ruteo).
 - Plano de datos: sistemas que reenvían paquetes en función de los campos y las tablas de ruteo.
- El software que implementa el plano de control no necesita correr en los equipos que conforman la red (routers).

SDN (Software Defined Networking) en redes WAN



Arquitectura típica de una SDN: El software de control corre en un sistema central que toma decisiones y las comunica a los dispositivos del plano de datos.

SDN (Software Defined Networking) en redes WAN

- Comunicación entre el plano de control y el plano de datos:
 - Puede ser cualquier protocolo o sistema que los dispositivos de red entiendan.
 - BGP fue uno de los primeros mecanismos.
 - Luego se crearon otras tecnologías: OpenFlow, NETCONF, YANG.
- Componentes de una SDN:
 - Tecnología que implementa el plano de control (software en lenguajes comunes como Python, Java o C).
 - Tecnología que hace el plano datos configurable (hardware programable y mecanismos que permiten configurar como los routers reenvían paquetes)
 - Telemetría de red.

SDN

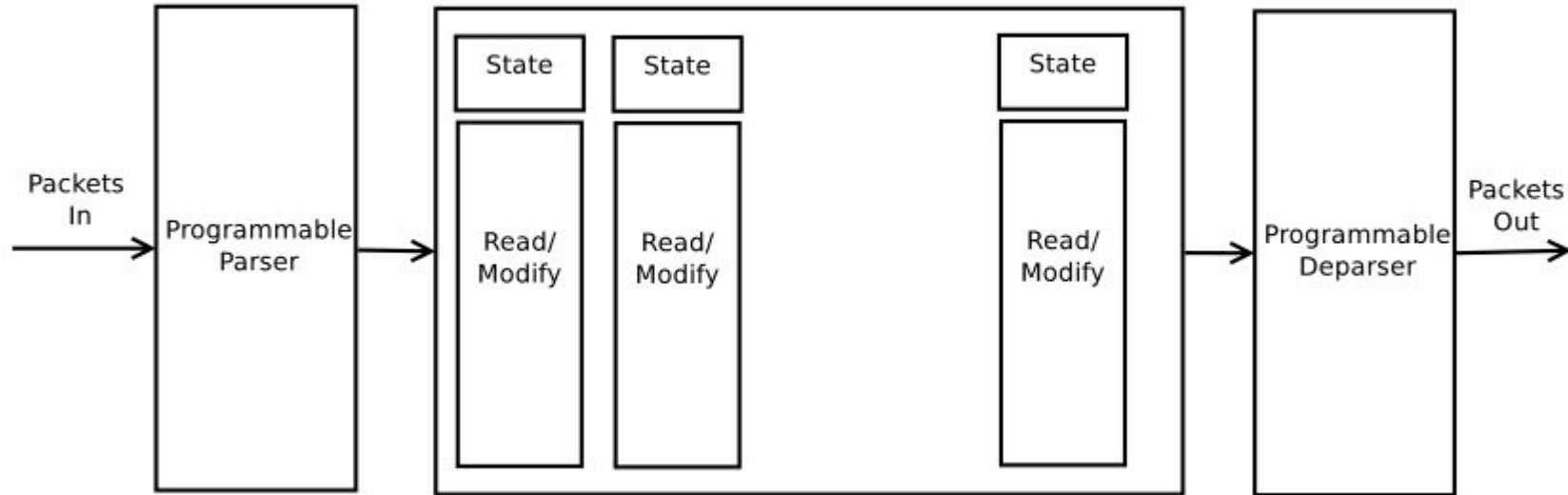
Planos de control

- **OpenFlow.**

- Primeras versiones: match-action table en los conmutadores: permitían indicar a los conmutadores tomar determinadas acciones en función de las direcciones IP o MAC de los paquetes:
 - Enviarlos a algún puerto de salida.
 - Descartarlos.
 - Pedir a un controller decidir que hacer con el paquete.
- Incorporaciones posteriores:
 - Posibilidad de expresar operaciones combinatorias más complejas.
 - Añadir la variable tiempo.
 - Utilización de lenguajes de alto nivel (Python y Java).

SDN

Stages



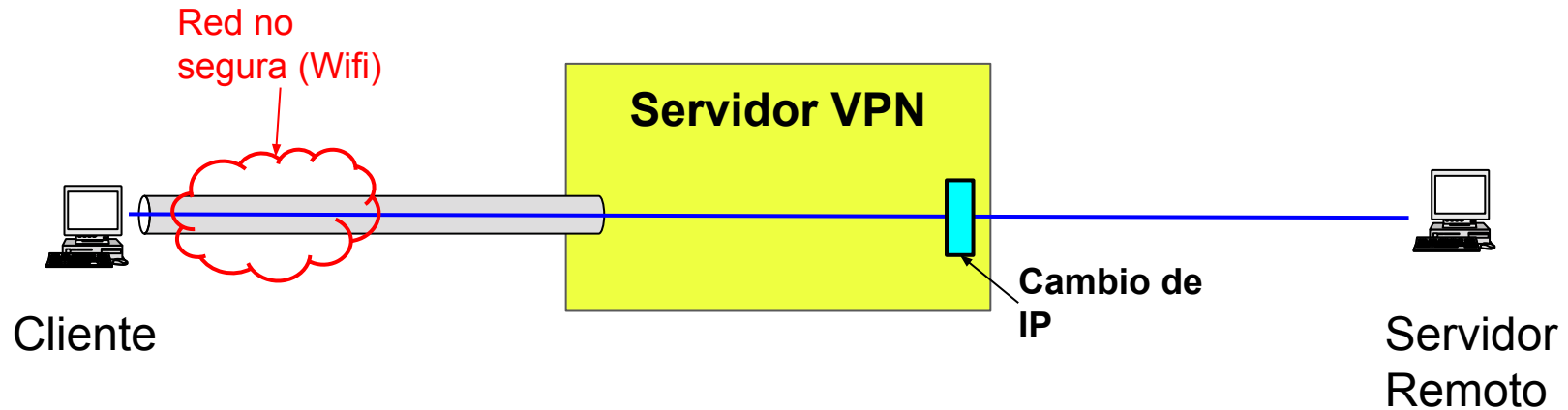
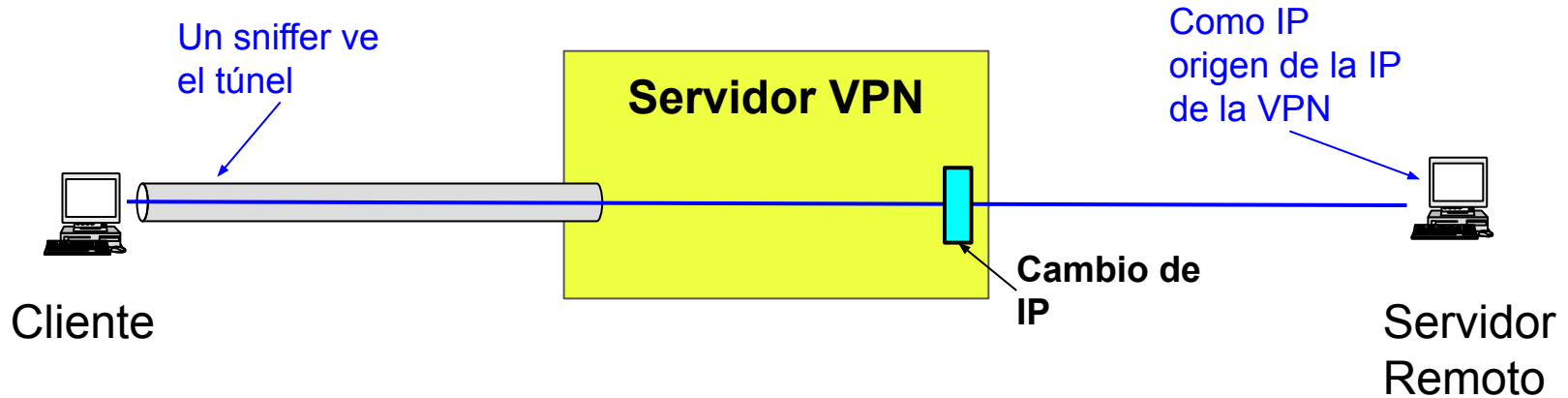
- Los programadores pueden definir match-tables de tamaño arbitrario.

VPN (Red privada virtual)

- **Red virtual** que funciona sobre una **red o red de redes real**.
 - La red virtual y la red real pueden ser de igual o diferente tecnología.
 - La red virtual y la red real pueden pertenecer a la misma capa o a diferentes capas del modelo OSI.
- Utilizan **encapsulamiento** y **tunelización**.
 - Pueden encapsular cualquier protocolo de cualquier capa en cualquier otro protocolo de cualquier otra capa.
- **Objetivos:**
 - Seguridad: utilizar encriptación segura sobre una red no segura (por ejemplo: Wifi).
 - Anonimato: Que un sniffer local no pueda ver las IPs a las que se accede o un servidor remoto no pueda obtener la IP del usuario.
 - Evadir firewalls, proxies con restricciones o restricciones geográficas.
 - Transición IPv6 sobre redes IPv4.
 - Utilizar software desarrollado para redes LAN sobre Internet.

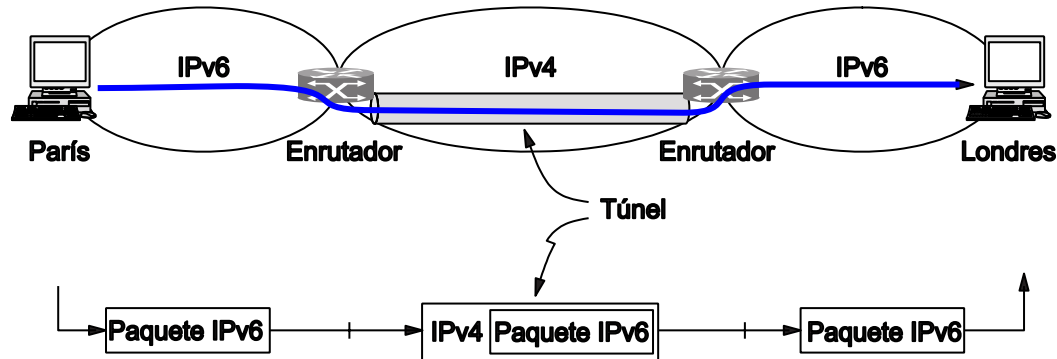
VPN comerciales que proveen seguridad, anonimato y/o evasión de restricciones geográficas

- Proveen un túnel entre la computadora del cliente y el proveedor.
 - Usualmente poseen servidores distribuidos geográficamente.
- Topologías punto a punto.
- Utilizan encapsulación, encriptación y/o anonimato.
 - IPsec, IP sobre TCP, IP sobre TSL o SSL.
- Requieren instalar software en la computadora del cliente que captura el tráfico y lo tuneliza.
- Ejemplos: <https://www.expressvpn.com>, <https://cyberghost.com.vpncenter.com>



VPN para transición IPv4 a IPv6

- Encapsulan paquetes IPv6 sobre paquetes IPv4.
- Ejemplo: Teredo.





VPN para desplegar redes LAN sobre Internet

- Objetivo: Ejecutar software (**juegos**) desarrollado para trabajar sobre redes LAN en Internet.
- Encapsulan tramas Ethernet sobre TCP, UDP o IP.
- Ejemplo: Hamachi (<https://vpn.net/>).
 - Encapsula tramas Ethernet sobre IP: