UNIDAD I.

Anatomía de Sistemas en Red

1.1 Introducción
1.2 Ejemplos de sistemas en red
1.3Protocolos de Internet
1.4Protocolos de transporte
1.5Calidad de servicio y control de tráfico
    1.5.1 Requerimientos de aplicaciones
    1.5.2 Modelado de trafico
    1.5.3 Servicios integrados y diferenciados

1.1 Introducción

Sistemas en red

El término Sistemas en red en este curso está relacionado con la tecnología y arquitecturas de redes de comunicaciones que permiten interconectar dispositivos de comunicación.
En este campo se encuentran las Redes de computadoras, la telefonía móvil, las redes personales, entre otras.

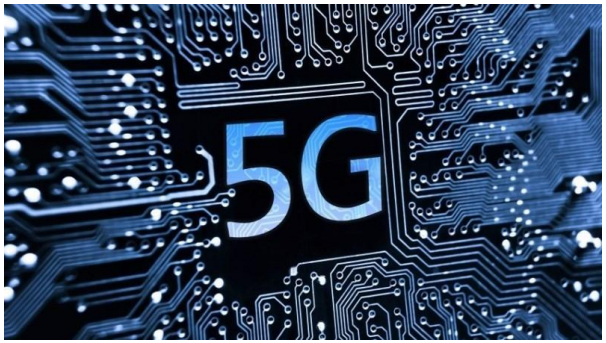
Las tendencias en la actualidad muestran que las telecomunicaciones efectivas y eficientes hoy en día son vitales para cualquier empresa u organización.

De acuerdo a Stallings *, tres factores claves han impactado la evolución de los sistemas en red:

*Stallings, William. *Data and computer communications*. Pearson/Prentice Hall, 2012.

1) Nuevos Servicios

Los usuarios desean cada vez mayor cantidad y variedad de servicios. Por ejemplo la utilización de servicios mas rápidos y de mejor calidad en los dispositivos móviles. De igual manera las redes cableadas terrestres son cada vez mas demandas para servicios públicos y privados, tales como redes de alta seguridad para transacciones bancarias, entre otras.



2) El aumento en el tráfico

En las ultimas décadas el trafico tanto local (en el mismo edificio) como remoto (a lugares distintos) ha aumentado rápidamente. Esta tendencia continuará por mucho tiempo, ya que cada vez son mayores las transacciones en línea, trabajo colaborativo, control remoto y transmisiones tanto de voz como video requeridas para el funcionamiento de una organización. La figura 1 (fuente: stallings) muestra el aumento importante en los tipos de trafico mas utilizados.

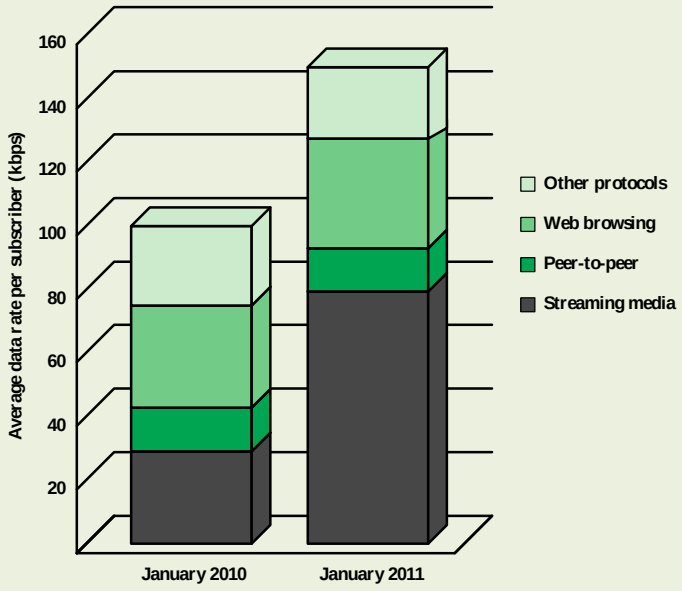


Figure 1.1 Average Downstream Traffic per Internet Subscriber

3) Avances en la tecnología

Las tendencias tecnológicas permiten proveer capacidad para el aumento del trafico y la gran variedad de servicios demandados. Pueden destacarse 4 tendencias tecnológicas actuales:

Computadoras y sistemas de comunicación mas rápidos pero mas económicos.

- Las computadoras y dispositivos son cada vez mas poderosos.
- El incremento en el uso de fibra óptica y sistemas inalámbricos de alta velocidad ha bajado precios y aumentado las capacidades de transmisión.

Las redes actuales son mas “inteligentes”

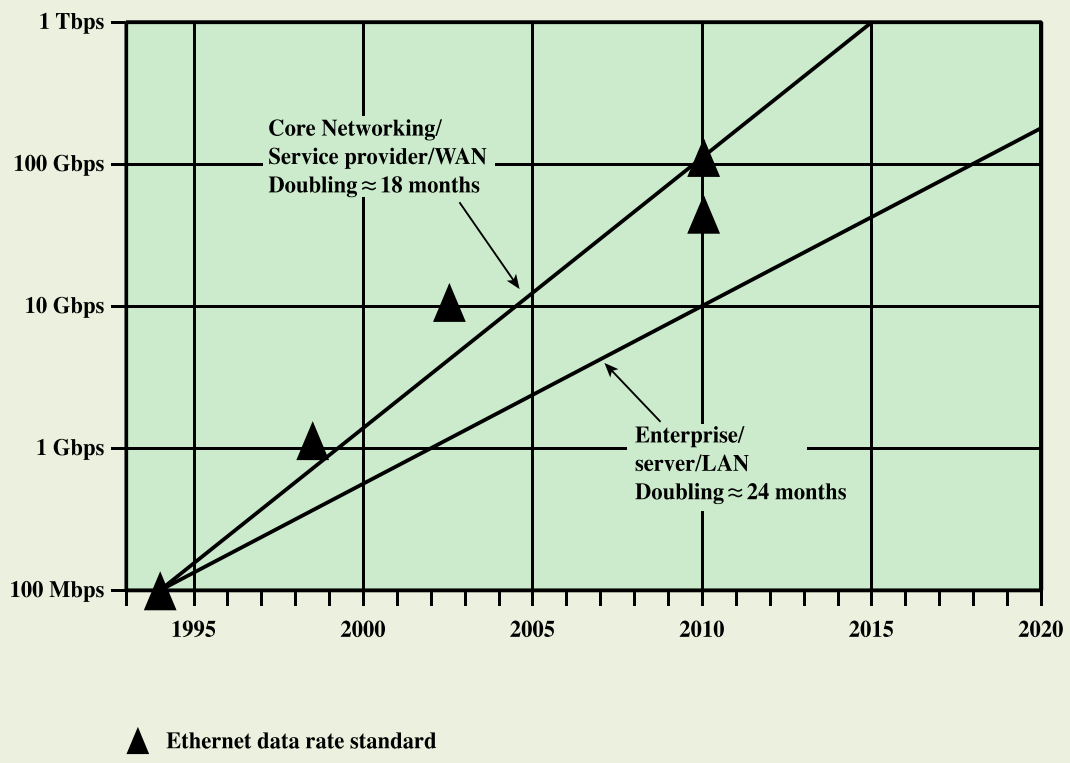
- Pueden ofrecer diferentes niveles en base a la calidad de servicio requerida(Quality of Service, QoS)
- Servicios personalizables en cuanto a requerimientos de seguridad y capacidad.

Internet, el Web y las aplicaciones emergentes asociadas se han convertido en las características dominantes para las organizaciones y sistemas personales.

- “Todo sobre IP”
- Intranets y extranets están siendo utilizadas para manejar información sensible de manera aislada.

Movilidad

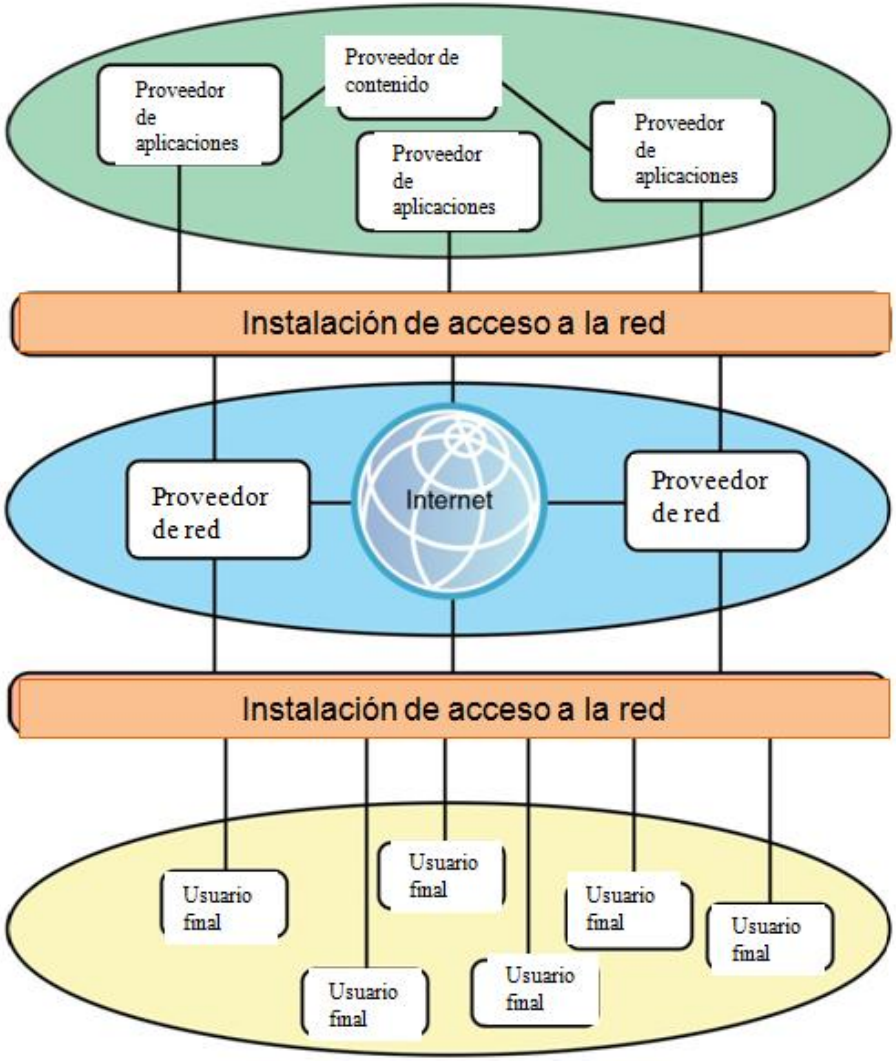
- iPhone, Droid, iPad , tabletas, son cada vez mas requeridos en los diferentes entornos.
- El computo en la nube es una tendencia general.



Crecimiento visto y proyectado en el aumento de las tasas de transmisión en Ethernet

La siguiente figura (fuente: IEEE), muestra como ha aumentado la demanda en los servicios de Ethernet. Los servicios demandos en la red dorsal se duplican aprox. Cada 18 meses, mientras que los servicios que requieren las empresas se duplican aprox. Cada 24 meses.

Ecosistema de redes

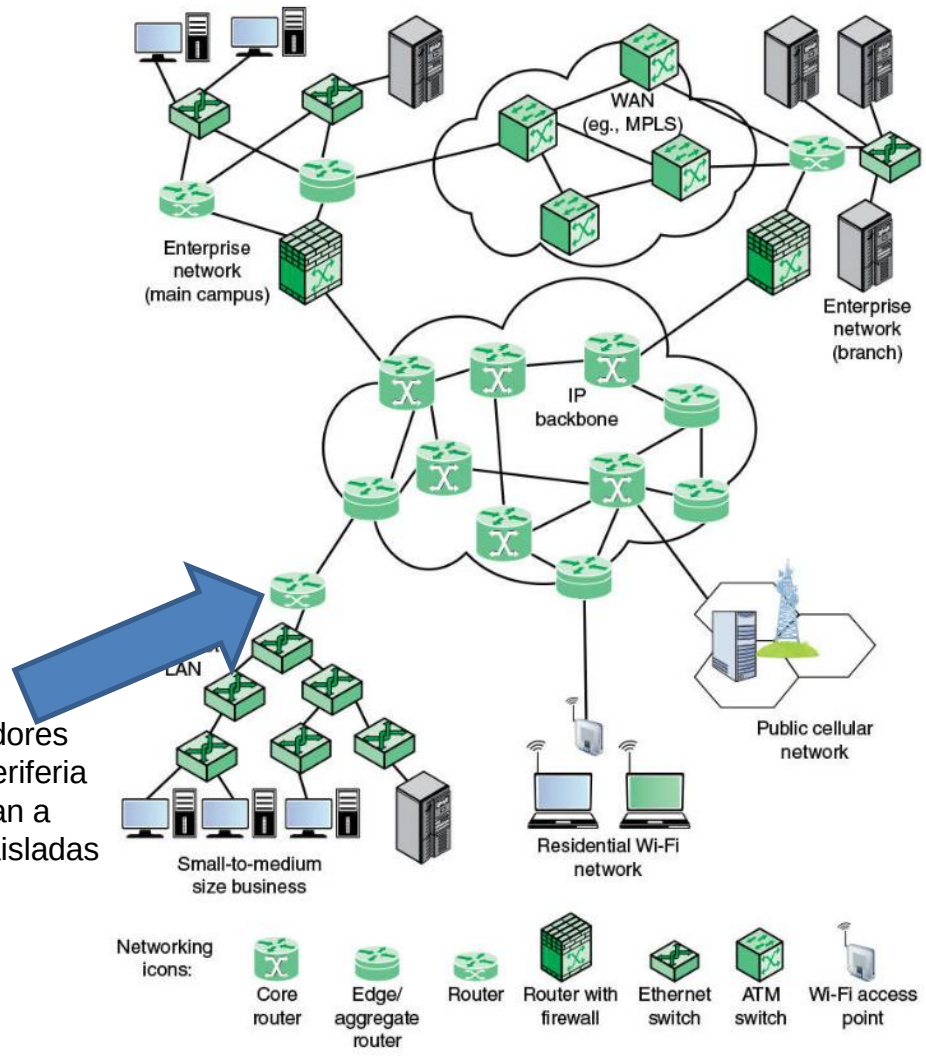


En la figura puede observarse lo que se ha denominado el ecosistema de Redes Modernas.
La finalidad del ecosistema es proveer servicios al usuario final. El usuario puede ser fijo o móvil (PC, tableta, teléfono móvil).
Diversas instalaciones de red permite el acceso al contenido y aplicaciones a través de distintas redes y proveedores (DSL, GSM, WiMax, WiFi, 4G, etc.)

Los proveedores finales pueden proporcionar:

-Acceso directo a aplicaciones (descarga de apps)
-Acceso a contenido para aplicaciones (servidores Web, e-mail, mapas, música, etc.)
-Acceso a contenido (cobran por el contenido descargado, no por el acceso a la aplicación)

Ejemplo de arquitecturas de sistemas en red

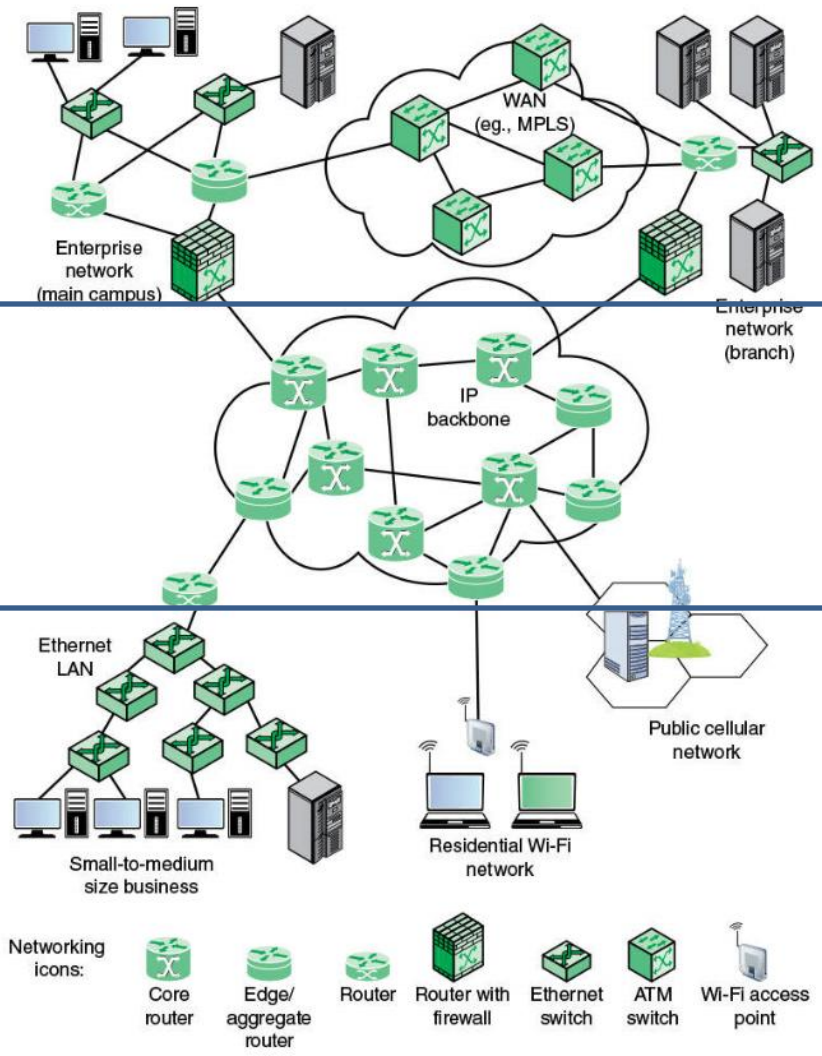


Enrutadores en la periferia conectan a redes aisladas

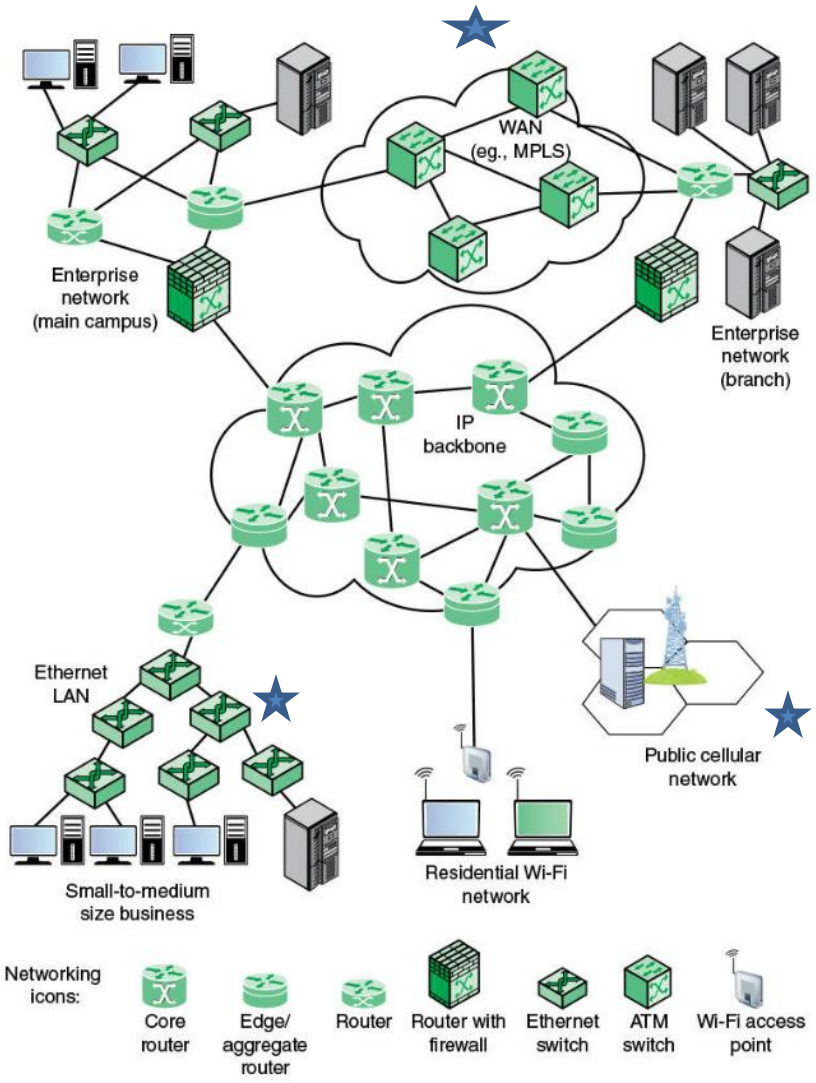
Sistema global (fuente: Stallings)

En un sistema global pueden observarse como se utilizan e interactúan diversos sistemas en red.:

Ejemplo de arquitecturas de sistemas en red

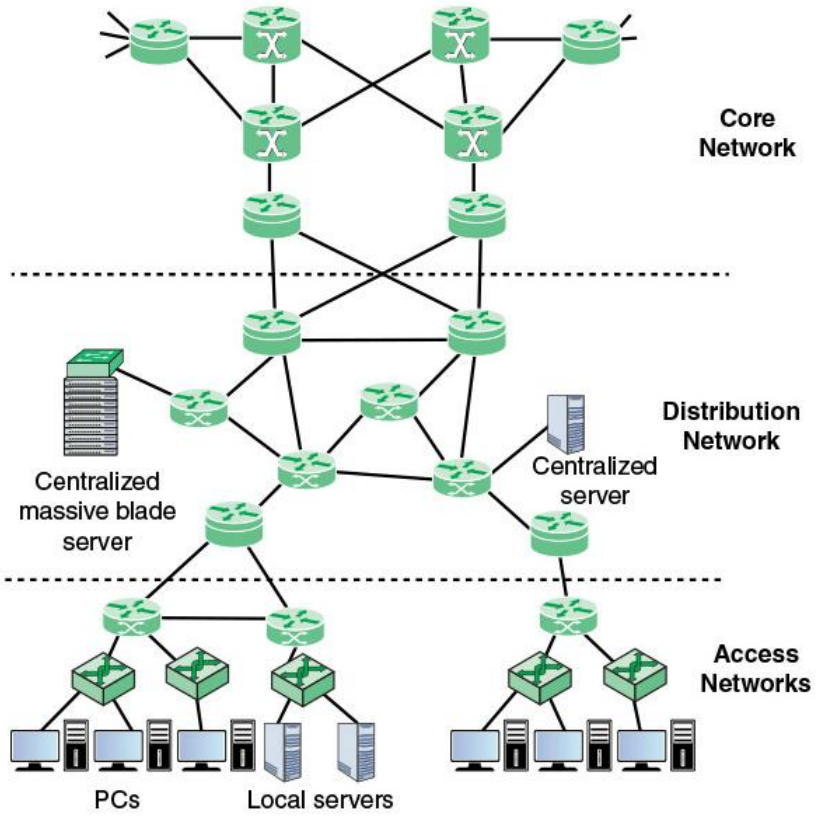


El centro de la red, representa el sistema dorsal, formado por enrutadores con alta capacidad de procesamiento y servicios de red cableada, normalmente de fibra óptica.



Dentro de las organizaciones, existen redes privadas (MPLS), usuarios móviles, y redes LAN que utilizan y proveen contenido.

Organización de sistemas en red



La organización típica en un sistema en red se muestra en la figura.
Normalmente consiste en tres niveles:
-**Red de acceso:**
Es la mas cercana al usuario final, incluye los dispositivos finales (PCs, dispositivos móviles) y servidores centrales. También incluye enrutadores para conectar la red al siguiente nivel

-Red de distribución.
Permite la interconexión de redes múltiples ubicadas en el nivel inferior y acceso a la red núcleo. Puede consistir en Internet o redes privadas de mayor seguridad.

-**Red núcleo**, conocida también como red dorsal permite la conexión de redes geográficamente dispersas. Consiste en servidores y enrutadores de muy alta capacidad. También incluye infraestructura de alta velocidad, normalmente fibra óptica.

1.2 Ejemplos de sistema en red

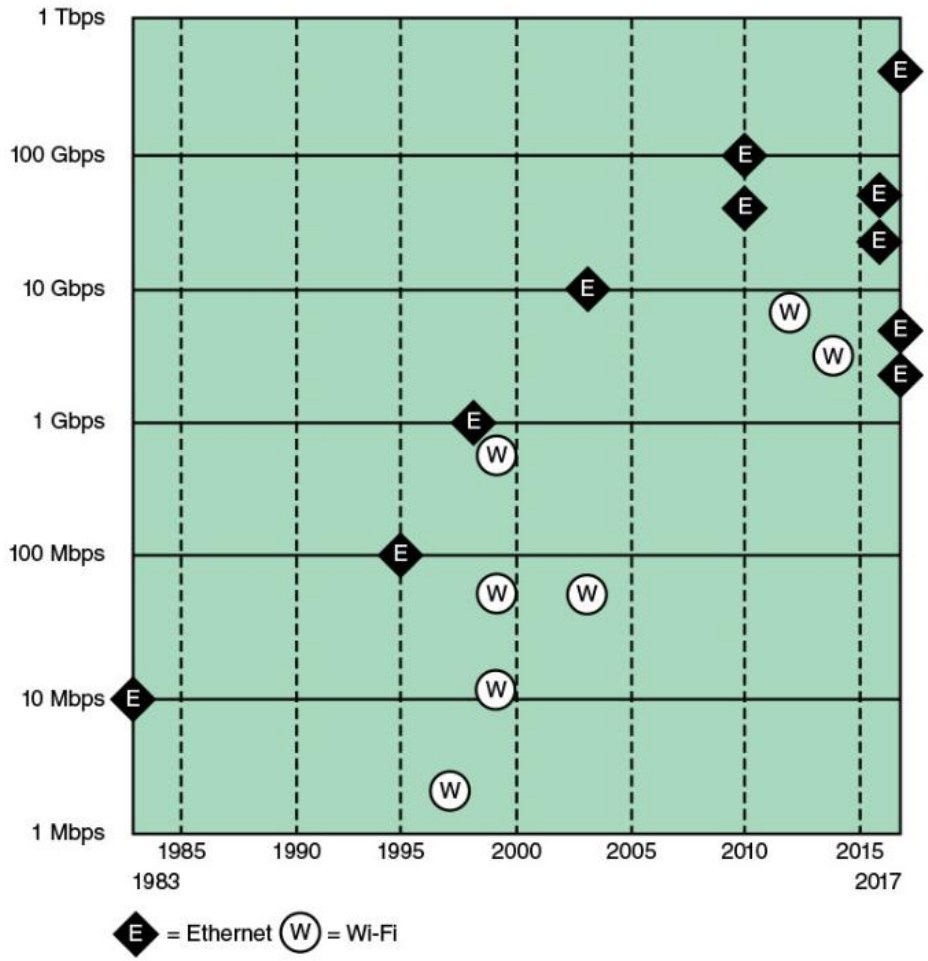
Como se observo anteriormente, en un entorno global, múltiples tipos de sistemas en red pueden interconectarse. Entre ellas se encuentran:

a) Redes Ethernet

Ethernet es la tecnología predominante para la implementación de sistemas en red cableados. Se utiliza en casas, oficinas, empresas y entornos globales. Es el estándar que mas ha evolucionado. Inicialmente soportaba 10Mbps, hoy en día alcanza velocidades de hasta 100 Gbps.

b) Redes WiFi

El estándar en la implementación de redes inalámbricas locales es hoy en día WiFi o IEEE 802.11. Es utilizada tanto en el hogar, como oficinas y empresas. Permite interconectar no solo PCs, si no también tabletas, teléfonos, televisiones, refrigeradores, etc.). IEEE 802.11 en sus estándares a,b,g, n y recientemente ac permite velocidades de 11 Mbps hasta 3.2 Gbps



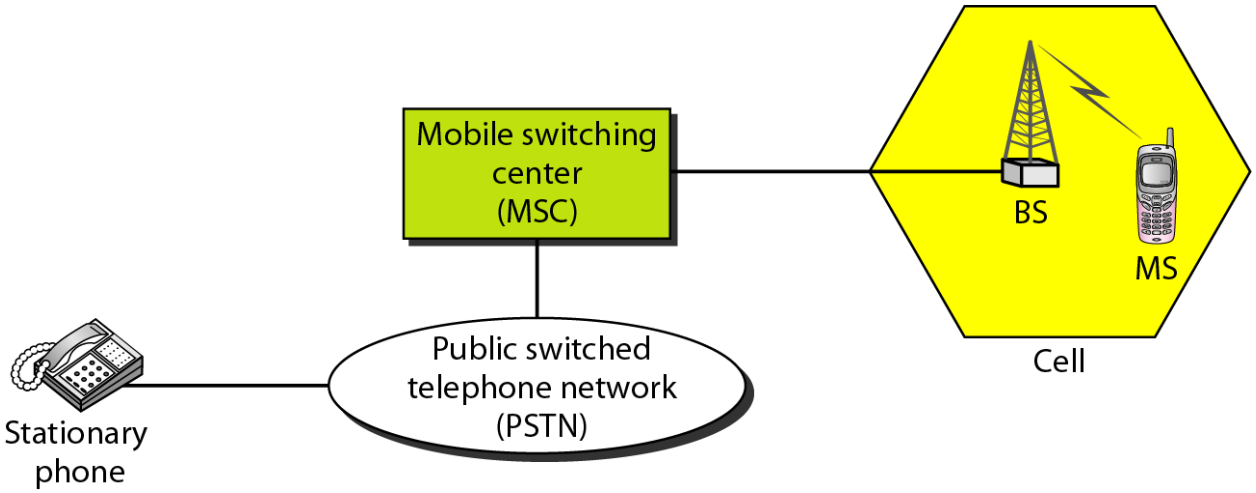
Las diferentes versiones de Ethernet y WiFi proveen soluciones con diferentes capacidades.

WiFi tiene la desventaja de ser sensible a interferencias y obstáculos, por lo que normalmente la red esta confinada y con menor alcance.

Ambas han lograda convivir ya que Ethernet permite aumentar el alcance de WiFi, incluso con nuevos estándares como Power Line Carrier (PLC) y Power over Ethernet (PoE), que permiten transmitir datos utilizando las líneas de corriente eléctrica.

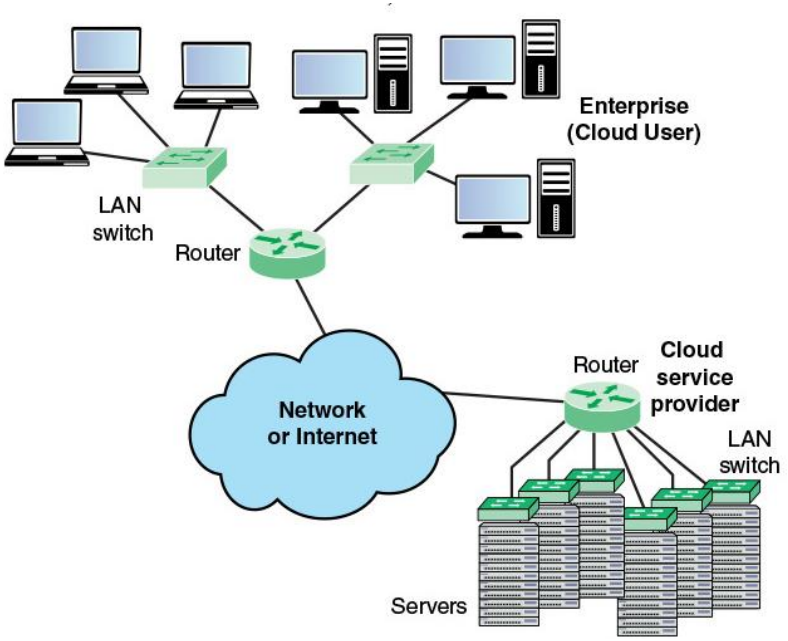
c) Tecnología celular

La redes de telefonía celular permiten el acceso en lugares remotos, en donde no hay alcance para redes inalámbricas o cableadas. La evoluciones de la tecnología celular se ha clasificado en generaciones. La primera generación consistía únicamente en llamadas de voz. A partir de la segunda generación comenzaron a surgir servicios como mensajes de texto y posibilidad de revisar e-mail.
Hoy en día se espera el lanzamiento de la 5ta generación, en donde todo el trafico será a través de IP y las tasas de transmisión permiten la incorporación de servicios novedosos.



d) Cómputo en la nube

El concepto de cómputo en la nube consiste en mover servicios de una empresa u organización a una infraestructura disponible a través de Internet. Aunque el concepto existe desde 1950, ha sido hasta el año 2000 que se ha implementado consistentemente y hoy en día es una tendencia mundial.
El cómputo en la nube basa su funcionamiento en sistemas en red de diversos tipos, ya que no solo se utiliza a nivel empresarial, si no que los individuos la utilizan para fines personales como almacenamiento de fotos y archivos desde dispositivos móviles.



e) Internet de las cosas

Internet de las Cosas (Internet of things, IoT), es el desarrollo más actual en el tema de Sistemas en Red. Permite la interconexión de dispositivos inteligentes, los cuales pueden consistir en electrodomésticos, accesorios y hasta sensores diminutos. Permite la interconexión de estos elementos de manera pervasiva, con los usuarios finales que pueden ser personas o incluso otros dispositivos sin requerir intervención humana (Machine to Machine)

IoT representa la 4ta generación de Internet:

1era: Interconexión entre computadoras

2da. Maquinaria con posibilidad de conectarse a Internet (ej: equipo medico).

3era. Interconexión de dispositivos personales(ej: teléfonos, ipads, etc.)

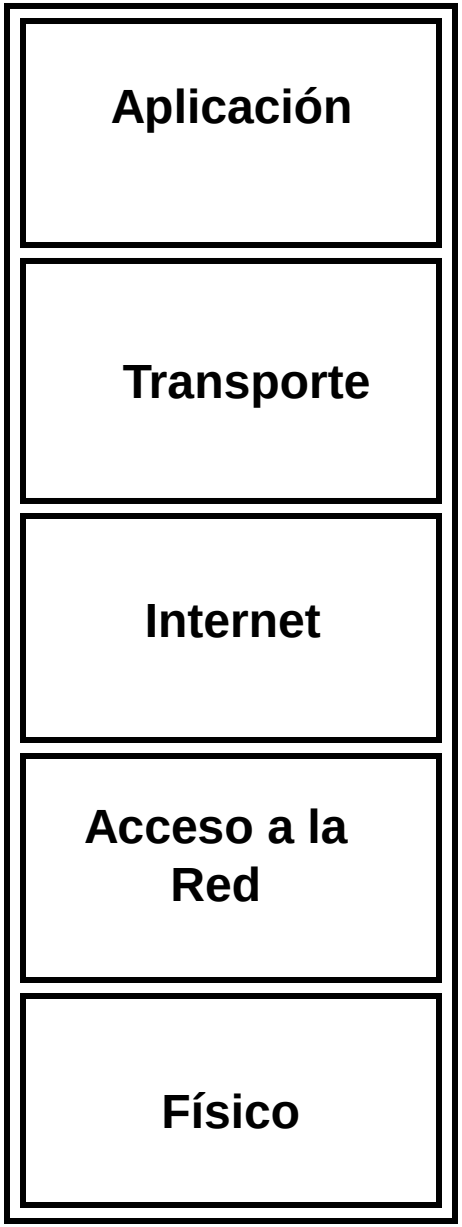
4ta. Interconexión de sensores y dispositivos inteligentes.

En un inicio los sistemas en red se clasificaban en base a sus funciones determinadas por el modelo OSI.

Hoy en día varias tecnologías de red basan su funcionamiento en el conjunto de protocolos TCP/IP

- El modelo de referencia OSI se ha convertido en el estándar para clasificar funciones de comunicación.
- **La implementación de protocolos se ha llevado a cabo en base al Modelo de Internet (Modelo TCP/IP).**

Modelo de Internet

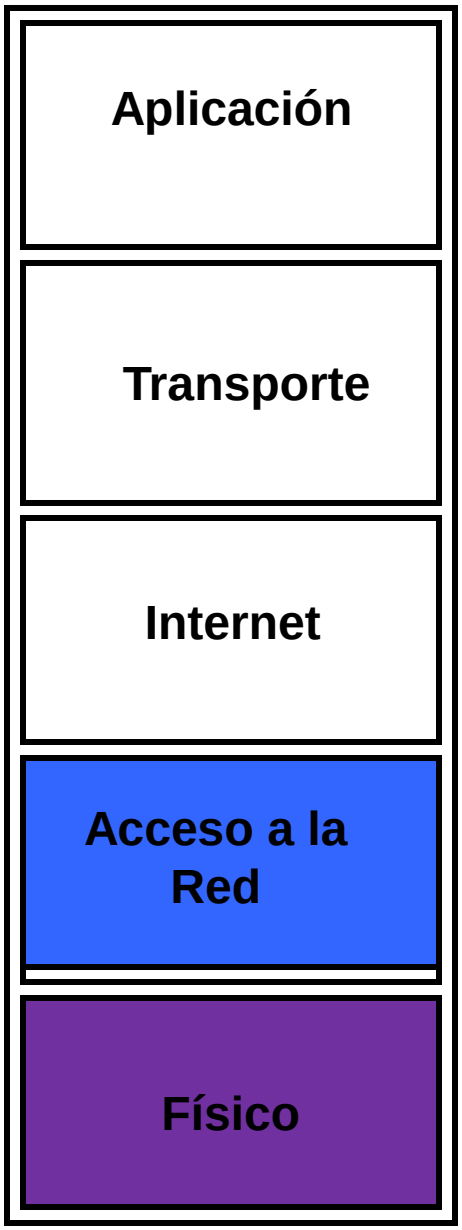


•El modelo de Internet es la arquitectura adoptada para la interconexión de sistemas, también conocido como arquitectura de protocolos TCP/IP.

•TCP/IP fue desarrollado en 1969 por la Agencia de Proyectos de Investigación Avanzada (ARPA) creadores de ARPANET.

•Similar al modelo OSI se divide en capas. Este modelo se compone de 5 capas: **Física, Acceso a la red, Internet, Transporte y Aplicación**.

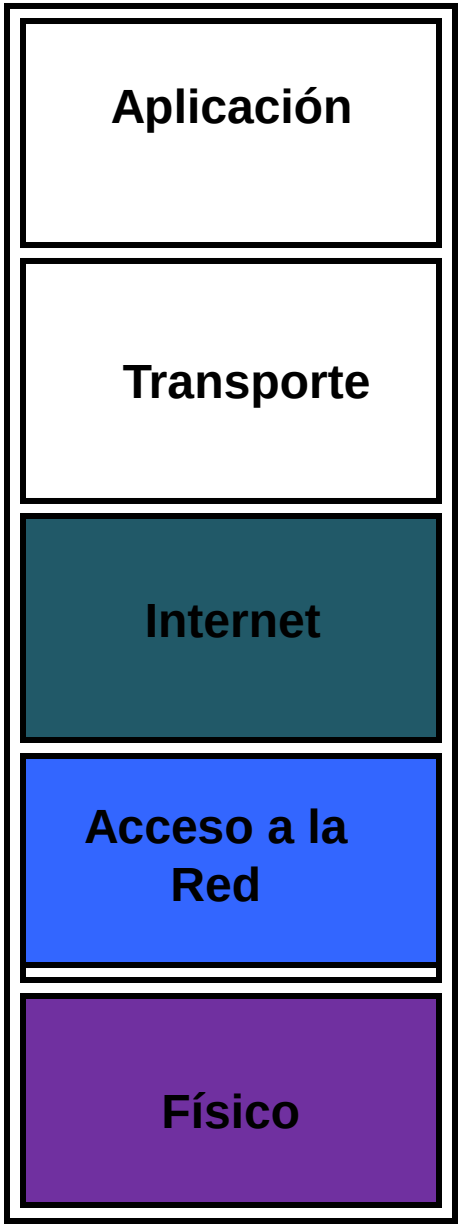
•Las dos ultimas capas muchas veces se unen en una sola: Acceso a la Red.



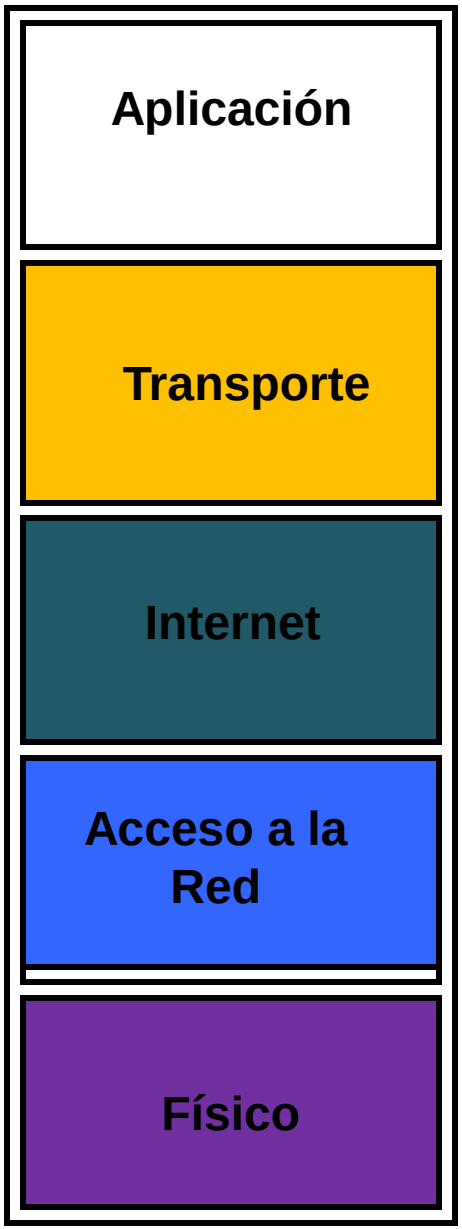
- La capa física se encarga únicamente del hardware: Cables, enlaces satelitales, interfaces de red, dispositivos de interconexión.
- Codificación y modulación si necesaria se llevan a cabo en esta capa.

La capa de Acceso a la Red se encarga de las técnicas de acceso al medio tales como: CSMA/CD, CSMA/CA y paso de testigo

Ethernet existe en las capas Física y de Acceso a la red – Su hardware en la capa física y la técnica de Acceso en la capa de Acceso a la red.

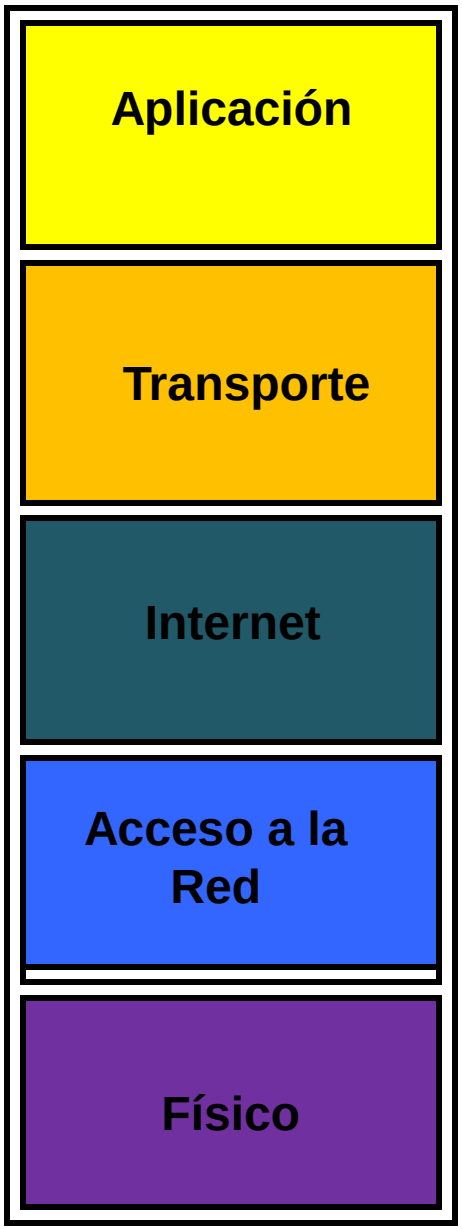


- La capa de Internet es responsable del enrutamiento y entrega de los datos a través de la red o redes.
- Permite la comunicación entre la misma o redes diferentes, además lleva a cabo traducciones para trabajar con diferentes tipos de direcciones de red.
- IP (Internet Protocol) y ARP (Address Resolution Protocol) Son protocolos de la capa de Internet



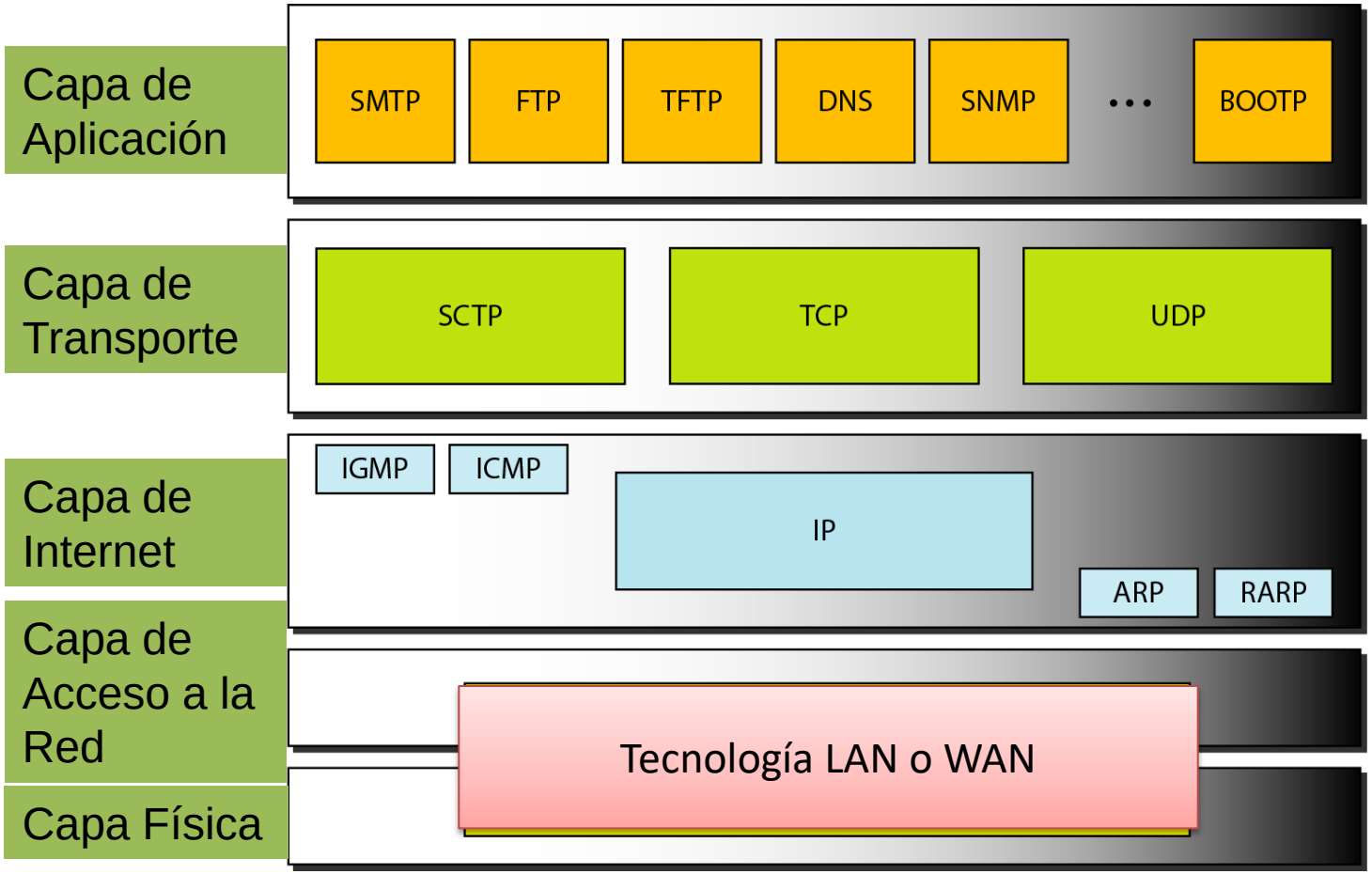
- La capa de transporte es similar a la capa de transporte del modelo OSI, pero incluye elementos de funcionalidad de la capa de Sesión del modelo OSI.

- Los tres protocolos que se encuentran en esta capa son:
  - TCP (Transmission Control Protocol): confiable, orientado a conexión, provee control de errores y control de flujo.
  - UDP (User Datagram Protocol): no seguro, no orientado a conexión que no provee control de errores ni de flujo.
  - SCTP (Stream Control Transmision Protocol), Diseñado para la transmisión de telefonía por Internet.



- Esta capa incluye funciones de las capas de sesión, presentación y aplicación del modelo OSI.
- Provee comunicación y capacidades de red a una aplicación
- Ejemplos:
  - Telnet
  - FTP
  - HTTP (Hyper Text Transfer Protocol)
  - SMTP (Simple Mail Transfer Protocol)

Modelo de Internet → Protocolos TCP/ IP



UNIDAD I.

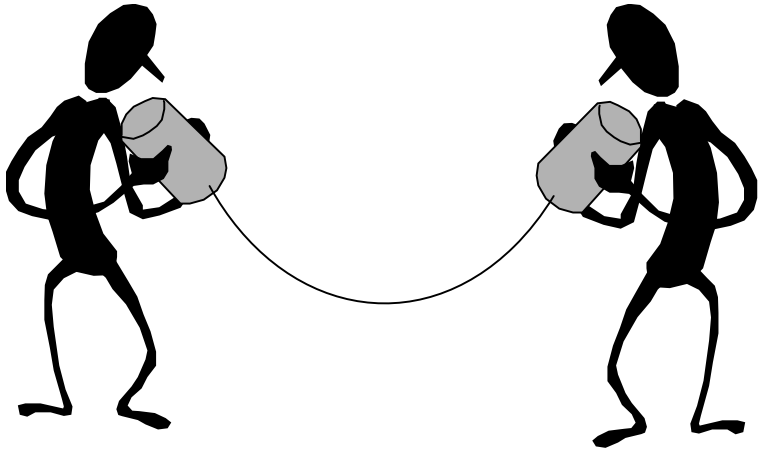
Anatomía de Sistemas en Red

1.1 Introducción
1.2 Ejemplos de sistemas en red
1.3Protocolos de Internet
1.4Protocolos de transporte
1.5Calidad de servicio y control de tráfico
    1.5.1 Requerimientos de aplicaciones
    1.5.2 Modelado de trafico
    1.5.3 Servicios integrados y diferenciados

Fuente de la presentacion:
Data and Computer Communications, Tenth Edition by William Stallings, (c) Pearson Education - Prentice Hall, 2013

Para destruir completamente la comunicación, no debe haber reglas en común entre el transmisor y el receptor- Tampoco alfabeto o sintaxis.

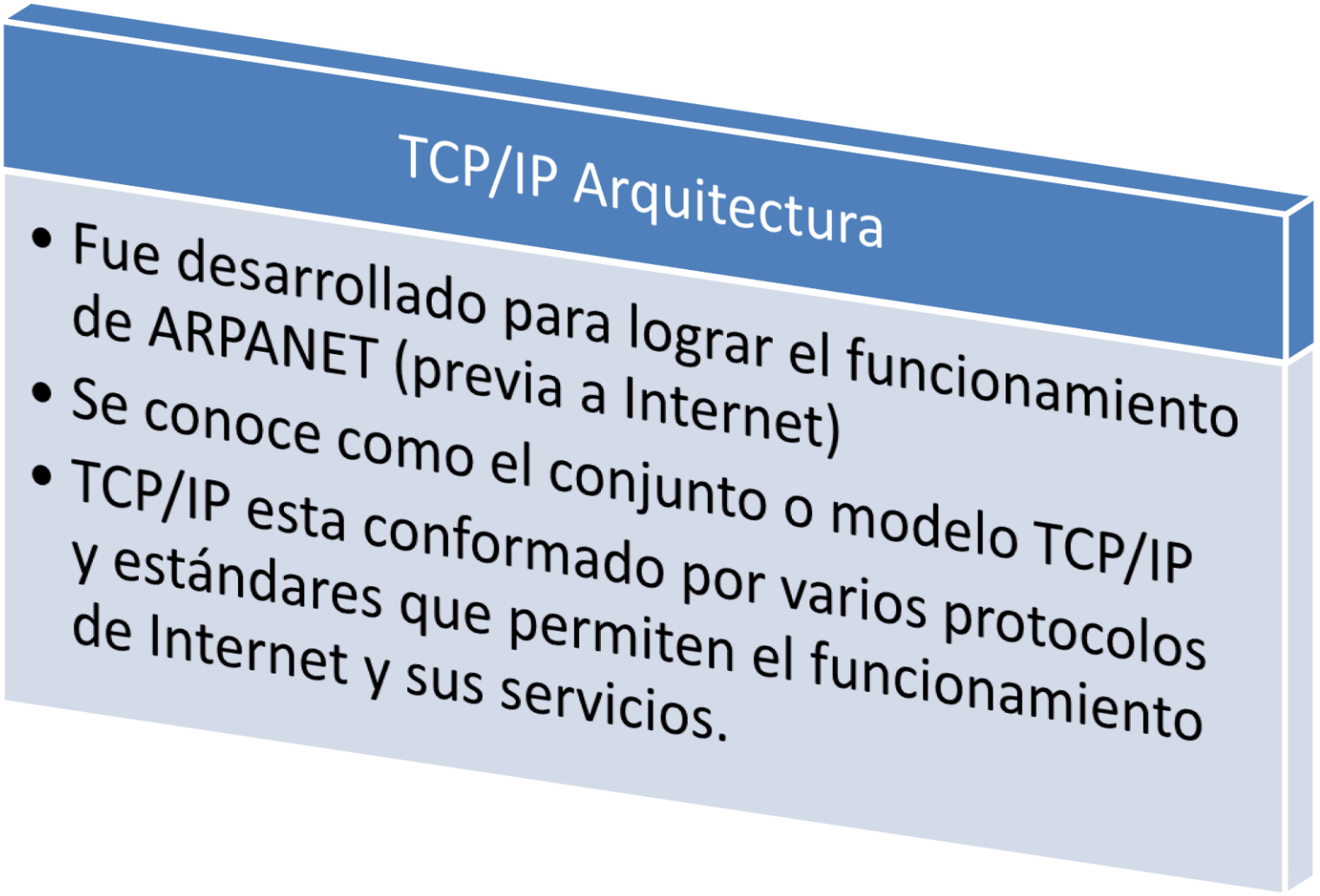
—En "Human Communication",
Colin Cherry

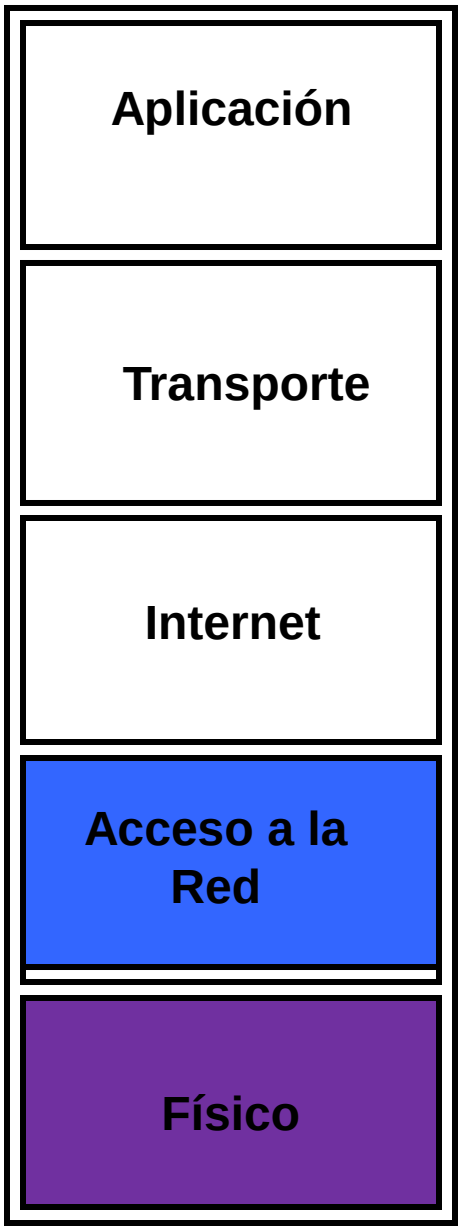


Similar, en los sistemas de comunicaciones debe haber reglas, éstas son establecidas por los protocolos.

Hoy en día, la base de los sistemas en red modernos esta dada por los protocolos que se encuentran en el Modelo TCP/IP

Arquitectura del protocolo TCP/IP

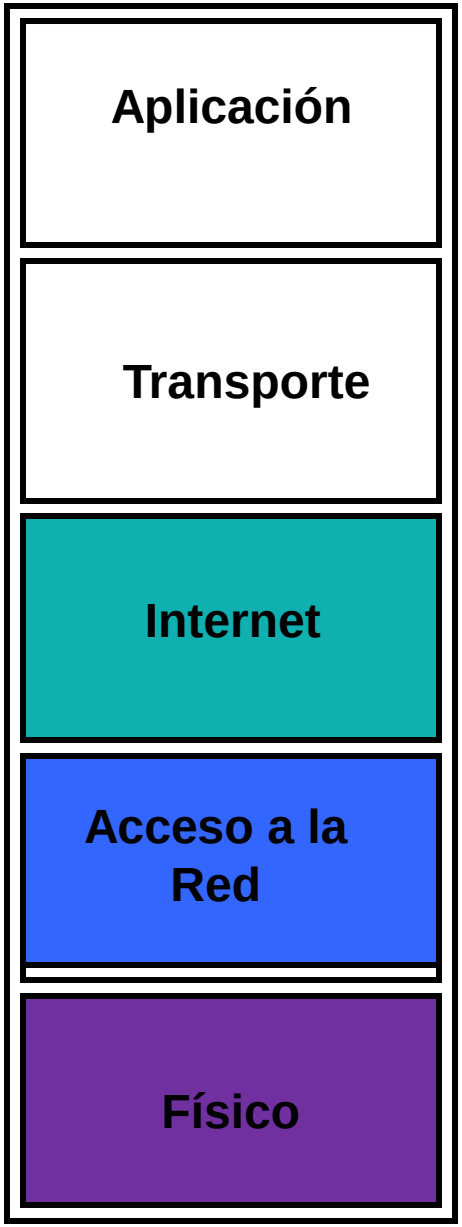




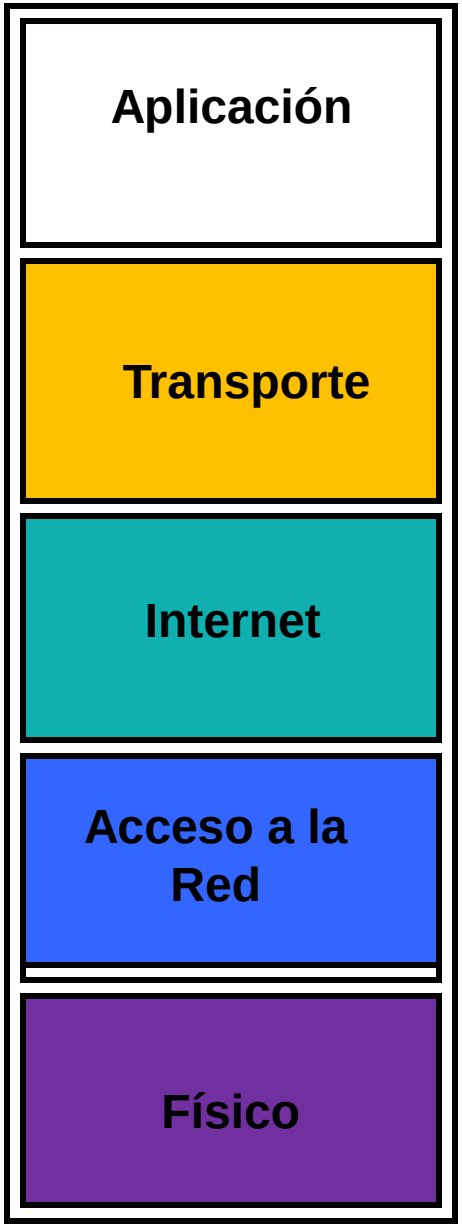
- La capa física se encarga únicamente del hardware: Cables, enlaces satelitales, interfaces de red, dispositivos de interconexión.
- Codificación y modulación si necesaria se llevan a cabo en esta capa.

La capa de Acceso a la Red se encarga de las técnicas de acceso al medio tales como: CSMA/CD, CSMA/CA y paso de testigo

Ethernet existe en las capas Física y de Acceso a la red – Su hardware en la capa física y la técnica de Acceso en la capa de Acceso a la red.

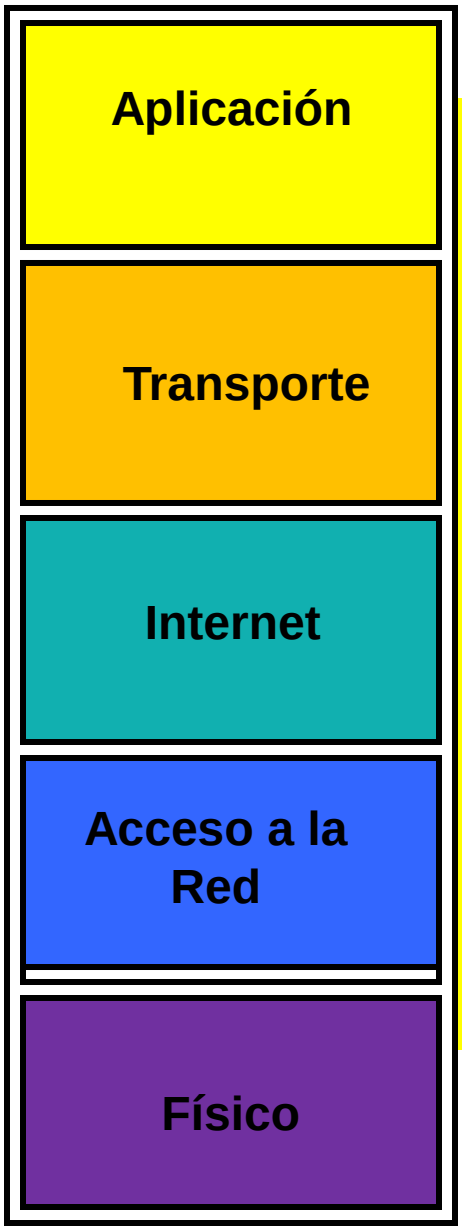


- La capa de Internet es responsable del enrutamiento y entrega de los datos a través de la red o redes.
- Permite la comunicación entre la misma o redes diferentes, además lleva a cabo traducciones para trabajar con diferentes tipos de direcciones de red.
- IP (Internet Protocol) y ARP (Address Resolution Protocol) Son protocolos de la capa de Internet



- La capa de transporte es similar a la capa de transporte del modelo OSI, pero incluye elementos de funcionalidad de la capa de Sesión del modelo OSI.

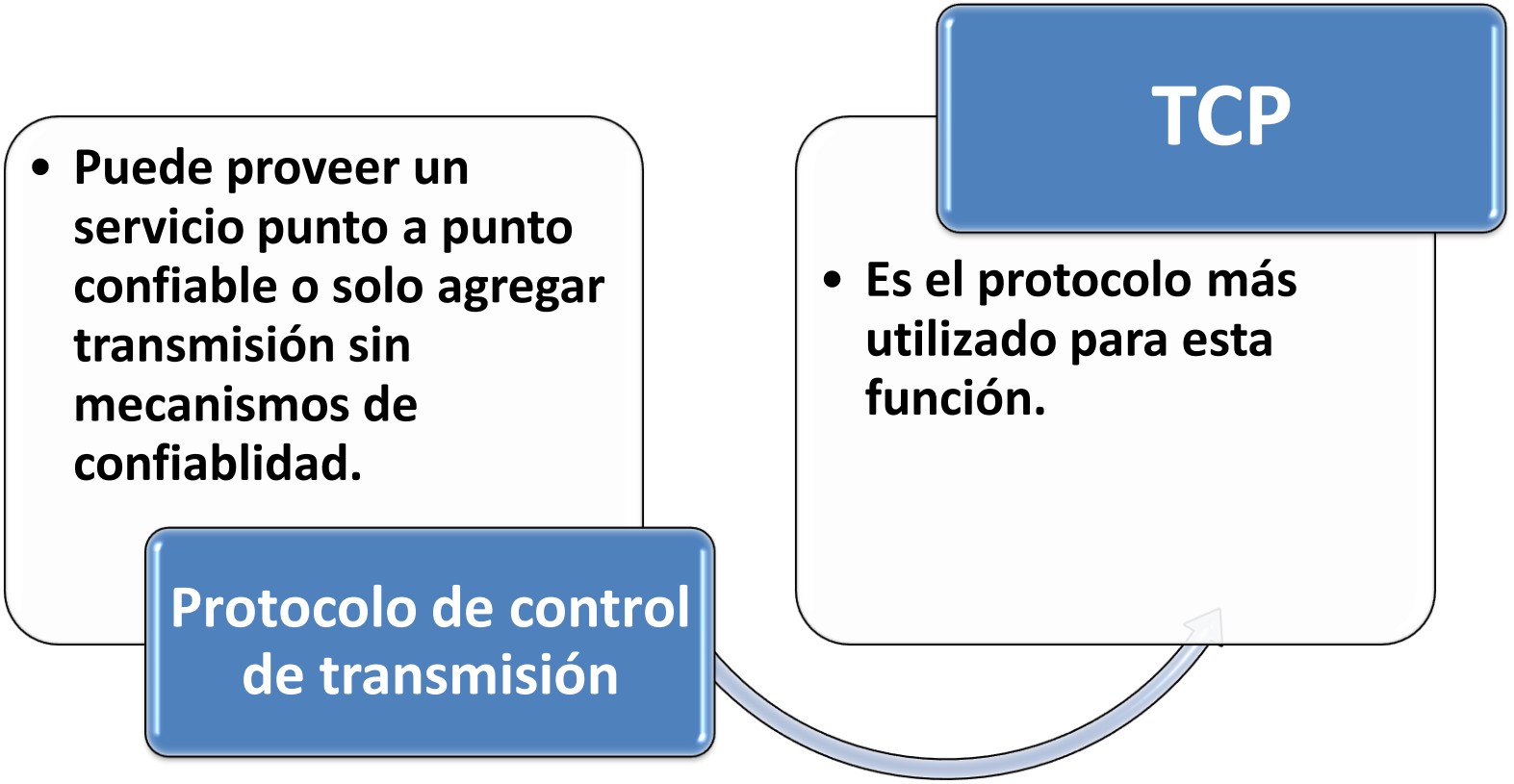
- Los tres protocolos que se encuentran en esta capa son:
  - TCP (Transmission Control Protocol): confiable, orientado a conexión, provee control de errores y control de flujo.
  - UDP (User Datagram Protocol): no seguro, no orientado a conexión que no provee control de errores ni de flujo.
  - SCTP (Stream Control Transmision Protocol), Diseñado para la transmisión de telefonía por Internet.



- Esta capa incluye funciones de las capas de sesión, presentación y aplicación del modelo OSI.
- Provee comunicación y capacidades de red a una aplicación
- Ejemplos:
  - Telnet
  - FTP
  - HTTP (Hyper Text Transfer Protocol)
  - SMTP (Simple Mail Transfer Protocol)

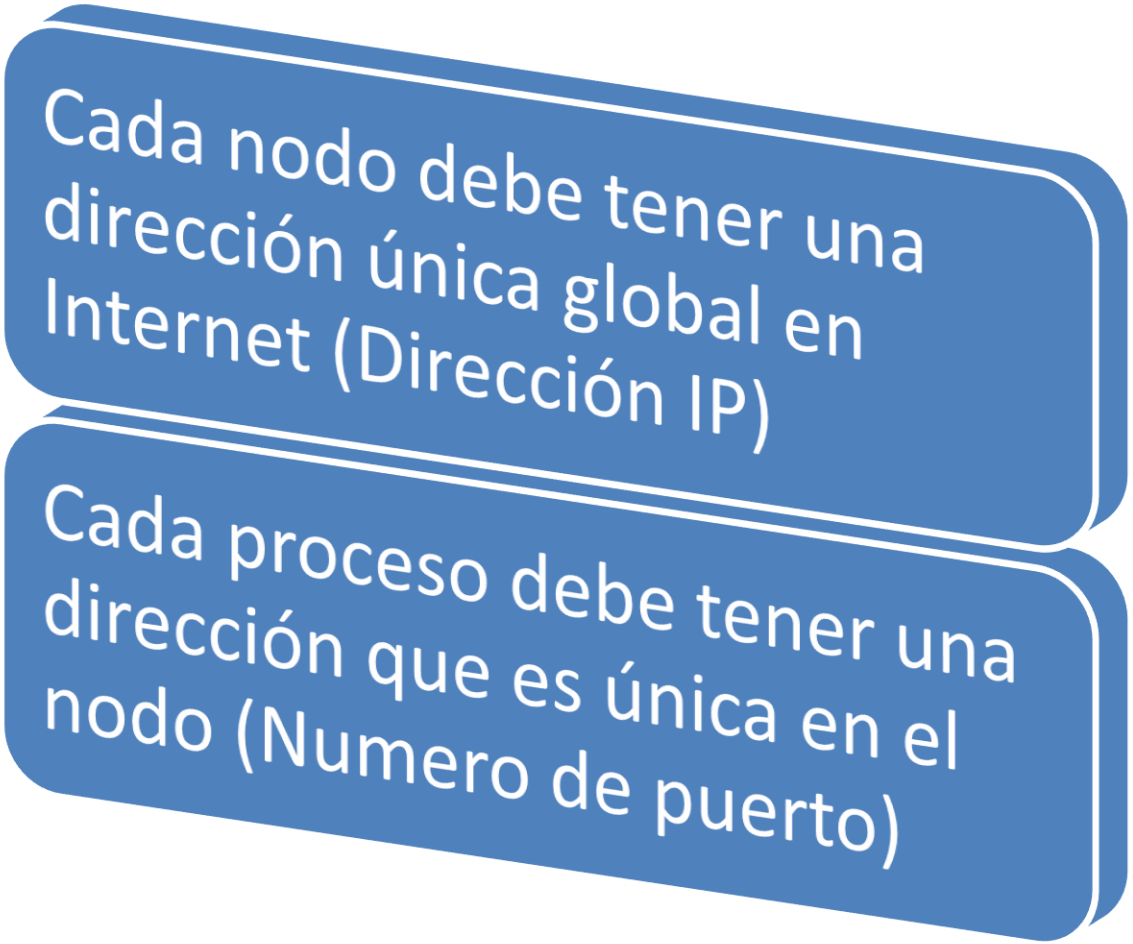
Internet Layer

Capa de transporte

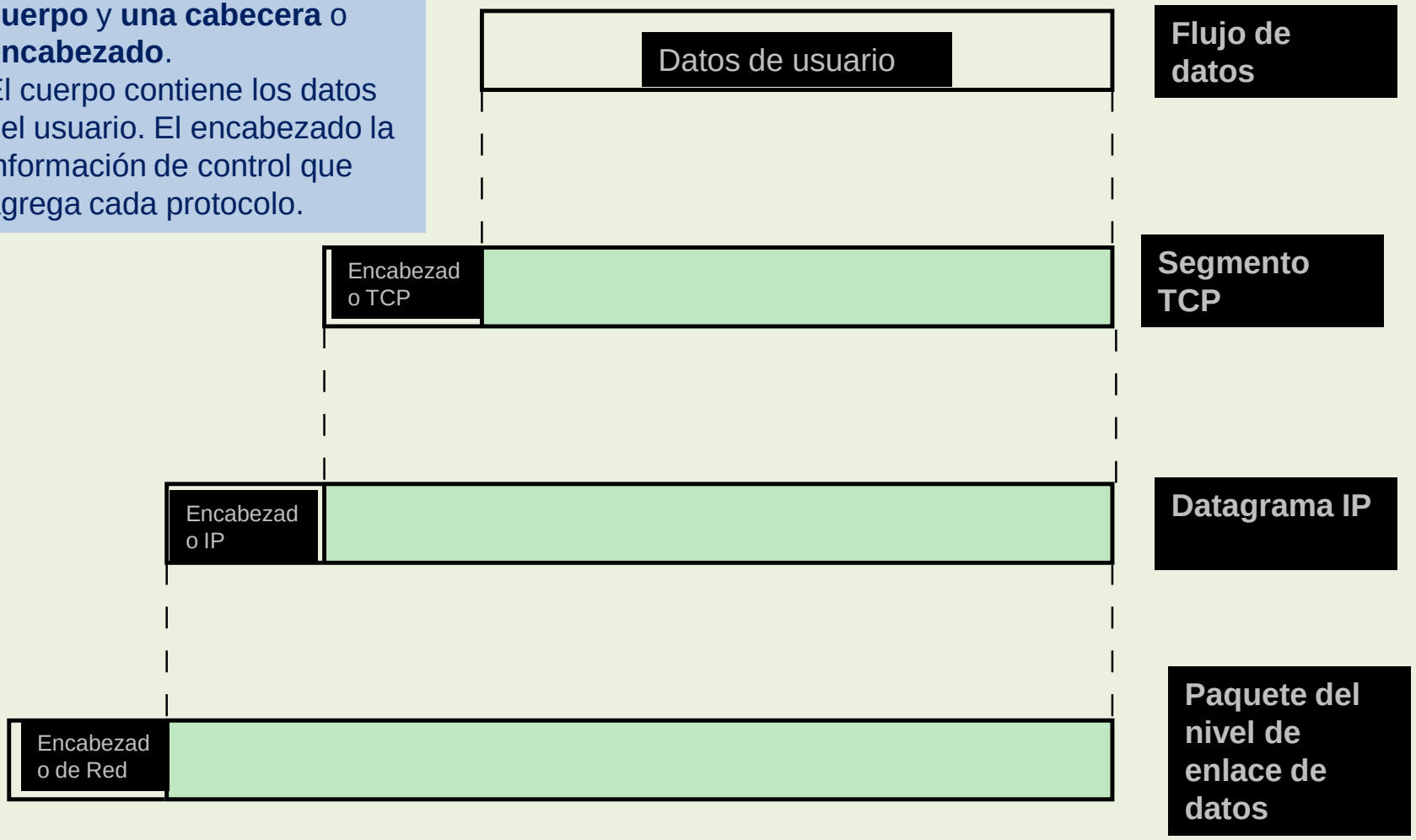


Direccionamiento en TCP/IP

Se requieren dos niveles de direccionamiento:



En TCP/IP, las unidades de protocolos se forman de un **cuerpo** y **una cabecera** o **encabezado**.
El cuerpo contiene los datos del usuario. El encabezado la información de control que agrega cada protocolo.

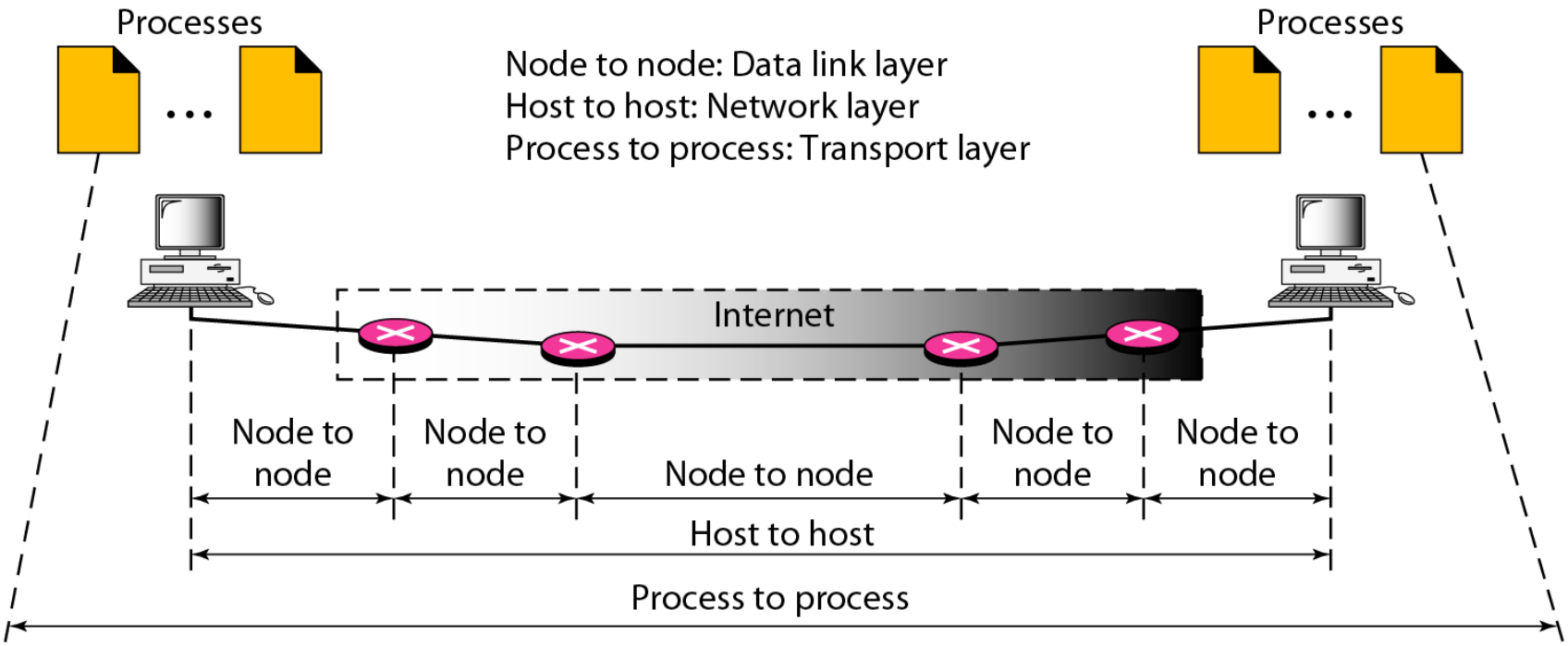


Unidades de Protocolos del modelo TCP/IP

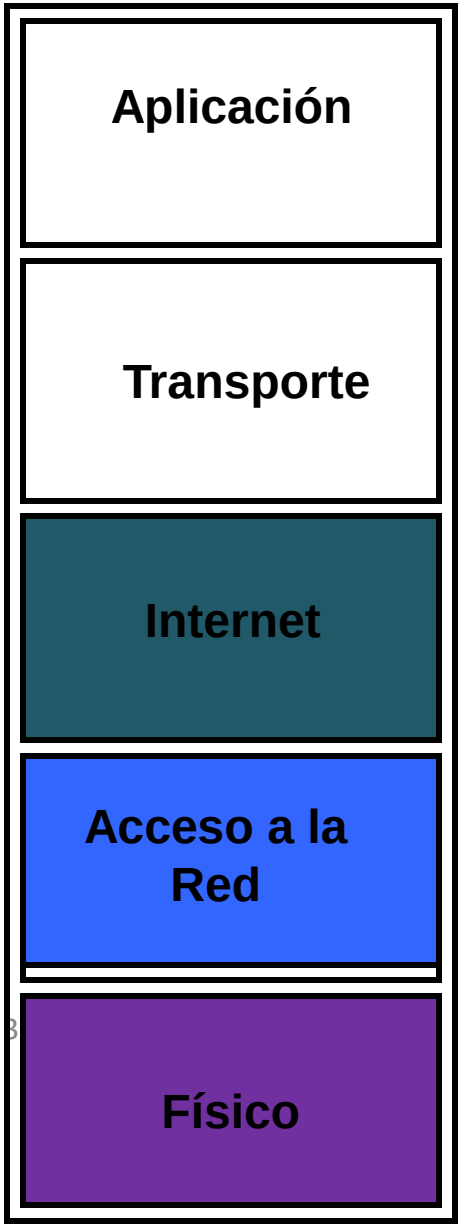
Protocolo de control de transmisión (TCP)

- TCP es el protocolo de transporte que utilizan la mayoría de las aplicaciones
- TCP provee una comunicación confiable entre aplicaciones. Garantizando que la información se entregue: ordenada y sin errores.
- La unidad del protocolo se conoce como Segmento.
- TCP lleva a cabo el seguimiento de Segmentos durante todo el tiempo que dure la transmisión.

El protocolo TCP garantiza la entrega del mensaje completo, como si existiera una ruta directa entre los procesos emisor y receptor.



Direccionamiento a nivel Transporte.



En capa de transporte Se utilizan **números de puerto. Los números de puerto son enteros de 16 bits entre 0 y 65,535.**

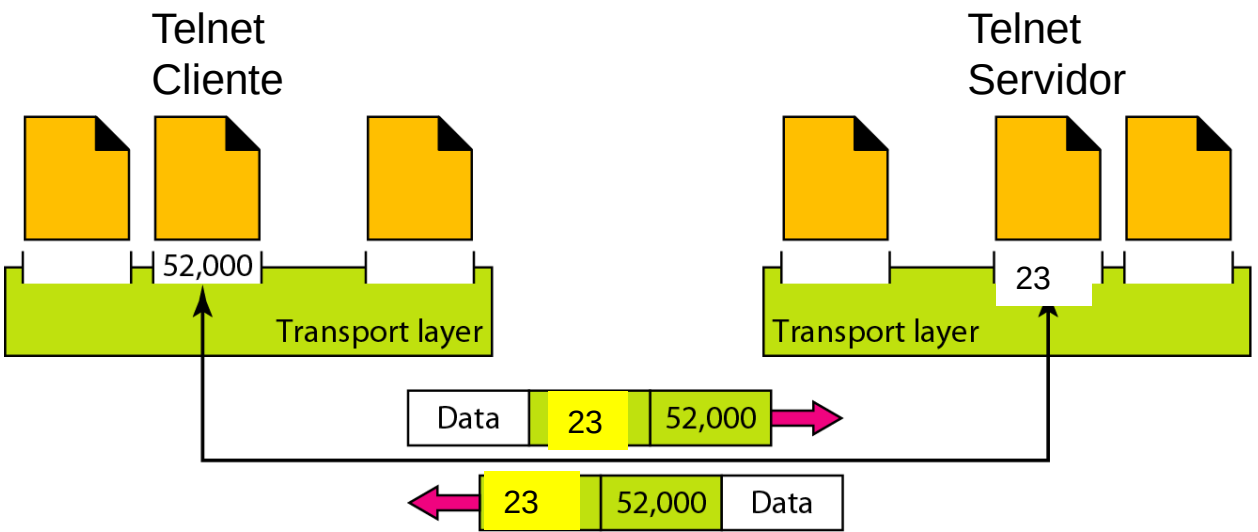
En la capa de Internet se utilizan direcciones lógicas → Direcciones IP

En capas inferiores se utilizan direcciones físicas, de la tarjeta MAC

Números de Puerto

Los números de puerto de los **procesos servidores**, corresponden a números de puerto bien conocidos definidos por la **Autoridad de Números Asignados de Internet (IANA,** Internet Assigned Number Authority). Estos números van de 0 hasta 49151

Los **números de puerto de los clientes** son asignados aleatoriamente de manera temporal, los números definidos para ello van de 49152 hasta 65535.



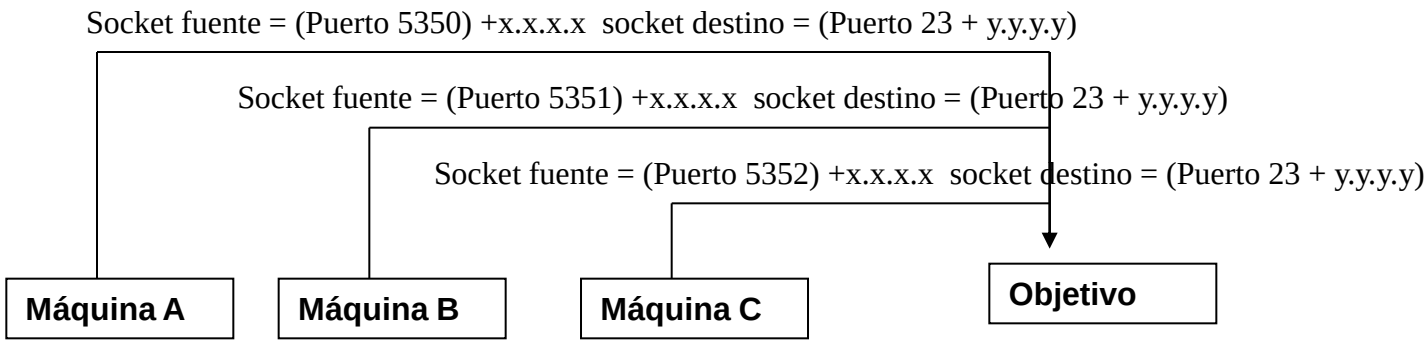
SOCKETS

La comunicación proceso a proceso en realidad requiere dos identificadores : Dirección IP + Numero de Puerto. A esta combinación se le conoce como **Socket.**

SOCKET = Puerto TCP + Dir. IP

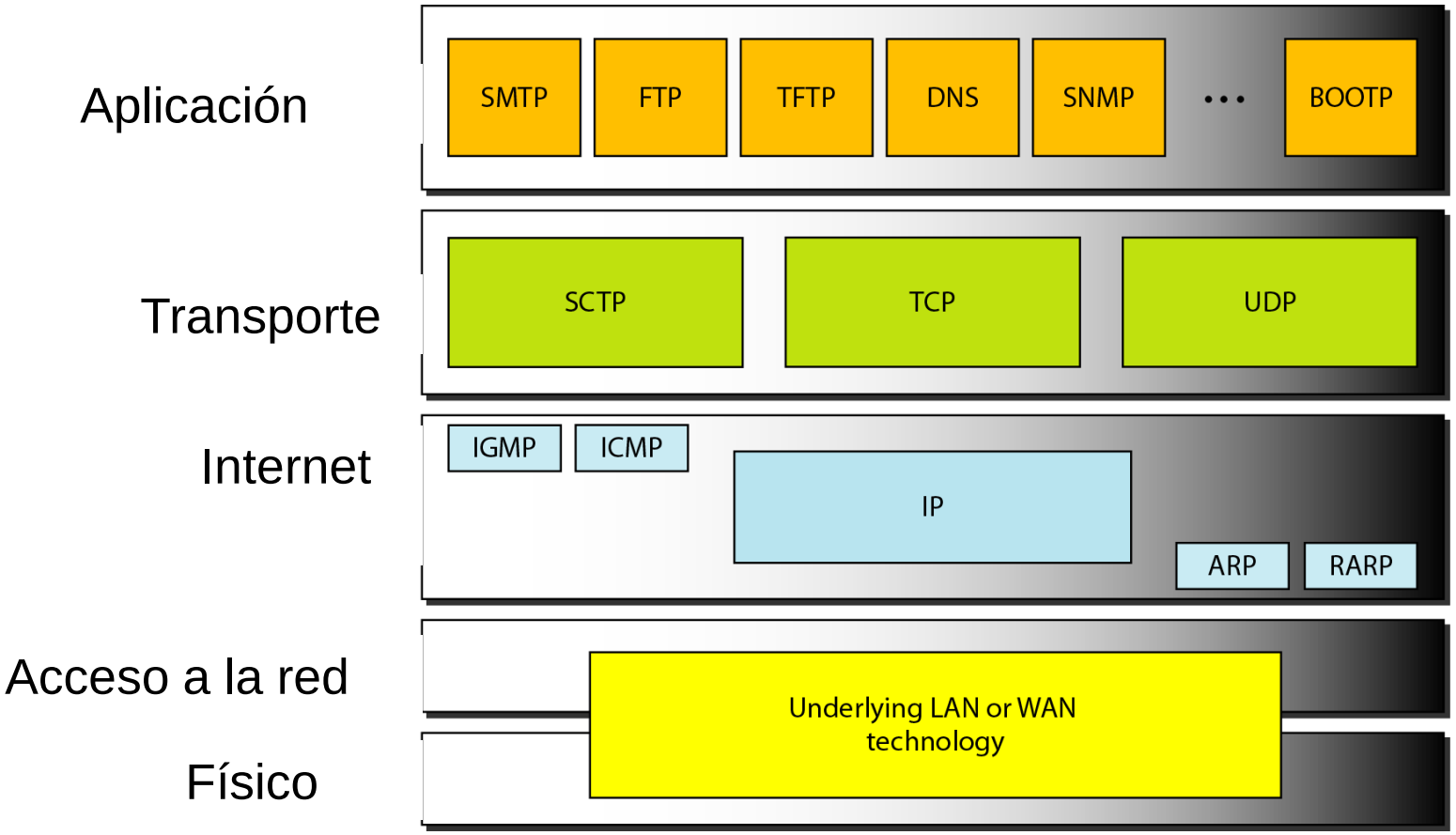
Algunos puertos conocidos:

No. Puerto	Servidor
22	SSH
23	Telnet
25	SMTP
80	HTTP
443	HTTPS
554	RTSP



Protocolos de Capa de Transporte:

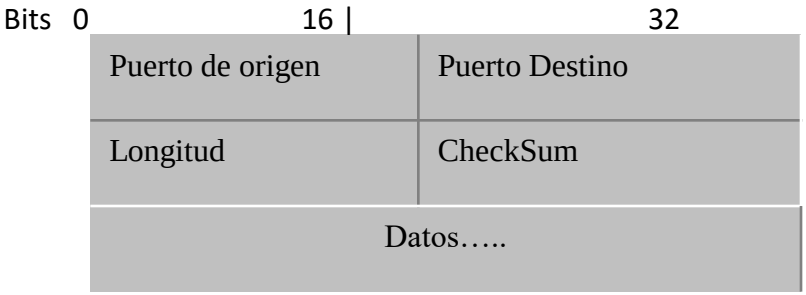
El modelo TCP/IP define tres protocolos de transporte: UDP, TCP, SCTP



UDP (Protocolo de Datagrama de Usuario)

- **Es un protocolo no orientado a conexión**
- **Proporciona servicio de datagrama no confiable**
- **No retransmite datos no recibidos**
- **Es utilizado por: TFTP, SNMP, RTSP**

Cabecera UDP: Es muy sencilla, solo 5 campos de control y datos.



Puertos origen y destino
Numero de puertos de los procesos

Longitud:
Numero de bytes en el paquete

Checksum:
Detección de errores

Utilidad de UDP

- UDP es un protocolo útil para ciertas aplicaciones porque
  - Un encabezado pequeño
  - Útil para transportar mensajes cortos
  - No requiere gran interacción entre cliente y servidor
- Algunas aplicaciones de UDP son:
  - Comunicación simple de peticiones y respuestas, sin requerir control de errores y flujo como el proporcionado por TCP
  - Cuando la aplicacion requiere multicasting, ya que TCP no lo soporta
  - En conjunto con RTP (Real Time Transport Protocol) para transmisiones en tiempo real.

Puertos bien conocidos usados por UDP

Puerto	Protocolo	Descripción
7	Echo	Devuelve el datagrama recibido al emisor
9	Discard	Descarta cualquier datagrama que recibe
11	Users	Usuarios activos
13	Daytime	Devuelve la fecha y la hora
53	NameServer	Servicio de nombres de dominio
67	BOOTPs	Puerto del servidor para localizar información de arranque
69	TFTP	Trivial File Transfer Protocol

TCP (Protocolo de Control de Transporte)

•Es un protocolo orientado a conexión.

•Proporciona una transmisión confiable de datos mediante detección y corrección de errores extremo a extremo.

•Garantiza que los datos sean transferidos a través de una red de manera exacta y en orden apropiado

•Retransmite los datos no recibidos por el nodo destino

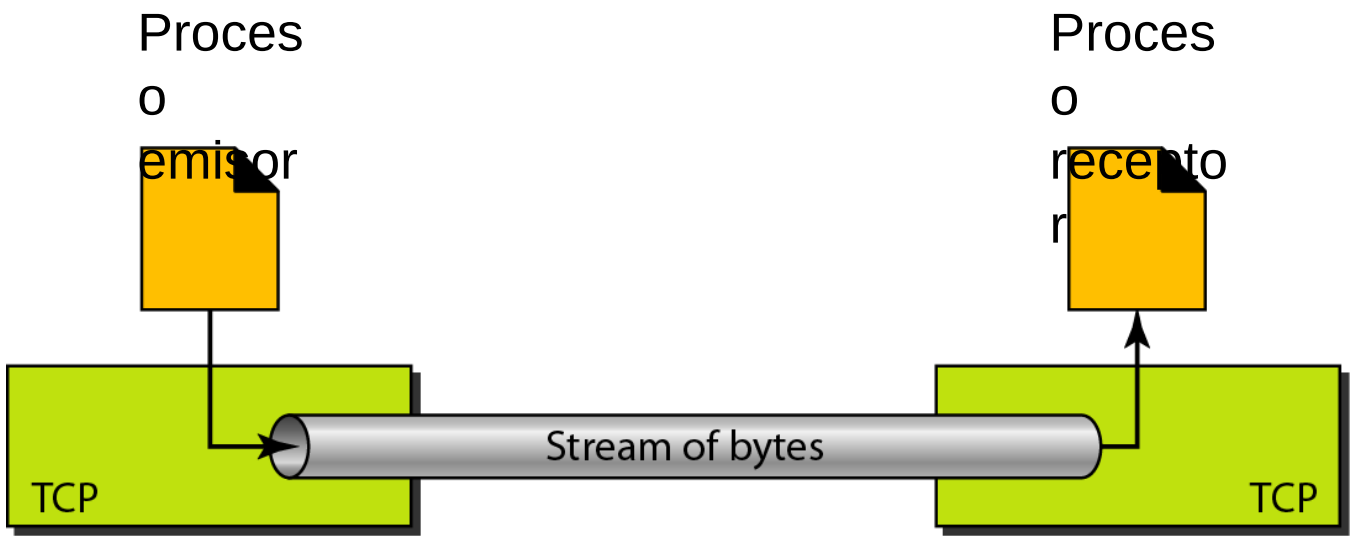
•Ofrece garantía contra datos duplicados

•Es utilizado por Telnet, FTP, SMTP, y POP

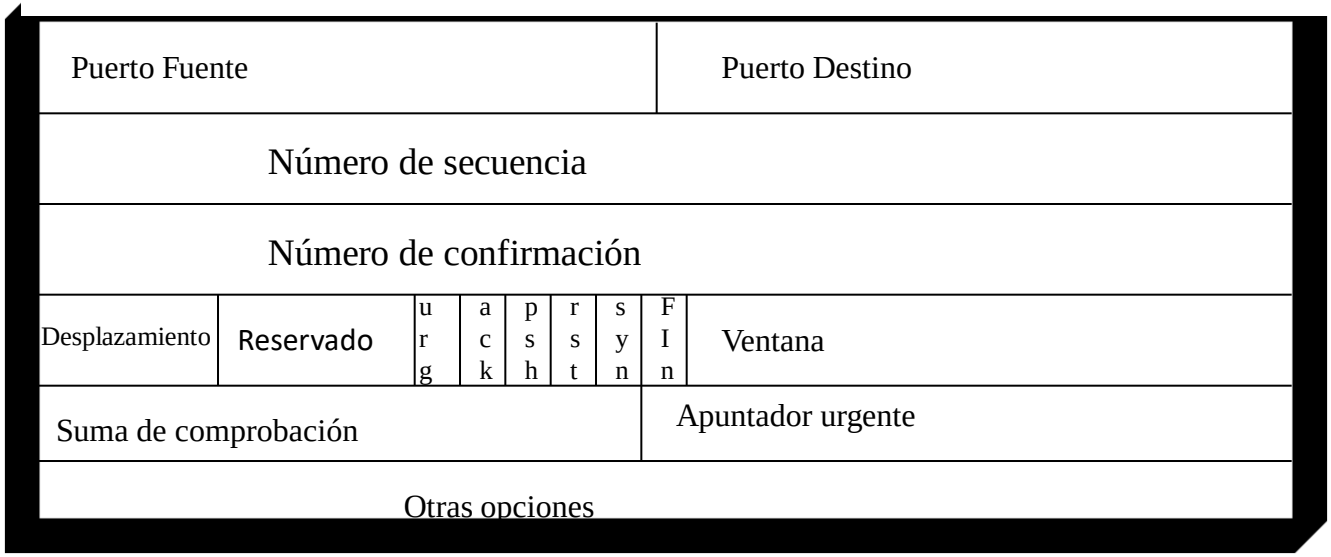
•Los mensajes largos son divididos en segmentos cada uno con un encabezado TCP

TCP envía un flujo de datos controlados, manteniendo una secuencia constante y orden de los datagramas enviados.

De esta manera puede considerarse que existe un canal directo de comunicación entre el proceso emisor y el receptor, donde cada uno recibe un flujo de bytes.



Encabezado TCP 0 31 bits



DATOS…..

- **Numero de secuencia (32 bits):** Indica la posición actual del bloque en el mensaje total. Si la bandera SYN = 1, es el número de secuencia inicial.
- **Numero de confirmación (32 bits):** Indica el siguiente numero de secuencia esperado.
- **Desplazamiento (4 bits)** Indica el número de palabras de 32 bits que contiene el encabezado.
- **Ventana (16 bits):** Cantidad de bloques de datos que puede aceptar la máquina receptora.
- **Suma de comprobación** (16 bits):
- **Apuntador urgente (16 bits**): Señala la parte del mensaje que es urgente.

Banderas (1 bit c/u):

URG: Si es 1 el campo del apuntador URGENTE es válido.

ACK: Si es 1 indica que el campo de confirmación es válido.

PSH: Si es 1 indica que los datos deben ser entregados de inmediato.

RST: Si es 1 indica que la conexión debe reiniciarse.

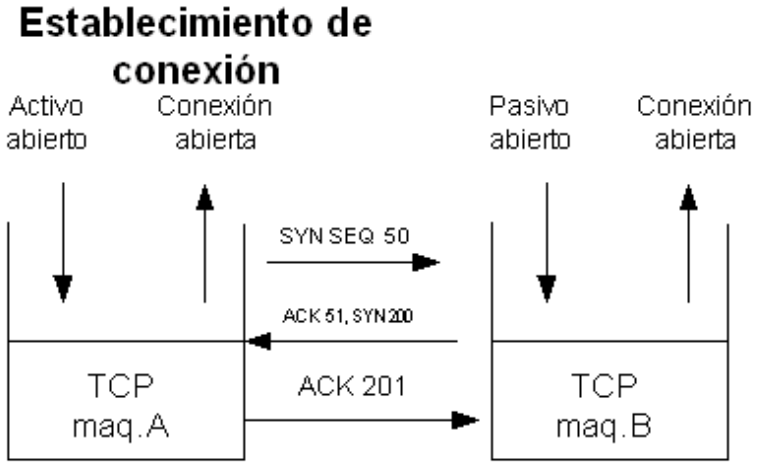
SYN: Si es 1 indica que los numeros de secuencia deben sincronizarse

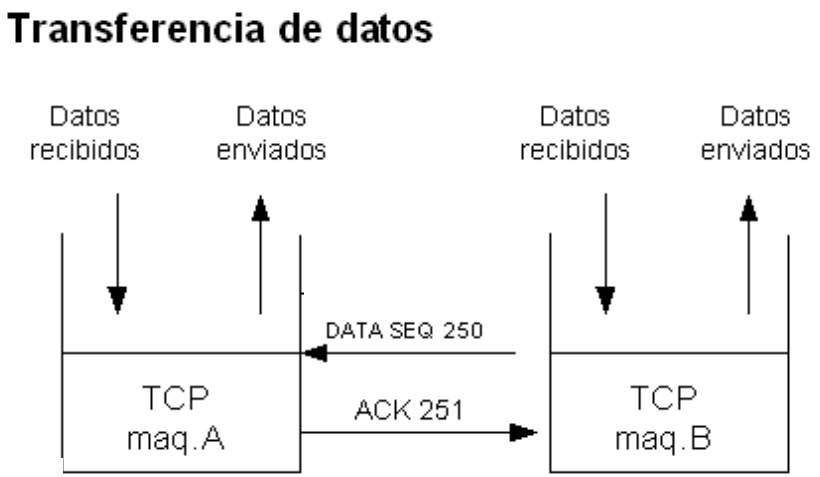
FIN: Si es 1 indica que el tx no tiene más datos que enviar.

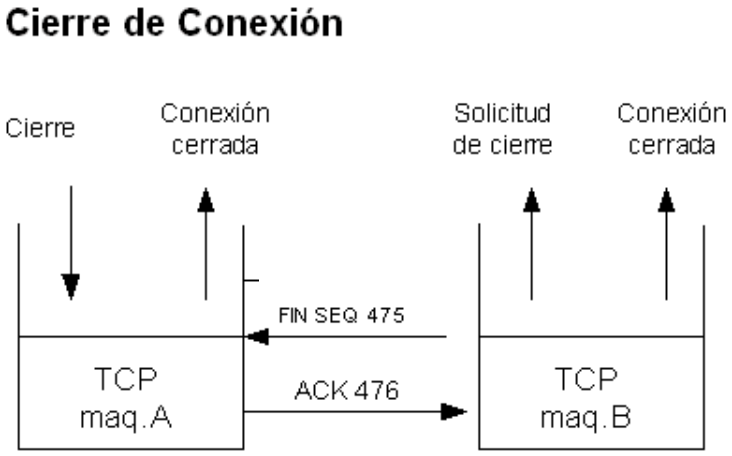
Puertos bien conocidos usados por TCP

Puerto	Protocolo	Descripción
20	FTP, datos	Conexión de datos con FTP
21	FTP, control	Conexión de control con FTP
23	Telnet	Terminal en Red
25	SMTP	Simple Mail Transfer Protocol
79	Finger	Servicio Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Llamada a procedimiento remoto

Mecanismos TCP







TCP siempre realiza tres pasos: Establecer conexión, solicitar confirmación por cada dato y cerrar conexión

TEMPORIZADORES UTILIZADOS EN TCP:

Debido a que TCP espera confirmaciones, se requieren temporizadores. El temporizador define el tiempo que el emisor espera una confirmación.

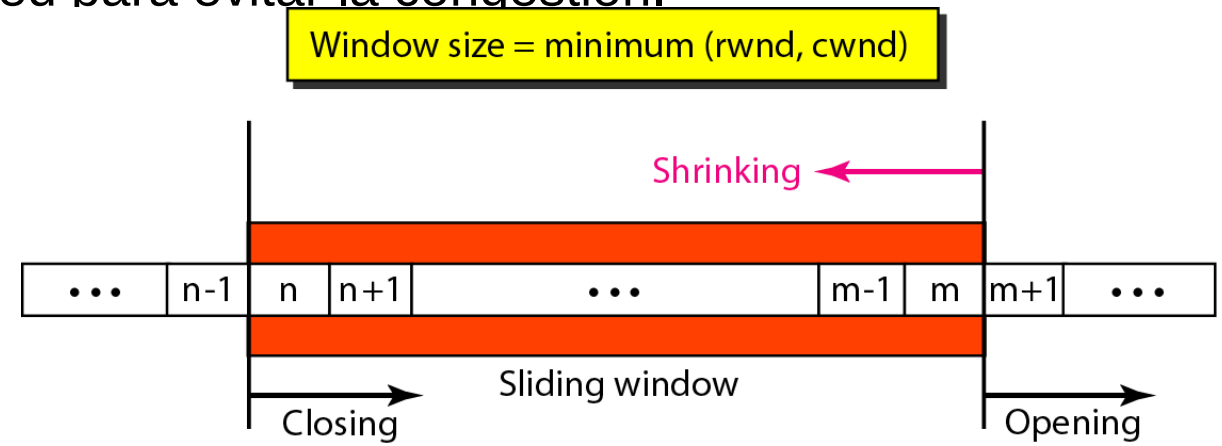
- **De Retransmisión**: Para transmitir un segmento no confirmado
- **De Reconexión**: Tiempo mínimo entre el cierre de una conexión y el establecimiento de otra con la misma dirección destino.
- **De Retransmisión de SYN**: Tiempo entre intentos de establecer una conexión.

Control de Flujo en TCP

TCP usa un mecanismo conocido como Ventana Deslizante.

El tamaño de la ventana le indica al receptor cuantos bytes puede enviar antes de recibir una confirmación, sin saturar al destino.

El tamaño de la ventana esta determinado por el menor de dos valores:
Ventana de recepción (rwnd): Es el numero de bytes que el receptor puede recibir sin desbordarse.
Ventana de congestión (cwnd): Es un valor determinado por la red para evitar la congestión.



Unidad 2. Internet y Sistemas inalámbricos.

Contenido de la unidad

2.1 Redes inalámbricas
2.2 Sistemas de telefonía móvil
2.3Tecnologías emergentes de sistemas inalámbricos

Existen varias tecnologías inalámbricas que permiten la transferencia de datos, entre ellas están:

IrDA (Infrared Data Association)

Velocidad: 16 Mbps

Distancia: 1 mtr.

•La tecnología celular.

Velocidad: 100 Mbps

•Bluetooth

Radiofrecuencia

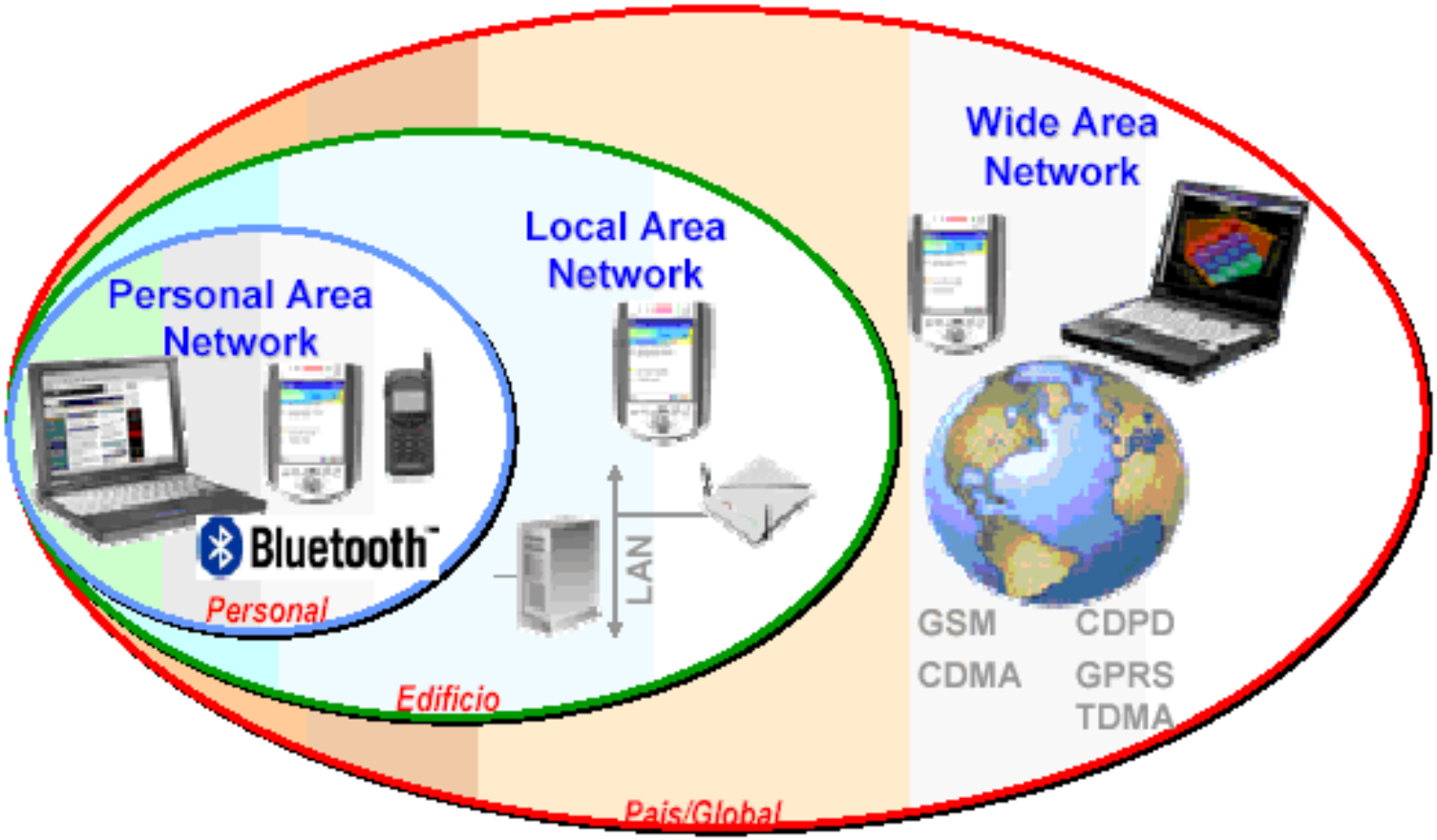
Velocidad: 25 Mbps aprox.

•El estándar 802.11

Velocidad: 2 Mbps - 7 Gbps

Reconocido por IEEE

TECNOLOGÍAS INALÁMBRICAS



En base a su alcance geográfico se pueden clasificar en: Redes de área personal, redes de área global y redes de área extensa

En la actualidad las redes LAN inalámbricas (WLAN) se han vuelto cada vez más populares.

El estándar WLAN mas utilizado es el IEEE 802.11

En 1997 la IEEE publicó el estándar 802.11 para una LAN en el nivel físico y de enlace de datos que cumple con lo siguiente:

•El protocolo admite estaciones fijas, portátiles o móviles dentro de un área local.

•El protocolo proporciona conectividad inalámbrica a maquinaria automática, equipos o estaciones rápidamente.

•El protocolo debe tener alcance global.

Las principales diferencias entre 802.11 y los estándares de LAN con medios acotados (802.3), es que se deben considerar los siguientes aspectos:

•Medios no acotados: No se tienen conexiones fijas a una red claramente observables ni se distinguen las fronteras.

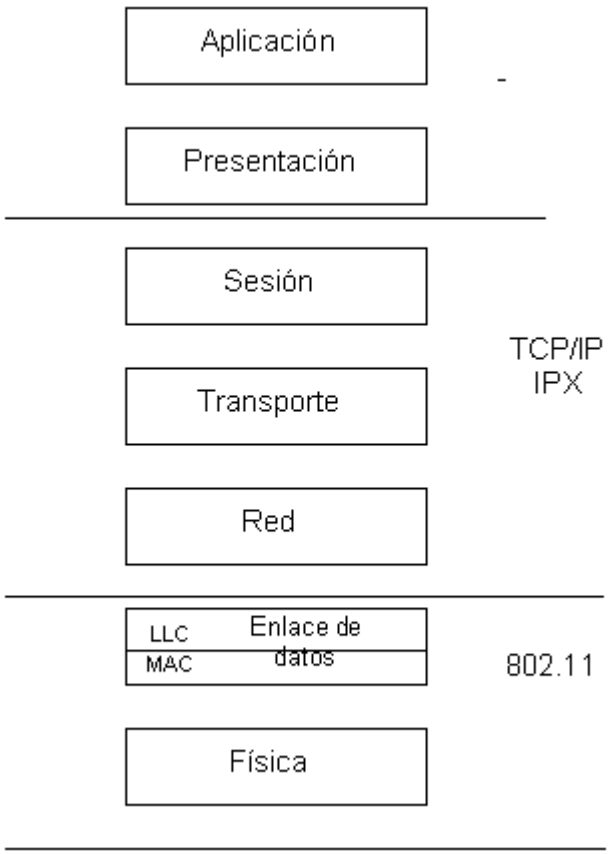
•Topología dinámica: La topología de una WLAN cambia frecuentemente.

•Medios no protegidos: Las estaciones no están protegidas de las señales exteriores, de manera que es probable que las estaciones portátiles puedan interferir con señales de otras redes, poniendo en peligro la seguridad.

•Medios no fiables: No se tiene la seguridad de que todas las estaciones reciben todos los paquetes y que se pueden comunicar con todas las otras estaciones.

•Medios asimétricos: El continuo movimiento de las estaciones provoca cambios en la velocidad de transmisión, por ello el mecanismo MAC debe tener un diseño diferente.

802.11 y OSI



Los elementos básicos para implementar una WLAN son:

•La tarjeta de red inalámbrica, la cual permite la interconexión con el resto de los clientes y con el punto de acceso.

•Punto de acceso, es el equipo de interconexión y permite la comunicación de la WLAN con una LAN cableada (Internet)

Además de estos dispositivos se tienen enrutadores, puentes, servidores de impresión, modems y otros inalámbricos desarrollados para 802.11

*TOPOLOGIA

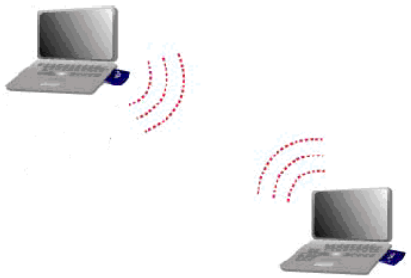
Para una WLAN la topología no define las posiciones estáticas de los dispositivos, si no las reglas básicas que se utilizarán para comunicarse entre ellos.

El área geográfica en la que las estaciones inalámbricas pueden comunicarse entre sí se conoce como BSS (conjunto de servicio básico, Basic service set).

Las dos topologías definidas por 802.11 son: ad-hoc (IBSS) y de Infraestructura:

Topología ad-hoc o IBSS (BSS independiente)

Consiste solamente en la comunicación entre dos o más equipos inalambricos que han entrado en un área de transmisión.

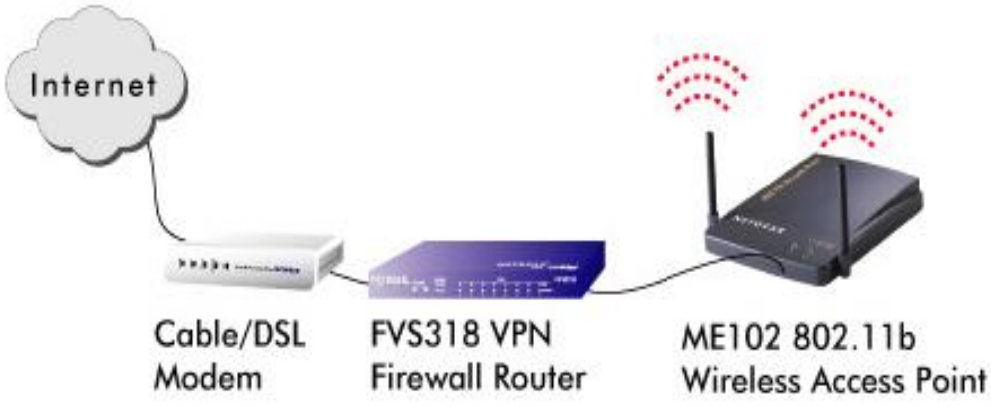


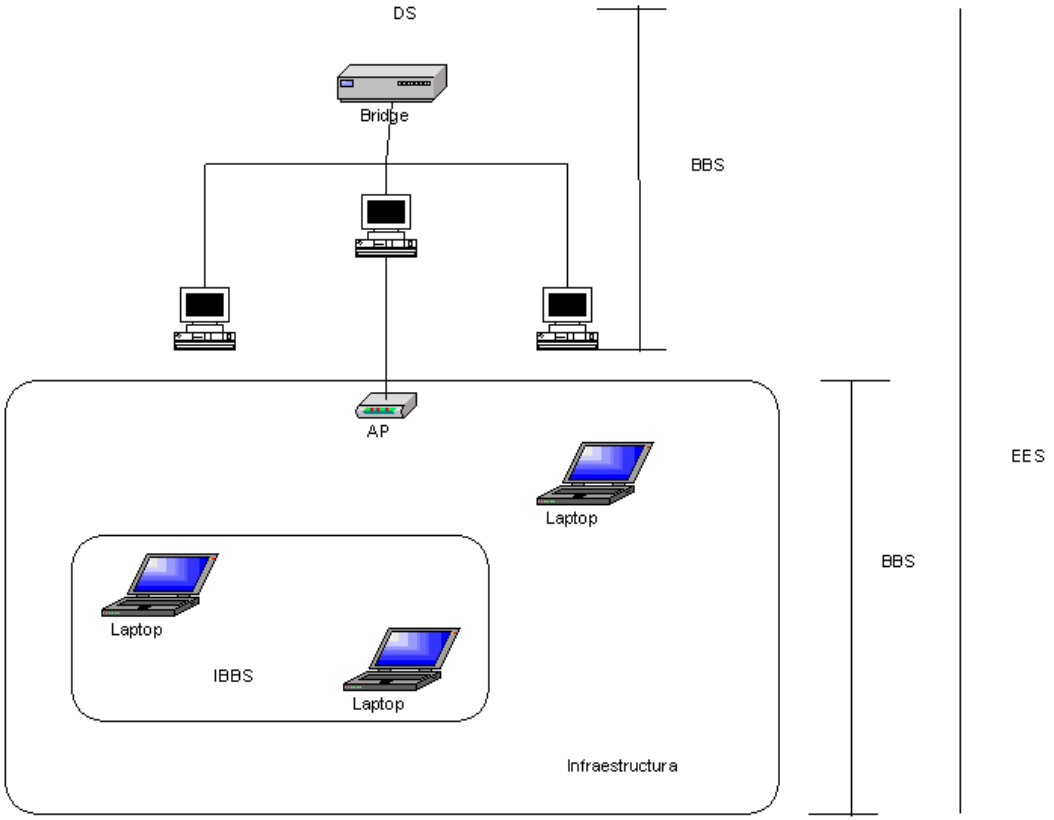
Generalmente cubre un área muy limitada y suele utilizarse para grupos colaborativos, juegos, transferencia de archivos y comunicaciones rápidas, en general.

Topología de infraestructura:

Utiliza al menos un AP, el cual tiene un alcance que es relativamente fijo en comparación a un IBSS, y funciona como una estación base. Cualquier estación que entra al BBS puede comunicarse con la red fija y a su vez con el resto de las estaciones.

Se utiliza para dar soporte a una red fija con servicios inalámbricos. Puede tener un numero ilimitado de AP.





Debido a que una red con topología de infraestructura puede tener cualquier numero de AP, puede por lo tanto tener un numero indefinido de BBS's, **en ese caso se cuenta con un Servicio de Distribución (DS), el cual es una red cableada (ejemp. 802.3)**

Los conjuntos de servicios básicos y el DS que los une se conoce como Conjunto de servicios ampliado (EES).

Los conjuntos de servicios básicos conectados por un sistema de distribución pueden estar configurados físicamente de cualquier forma, los DS pueden estar incluso muy distantes entre si.

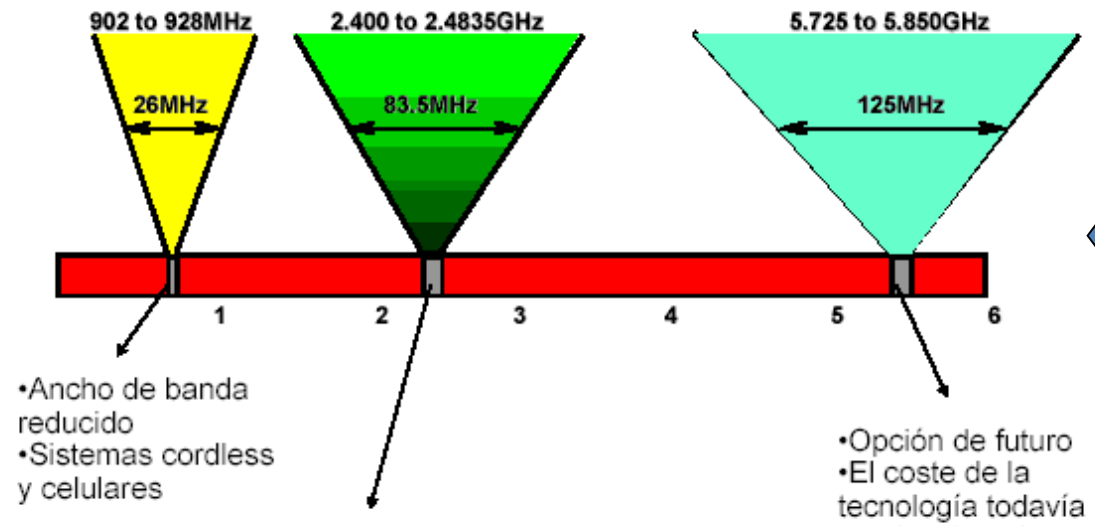
También es posible tener sistemas IBSS y de infraestructura en la misma red.

Las redes WLAN están definidas en las dos primeras capas del modelo OSI: Capa Física y Capa de Enlace de Datos

La capa física define la técnica de modulación que se utilizara para enviar los datos a través del espacio libre

La capa de enlace de datos define la trama y la técnica de acceso al medio.

Capa física 802.11



Disponibilidad de espectro

UPC

IEEE 802.11 puede utilizar diferentes canales para enviar la información. En base a la disponibilidad del espectro cada canal tiene distinto ancho de banda.
Las versiones mas conocidas utilizan las bandas 2.4 o 5 GHz

Para modular la información y enviarla por los distintos canales se utilizan diferentes técnicas entre las que se encuentran:

-FHSS (Espectro extendido de salto de frecuencia)

-DSSS (Espectro extendido de secuencia directa)

-OFDM (Multicanalización por división de frecuencias ortogonales)

-MIMO (Multiple Input Multiple Output)

-MU MIMO

- **FHSS**;

•Utiliza un código o algoritmo predeterminado para imponer cambios de frecuencia continuamente, en incrementos discretos, sobre una amplia banda de frecuencias

•Cada conversación se lleva a cabo en un patrón de frecuencia distinta, de manera que la posibilidad de traslape sea mínima.

• **DSSS:**

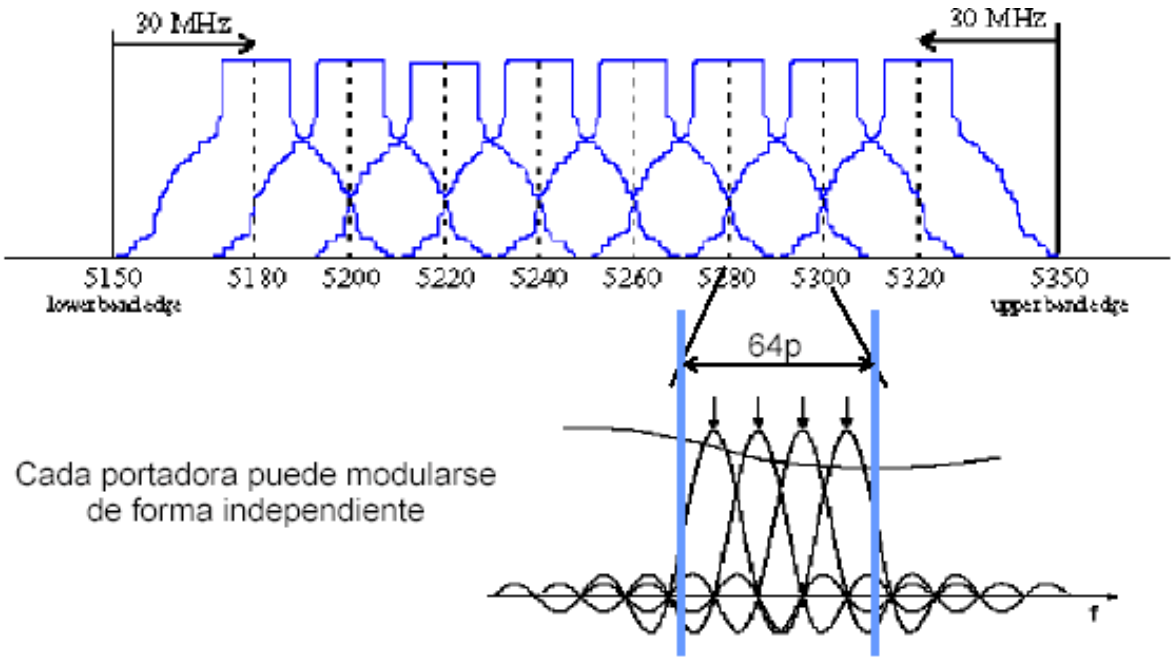
En este caso la señal a transmitir se modula por medio de un código digital llamado chip o código del chip. El chip es un patrón redundante de bits que convierte cada bit de la señal de datos en varios bits, los cuales se transmiten lentamente. Entre mayor sea el chip utilizado, mayor sera el aumento en la señal original, esto hace que sea mas facil recuperar información en caso que se presenten errores.

Para poder leer la información el receptor y el emisor deben conocer el chip utilizado.

OFDM

Se trata de una técnica de modulación digital de espectro ensanchado de gran complejidad que permite alcanzar una buena calidad en entornos hostiles como es el canal radio.

La idea básica de OFDM es dividir el espectro disponible en varias portadoras de tasas bajas de transmisión, para obtener una transmisión de alta eficiencia espectral todas las portadoras son traslapadas de manera ortogonal utilizando IFFT. Cada subportadora puede ser modulada con un esquema diferente como BPSK, QPSK y QAM

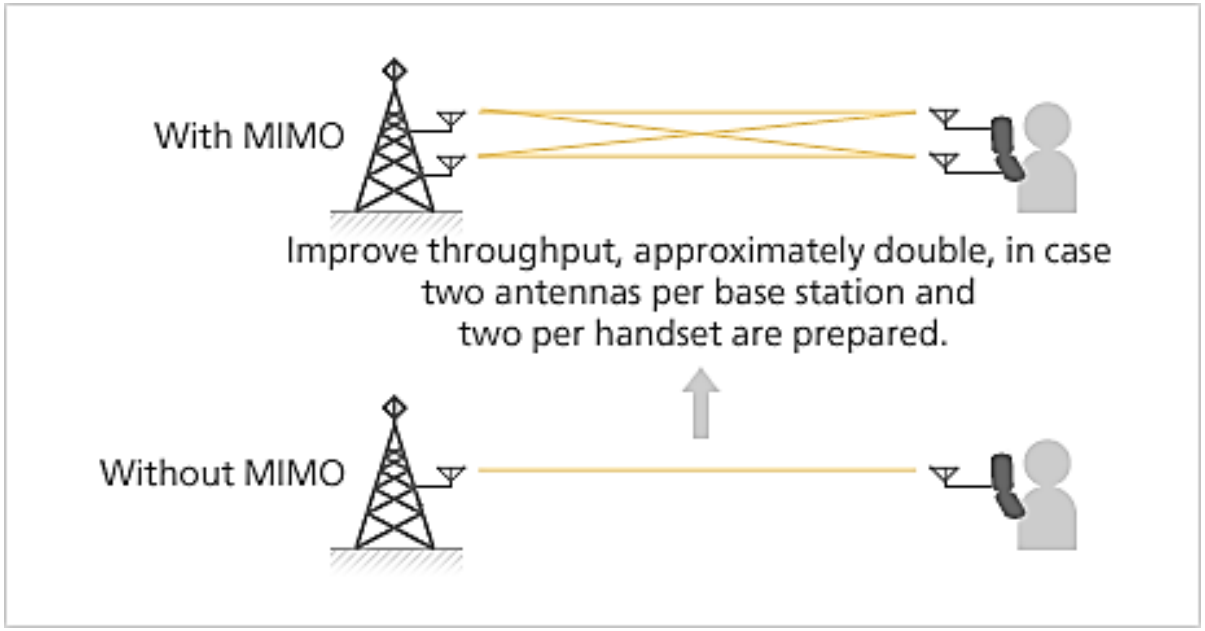


Utiliza 52 portadoras de datos en un canal con tiempos de guardas entre ellas de 400 ns

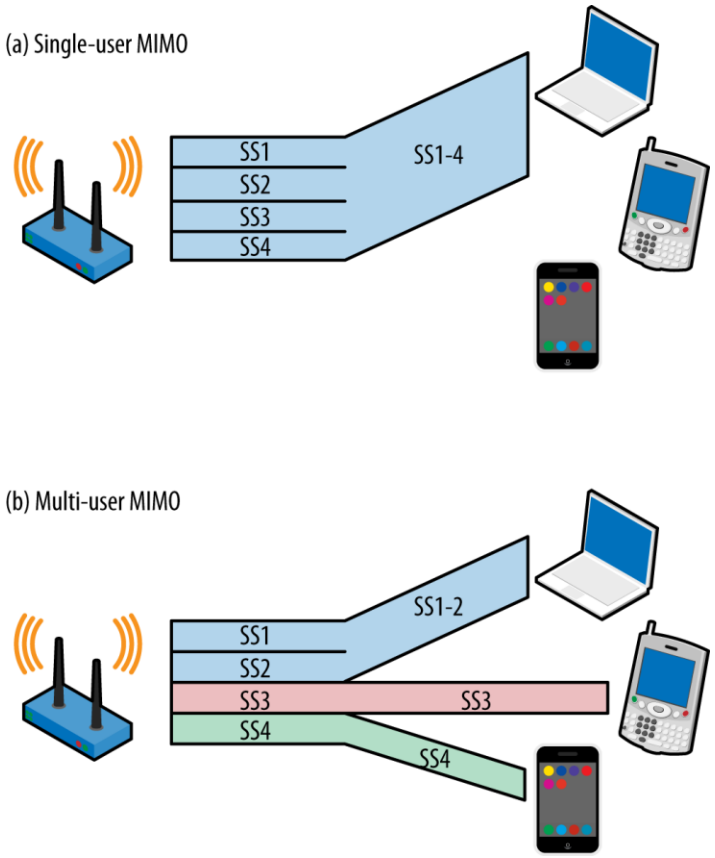
MIMO

MIMO es el acrónimo en inglés de Multiple-input Multiple-output (en español, Múltiple entrada múltiple salida).

MIMO aprovecha fenómenos físicos como la propagación multicamino para incrementar la tasa de transmisión y reducir la tasa de error. Aumenta la eficiencia espectral de un sistema de comunicación inalámbrica por medio de la utilización del dominio espacial (antenas físicamente separadas).



MU MIMO
(MIMO Multiusuario)



Agrega la capacidad de poder transmistir múltiples cadenas a múltiples usuarios, pudiendo redireccionarlas según se requiera.

ESPECIFICACIONES GENERALES DE 802.11

El estándar general 802.11 define el uso de FHSS para operar a velocidades máximas de 1 Mbps, las nuevas especificaciones defines:

802.11 a Utiliza OFDM y opera a 54 Mbps en la banda de 5 GHz

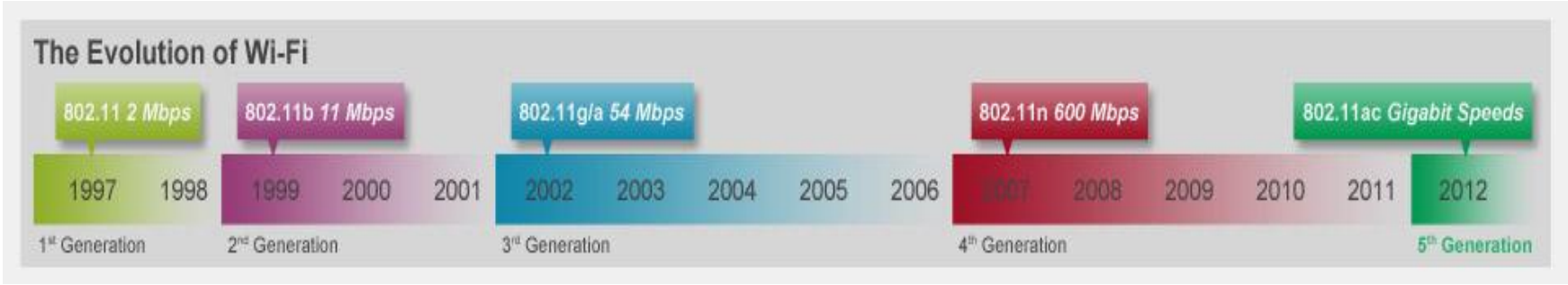
802.11b Utiliza DSSS y opera a 1,2,5.5 y 11 Mbps, en la banda de 2.4 GHz

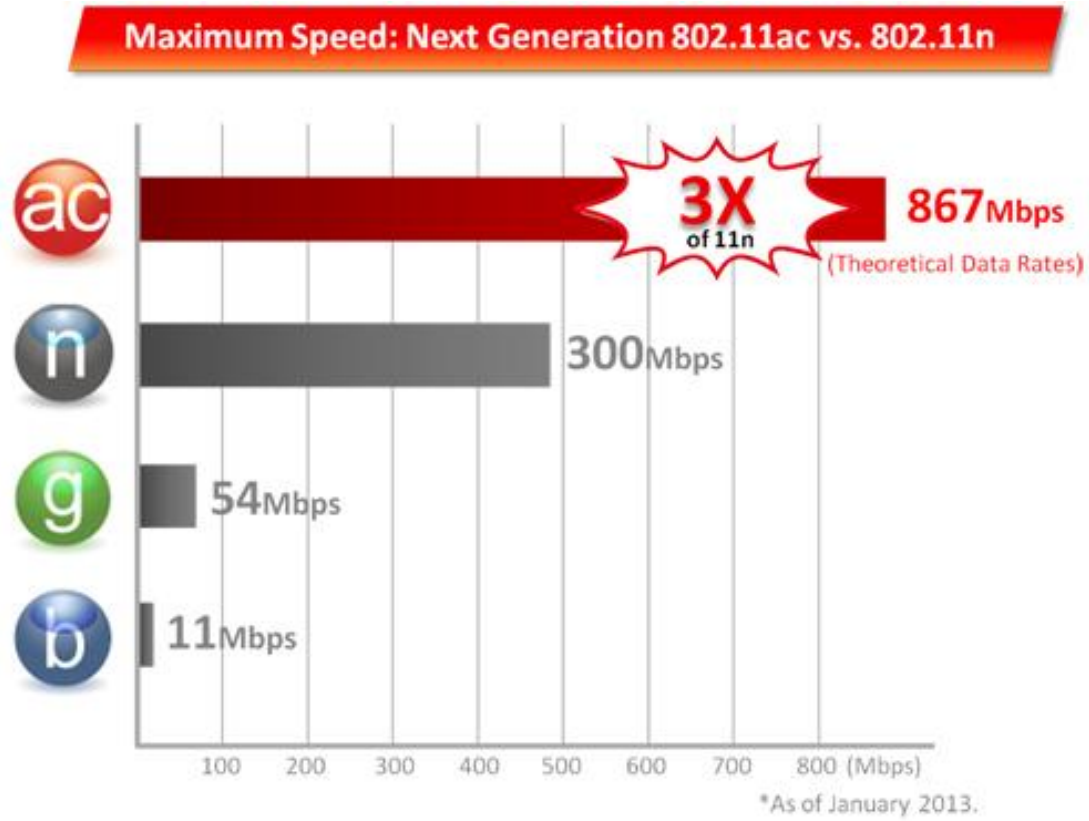
802.11g Utiliza OFDM y opera a 22 o 54 Mbps, en la banda de 2.4 GHz

802.11n utiliza MIMO (Multiple Input- Multiple Output) Hace un mejor uso del ancho de banda que SS, por lo que se puede enviar mas información.

802.11ac. Banda de 5 Ghz, Utiliza Multi User-MIMO (MU-MIMO) y mas canales incluidos incluidas las bandas de 80 y 160 MHZ Equipos de hasta 8 antenas, velocidades de 1Gbps

Evolución de WiFI





Especificaciones 802.11 mas utilizadas.

802.11a:

54 Mbps (27 Mbps reales), 64 usuarios por AP. Opera en la banda de 5 GHz. Sufre pocas interferencias. Tiene poco alcance y presenta problemas antes obstáculos como paredes. Requiere mucha energía eléctrica. No es compatible con b y g. Emplea una modulación 64-QAM y codificacion OFDM (Orthogonal Frequency Division Multiplexing)

802.11b:

11 Mbps, 32 usuarios por AP. Opera en la banda de 2.4 GHz. Alta compatibilidad. Requiere menos energía eléctrica. Excelente alcance. También se conoce como WiFi. Utiliza DSSS

802.11g:

54 Mbps, opera a 2.4 GHz., compatible con 802.11b. Excelente alcance. Utiliza OFDM.

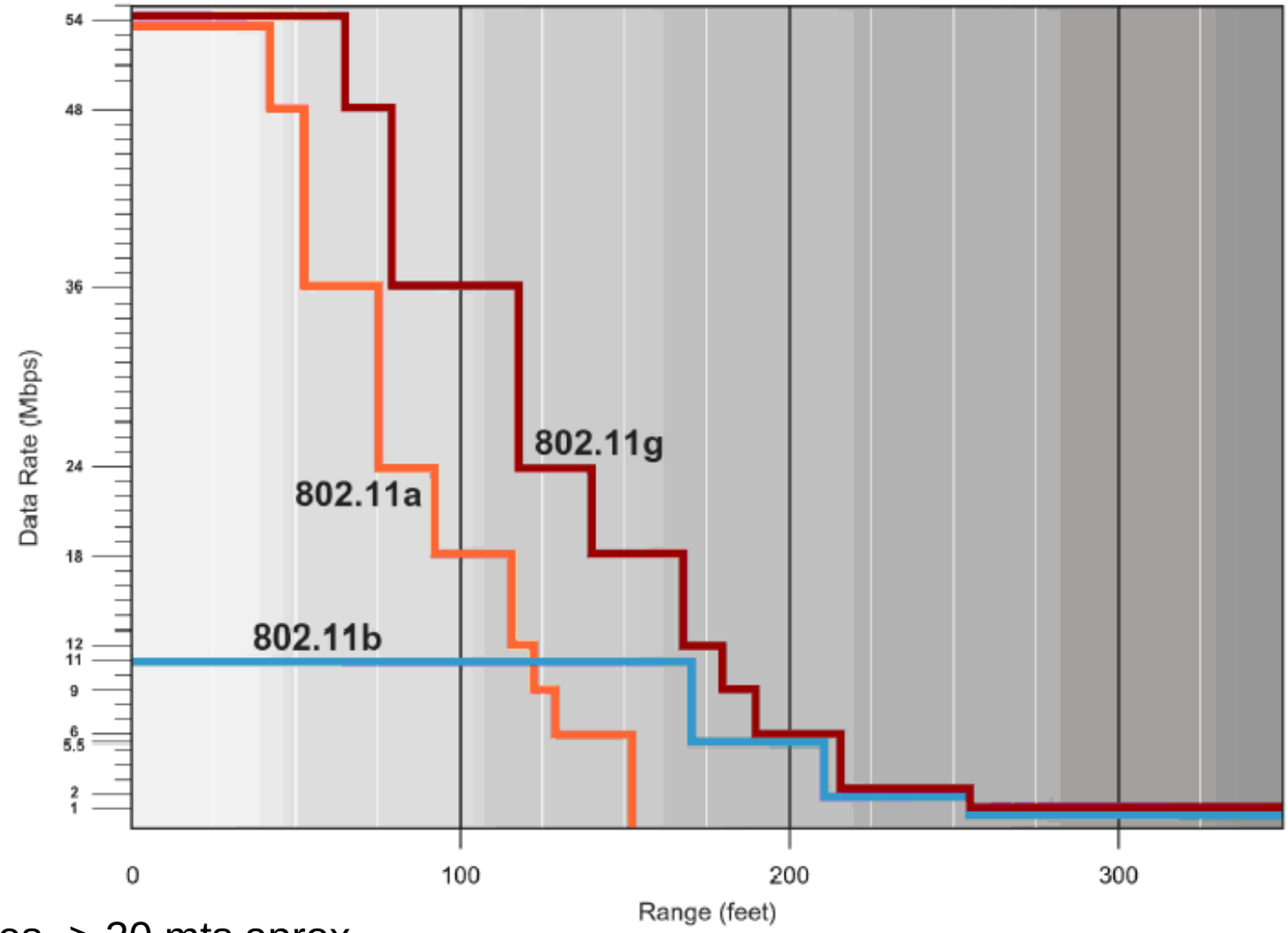
802.11n:

Ofrece tasas de hasta 100 Mbps teóricamente de hasta 600 Mbps. Es compatible con las especificaciones a, b y g. Utiliza canales de 40 MHz (el doble que las anteriores). Opera en las bandas 2.4 GHz o 5 GHz. Utiliza una técnica conocida como MIMO que envía múltiples señales.

Recientemente 802.11 ad, por lo que las Versiones actuales de IEEE 802.11 son:

Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ad
Year introduced	1999	1999	2003	2000	2012	2014
Maximum data transfer speed	54 Mbps	11 Mbps	54 Mbps	65 to 600 Mbps	78 Mbps to 3.2 Gbps	6.76 Gbps
Frequency band	5 GHz	2.4 GHz	2.4 GHz	2.4 or 5 GHz	5 GHz	60 GHz
Channel bandwidth	20 MHz	20 MHz	20 MHz	20, 40 MHz	40, 80, 160 MHz	2160 MHz
Highest order modulation	64 QAM	11 CCK	64 QAM	64 QAM	256 QAM	64 QAM
Spectrum usage	DSSS	OFDM	DSSS, OFDM	OFDM	SC-OFDM	SC, OFDM
Antenna configuration	1´1 SISO	1´1 SISO	1´1 SISO	Up to 4´4 MIMO	Up to 8´8 MIMO, MU-MIMO	1´1 SISO

El alcance de las redes es sensible a la distancia y a las interferencias.



100 pies -> 30 mts aprox

www.54g.org

NIVEL DE ENLACE DE DATOS 802.11

El estándar IEEE 802.11 define sólo la capa MAC para el nivel de enlace de datos.

•La funcionalidad del subnivel MAC consiste en un servicio de transporte no orientado a conexión, el cual se define en base a un formato de trama y un mecanismo de control de acceso al medio.

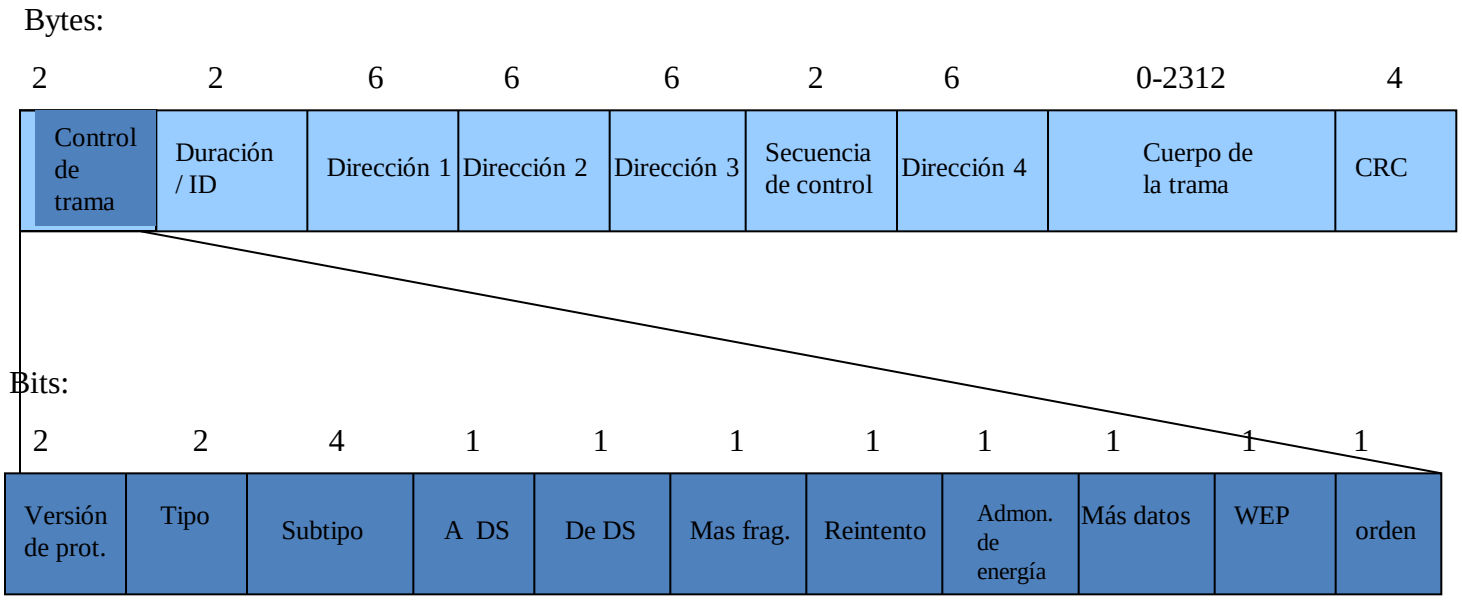
El estándar define en realidad 3 tipos básicos de trama:

•De datos: Utilizadas para transmitir datos de los niveles superiores entre estaciones

•De control: Utilizadas para regular el acceso al medio de la red y para reconocer las tramas de datos transmitidas.

•De administración: Utilizadas para intercambiar información de administración de la red y realizar funciones de autenticación.

Trama 802.11



•Control de trama: se encarga de habilitar las diversas funciones de los campos de la trama, las cuales son:

•Versión del protocolo: Actualmente la versión de este campo es 0

•Tipo: Especifica si es una trama de administración (00), de control (01) o de datos (10)

•A DS:Especifica si la trama va dirigida hacia (AP) al Sistema de Distribución.

•D DS: En 1 indica que la trama se ha recibido de un Sistema de distribución.

•Más fragmentos: Indica que el paquete contiene un fragmento de una trama y que hay más.

•Reintento: En 1 indica que el paquete contiene un fragmento que se está retransmitiendo.

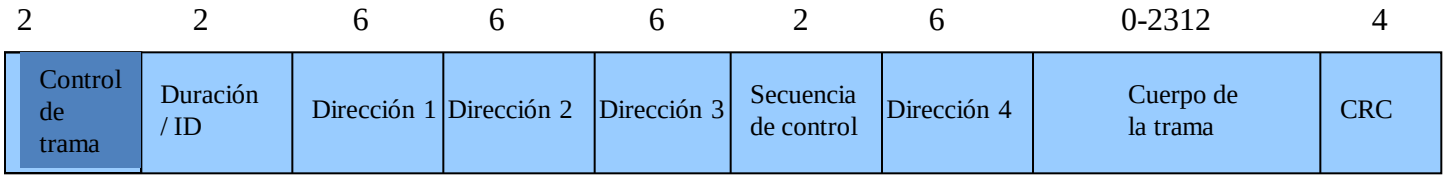
•Administración de energía: un valor 0 indica que la estación esta funcionando en modo activo; un valor 1 indica que la estación se encuentra en modo de ahorro de energía

•Más datos: Un valor 1 indica que un AP tiene más paquetes para la estación que están almacenados.

•WEP: Indica si se ha utilizado WEP

•Orden: Indica que la trama se transmite utilizado la clase de servicio “Estrictamente ordenado”

Bytes:



•DURACIÓN: Contiene la identidad de la estación que transmite la trama cuando se utiliza ahorro de energía. Si no se utiliza Ahorro de energía este campo contiene el tiempo para transmitir una trama.

•DIRECCIÓN 1 - 4: Contiene una dirección que identifica al receptor de la trama, usando una de las direcciones distintas definidas en las comunicaciones del subnivel MAC, dependiendo de los valores A DS y de DS.

•CONTROL DE SECUENCIA: Contiene dos campos utilizados para asociar los fragmentos de una secuencia particular y reemsamblarlos en el orden correcto.

•CUERPO DE LA TRAMA: Contiene la información que se está transmitiendo a la estación receptora actualmente.

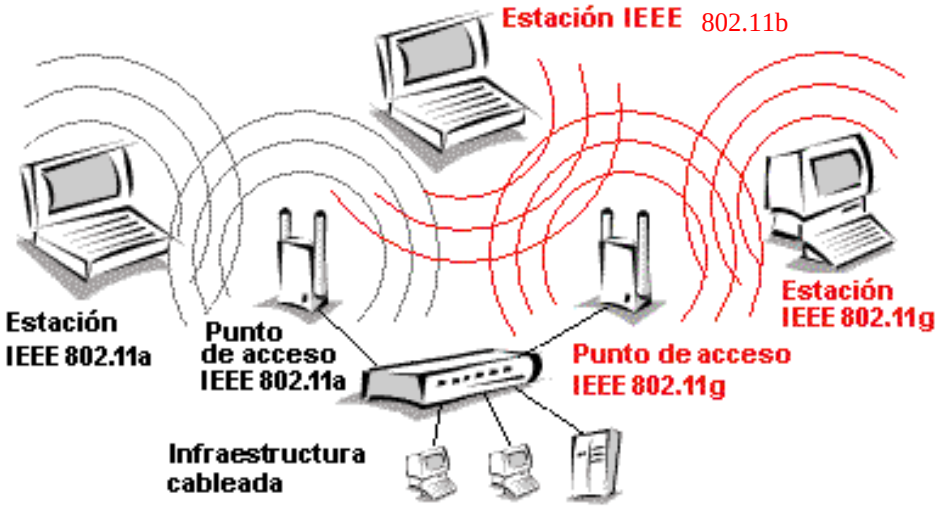
•SECUENCIA DE VERIFICACIÓN DE TRAMA: Contiene el valor de comprobación de redundancia cíclica usado por el sistema receptor para verificar que la trama se transmitió sin errores.

TIPOS DE DIRECCIONES DEL SUBNIVEL MAC

Al DS	Del DS	Función	Valor de la Dirección 1	Valor de la Dirección 2	Valor de la Dirección 3	Valor de la Dirección 4
0	0	Tramas de datos intercambiado por estaciones del mismo IBSS y todas las tramas de control y de administración	DA	SA	BSSID	No usado
1	0	Tramas de datos transmitidas al DS	DA	BSSID	SA	No usado
0	1	Tramas de datos que salen del DS	BSSID	SA	DA	No usado
1	1	Tramas del sistema de distribución intercambiadas por los AP de un DS	RA	TA	DA	SA

SA: Dirección del origen
DA: Dirección del destino
TA: Dirección del emisor
RA: Dirección del receptor

A pesar de que la especificación a no es compatible puede coexistir con g y b.



Control de acceso al medio.

Es similar al utilizado en Ethernet, ya que se trata de una técnica de contienda, sin embargo el medio físico utilizado (canal radio) tiene ciertas características diferentes a los medios guiados:

•Esta sujeto a interferencias, por lo que es menos confiable.

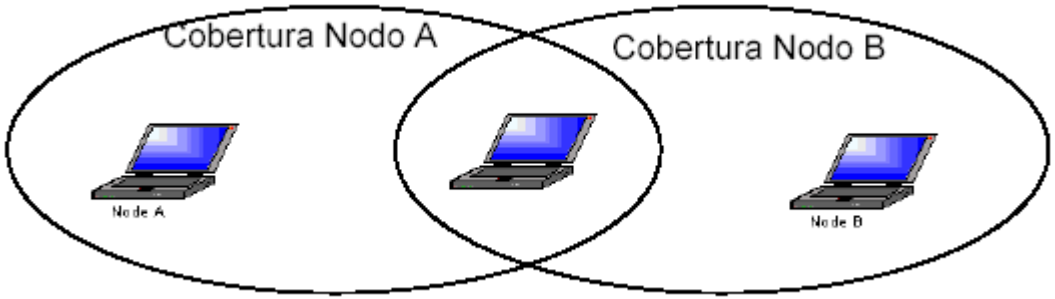
•Las terminales no pueden monitorizar fácilmente el canal.

•Las terminales cambian continuamente su posición debido a la movilidad.

•No todas las estaciones reciben todas las transmisiones (Por lo tanto no es posible detectar todas las colisiones)

•La zona de cobertura no está perfectamente delimitada.

•Se presenta el problema de “estación oculta”

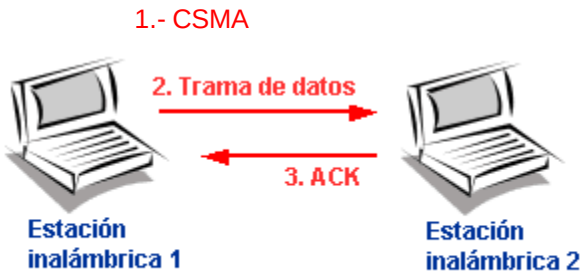


La estación A no “ve” a la estación B

Debido a las características del canal radio la técnica de acceso al medio utilizada en 802.11 es CSMA/CA (Acceso múltiple con detección de portadora evitando colisiones)

1.- CSMA

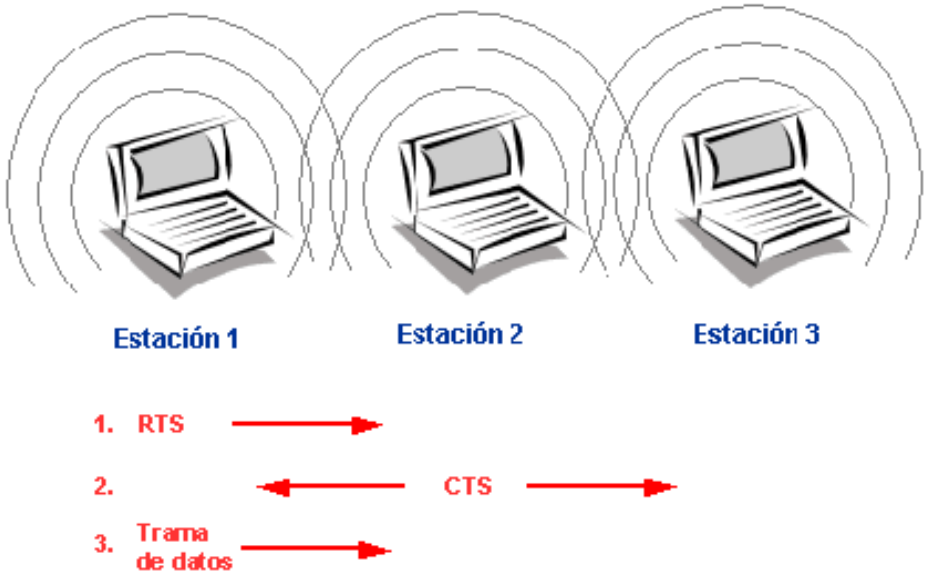
CSMA/CA (Acceso múltiple con detección de portadora y evitación de colisiones)



Las banderas de control ACK y el tiempo de retroceso se colocan en el campo Duración/ID

- La estación que desee transmitir debe escuchar el canal y posteriormente transmitir si el canal está libre
    - Una vez que transmite su información la estación destino envia un ACK (trama de control) para indicar que se recibio la información sin errores (checa el CRC)
- Si el canal esta ocupado la estación calcula un tiempo de retroceso aleatorio para volver a intentar transmitir.
- La utilización de este tiempo de retirada aleatorio, provoca que las distintas estaciones que están a la espera de transmitir no lo hagan al mismo tiempo y se evitan colisiones.

Para evitar el problema de “estación oculta” el mecanismo CSMA/CA puede ser modificado opcionalmente agregando el envio de una trama de control (RTS/CTS) de solicitud con confirmación antes del envio de la información. RTS/CTS son tramas de menor tamaño en comparación a las tramas de datos.



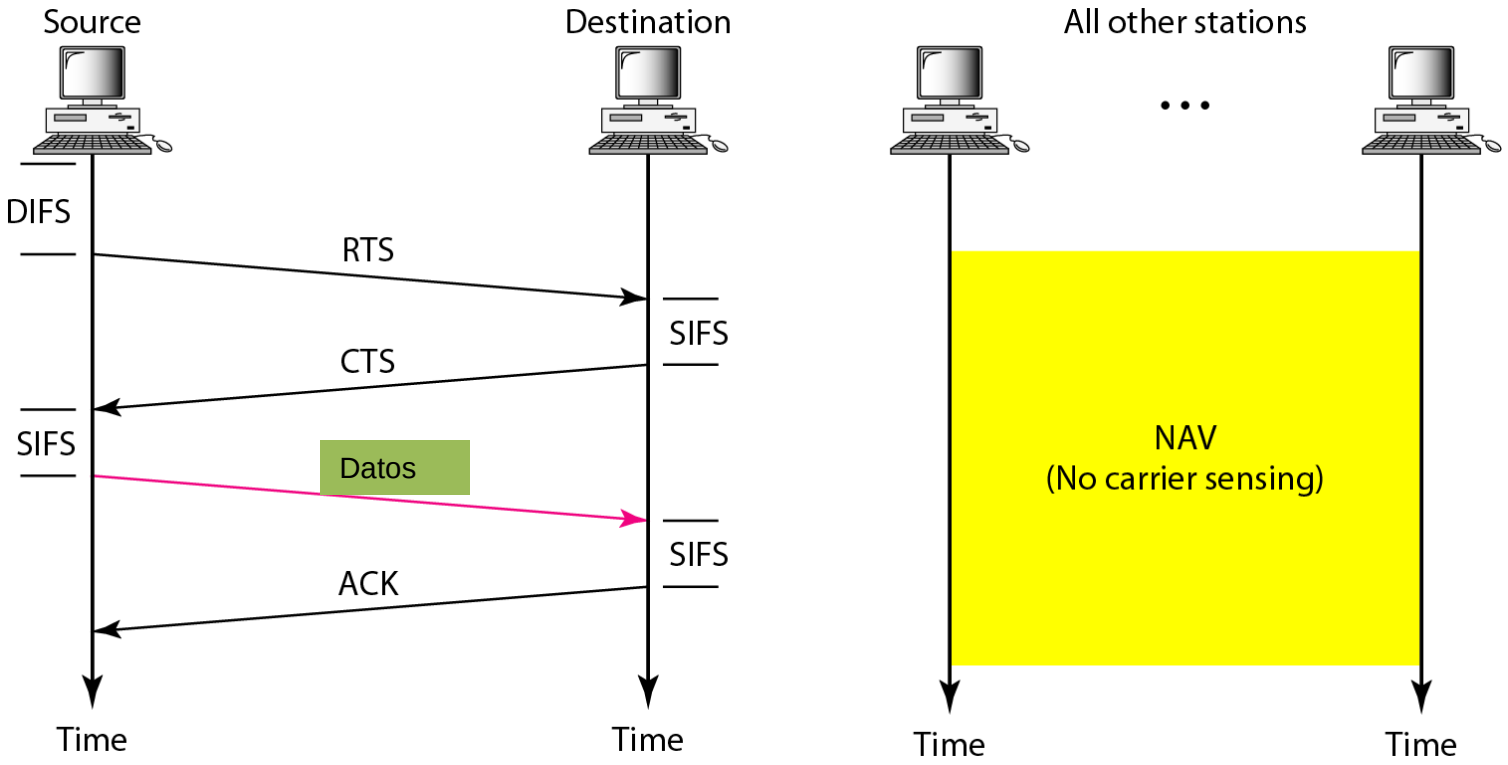
RTS: Request to send

CTS: Clear to Send

Ambos banderas son colocadas en el campo Duración/ID

Debido a que este mecanismo aumenta el tráfico, su utilización es opcional y puede administrarse con la utileria del equipo. Asi mismo con la finalidad de reducir la cantidad de información con error también es posible determinar el tamaño máximo de una trama de datos.

CSMA/CA



DIFS→ Espacio entre tramas distribuido (Distribuited InterFrames Space)
SIFS → Espacio corto entre tramas
RTS → Permiso para enviar (Request to Send)
CTS → Libre para enviar (Clear to Send)
NAV → Vector de asignacion de red (Network Address Vector)

Unidad 2. Internet y Sistemas inalámbricos.

Contenido de la unidad

2.1 Redes inalámbricas
2.2 Sistemas de telefonía móvil
2.3Tecnologías emergentes de sistemas inalámbricos

¿Qué es un dispositivo móvil?

Un dispositivo de bolsillo, con capacidades limitadas de cómputo, capaz de mantener una conexión mientras está en movimiento.
Comunicación inalámbrica y móvil

Los dispositivos móviles basan sus capacidades de conexión en los sistemas de comunicación móvil inalámbricos.

Los sistemas de comunicación móvil utilizan el aire como medio de transmisión a través de ondas de radio.

Ofrecen conectividad total tanto espacial como temporal.

Sus principales ventajas son:

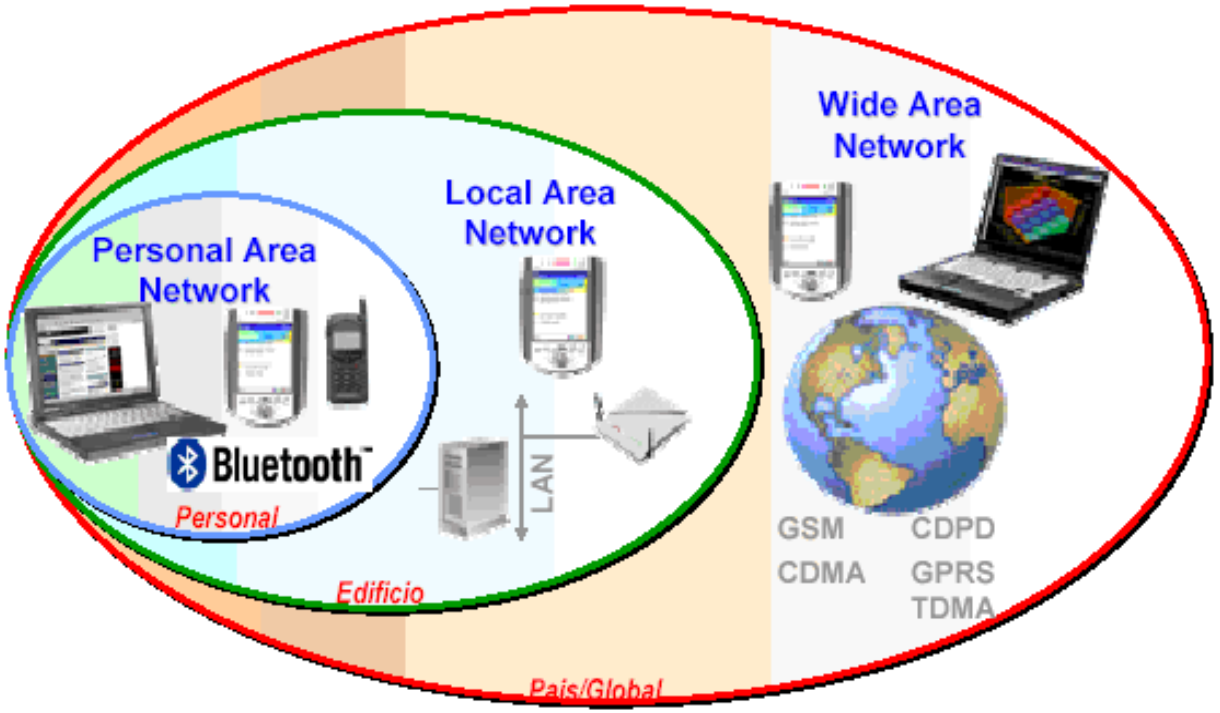
- Flexibilidad: Los nodos no están atados a un cable
- Poca planeación: Se elimina el concepto de topología de red.
- Robustez: Funcionan cuando las redes cableadas no.

También tienen desventajas:

•Ofrecen peor calidad de servicio que las redes cableadas.
•Son susceptibles a interferencias.
•Más costosas
•Restricciones de ancho de banda
•Menos seguras.

Hoy en día existen una multitud de tecnologías inalámbricas

- Telefonía móvil
- Las redes inalámbricas personales, WPAN (Bluetooth, NFC)
- Redes locales (Wi-Fi),
- Redes metropolitanas (Wi-Max)



Estándares inalámbricos

- Estándares de telefonía: GSM / GPRS / UMTS, LTE
- Redes inalámbricas de área personal (PAN) Bluetooth y Zigbee (802.15.1/2/3/4),
- Redes inalámbricas de área local (WLAN): 802.11a/b/g/n Wi-Fi
- Redes inalámbricas de área metropolitana (WMAN): 802.16a/b Wi-Max

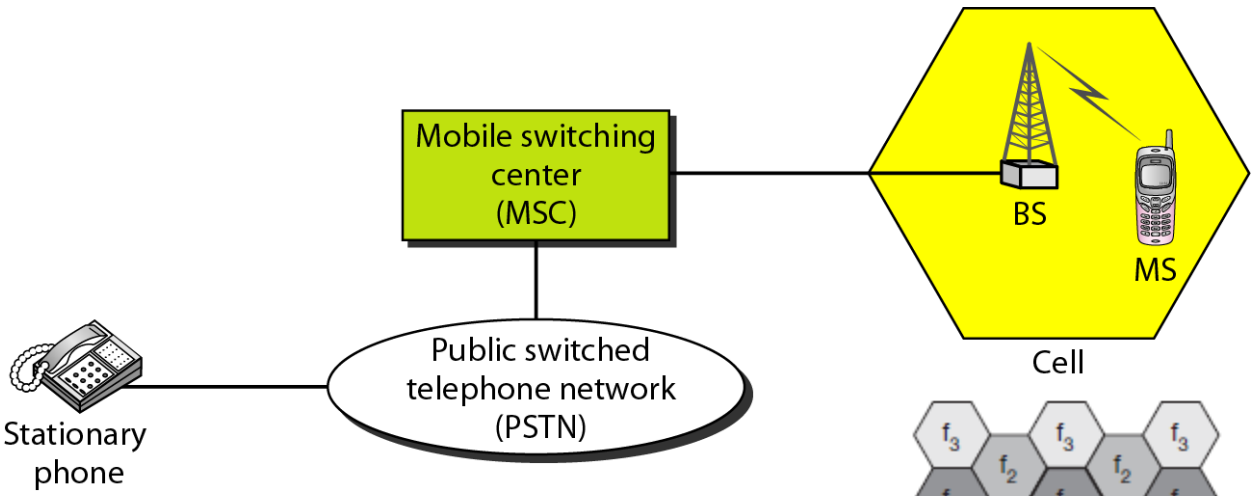
Los teléfonos móviles son los dispositivos móviles mas usados en la actualidad.

Su capacidad de conexión se basa principalmente en las redes de telefonía móvil, pero tienen capacidades de conexión a otros tipos de redes.

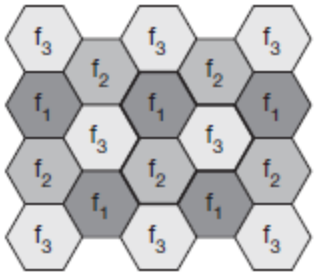
Telefonía Móvil

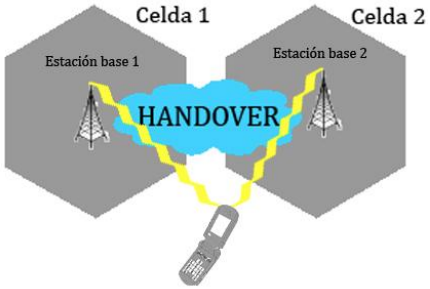
La red de telefonía móvil o sistema de comunicación móvil también es conocido como telefonía celular.

Este sistema esta diseñado para proveer comunicación entre unidades móviles de baja potencia a través de estaciones base (BSs) o entre una unidad móvil y una unidad estacionaria.



El numero y forma de células depende del entorno y clima





Redes de telefonía Móviles

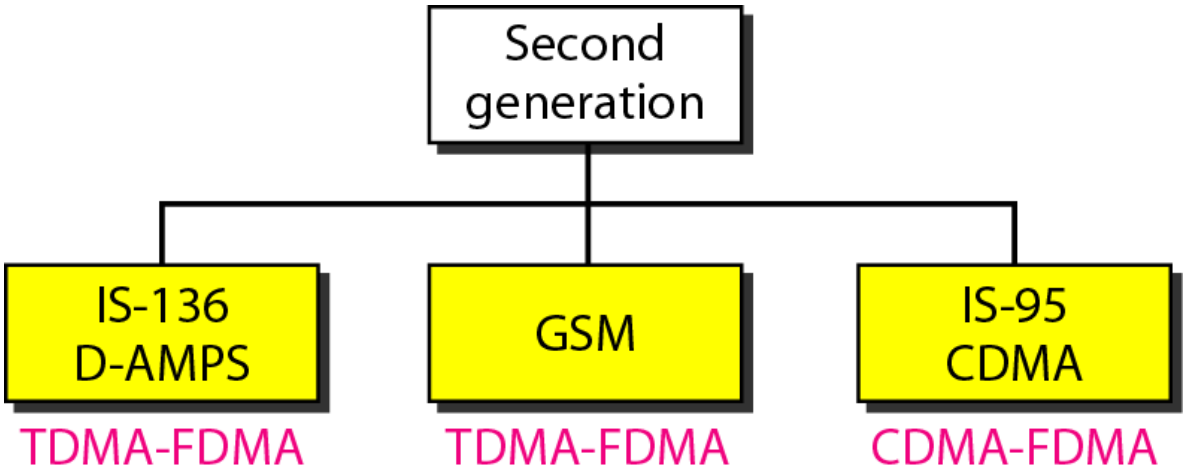
- **Primera Generación**
  - A mediados de los 80 surge el sistema AMPS (American (Analog, Advanced Mobile Phone System), con capacidad para transmitir voz pero no datos. **Transmisión analógica. Conmutación de circuitos.**

En los países europeos, se implantaron varios sistema 1G muy similares a AMPS , entre ellos:

† Total Access Communications System (**TACS**) en el Reino Unido, Italia, España, Austria e Irlanda.
† Nordic Mobile Telephone **(NMT**) en varios países
† **C-450** en Alemania y Portugal
† **Radiocom 2000** en Francia

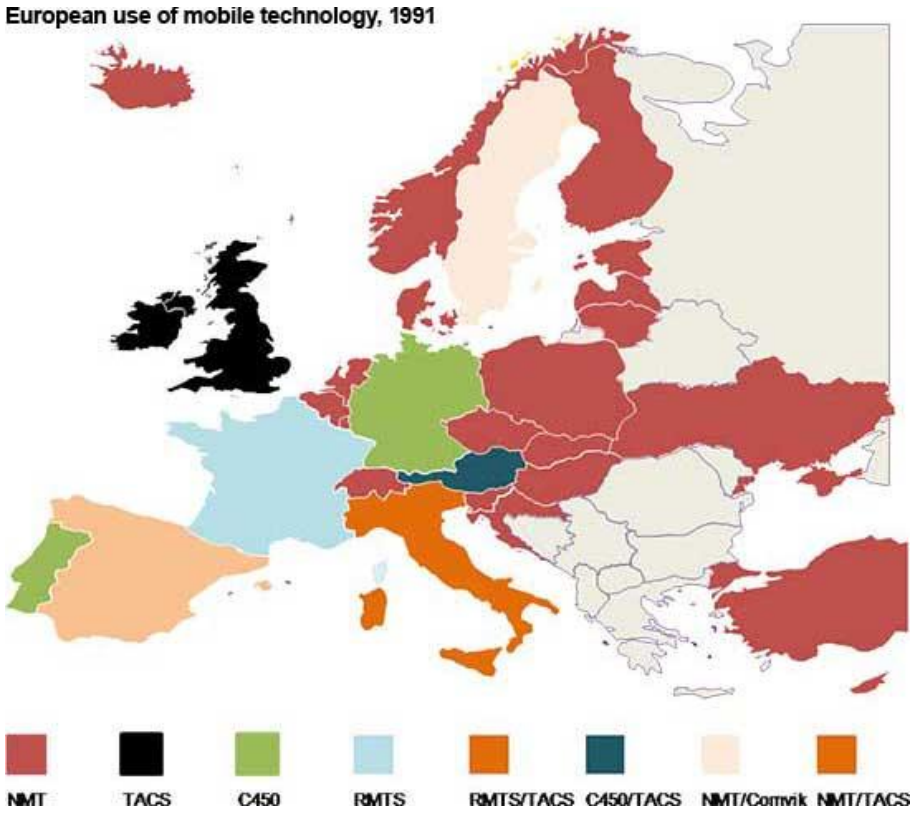
Segunda Generación

En los 90’s se desarrolla el sistema GSM, que permite la transmisión de datos a baja velocidad 9600 bit/s, lo que supuso la revolución del servicio SMS. **Transmisión Digital.**



GSM (2G)

1991



NMT → Nordic Mobile Telephony

TACS → Total Access Communications System

Sistema Global de Comunicaciones Móviles

(Global System for Mobile communications o Groupe Special Mobile)

Estándar de sistema de comunicaciones móviles que surge en Europa para resolver el problema de no poder disponer de un mismo teléfono móvil al pasar de un país a otro.

Propiedades de GSM

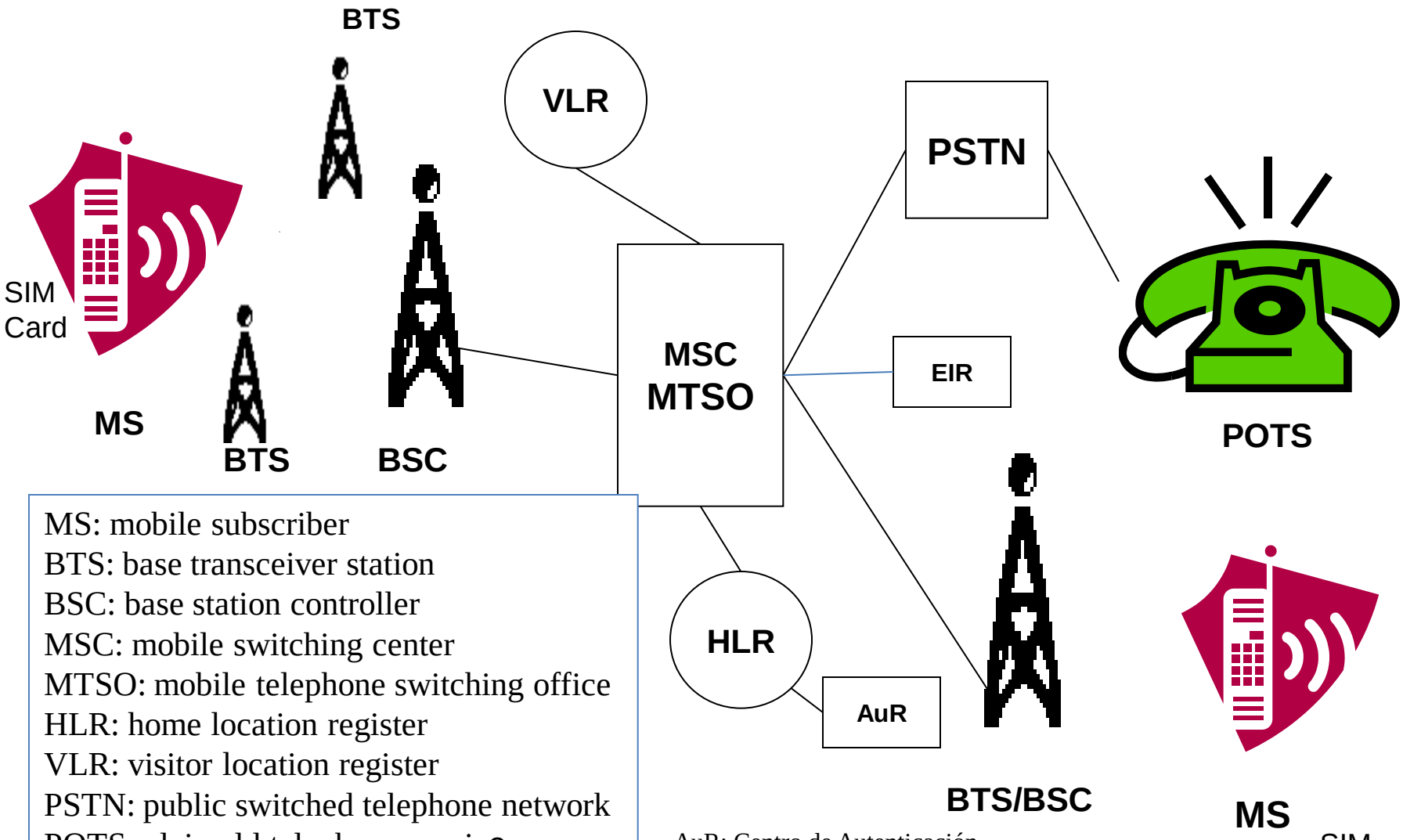
- Sistema digital: mejora la eficiencia espectral, mejor calidad de transmisión, posibilidades de nuevos servicios y más seguridad.
- Velocidad 9.6 kbps – 13 kbps
- Utiliza un hibrido o combinación de TDMA y FDMA
- Emplea mecanismos de autentificación y cifrado para garantizar la privacidad de las comunicaciones. (Además uso de SIM en el terminal)
- Se puso en servicio en 1991 con trece operadores, en 1993 aumento a 45 operadores, y en 1994 ya se disponía de 104 operadores en 60 países.
- Hoy en día sigue siendo el estándar de telefonía móvil más extendido.

Servicios Ofrecidos por GSM

- **Servicios básicos**
  - *Voz*
  - *Llamadas de emergencia*
  - *Fax*
  - *Servicios de mensajes cortos*
  - *Buzón de voz*
  - *Buzón de fax*

- **Servicios suplementarios**
  - Desvío de llamadas
  - Restricción de llamadas salientes y entrantes
  - Aviso de tarifa
  - Llamada en espera
  - Multiconferencia

Arquitectura GSM



MS: mobile subscriber
BTS: base transceiver station
BSC: base station controller
MSC: mobile switching center
MTSO: mobile telephone switching office
HLR: home location register
VLR: visitor location register
PSTN: public switched telephone network
POTS: plain old telephone service

AuR: Centro de Autenticación

EIR: Registro de Identidad del equipo

GPRS (2.5G)

1999

General Packet Radio Service

- Basado en GSM
- Comparte el rango de frecuencias de la red GSM
- Transmisión de datos por medio de 'paquetes' al contrario de GSM que utiliza conmutación de circuitos
- Soporta el uso del protocolo IP en la transmisión de paquetes.
- Always-on: Factura solo los datos enviados o recibidos
- Velocidad de transmisión teórica de 171,2 Kbps

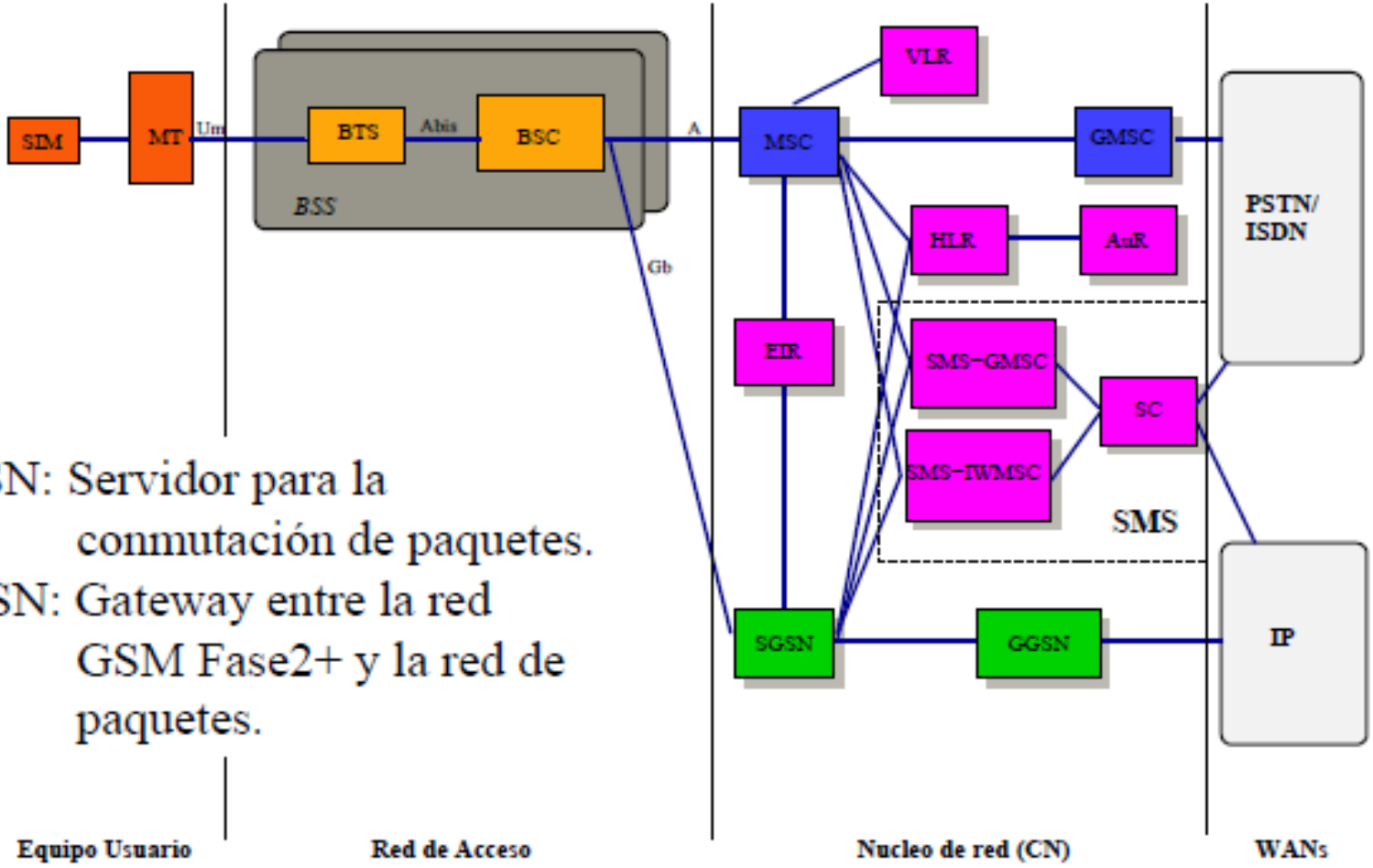
GPRS Propiedades

- Canal compartido: los canales se comparten entre usuarios, solamente se les asigna el canal cuando realmente están transmitiendo datos.

- GPRS utiliza un numero variable de ranuras TDMA

- Mayor velocidad y eficiencia: (unas 18 veces mayor que GSM), además la tecnología utilizada permite compartir cada canal por varios usuarios, mejorando así la eficiencia en la utilización de los recursos de red.

Arquitectura GPRS



SGSN: Servidor para la conmutación de paquetes.

GGSN: Gateway entre la red GSM Fase2+ y la red de paquetes.

Cambios en la infraestructura con GPRS

BTS: Actualización del software
BSC: Actualización del software y un nuevo componente de hardware para encaminar el tráfico a la red GPRS.

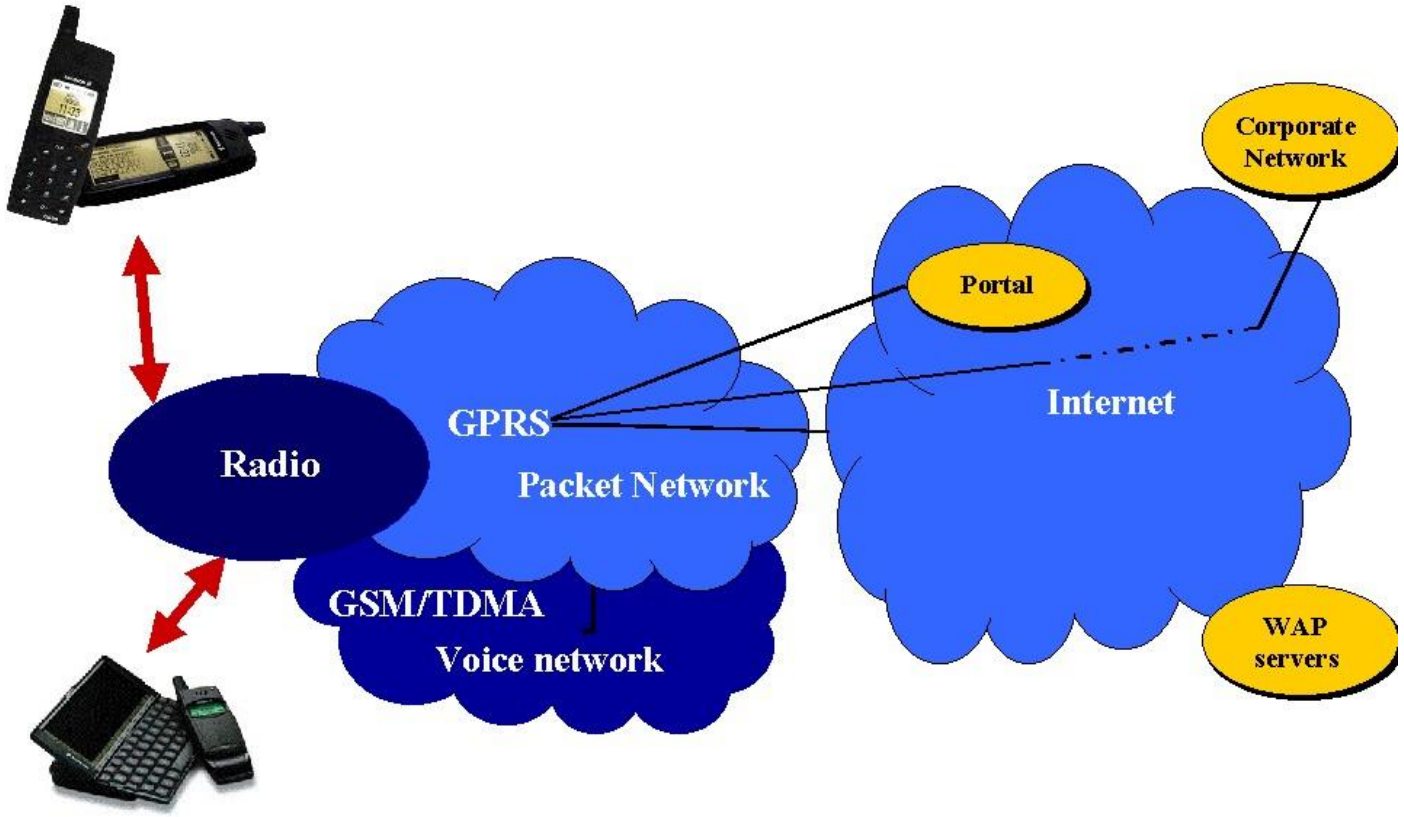
Red Troncal: Implantación de dos nuevos elementos: SGSN y GGSN

SGSN (Serving GPRS Support Node): Es un nuevo centro de conmutación. Es el encargado de enviar paquetes de las terminales móviles de su área de servicio y funciones de gestión de movilidad.

GGSN (Gateway GPRS Support Node): Representan interfaces a redes externas IP, realizando encaminamiento y traducción de direcciones.

Los terminales son completamente distintos

Arquitectura GPRS



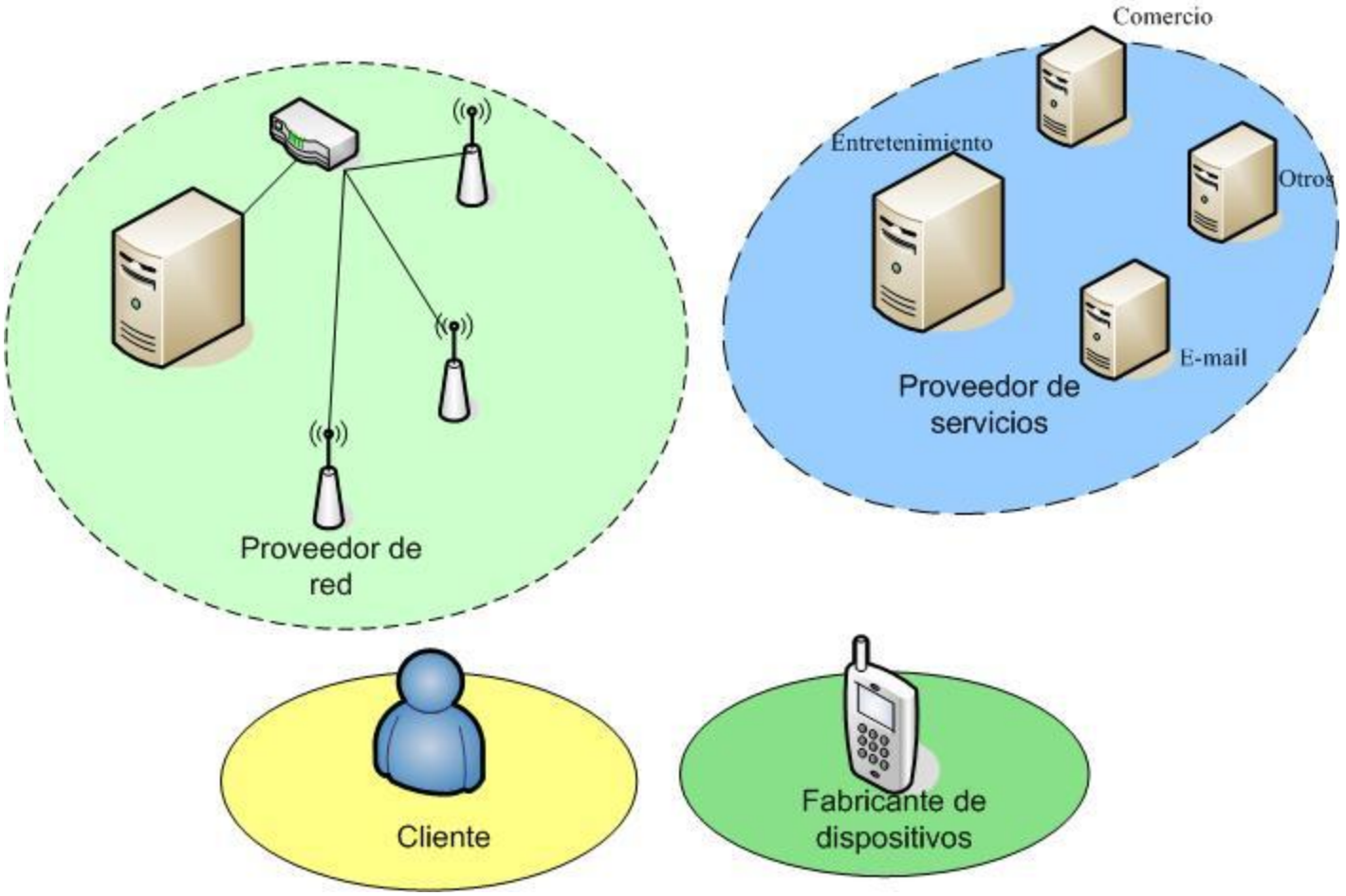
Servicios GPRS

- Acceder en movilidad a Internet y al correo electrónico.
- Acceder con facilidad a la intranet corporativa
- Acceso a cuentas de correo corporativas (intranet)
- Acceso a bases de datos y aplicaciones corporativas desde un dispositivo móvil
- Acceso GPRS a aplicaciones WAP (Wireless Application Protocol) para usos empresariales (a través del servicio WAP).
- Acceso a servicios de información (a través del servicio WAP).

GPRS vs GSM

- Velocidad de transferencia mayor que en GSM, hasta 171 Kbps
- Conexión permanente: Tiempo de establecimiento de conexión inferior al segundo
- Pago por cantidad de información transmitida, no por tiempo de conexión.
- Coste nulo de establecimiento de la transmisión

Uno de los principales cambios con los sistemas 2G fue la separación de los elementos del sistema.



EDGE (2.5)

2002

Enhanced data rates for GSM Evolution o EGPRS

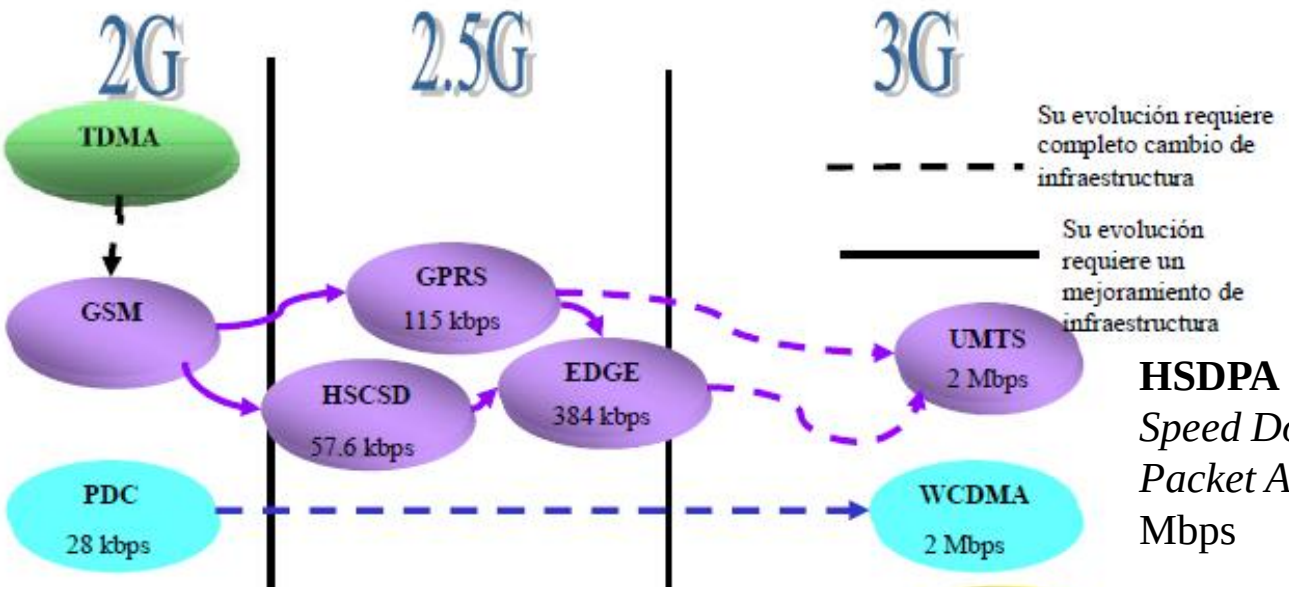
- No hubo cambios en la estructura de la red. Solo a nivel físico.
- Introducir un nuevo esquema de modulación y codificación de canal (8-PSK/GMSK (Gaussian Minimum Shift Keying))
- Re-usar tanto de la capa física de GSM como sea posible
- Soporta tasas de bits hasta 473 Kbps
- Emplea redundancia incremental a fin de mejorar la eficiencia en el uso del canal
- Apropiado para aplicaciones con requerimientos de retardo relajados

Redes Móviles

- **Segunda Generación y media**
  - Surge HSCSD (High Speed Circuit Switched Data), con pocos cambios en el servicio.
  - Se mejora la capacidad de transmisión de datos con GPRS.
  - También surge EDGE que permite la transmisión de 384 Kbits/s mejorando a GPRS y GSM.
- **Tercera Generación**
  - Añade más funcionalidades: acceso a internet, servicios de banda ancha, roaming
  - Aparece UMTS, permitiendo la transmisión de video e imágenes en tiempo real.
- **Cuarta Generación**

  LTE

Evolución de las Redes Celulares



PDC-Personal digital celluar, se utiliza solo en Japón

HSDPA (*High Speed Downlink Packet Access*) – 14 Mbps

Además de estas existen otras tecnologías que se han desarrollado en el mundo.

Pero no termina aquí…

4G

Cuarta Generación de telefonía celular (4G)

3G

2G

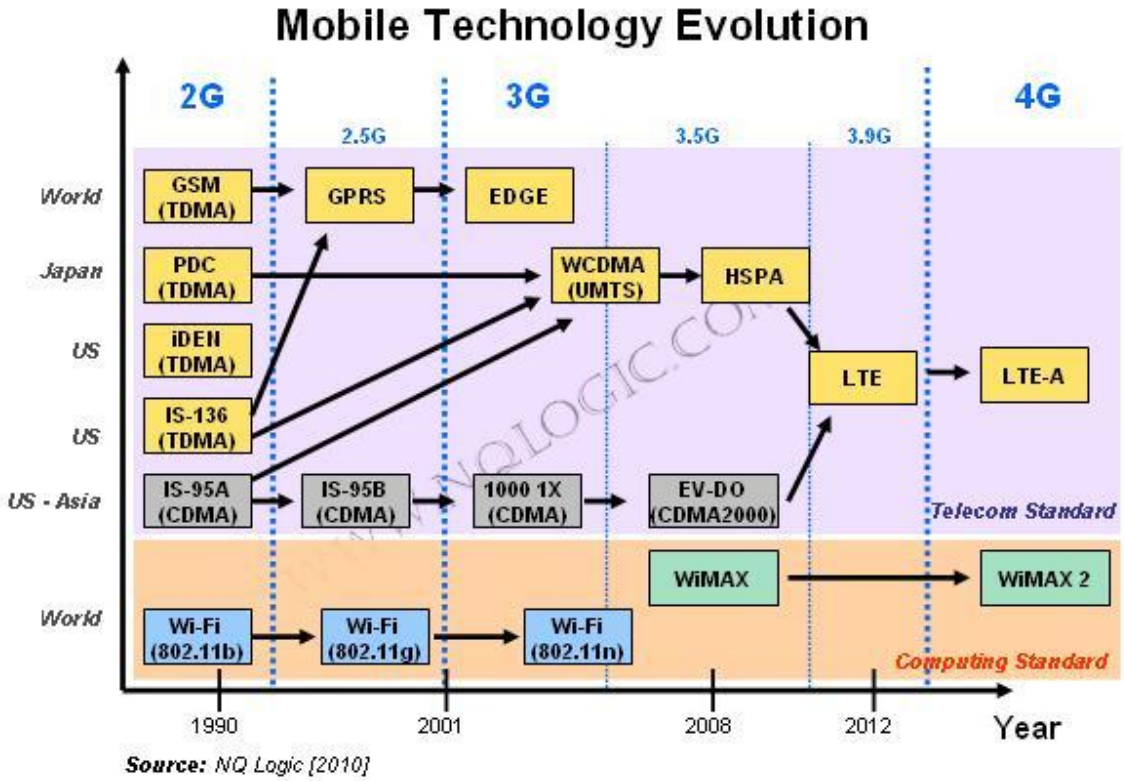
1G

0G

4G no es una tecnología o estándar definido, puede considerarse como una colección de tecnologías y protocolos que permiten crear redes optimizadas para la transmisión de datos.

Las redes 4G están planeadas para proveer velocidades de ***100 Mbps*** para terminales móviles y de ***1 Gbps*** para terminales estacionarias.

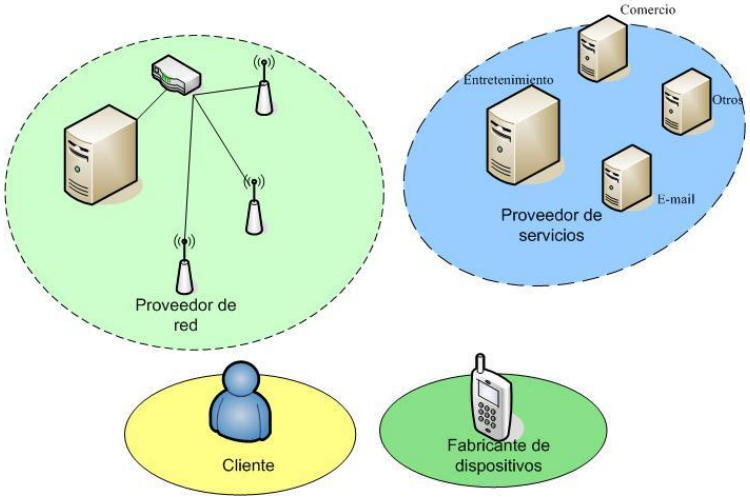
Evolución de telefonía móvil



Source: *NQ Logic [2010]*

1G	2G	3G	4G	5G
1981	1992	2001	2010	2020(?)
2 Kbps	64 Kbps	2 Mbps	100 Mbps	10 Gbps
Basic voice service using analog protocols	Designed primarily for voice using the digital standards (GSM/CDMA)	First mobile broadband utilizing IP protocols (WCDMA / CDMA2000)	True mobile broadband on a unified standard (LTE)	'Tactile Internet' with service-aware devices and fiber-like speeds
				?

Uno de los principales cambios con los sistemas 2G fue la separación de los elementos del sistema.



1G	2G	3G	4G	5G
1981	1992	2001	2010	2020(?)
2 Kbps	64 Kbps	2 Mbps	100 Mbps	10 Gbps
Basic voice service using analog protocols	Designed primarily for voice using the digital standards (GSM/CDMA)	First mobile broadband utilizing IP protocols (WCDMA / CDMA2000)	True mobile broadband on a unified standard (LTE)	'Tactile Internet' with service-aware devices and fiber-like speeds
				?

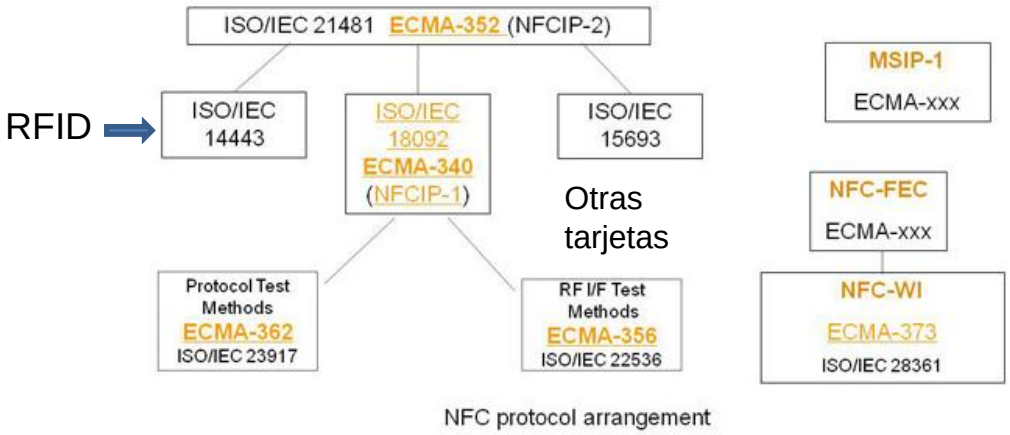
Near Field Communication (NFC)

NFC son las siglas en inglés de Near Field Communication → **comunicación de proximidad.?**

Se trata de un protocolo de comunicación inalámbrica limitado a distancias cortas de unos diez centímetros. Es un sistema diseñado específicamente para la realización de transacciones.

NFC tiene su equivalencia en la norma ISO18092 (NFCIP-1) y en ISO 21481 (NFCIP-2)

Esta tecnología fue desarrollada por NXP, filial de semiconductores de Philips, para la implantación de un sistema de pago con teléfonos móviles que fuera robusto y rápido en 2004.



NFC protocol arrangement

ISO21481/ ECMA 352 (NFC interface and protocol)

Fuente: NFC forum

WHAT'S THE DIFFERENCE BETWEEN ... RFID & NFC?

RADIO FREQUENCY IDENTIFICATION

NEAR FIELD COMMUNICATION

3 PARTS OF A TYPICAL RFID SYSTEM:

RFID FREQUENCY RANGES:

Low Frequency (LF):	High Frequency (HF):	Ultra High Frequency (UHF):
125–134 kHz	13.56 MHz	856 MHz to 960 MHz
(LF)	(HF)	(UHF)
Range: Up to 10 cm	Range: Up to 30 cm	Range: Up to 100 m

RFID CAN BE EITHER...

ACTIVE
- Own power source
- Broadcast range up to 100 meters
- Ideal for material location

...or PASSIVE
- No power source
- Powered by a reader
- Read range from near contact up to 25 meters

POPULAR USES:

- Asset Tracking
- Race Timing
- Inventory Management
- Tool Tracking
- Access Control
- Attendee Tracking

- Operate at the same frequency (13.56 MHz) as HF RFID readers and tags
- May act as both a reader and a tag
- Devices must be in close proximity due to the short read range limitations of its radio frequency (usually no more than a few centimeters)

POPULAR USES:

INFORMATION SHARING
Transferring info between smartphones by tapping two devices together

CONTACTLESS PAYMENT
Credit cards, debit cards, key fobs and other devices use NFC to make secure payments

"There are 150 million NFC devices now. By 2014, there will be 300 MILLION."

Reed Peterson, Head of Business & Market Development for the GSMA

SMART POSTERS
Using an NFC-enabled smartphone, viewers can access exclusive content

NINE OF THE TOP TEN

HANDSET MAKERS HAVE NFC-ENABLED DEVICES AND BOTH ANDROID & WINDOWS PHONES SUPPORT THE TECHNOLOGY

NFC es un subconjunto de RFID

- Tecnología NFC = RFID (Identificación sin contacto físico) + Tecnologías interconectadas.
- Trabaja en la banda de los 13,56 MHz → No se le aplica ninguna restricción y no requiere ninguna licencia para su uso.
- Velocidad: 106 kbit/s, 212 kbit/s, 424 kbit/s, 848 kbps
- Se puede usar para configurar e iniciar otras conexiones wireless como son Bluetooth, Wi-fi o UltraWireband.

NFCIP→ NFC Interfaz y Protocolo
Describe funcionamiento, modos de funcionamiento (estandarizado en ISO y ECMA)

Funcionamiento de NFC

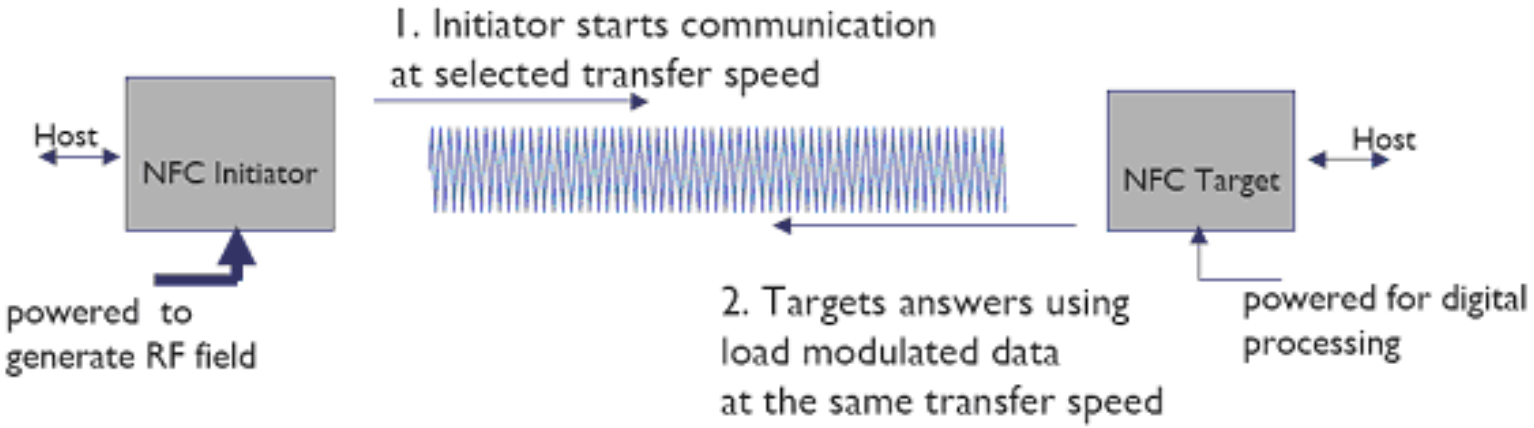
- NFC está basado en tecnologías sin contacto e Identificación por Radio Frecuencia (RFID), por lo que es necesario un lector y una etiqueta.
- Cuando se enciende el lector, emite una señal de radio de corto alcance que activa el microchip de la etiqueta con lo que podremos leer una pequeña cantidad de datos que se encuentra almacenado en ella.

Modos de Operación

- En el protocolo NFC siempre hay uno que inicia la conversación y es este el que monitorizará la misma, este rol es intercambiable entre las dos partes implicadas.
- Existen dos modos de funcionamiento:
  - Activo
  - Pasivo
- Todos los dispositivos del estándar NFCIP deben soportar ambos modos.

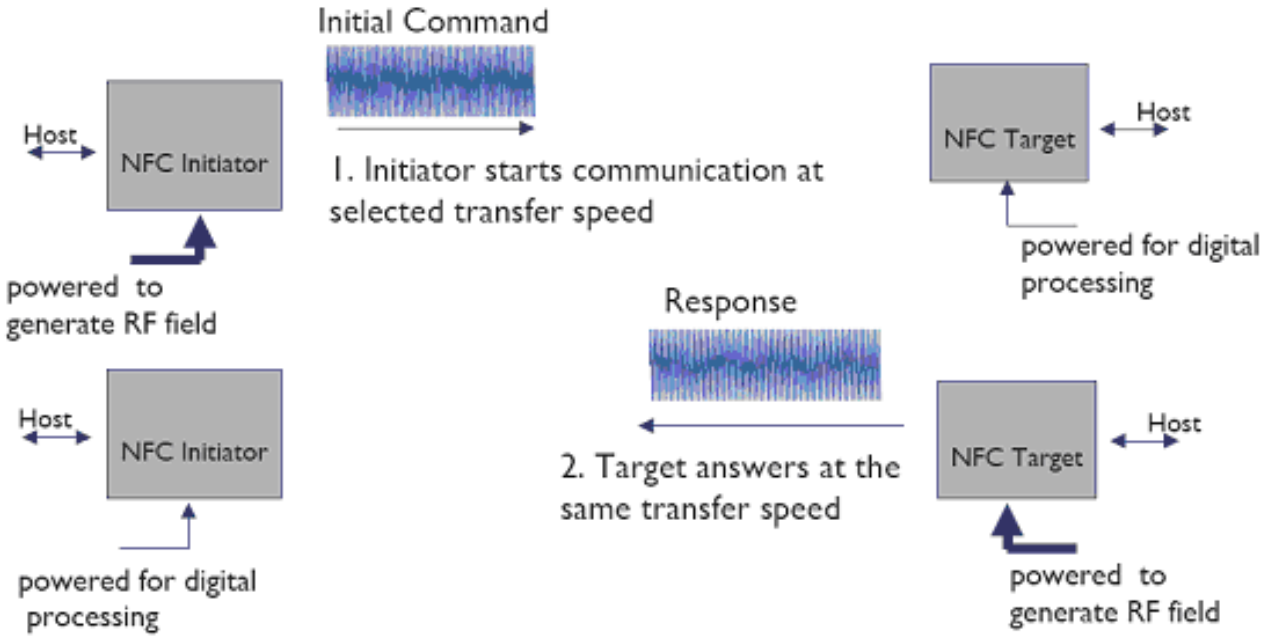
Modos de Funcionamiento

- **Pasivo:** Sólo un dispositivo genera el campo electromagnético y el otro se aprovecha de la modulación de la carga para poder transferir los datos. El iniciador de la comunicación es el encargado de generar el campo electromagnético.



Modos de Funcionamiento

- **Activo:** Ambos dispositivos generan su propio campo electromagnético, que utilizarán para transmitir sus datos. Ambos dispositivos necesitan energía para funcionar.



Tipos de comunicación NFC

Dispositivo A	Dispositivo B	Descripción
ACTIVO	ACTIVO	Cuando se envian datos desde un dispositivo activo se genera un campo de radio-frecuencia y no se hace cuando se reciben. Por lo tanto, se generarán campos de RF de forma alternada entre ambos dispositivos activos.
ACTIVO	PASIVO	El campo de radio-frecuencia sólo lo genera el dispositivo A.
PASIVO	ACTIVO	El campo de radio-frecuencia sólo lo genera el dispositivo B.

Transacciones

- Toda comunicación NFC consta de 5 fases:
  - Descubrimiento
  - Autenticación
  - Negociación
  - Transferencia
  - Reconocimiento
- Además, NFC también incluye:
  - Procedimiento de autenticación seguro
  - Mecanismo anti-colisiones

Comparación con otras tecnologías

	NFC	RFID	IrDa	Bluetooth
Set -up time	<0.1ms	<0.1ms	~0.5s	~6 sec
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy, intuitive, fast	Item centric Easy	Data centric Easy	Data centric Medium
Selectivity	High, given, security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

Foro NFC

- El Near Field Communication (NFC) Forum es una asociación industrial sin animo de lucro fundada por NXP Semiconductors, Sony Corporation y Nokia para regular el uso de la interacción inalámbrica de corto alcance en la electrónica de consumo, dispositivos móviles y los PCs.

- Web → http://www.nfc-forum.org/

El NFC Forum promueve la implantación y la estandarización de la Tecnología NFC como mecanismo para la interoperabilidad entre dispositivos y servicios.

Para conseguir esto, se encarga de:

- Desarrollar especificaciones basadas en estándares
- Asegurarse del uso de las especificaciones del NFC Forum
- Trabajar para que los productos con tecnología NFC cumplan con las especificaciones del NFC Forum
- Educar a los consumidores y las empresas respecto de la Tecnología NFC

El NFC Forum ha establecido mecanismos de comunicación y operaciones entre dispositivos compatibles.

Table 1. NFC Forum Device communication links

		Communication link between NFC Forum Device in:		
		Peer mode	**Reader/Writer mode**	**Card emulation mode**
and an NFC Forum Device in:	NFC Forum Peer mode:	yes	-	-
	NFC Forum Reader/Writer mode:	-	-	yes
	NFC Forum card emulation mode:	-	yes	-
and an NFC Forum Tag in:	operating as ISO18092 Target:	-	yes	-
	operating as one of the NFC Forum Type Tag Platforms:	-	yes[1]	-
and a Reader/Writer terminal:	-	-	-	yes

Fuente: NFC Tags white paper NXP

Foro NFC

El NFC Forum ha establecido un estándar en la que se registra un formato común para poder compartir datos entre los dispositivos NFC entre sí y/o entre los dispositivos y las etiquetas NFC.

- **NFC Data Exchange Format (NDEF)**

  Especifica un formato común y compacto para el intercambio de datos.

- **NFC Record Type Definition (RTD)**

  Especifica tipos de registros estándar que pueden ser enviados en los mensajes intercambiados entre los dispositivos NFC.

  - **Smart Poster RTD**

    Para posters que incorporen etiquetas con datos (URLs, SMSs o números de teléfono).

  - **Text RTD**

    Para registros que solo contienen texto.

  - **Uniform Resource Identifier (URI) RTD**

    Para registros que se refieren a un recurso de Internet

Otros: Handover, vCall, Call Request.

Tipos de Etiquetas NFC

	Type 1	Type 2	Type 3	Type 4
RF Interface	ISO 14443 A-2	ISO 14443 A-2	FeliCa (ISO 18092, passive communication mode at 212 kbits/sec)	ISO 14443-2
Initialization	ISO 14443 A-3	ISO 14443 A-3	FeliCa (ISO 18092, passive communication mode at 212 kbits/sec)	ISO 14443-3
Speed	106 kbits/sec	106 kbits/sec	212 kbits/sec	106-424 kbits/sec
Protocol	Specific Command set	Specific Command Set	FeliCa protocol	ISO 14443-4 ISO 7816-4 commands
Memory Size	Up to 1 KB	Up to 2 KB	Up to 1 MB	Up to 64KB
Cost (memory dependent)	Low	Low	Moderate	Moderate
Use cases	Tags with small memory for single application		Flexible tags with larger memory offering multi-application capabilities	

Constructing NDEF

NFC BOOTCAMP
HOW TO BUILD AN NFC APPLICATION

NDEF Header

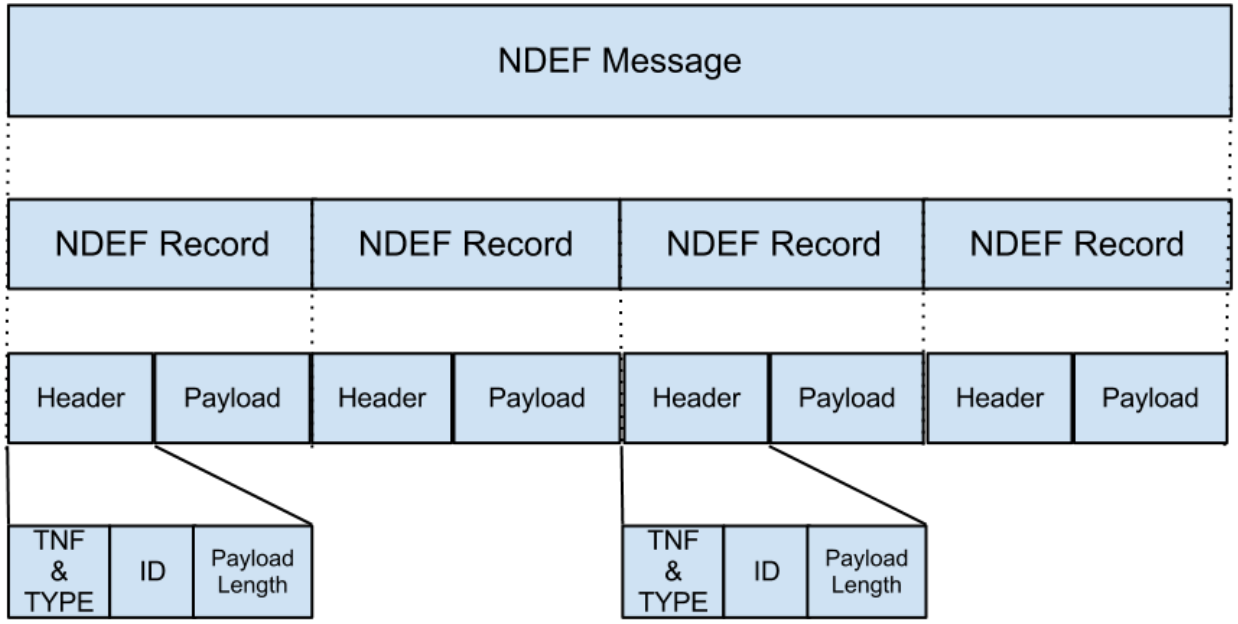
Location	Abbrev	Name	FALSE	TRUE
7	MB	Message Begin	0	1
6	ME	Message End	0	1
5	CF	Chunk Flag	0	1
4	SR	Short Record	0	1
3	IL	ID Length	0	1
2	TNF	Type Name Format	0	1
1			0	1
0			0	1

NDEF Block

1	1	0	1	0	0	0	1
7	6	5	4	3	2	1	0
MB	ME	CF	SR	IL	TNF		
Type Length							
Payload Length							
Type							
ID							
Payload							

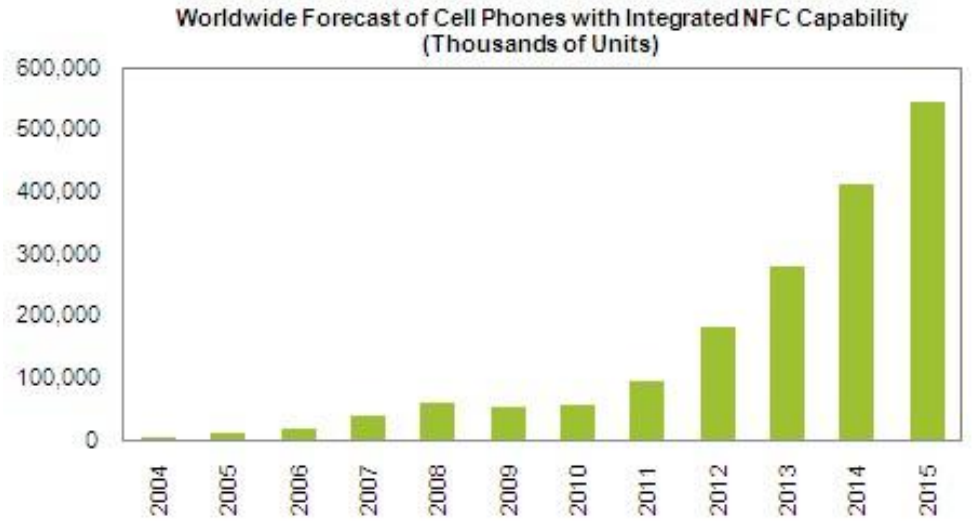
La información en una etiqueta NFC puede guardarse en una estructura conocida como NDEF Record

Una etiqueta puede contener un NDEF Message que a su vez se compone de varios NDEF Record

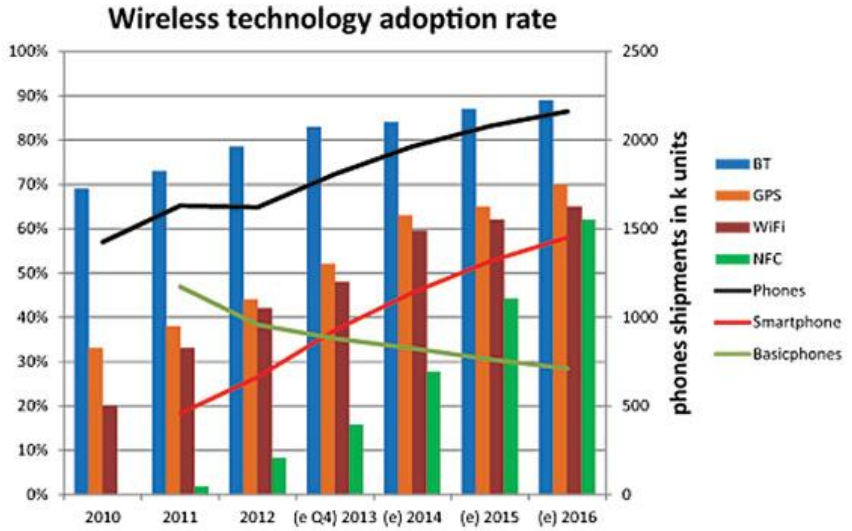


NFC es cada vez mas utilizado en el mercado

Teléfonos con NFC



Source: IHS iSuppli May 2011



Household appliances enero 2014

Ejemplos de Uso

Obtener Información de un póster

Usarlo como entrada

Imprimir fotos directamente desde el móvil

Envío de información a otros dispositivos

Intercambiar tarjetas de negocios

Usar el teléfono móvil como boleto de transporte

Usar el teléfono como una tarjeta de crédito

Muchos otras servicios

Fuente: NFC Forum (http://nfc-forum.org/what-is-nfc/nfc-in-action/)

Ejemplos
https://www.youtube.com/watch?v=lpNpeNfpxFY

Part I

Introduction to Cloud Computing

1

Cloud Computing: An Overview

San Murugesan[1] and Irena Bojanova[2]*

[1] *BRITE Professional Services and Western Sydney University, Australia*
[2] *National Institute of Standards and Technology (NIST), USA*

1.1 Introduction

Cloud computing is receiving keen interest and is being widely adopted. It offers clients applications, data, computing resources, and information technology (IT) management functions as a service through the Internet or a dedicated network. Several converging and complementary factors have led to cloud computing's emergence as a popular IT service-delivery model that appeals to all stakeholders. Considered as paradigm change in IT, it is being adopted for a variety of applications – personal, academic, business, government, and more – not only for cost savings and expediency but also to meet strategic IT and business goals. It is transforming every sector of society and is having a profound impact, especially on the IT industry and on IT professionals – application developers, enterprise IT administrators, and IT executives. Driven by advances in cloud technology, the proliferation of mobile devices such as smartphones and tablets, and use of a variety of applications supported by ubiquitous broadband Internet access, the computing landscape is continuing to change. There is an accompanying paradigm shift in the way we deliver and use IT.

Cloud computing is a radical new IT delivery and business model. Users can use cloud services when and where they need them and in the quantity that they need, and pay for only the resources they use. It also offers huge computing power, on-demand scalability, and utility-like availability at low cost.

Cloud computing is no longer hype. Individuals are using cloud-based applications, such as Web mail and Web-based calendar or photo-sharing Web sites (e.g., Flickr, Picasa) and online data storage. Small- and medium-sized enterprises are using cloud-based applications for accounting, payroll processing, customer

*This work was completed by Irena Bojanova and accepted for publication prior to her joining NIST.

Encyclopedia of Cloud Computing, First Edition. Edited by San Murugesan and Irena Bojanova.

relationship management (CRM), business intelligence, and data mining. Large enterprises use cloud services for business functions, such as supply-chain management, data storage, big data analytics, business process management, CRM, modeling and simulation, and application development. Research studies reveal that users give convenience, flexibility, the ability to share information, and data safety as major reasons for engaging in cloud computing activities.

As cloud computing is moving towards mainstream adoption, there is considerable excitement and optimism, as well as concerns and criticism. Many people have incomplete information or are confused about cloud computing's real benefits and key risks, which matter to them. Given its transformational potential and significance, it is important that students, IT professionals, business managers and government leaders have an informed, holistic understanding of cloud computing and how they can embrace it.

In this chapter, we present an overview of cloud computing concepts, cloud services, cloud-hosting models, and applications. We also outline the benefits and limitations of cloud computing, identify its potential risks, and discuss the prospects for the cloud and what businesses and individuals can do to embrace cloud computing successfully. Finally, we discuss the prospects and implications of cloud computing for businesses, the IT industry, and IT professionals.

1.2 Cloud Computing

In its evolution since the mid-1970s, computing has passed through several stages – from mainframe computers to minicomputers to personal computers to network computing, client-server computing, and distributed computing. Now, coming full circle, computing is migrating outward to the clouds, to distant computing resources reached through the Internet.

Depending on how you view cloud computing, it can be described in different ways. There are several definitions, but the National Institute of Standards and Technology (NIST) offers a classic definition that encompasses the key elements and characteristics of cloud computing (Mell and Grance, 2011):

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The International Organization for Standardization (ISO) provides a similar definition, choosing to call cloud computing an "evolving paradigm": "Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand" (ISO/IEC DIS 17789:2014, 2014).

Gartner defines cloud computing in simplistic terms as "A style of computing where scalable and elastic IT-enabled capabilities are provided as a service to multiple customers using Internet technologies" (http://www.gartner.com/it-glossary/cloud-computing, accessed November 25, 2015).

Another definition encompasses several key characteristics of cloud computing and presents a broader and practical view of it (Vaquero *et al.,* 2009):

> Clouds [are] a large pool of easily usable and accessible virtualized resources such as hardware, development platforms and/or services. These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs [service-level agreements].

Table 1.1 *Cloud characteristics*

Cloud characteristic	Description
On-demand self-service	Computing capabilities (e.g. server time and network storage) can be unilaterally automatically provisioned as needed).
Broad network access	Capabilities are accessible through heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
Resource pooling	Computing resources (e.g. storage, processing, memory, and bandwidth) are pooled to serve multiple consumers, and are dynamically assigned and reassigned according to demand. Customers have no control over the exact location of resources, but may be able to specify location (e.g., country, state, or datacenter).
Rapid elasticity	Capabilities can be elastically provisioned and released commensurate with demand. Available capabilities often appear to be unlimited.
Measured service	Resource use is automatically controlled and optimized through metering capabilities, appropriate to type of service (e.g., storage, processing, bandwidth, and active user accounts).
Multitenancy	Cloud computing is a shared resource that draws on resource pooling as an important feature. It implies use of same resources by multiple consumers, called tenants.

1.2.1 Key Cloud Characteristics

Cloud computing has the following key distinguishing characteristics:

- on-demand self-service;
- broad network access;
- resource pooling;
- rapid elasticity and scalability;
- measured service;
- multitenancy.

These characteristics, briefly outlined in Table 1.1, differentiate cloud computing from other forms of traditional computing.

The cloud draws on some of the older foundations of IT such as centralized, shared resource pooling, utility computing, and virtualization, and incorporates new mechanisms for resource provisioning and dynamic scaling. It adopts new business and revenue models and incorporates monitoring provisions for charging for the resources used. Cloud computing became more widely available only with the adoption of broadband Internet access and advances in virtualization and datacenter design and operation. Philosophical and attitude changes by IT vendors and users were also drivers for cloud's popularity.

1.2.2 Cloud computing attributes

Computing clouds have several distinguishing attributes. They:

- have massive resources at their disposal and support several users simultaneously;
- support on-demand scalability of users' computational needs;

- offer ubiquitous access – stored data and applications are accessible by authorized users anywhere, anytime;
- facilitate data sharing, enterprise-wide data analysis, and collaboration;
- are generally self-healing, and can self-reconfigure providing continuous availability in case of failure of their computing resources;
- offer enhanced user experience via a simplified Web-browser user interface.

1.3 Cloud Service Models

A computational or network resource, an application or any other kind of IT service offered to a user by a cloud is called a cloud service. Cloud services range from simple applications such as e-mail, calendar, word processing, and photo sharing to various types of complex enterprise applications and computing resources offered as services by major providers. For comprehensive information on cloud offerings currently available from several vendors, see the Cloud Computing Directory (http://www.cloudbook.net/directories/product-services/cloud-computing-directory, accessed November 25, 2015) and also refer to Chapter 2.

Depending on the type of services offered, cloud services can be classified into three major categories (see Table 1.2): software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In addition to these foundational services, several cloud support services, such as security as a service and identity and access management as a service, are on offer. Each service category can be used independently or used in combination with others.

1.3.1 Software as a Service

"Software as a service" clouds are also called *software clouds*. In the SaaS model, an application is hosted by a cloud vendor and delivered as a service to users, primarily via the Internet or a dedicated network. It eliminates the need to install and run the application locally, on a user's computer, and thereby also relieves the users from the burden of hardware and software maintenance and upgrades. The software license is not

Table 1.2 *Cloud service models*

Service model	Capability offered to the user	Controllability by users
Software as a service (SaaS)	Use of applications that run on the cloud.	Limited application configuration settings, but no control over underlying cloud infrastructure – network, servers, operating systems, storage, or individual application capabilities.
Platform as a service (PaaS)	Deployment of applications on the cloud infrastructure; may use supported programming languages, libraries, services, and tools.	The user has control of deployed applications and their environment settings, but no control of cloud infrastructure – network, servers, operating systems, or storage.
Infrastructure as a service (IaaS)	Provisioning of processing, storage, networks, etc.; may deploy and run operating systems, applications, etc.	The user has control of operating systems, storage, and deployed applications running on virtualized resources assigned to the user, but no control over underlying cloud infrastructure.

owned by the user. Users are billed for the service(s) used, depending on their usage. Hence, costs to use a service become a continuous expense rather than a huge up-front capital expense at the time of purchase. Examples of SaaS include Webmail, Google Apps, Force.com CRM, Quicken online accounting, NetSuite's Business Software Suite**,** Sun Java Communications Suite, and Paychex payroll management system.

1.3.2 Platform as a Service

In the PaaS model, the platform and tools for application development and middleware systems are hosted by a vendor and offered to application developers, allowing them simply to code and deploy without directly interacting with the underlying infrastructure. The platform provides most of the tools and facilities required for building and delivering applications and services such as workflow facilities for application design, development, testing, deployment, and hosting, as well as application services such as Web service integration, database integration, security, storage, application versioning, and team communication and collaboration. Examples of PaaS include Google App Engine, Microsoft Azure, Amazon's Web services and Sun Microsystems NetBeans IDE. The PaaS cloud is also called *platform cloud or cloudware*.

1.3.3 Infrastructure as a Service

In an IaaS cloud, raw computer infrastructure, such as servers, CPU, storage, network equipment, and datacenter facilities, are delivered as a service on demand. Rather than purchasing these resources, clients get them as a fully outsourced service for the duration that they need them. The service is billed according to the resources consumed. Amazon Elastic Compute Cloud (EC2), GoGrid, and FlexiScale are some of the examples of IaaS clouds. This type of cloud is also called a *utility cloud* or *infrastructure cloud*.

An IaaS cloud exhibits the following characteristics:

- availability of a huge volume of computational resources such as servers, network equipment, memory, CPU, disk space and datacenter facilities on demand;
- use of enterprise-grade infrastructure at reduced cost (pay for the use), allowing small and midsize enterprises to benefit from the aggregate compute resource pools;
- dynamic scalability of infrastructure; on-demand capacity can be easily scaled up and down based on resource requirements.

1.3.4 Cloud Support Services

In order to embrace the promise of clouds fully and successfully, adopters must use one or more of the three foundational cloud services – software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS). But they must also address several other related factors, such as security, privacy, user access management, compliance requirements, and business continuity. Furthermore, would-be adopters may have to use services from more than one service provider, aggregate those services, and integrate them with each other and with the organization's legacy applications / systems. Thus they need to create a cloud-based system to meet their specific requirements. To assist them in this, and to facilitate transition to the cloud, a cloud ecosystem is emerging that aims to offer a spectrum of new cloud support services that augment, complement, or assist the popular SaaS, IaaS, and PaaS offerings. Examples of such cloud support services are data storage as a service (DSaaS), analytics as service (AaaS), desktop as a service (DAAS), security as a service (SecaaS), identity and access management as a service (IAMaaS), and monitoring as a service (MaaS).

1.3.4.1 Data Storage as a Service (DSaaS)

With cloud storage, data is stored in multiple third-party servers, rather than on dedicated servers used in traditional networked storage, and users access a virtual storage. The actual storage location may change as the cloud dynamically manages available storage space; however, the users see a static location for their data. Key advantages of cloud storage are reduced cost and better data safety and availability. Virtual resources in the cloud are typically cheaper than dedicated physical resources connected to a PC or the network. Data stored in a cloud is generally safe against accidental erasure or hard-drive failures as Cloud Service Providers (CSPs) keep multiple copies of data across multiple physical machines continually. If one machine crashes, the data that was on that machine can be retrieved from other machine(s) in the cloud. Cloud vendors generally offer better security measures than a small business could afford. Enterprise data storage in clouds, however, raises some concerns, which are discussed later.

1.3.4.2 Analytics as a Service (AaaS)

Analytics as a service (AaaS), also known as data analytics as a service (DAaaS), refers to the provision of analytics platforms – software and tools – on a cloud for analysis and mining of large volumes of data (big data). Several vendors, such as IBM, Amazon, Alpine Data Labs, and Kontagent, offer such services. Customers can feed their data into the platform and get back useful analytic insights. It lets clients use particular analytic software for as long as it is needed and they pay only for the resources used. As a general analytic solution, AaaS has potential use cases in a range of areas and offers businesses an alternative to developing costly in-house high-performance systems for business analytics. An AaaS platform is extensible and scalable and can handle various potential use cases. It lets businesses get their data analytics initiatives up and running quickly.

1.3.4.3 Desktop as a Service (DaaS)

Desktop as a Service (DaaS) is a cloud service in which the back-end of a virtual desktop infrastructure (VDI) is hosted by a cloud service provider. It provides users with the ability to build, configure, manage, store, execute, and deliver their desktop functions remotely. Examples of such service are VMware Horizon Air, Amazon WorkSpaces and Citrix XenDesktop. Clients can purchase DaaS on a subscription basis and the service provider manages the back-end responsibilities of data storage, backup, security and upgrades. DaaS is well suited for a small or mid-size businesses that want to provide their users with a virtual desktop infrastructure (VDI), but find that deploying a VDI in-house is not feasible due to cost, implementation, staffing and other constraints.

1.3.4.4 Security as a Service (SecaaS)

Security as a Service (SecaaS) refers to the provision of security applications and services via the cloud, either to cloud-based infrastructure and software or from the cloud to the customers' on-premises systems. This enables enterprises to make use of security services in new ways, or in ways that would not be cost effective if provisioned locally. The services provided include authentication, virus detection, antimalware/spyware, intrusion detection, encryption, e-mail security, Web security, and security event management.

1.3.4.5 Identity and Access Management as Service (IAMaaS)

Identity and access management as a service (IAMaaS) offers cloud-based IAM services to clients and requires minimal or no on-premises presence of hardware or software. Services include user provisioning, authentication, authorization, self-service, password management, and deprovisioning.

1.3.4.6 Monitoring as a Service (MaaS)

Monitoring-as-a-service (MaaS) facilitates the deployment of monitoring functionalities for various other services and applications within the cloud. Monitoring focuses on how services are performing. The common application for MaaS is online state monitoring, which continuously tracks certain states of applications, networks, systems, instances or any element that may be deployable within the cloud.

1.4 Cloud Computing Deployment Models

Based on where the cloud is deployed and by whom, who owns and manages it, and who its primary users are, clouds are classified into five categories: public cloud, private cloud, virtual private cloud, community cloud, and hybrid cloud.

1.4.1 Public Cloud

The public cloud is the most common and widely known form of cloud, and is open for anyone – business, industry, government, nonprofit organizations and individuals – to use. The cloud infrastructure is, however, owned and managed by the cloud service provider – the organization that offers the cloud services. Public cloud services are offered on a pay-per-usage model; however, some applications on public clouds are accessible for free.

1.4.2 Private Cloud

A private cloud is deployed, provided, and controlled by an enterprise behind its firewall for its own use. Unwilling to head into public clouds because of concerns surrounding them and compliance requirements, some enterprises deploy their own cloud computing environments for their own (and their business partners') exclusive use. Thus, by having their own cloud, they gain operational efficiencies, effectively use their existing resources, if any, and have full control over the cloud, the applications, and data on the cloud.

1.4.3 Virtual Private Cloud

A virtual private cloud (VPC) is a segment of a public cloud, designated for a user with additional provisions and features for meeting that user's specific security and compliance requirements. Virtual private clouds provide users with more control over the resources they use than a pure public cloud does. An example of this type of cloud is Amazon's VPC.

1.4.4 Community Cloud

A community cloud is known as an industry cloud or vertical cloud. It is optimized and specially deployed for use by a particular industry sector or a group of users so that it meets specific requirements to address issues that are crucial to them. AcademyOne's Navigator Suite (aimed at academics and students) and Asite Solutions (specifically designed for construction industry) are examples of these types of clouds.

1.4.5 Hybrid Clouds

A hybrid cloud is a combination of two or more of the above cloud models. In this model, an enterprise makes use of both public and private clouds – deploying its less critical, low-risk services on a public cloud and business-critical core applications on its internal private cloud. A hybrid model allows for selective

implementation addressing concerns about security, compliance, and loss of control, as well as enabling adoption of public clouds that offer cost benefits and more application options.

1.5 Benefits, Limitations, and Concerns associated with Cloud Computing

Cloud computing offers several substantial benefits to its users – individuals and enterprises. But it also has limitations and poses some risks, the effects of which depend on the application type and liabilities involved. In embracing cloud computing, therefore, users must understand, acknowledge, and address its limitations and risks.

1.5.1 Benefits of Cloud Computing

The key benefits of embracing a cloud include reduced capital and operational cost, improved flexibility, on-demand scalability, easier and quicker application deployment, ease of use, and availability of vast cloud resources for every kind of application or use. Many applications, including e-mail, office document creation, and much data storage continue to move into the clouds to reap the benefits of this new paradigm in IT.

Cloud computing frees users and businesses from the limitations of local computing resources and allows them to access the vast computational resources and computation power out in the cloud. For users to make use of cloud resources from anywhere in the world at any time, all that is needed is an Internet connection and a Web browser. The cloud lets the users run even computationally intensive or storage-intensive applications, as all of their computing and storage needs are sourced from the cloud.

Public clouds eliminate significant capital expenses for hardware and upfront license fees for software, as well as the headaches of hardware and software maintenance and upgrade by users. Cloud applications can be deployed instantly and simultaneously to thousands of users in different locations around the world, and can be regularly updated easily. Further, as clouds provide improved business continuity and data safety, they are particularly attractive to small- and medium-size enterprises, as well as enterprises in disaster-prone areas. Startups and application developers can use computing clouds to try their ideas without having to invest in their own infrastructure.

Other benefits of using a cloud are:

- lower operational and service cost to users – they pay for what they use;
- on-demand scalability to meet peak and uncertain computing demands;
- shared access to data/application-supporting collaboration and teamwork;
- greater data safety than most businesses can provide and manage in their own on-premises IT systems;
- ease of, and quicker, application deployment;
- freedom to use a vast array of computational resources on the cloud.

1.5.2 Limitations of Cloud Computing

There are a few limitations that users must consider before moving to the cloud. The key limitations of the cloud are:

- need for a reliable, always-available high-speed network access to connect to clouds;
- possibility of slow response at times due to increased traffic or uncertainties on the network, or higher load on computers in the cloud;
- additional vulnerabilities to security of data and processes on clouds;
- risk of unauthorized access to users' data;

- loss of data due to cloud failure (despite replication across multiple machines);
- reliability and continued availability of services offered by cloud service providers.

1.5.3 Cloud Concerns

Despite its promises, cloud computing's mainstream adoption is constrained by perceived and real barriers and concerns. Security and privacy of data and applications on the cloud are two of the top concerns of users in moving into clouds followed by reliability and availability of cloud services, as well as adherence to compliance requirements, where applicable. External clouds raise additional concerns about loss of control and sharing data outside the enterprise firewall.

Many people think that because they don't know where their data is stored remotely, and because the applications are accessed over the Internet, cloud services are insecure. They believe that if data and applications were physically housed in computers under their control, they would protect them better. But this is not necessarily the case as economies of scale allow a CSP to offer more sophisticated security, disaster recovery, and service reliability than an individual institution (particularly a small enterprise) can afford to deploy on its own.

Cloud computing security concerns and requirements can differ considerably among the stakeholders – end-user service consumers, cloud service providers and cloud infrastructure providers – and are determined by the specific services they provide or consume. The Cloud Security Alliance (CSA) has identified seven top cloud security threats and outlined impact of those threats as well as remediation for them (Cloud Security Alliance, 2009, 2010).

They are:

1. Abuse and nefarious use of cloud computing.
2. Insecure application programming interfaces.
3. Malicious insiders.
4. Shared technology vulnerabilities.
5. Data loss/leakage.
6. Account, service & traffic hijacking.
7. Unknown risk profile.

Based on a 2013 survey, CSA has also identified nine critical threats to data security in the order of severity:

1. Data breaches.
2. Data loss.
3. Account hijacking.
4. Insecure APIs.
5. Denial of service.
6. Malicious insiders.
7. Abuse of cloud services.
8. Insufficient due diligence.
9. Shared technology issues. (Cloud Security Alliance, 2013)

Many enterprise computing applications must meet compliance requirements, which depend on the type of business and customer base. To better ensure the desired level of service delivery and to limit liabilities, service level agreements (SLAs) with the cloud vendors are highly recommended when consuming cloud services. A cloud SLA specifies terms and conditions as well as expectations and obligations of the cloud service provider and the user.

By careful planning and incorporating the user's requirements into cloud service offerings, both the cloud vendors and users can reduce risk and reap the rewards of cloud-based hosted services.

1.6 Migrating to Clouds

A new mindset is needed to embrace cloud computing. To use and benefit from clouds successfully, an enterprise must prepare itself strategically, culturally and organizationally, and take a holistic view of cloud computing. It must develop its strategic plan and follow a phased, pragmatic, step-by-step approach that provides a business context for its cloud adoption. It must choose a cloud option that is appropriate for the application, considering and managing the risks of migrating to clouds by applying safeguards. Moving into clouds is not just about technology; the cloud migration should also factor in the role of people, processes, and services, and the change-management process. Migration to clouds will also demand a new kind of IT management and governance framework.

1.6.1 Choosing your Cloud

A major decision that IT managers and enterprises have to make is the type of cloud – public clouds, private clouds, or variations of them – that is well suited for their application. To arrive at a better decision, they have to understand the differences between these deployments, and understand the risks associated with each in the context of the characteristics and requirements of their applications. They also have to consider:

- performance requirements, security requirements, and cloud service availability and continuity;
- amount of data transfer between the user and the clouds and/or between the clouds;
- sensitive nature of the applications;
- control of their application and data;
- total costs involved;
- whether the external cloud providers are trusted;
- terms and conditions imposed by the external cloud providers; and
- in-house technical capabilities. (Claybrook, 2010)

1.7 Cloud Prospects and Implications

Computing clouds are powerful change-agents and enablers. Soon the core competency for most enterprises would be using IT services and infrastructure that cloud computing offers as hosted services, not building their own IT infrastructure. Cloud computing will profoundly change the way people and enterprises use computers and their work practices, as well as how companies and governments deploy their computer applications. It is transforming the way we think about computing environments and will drastically improve access to information for all, as well as cutting IT costs. Ongoing developments – the increasing maturity of clouds, the introduction of new cloud computing platforms and applications, the growth in adoption of cloud computing services, and the emergence of open standards for cloud computing – will boost cloud computing's appeal to both cloud providers and users.

Clouds will enable open-source and freelance developers to deploy their applications in the clouds and profit from their developments. As a result, more open-source software will be published in the cloud. Clouds will also help close the digital divide prevalent in emerging and underdeveloped economies and may help save our planet by providing a greener computing environment.

Major stumbling blocks for enterprises moving their applications into the cloud in a big way are reliability, performance, bandwidth requirements, trust, and security issues. However, these barriers are gradually being lowered or removed. Government regulations and other compliance requirements lag behind market developments and demand, and these aspects need to be addressed swiftly.

Driven by economic imperatives and the promise of flexibility and convenience, cloud computing will gain wider acceptance. Like the Internet, cloud computing is a transformational technology. It will mature rapidly, as vendors and enterprises come to grip with the opportunities and challenges that it presents.

Cloud computing creates new possibilities for businesses – IT and non-IT – and there will be new investments. Researchers will be better able to run experiments quickly on clouds, share their data globally, and perform complex analysis and simulations. Universities and training institutions will offer new courses and programs, focused on cloud computing.

Some IT professionals, particularly those who work with on-premises IT systems, might be afraid of losing their jobs because of the ongoing adoption of cloud computing. The truth is that while some might lose their current job, they might be absorbed in other roles. So, they should be prepared to learn new skills and evolve in these new roles. They might need to learn how to deploy and manage applications in the cloud and minimize risks, as well as how to work with cloud providers. There will be a need for professionals to develop new kinds of cloud applications and to design, deploy, and maintain computing clouds.

Cloud service providers, the IT industry, professional and industry associations, governments, and IT professionals all have a role to play in shaping, fostering, and harnessing the full potential of the cloud ecosystem.

1.8 Conclusions

The cloud ecosystem is evolving to provide a vast array of services that support and aid deployment of cloud-based solutions for a variety of applications across many different domains. Further, new types of cloud deployments, new models that deliver value-added services, and new costing and business models are on the horizon. Besides cloud service providers and users, many new players that perform niche roles are getting into the cloud arena. Cloud-based applications are being adopted widely by individuals and businesses in developed countries, and even more so in developing economies such as India, South Africa, and China. Governments in many countries are promoting adoption of clouds by businesses – particularly micro, small, and medium enterprises, as well as individuals. As a result, a new bigger cloud ecosystem is emerging.

References

Claybrook, B. (2010) Cloud vs. in-house: Where to run that app? *Computer World*, http://www.computerworld.com/article/2520140/networking/cloud-vs--in-house--where-to-run-that-app-.html (accessed November 25, 2015).

Cloud Security Alliance (2009) *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, https://cloudsecurityalliance.org/csaguide.pdf (accessed November 25, 2015).

Cloud Security Alliance (2010) *Top Threats to Cloud Computing V1.0*, http://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (accessed November 25, 2015).

Cloud Security Alliance (2013) The Notorious Nine: Cloud Computing Top Threats in 2013, Cloud Security Alliance, https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf (accessed November 25, 2015).

ISO/IEC DIS 17789:2014 (2014) *Information Technology – Cloud Computing – Reference Architecture*, International Organization for Standardization, Geneva.

Mell, P. M., and Grance, T. (2011) *The NIST Definition of Cloud Computing*. Special Publication 800-145. NIST, Gaithersburg, MD, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909616 (accessed November 25, 2015).
Vaquero, L. M, Rodino-Merino, L., Caceres, J., and Lindner, M. (2009) A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Computer Communication Review* **39**(1), 50–55.

Cloud Vocabulary

The following are some of the key terms commonly used in cloud computing:

Cloudburst. The term is used in a positive and a negative sense. Cloudburst (positive) refers to the dynamic deployment of a software application that runs on an enterprise's in-house computing resources to a public cloud to address a spike in demand. But cloudburst (negative) conveys the failure of a cloud computing environment due to its inability to handle a spike in demand.
Cloudstorming. This term refers to the act of connecting multiple cloud computing environments.
Cloudware. This is a general term referring to a variety of software, typically at the infrastructure level, which enables building, deploying, running, or managing applications in a cloud computing environment.
Cloud provider. A cloud provider is an organization that makes a cloud computing environment available to others, such as an external or public cloud.
Cloud enabler. This term refers to an organization or a vendor that is not a cloud provider per se but makes technology and services available, such as cloudware, which enables cloud computing.
Cloud portability. This term refers to the ability to move applications (and often their associated data) across cloud computing environments from different cloud providers, as well as across private or internal cloud and public or external clouds.
Cloud interoperability. This term refers to the ability of two or more systems or applications to exchange information and to use the information that has been exchanged together.
Cloud sourcing. This term refers to leveraging services in the network cloud – raw computing, storage, messaging, or more structured capabilities, such as vertical and horizontal business applications, even community – to provide external computing capabilities, often to replace more expensive local IT capabilities. While it might provide significant economic benefits, there are some attendant tradeoffs, such as security and performance. These services are delivered over the network but generally behave as if they are local.