



# **REDES DE COMPUTADORAS**

Dra. MABEL VÁZQUEZ BRISEÑO.

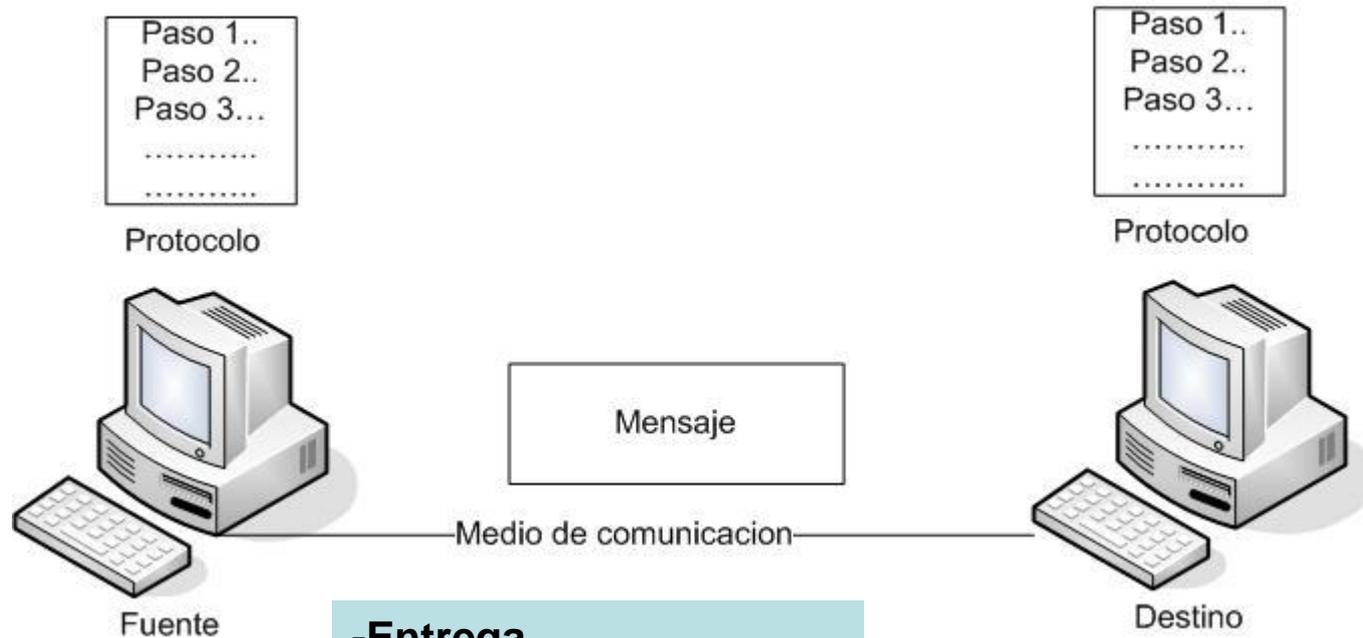
## **Unidad I Fundamentos de redes de Computadoras.**

- 1.1 Protocolos de comunicación**
- 1.2 Modelo de referencia OSI**
- 1.3 Organizaciones y estándares**



## Componentes básicos del sistema de comunicación:

- Mensaje
- Fuente
- Destino
- Medio de Tx
- Protocolo



- Entrega
- Exactitud
- Puntualidad



## ¿PROCOLO?

**Las redes de computadoras establecen la comunicación entre entidades en diferentes sistemas.**

**Las entidades se comunican entre si en base a protocolos de comunicación.**

**¿Qué es un protocolo de comunicación y cuales son sus características?**



## •Protocolo de comunicación:

Es un conjunto de reglas que indican como se debe llevar a cabo un intercambio de datos o información.

**Los principales elementos de un protocolo son :**

### •Sintaxis. (como?)

**La estructura o el formato de los datos.**

### •Semántica (Que?)

**Significado de cada una de las secciones de los bits.**

### •Sincronización (Cuando?)

**-Cuando los datos deben ser enviados**

**-Que tan rápido deben ser enviados.**



## Características importantes de un protocolo:.

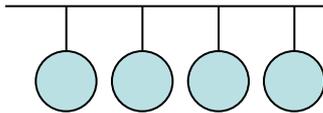
Dependiendo del tipo de conexión que controle, un protocolo puede ser **Directo** o **Indirecto**

### •Directo.

-Las entidades se comunican directamente sin requerir un elementos intermedios.



a) Punto a punto

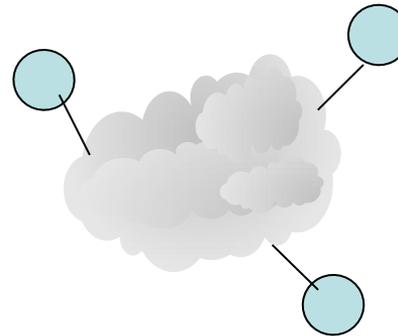


b) multipunto

### •Indirecto

-Las entidades se conectan a través de diferentes sistemas de comunicación.

a) A través de una red conmutada o interconexión de redes





## Características importantes de un protocolo (cont...)

### •**Monolítico / Estructurado.**

Una sola unidad o estructura jerárquica o en capas (varios protocolos).

Monolítico es aquel en que el emisor tiene el control en una sola capa de todo el proceso de transferencia . En protocolos estructurados , hay varias capas que se coordinan y que dividen la tarea de comunicación .

### •**Simétrico/asimétrico**

**Comunicación entre entidades paritarias o de diferente nivel.**

Un protocolo es asimétrico si una de las entidades tiene funciones diferentes de la otra ( por ejemplo en clientes y servidores ) .

### •**Normalizado/ No normalizado**

**Estandarizado o diseñado para un modelo particular de sistema (ejem: un solo tipo de PC)**



# Funciones de un protocolo de comunicaciones.

Un protocolo realiza la mayor parte de las tareas requeridas en un sistema de comunicaciones.

## *Lectura 1*

**Resumen de las tareas de los sist. de comunicación:**

- Utilización del sistema de transmisión
- Implementación de la interfaz
- Generación de la señal
- Sincronización
- Gestión del Intercambio
- Detección y corrección de errores
- Control de flujo
- Encaminamiento
- Recuperación
- Seguridad
- Gestión de red



**Estas y otras funciones pueden englobarse en :**

- **Segmentación y ensamblado**
- **Encapsulado**
- **Control de Conexión**
- **Envío ordenado**
- **Control de Flujo**
- **Control de errores**
- **Direccionamiento**
- **Multiplexación**
- **Servicios de transmisión**



## •Segmentación y ensamblado

- Generalmente es necesario dividir los bloques de datos en unidades pequeñas e iguales en tamaño,
- Creación de PDU (Protocol Data Unit).
- En base al MTU (Maximum Transfer Unit)

La segmentación es útil para:

- Control de errores mas eficiente
- Evitar monopolizar la red

## •Encapsulado



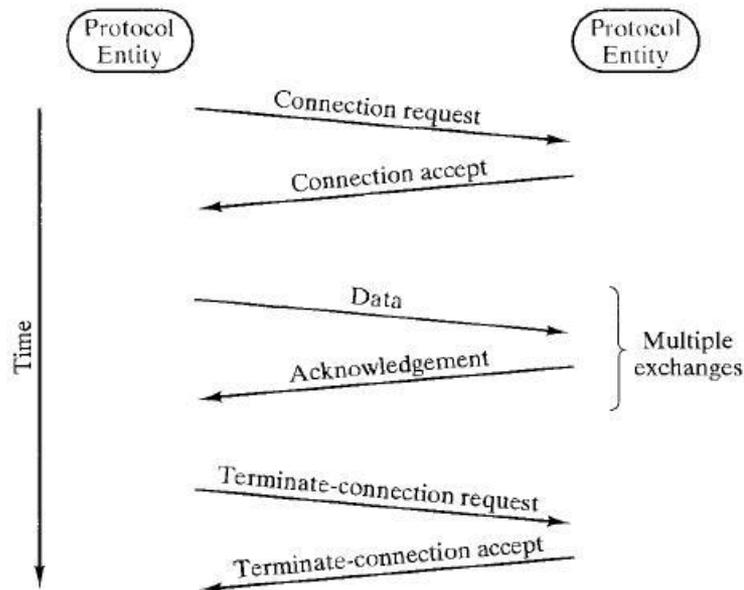


## •Control de Conexión

La transferencia de PDUs entre entidades puede ser:

-No orientada a conexión

-Orientada a Conexión:



**3 Fases obligatorias**

- Establecimiento
- Transferencia
- Liberación



## •Envío ordenado

Esquema de aseguramiento de recepción de PDUs.

El envío de PDUs puede llevarse a cabo por caminos distintos.

Números de secuencia.

## Control de Flujo

La entidad receptora debe limitar la cantidad o tasa de datos que envía la entidad emisora.

Existen diferentes esquemas. Ejem: Stop-and-wait, Ventana deslizante.

## Control de errores.

Técnicas para gestionar la pérdida o los errores en los datos. Ejemplo: Detección de errores, checksum, retransmisión.



## •Direcccionamiento

Identificar el punto o entidad destino en diferentes puntos del sistema.

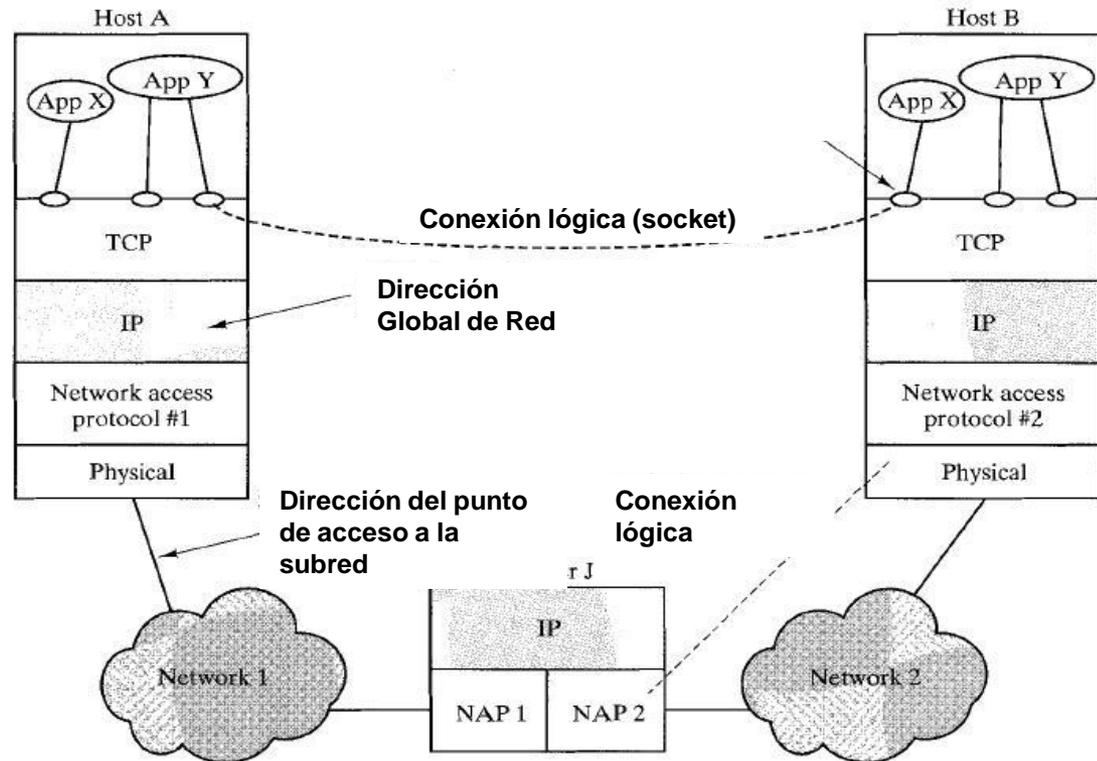
Debe identificar:

Nivel: (red, aplicación..),

Ámbito: (global, local),

Identificador de conexión: (para servicios orientados a conexión, requieren un identificador de conexión).

Modo: unicast, multicast, broadcast.





## •Múltiplexación

Relacionado con direccionamiento. Proveer múltiples conexiones. Ejem: varios puertos TCP abiertos.

### •Servicios de transmisión

- Prioridad (Ejemplo: hay mensajes ( los de control ) que deben tener prioridad respecto a otros .
- Grado de servicio ( Ejemplo: hay datos que deben acelerarse mas que otros ( vídeo ) ) .
- Seguridad.



**El avance y desarrollo de las redes depende de la especificación de modelos y normas.**

**Es importante definir:**

## **ESTÁNDARES Y MODELO**

**El mismo Internet fue creado en base a diferentes estándares y el modelo TCP/IP**

**¿Quién inventó Internet?**

**<https://www.youtube.com/watch?v=l-zFtlzanvQ>**



## CONCEPTO DE ESTÁNDAR.

Es el conjunto de criterios y principios que constituyen una base para construir y comparar sistemas.

Un estándar es una norma reconocida por un conjunto de instituciones legalmente establecidas y con un objetivo bien definido en el ambiente de comunicaciones. Estas instituciones puede ser:

- Asociación de fabricantes de equipo y de software
- Instituciones de investigación y desarrollo
- Comités internacionales
- Empresas de la industria electrónica.



## **Ventajas de la normalización:**

- **Asegura un gran mercado (Ejemplo: franquicias)**
- **Flexibilidad para el usuario (permite que productos de diferentes proveedores se comuniquen)**

## **Desventajas:**

- **Pueden congelar la tecnología (requieren tiempo para ser aceptados)**
- **Varios estándares en colisión (sirven para lo mismo)**



Algunas de estas instituciones que establecen estándares son:

- ANSI: American National Standards Institute:**
- EIA: Electronic Industries association**
- IEEE: Institute of Electronic and Electrical Engineers**
- ISO: International Standard Organization.**
- IETF: Internet Engineering Task Force**

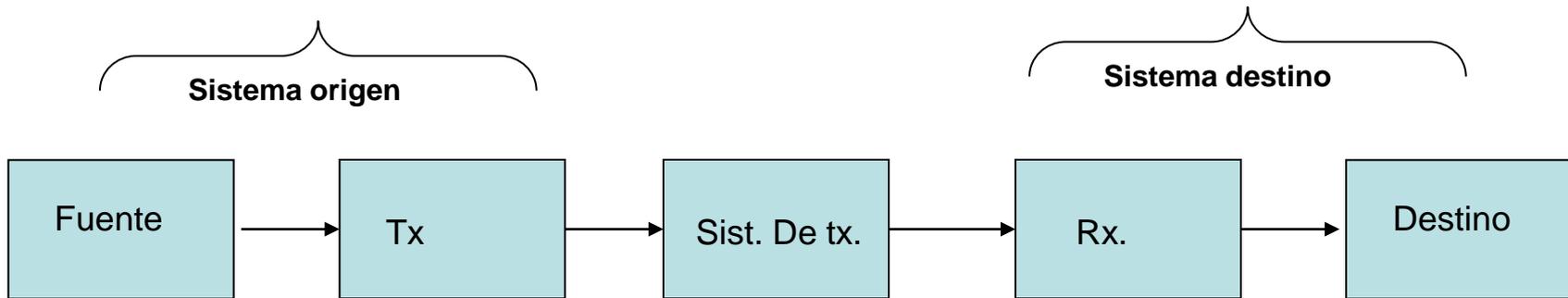
**Estas instituciones han estandarizado las comunicaciones y definido el concepto de modelo de comunicaciones.**



## •CONCEPTO DE MODELO.

Un modelo es la descripción muy general de una idea ó prototipo. En términos de cómputo: Modelo es la descripción muy general, tanto del hardware como del software en cualquier implementación dada.

### Modelo de un sistema de comunicaciones





## MODELO OSI/ISO

Es un modelo muy importante dentro de la comunicación de computadoras, y es utilizado principalmente para diseñar la comunicación entre computadoras en Redes Locales.

El Modelo de Referencia para la [Interconexión de Sistemas Abiertos \(OSI, Open System Interconnection\)](#) fue creado en 1977 por la [Organización Internacional de Estándares \(ISO\)](#).

Nace de la necesidad de uniformizar los elementos que participan en la solución del problema de comunicación entre equipos de cómputo de diferentes fabricantes.

Tales diferencias son:

- Procesador
- Velocidad
- Memoria
- Dispositivos de almacenamiento
- Interfases para comunicaciones
  - Códigos de caracteres
  - Sistemas operativos

**El modelo OSI permite dividir el problema general de la comunicación, en problemas específicos,**



## El modelo OSI permite definir y establecer servicios entre Interfaces y entidades.

- **Interfaz:** Corresponde a la separación o división entre dos capas de un modelo de comunicación.
- **Servicios:** Son un conjunto de operaciones que un nivel provee al nivel superior. Define las operaciones que una capa puede realizar, aunque no se determina como.
- **Entidades:** Son elementos activos en cada nivel del modelo. Una entidad puede ser software (procesos) o hardware (ej. Chips)



## Objetivo del modelo OSI.

**Formalizar los diferentes niveles de interacción para la conexión de computadoras habilitando así la comunicación del sistema de cómputo independiente del:**

- **Fabricante**
- **Localización**
- **Sistema operativo.**

Este objetivo tiene las siguientes implicaciones:

1. Obtener un modelo de referencia estructurado en varios niveles en los que se contemple desde el concepto BIT hasta el concepto APLICACIÓN.
2. Desarrollar un modelo en el cual cada nivel define un protocolo que realiza funciones específicas diseñadas para atender al protocolo de la capa superior.
3. No especificar detalles de cada protocolo.
4. Especificar la forma de diseñar familias de protocolos, esto es, definir las funciones que debe realizar cada capa.



## ESTRUCTURA DEL MODELO OSI.

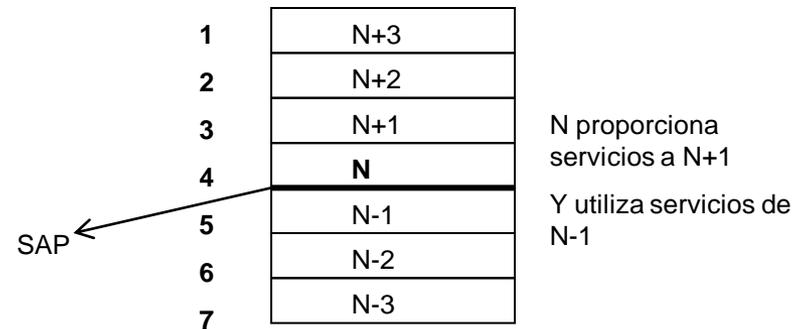
- Se diseñó en una estructura multinivel o capas con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación.

- La capa superior utiliza los servicios de las capas inferiores. Aunque en algunas redes algunas capas pueden ser nulas.

- Utilizando un servicio de Niveles o capas, una capa N, usa los servicios proporcionados por una capa N-1 y provee servicios a una capa N+1.

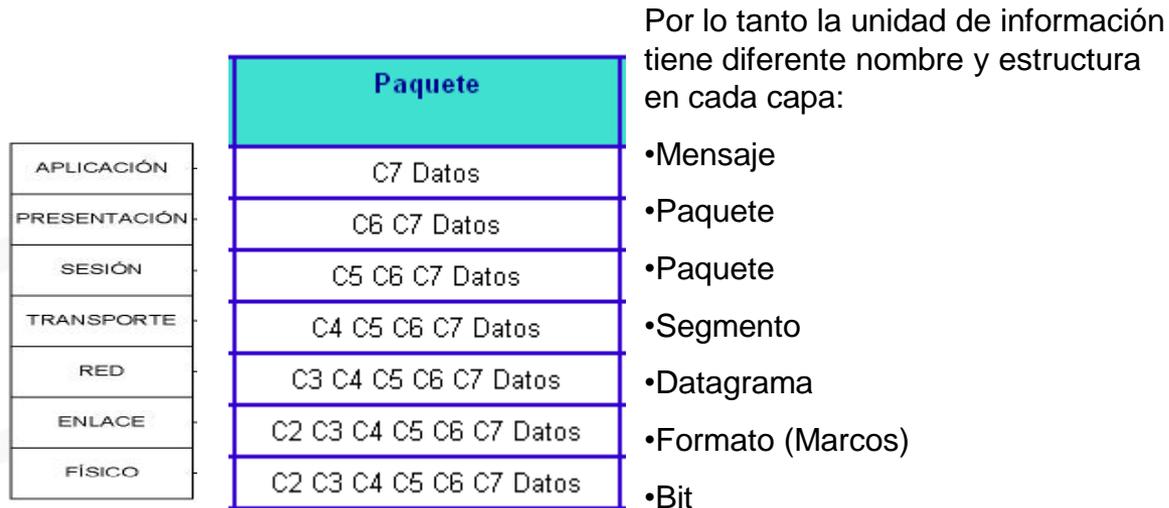
- Entre las capas existen interfaces, llamadas, **puntos de acceso a los servicios (SAP)**.

- Cada capa es dependiente de la capa superior e inferior.





En cada nivel, se incorpora al mensaje un formato de control, lo que permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información.





A través de la red, los procesos en la misma capa pueden comunicarse de manera Ejemplo:, Web server & browser se ejecutan en la capa de aplicación, se comunican vía HTTP

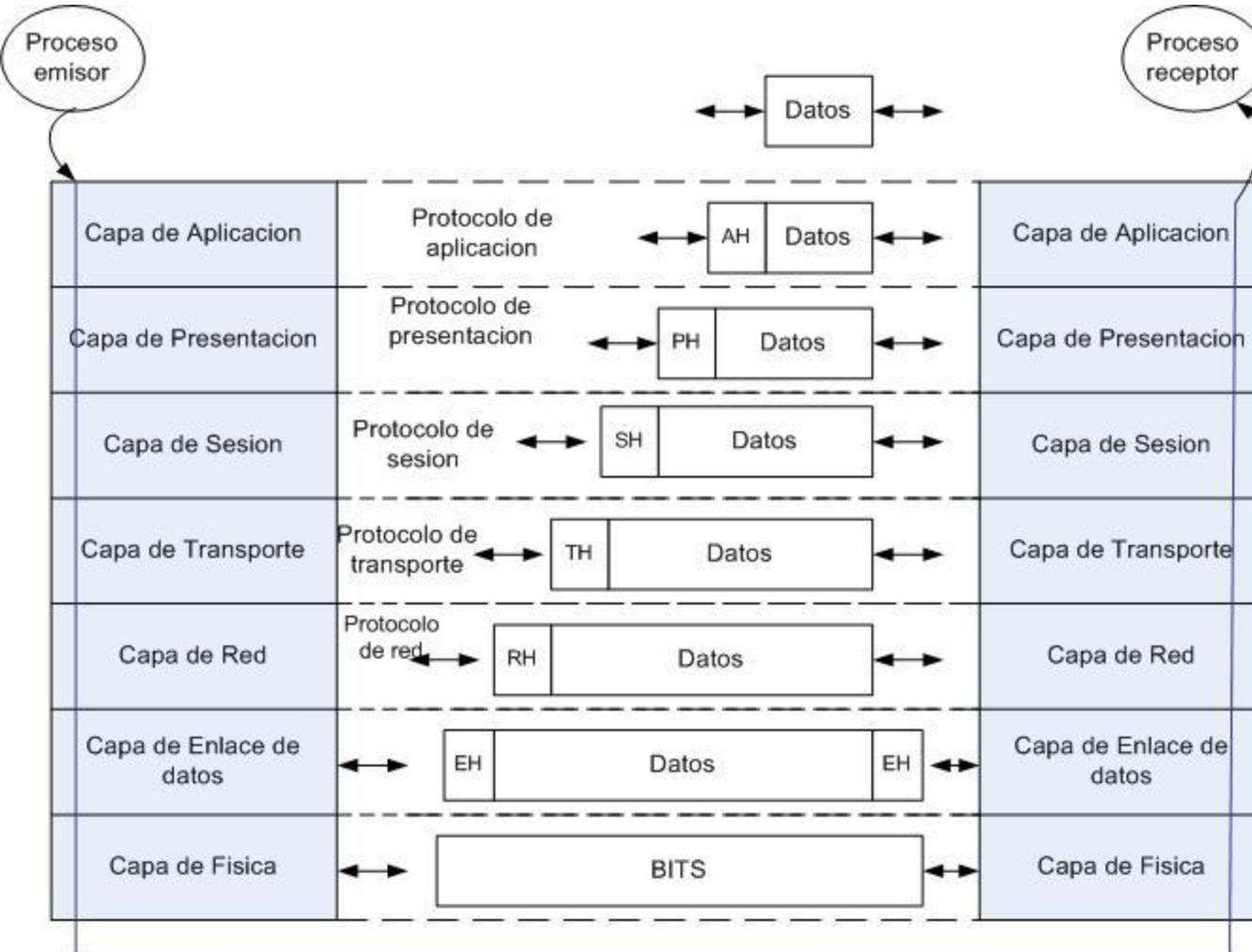
En realidad, la comunicación real se lleva a cabo en el nivel físico:

*En la fuente,*  
Conforme la información es enviada a las capas inferiores:

El protocolo correspondiente a cada capa agrega información de control a los datos.

*En el destino ,*  
Conforme la información es enviada a las capas superiores:

El protocolo correspondiente a cada capa lee y analiza la información de control.





## **Tarea: Presentación de tema**

**De cada una de las capas del modelo OSI  
(funciones principales, relación con las otras capas, ejemplos  
de servicios...)**

- 1) Física** → (Martorell Camacho Jose)
- 2) Enlace de datos** → (Gómez Abarca Igor)
- 3) Red** → **explicar direcciones usadas** (Ruiz Guerrero B.)
- 4) Transporte** → **explicar direcciones usadas** (Melchor Sánchez)
- 5) Sesión** (Garcia Soto Luis)
- 6) Presentación** (López Mora Elias)
- 7) Aplicación** (Beltrán Silva David)

**Prox. Miércoles 30 de Agosto**



# MODELO OSI/ISO

Es un modelo muy importante dentro de la comunicación de computadoras, y es utilizado principalmente para diseñar la comunicación entre computadoras en Redes Locales.

El Modelo de Referencia para la **Interconexión de Sistemas Abiertos (OSI, Open System Interconnection)** fue creado en 1977 por la **Organización Internacional de Estándares (ISO)**.

Nace de la necesidad de uniformizar los elementos que participan en la solución del problema de comunicación entre equipos de cómputo de diferentes fabricantes.

Tales diferencias son:

- Procesador
- Velocidad
- Memoria
- Dispositivos de almacenamiento
- Interfases para comunicaciones
  - Códigos de caracteres
  - Sistemas operativos

El modelo OSI permite dividir el problema general de la comunicación, en problemas específicos, facilitando la solución.



## **Objetivo del modelo OSI.**

**Formalizar los diferentes niveles de interacción para la conexión de computadoras habilitando así la comunicación del sistema de cómputo independiente del:**

- **Fabricante**
- **Localización**
- **Sistema operativo.**

**Este objetivo tiene las siguientes implicaciones:**

1. **Obtener un modelo de referencia estructurado en varios niveles en los que se contemple desde el concepto BIT hasta el concepto APLICACIÓN.**
2. **Desarrollar un modelo en el cual cada nivel define un protocolo que realiza funciones específicas diseñadas para atender al protocolo de la capa superior.**
3. **No especificar detalles de cada protocolo.**
4. **Especificar la forma de diseñar familias de protocolos, esto es, definir las funciones que debe realizar cada capa.**



## ESTRUCTURA DEL MODELO OSI.

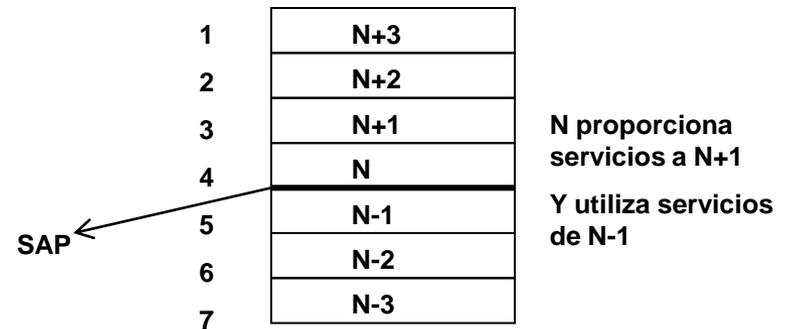
- Se diseñó en una estructura multinivel o capas con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación.

- La capa superior utiliza los servicios de las capas inferiores. Aunque en algunas redes algunas capas pueden ser nulas.

- Utilizando un servicio de Niveles o capas, una capa N, usa los servicios proporcionados por una capa N-1 y provee servicios a una capa N+1.

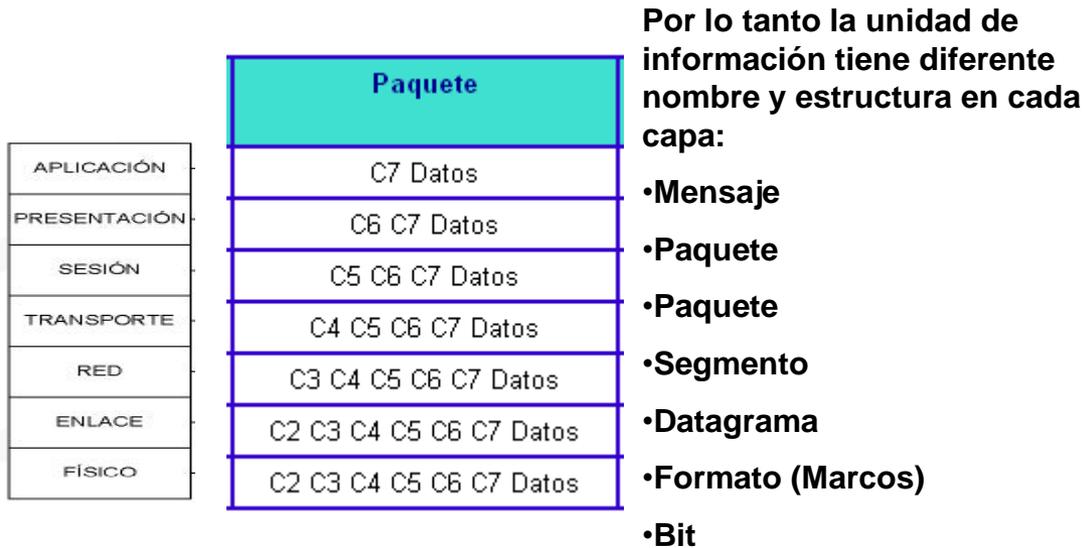
- Entre las capas existen interfaces, llamadas, puntos de acceso a los servicios (SAP).

- Cada capa es dependiente de la capa superior e inferior.





En cada nivel, se incorpora al mensaje un formato de control, lo que permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información.





A través de la red, los procesos en la misma capa pueden comunicarse de manera  
Ejemplo:, Web server & browser se ejecutan en la capa de aplicación, se comunican vía HTTP

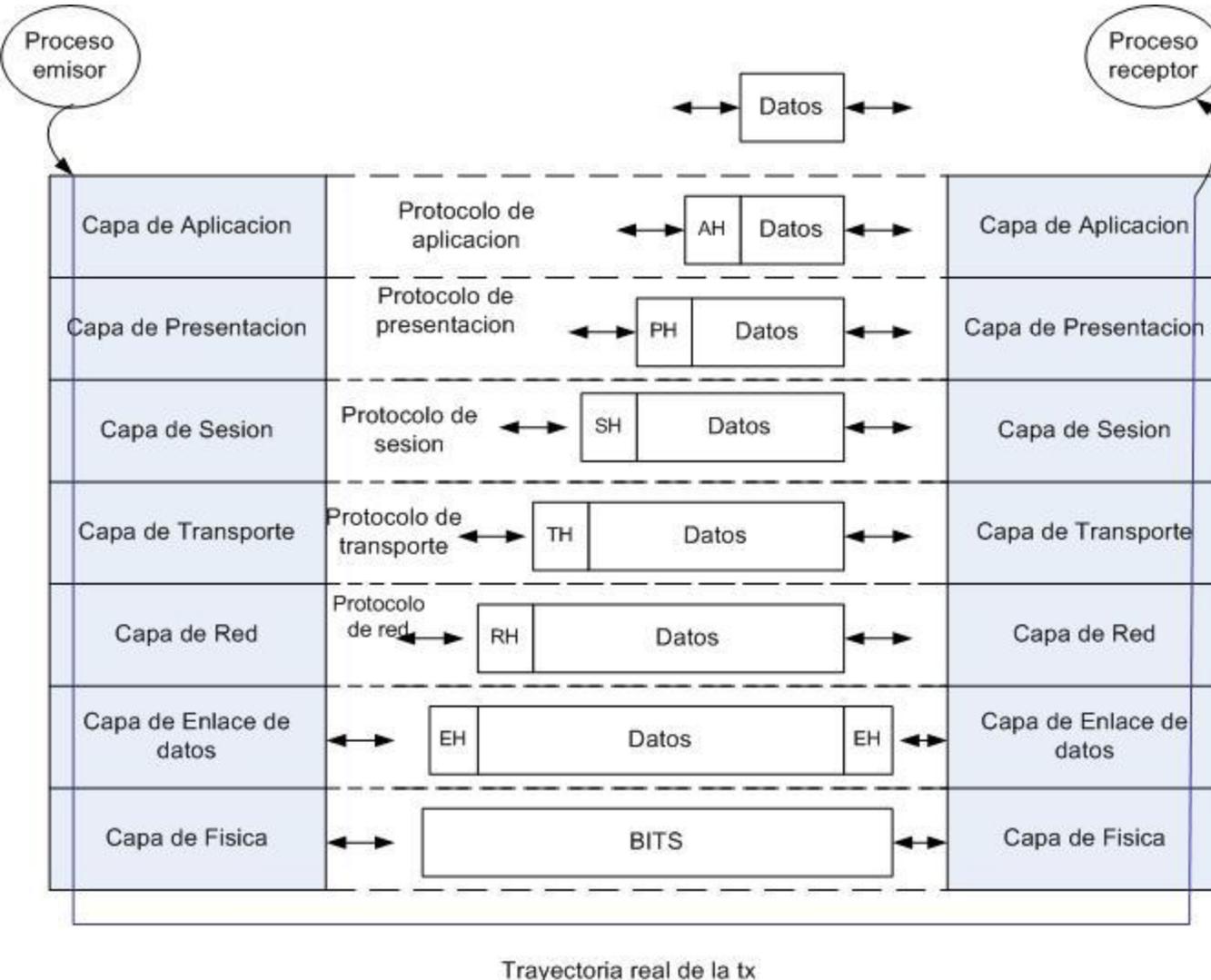
En realidad, la comunicación real se lleva a cabo en el nivel físico:

*En la fuente,*  
Conforme la información es enviada a las capas inferiores:

El protocolo correspondiente e a cada capa agrega información de control a los datos.

*En el destino ,*  
Conforme la información es enviada a las capas superiores:

El protocolo correspondiente e a cada capa lee y analiza la información de control.



Trayectoria real de la tx



## Capas del modelo OSI



La comunicación entre capas se realiza por medio de primitivas y parámetros:

**Primitiva:** Especifica una función que se va a llevar a cabo

**Parámetros:** Permiten enviar información de control y datos.

Lectura  
justificación  
Capas



## 1. CAPA FISICA



Define el medio de comunicación utilizado para la transferencia de información, y coordina las funciones requeridas para transmitir una cadena de bits sobre el medio.

Especifica:

- Características físicas de las interfaces y los medios de comunicación.
- La representación de los bits.
- Tasa de transmisión.
- Sincronización de los bits.
- Configuración de las líneas (punto a punto, multipunto)
- La topología física.
- El modo de transmisión. (simplex, half duplex, full duplex)
- Técnica de modulación.
- Tipo de conexión

Ejemplo: RS232, V.28, V.35, etc.



## 2. CAPA DE ENLACE DE DATOS.



El objetivo principal de esta capa son los métodos para la comunicación confiable y eficiente entre dos máquinas. Se encarga de las siguientes funciones:

- **Transferencia de datos:** Establecimiento de servicios orientados y no orientados a conexión
- **Creación de marcos:** Divide la secuencia de bits en unidades de datos llamadas marcos, agrega el control necesario para la sincronización, control de errores y flujo.
- **Direcciones físicas:** Si los marcos son distribuidos a diferentes sistemas en la red, la capa de enlace agrega un encabezado al marco para definir la dirección física del receptor y/o del emisor.



## Capa de enlace de datos..

**Control de flujo**

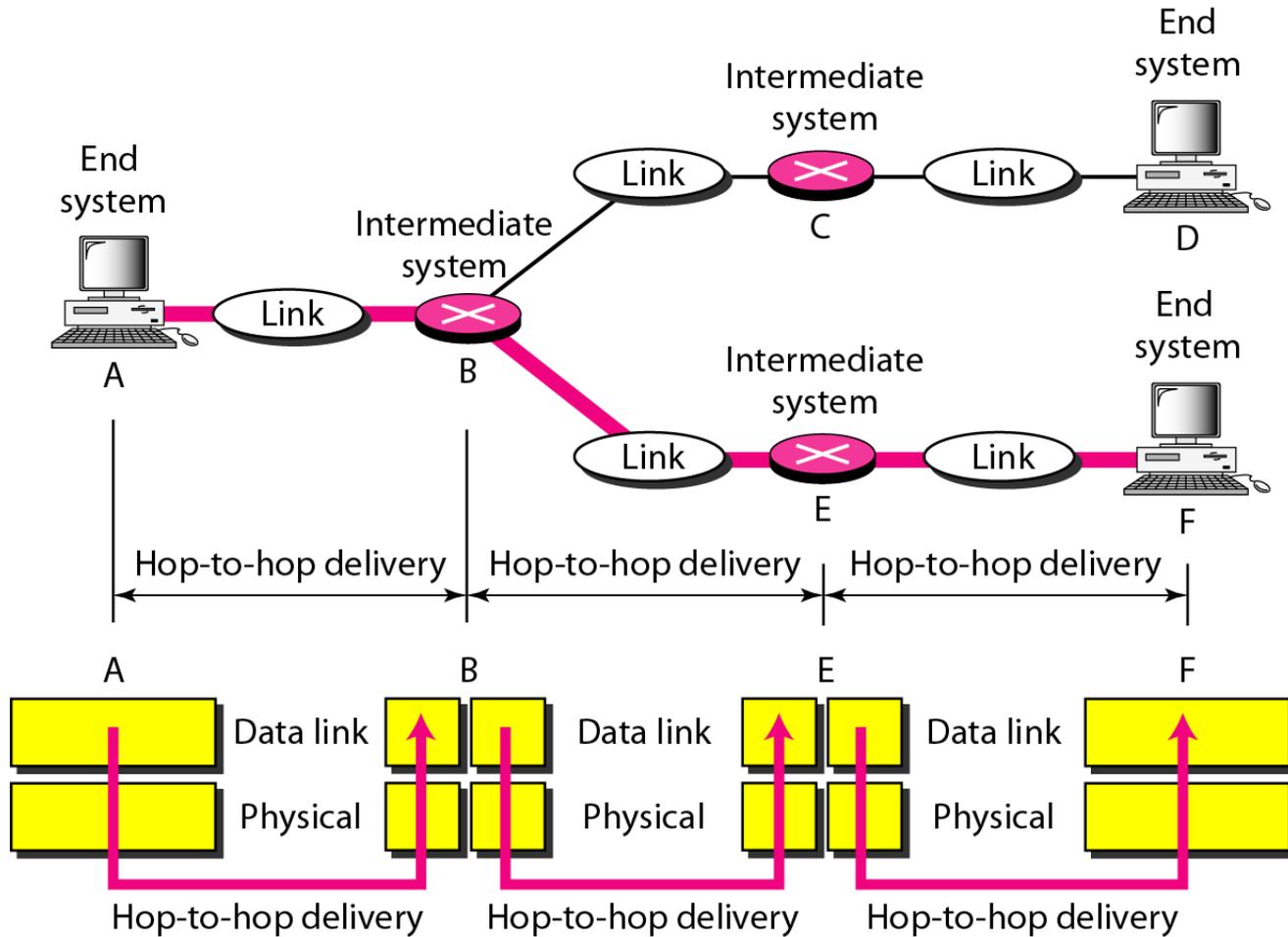
**Control de errores:**

**Control de acceso: Son protocolos destinados a determinar que dispositivo tiene control sobre el enlace de comunicación para poder transmitir.**

**Algunos protocolos que definen la capa de enlace de datos son: HDLC, LAPB,ADCCP**



En la capa de enlace de datos la entrega es de Nodo a Nodo.





### 3. CAPA DE RED

Es responsable de la de paquetes desde una fuente hasta el destino a través de multiples redes o enlaces. Se asegura que cada paquete llegue desde el punto de origen hasta su destino final.

Sus responsabilidades especificas son:

- Direcccionamiento lógico
- Enrutamiento.
- Establece, mantiene y termina las conexiones
- Conmuta, enruta y controla la congestión de los paquetes de información en una subnet.

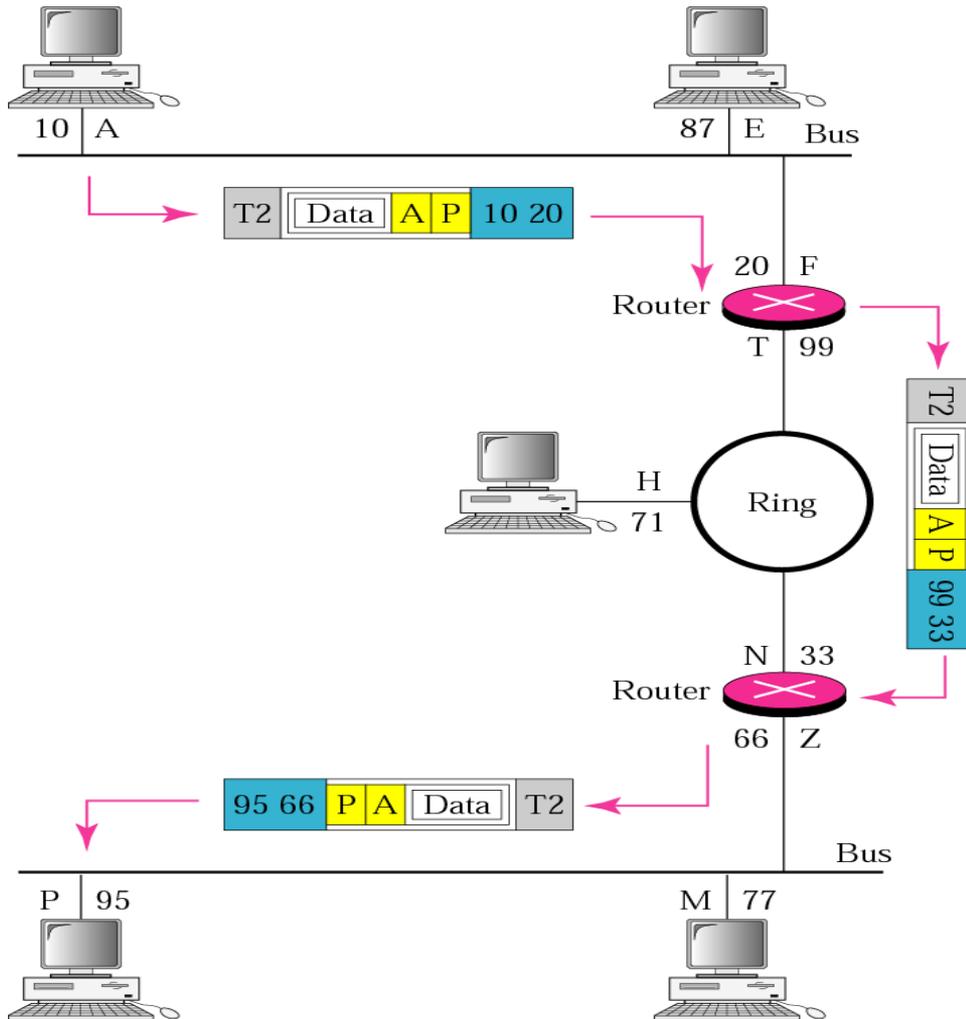
Existen múltiples protocolos que permiten llevar a cabo el enrutamiento de paquetes entre ellos:

Ruteo por el camino más corto,  
Ruteo basado en flujo,  
por vector de distancia,  
multicamino, entre otros...



### 3. CAPA DE RED

PC con dirección lógica A (física 10), desea comunicarse con la PC P (dir. Física 95). El primer paso es entregar la info. Al router con dirección lógica F (física 20)



La información pasa a cada dispositivo de red, donde la dirección física indica el dispositivo de interconexión mas cercano.

Finalmente la info. es entregada. La dirección de lógica nunca cambia.



## 4. CAPA DE TRANSPORTE

Esta capa asegura que la llegada de datos de la capa de red encuentren las características de transmisión y calidad de servicio requerido por la capa de sesión. La capa de transporte asegura la entrega del mensaje total de la fuente hacia el destino.

Las responsabilidades específicas de esta capa son:

- Direccionamiento de puntos de servicio. (puertos / sockets).
- Segmentación y reensamble. Un mensaje se divide en segmentos transmitibles, cada segmento contiene un número secuencial. Estos números permiten reensamblar el mensaje e identificar paquetes perdidos.
- Control de Conexión: Puede ser sin conexión u orientada a la conexión.

Esta capa además:

- Define como direccionar la localidad física de los dispositivos de red
- Asigna una dirección única de transporte a cada usuario
- Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.
- Establece como hacer y deshacer las conexiones entre los nodos.

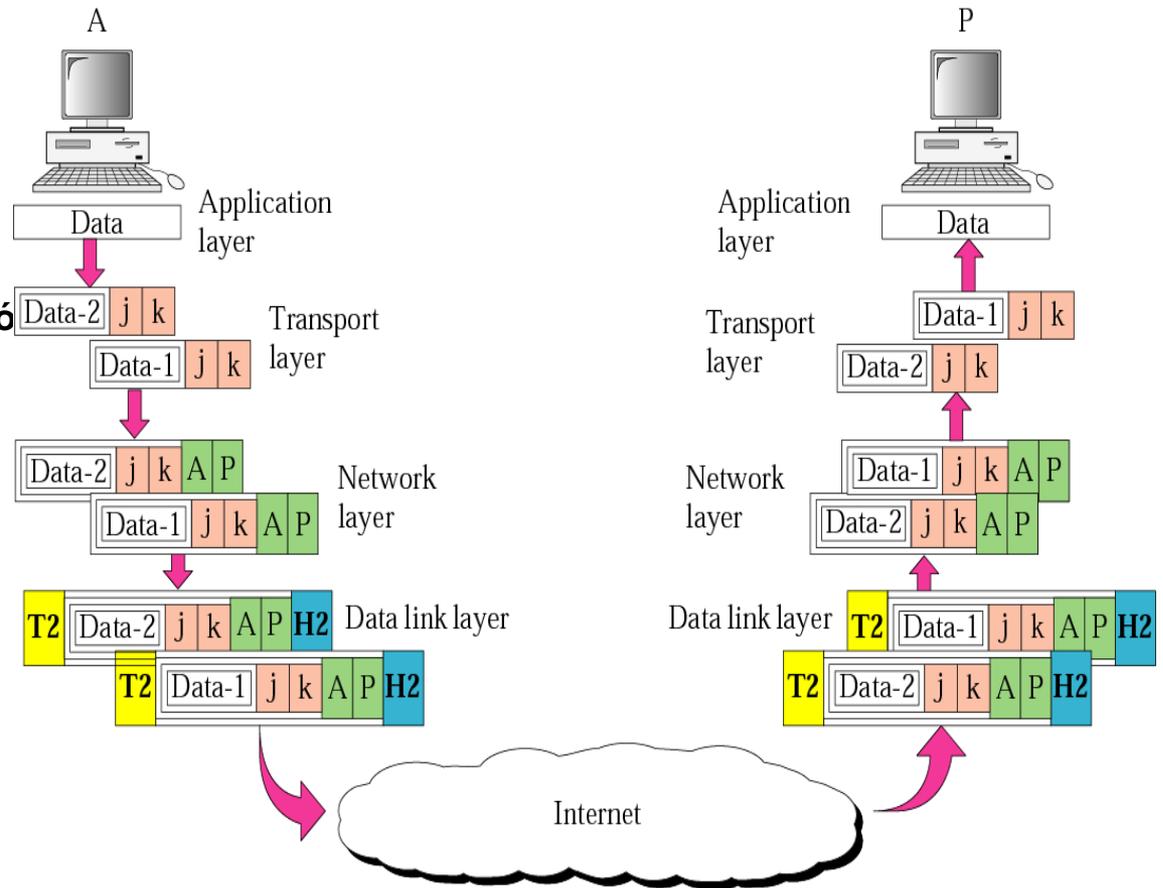


## 4. CAPA DE TRANSPORTE

Las direcciones corresponden a puertos

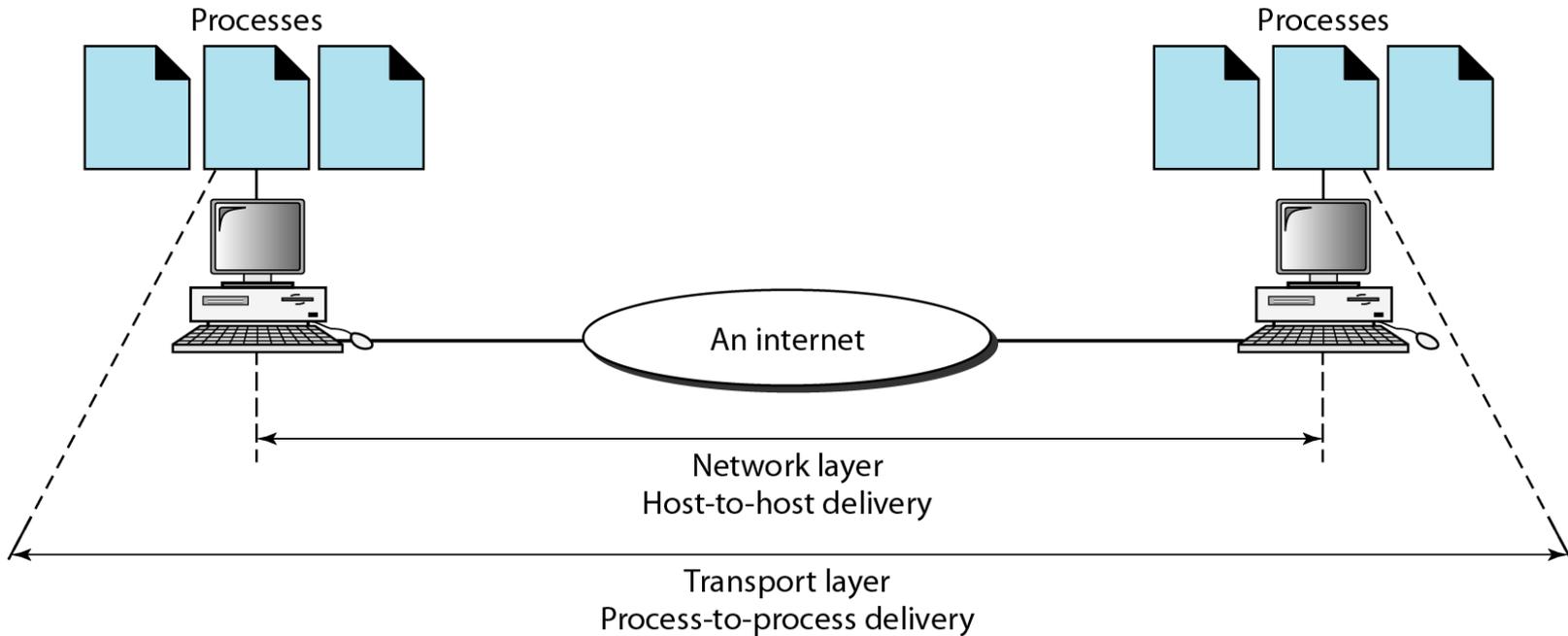
Los datos se dividen en dos datagramas y se agregan la dirección de red

Los paquetes son encapsulados





**El nivel de transporte se encarga de la entrega de mensajes completos desde un proceso a otro.**





## **5.- CAPA DE SESION**

**Provee los servicios utilizados para la organización y sincronización del diálogo entre usuario y el manejo e intercambio de datos..**

**Sus responsabilidades específicas son:**

- Control de dialogo.**
- Sincronización.**

**Sus principales funciones son:**

- Establecer el inicio y termino de una sesión**
- Recuperación de la sesión**
- Referencia de los dispositivos por nombre y no por dirección**
- Permite desarrollar software para ejecutarse en cualquier instalación de red.**



## 6. CAPA DE PRESENTACIÓN

**Esta relacionada con la sintaxis y la semántica de la información intercambiada entre los sistemas.**

**Sus responsabilidades son:**

- **Traducción. Se encarga de traducir los caracteres a cadenas de bits en el sistema de codificación correspondiente.**
- **Encriptado.**
- **Compresión.**

**Sus funciones son:**

- **Determina la forma de presentación de los datos sin preocuparse de su significado.**
- **Establece independencia de procesos de aplicación considerando las diferencias en la representación de los datos.**
- **Opera el intercambio y la visualización.**



## **7. CAPA DE APLICACIÓN.**

**Esta capa permite que el usuario final, ya sea un humano o una computadora, tenga acceso a la red. Provee las interfaces y los servicios que permitan la transferencia de información tales como: correo electrónico, acceso a archivos remotos, administración de b.d. compartidas, etc.**

**Los servicios específicos que provee son:**

- Terminal Virtual de Red.**
- Transferencia de Archivos.**
- Servicios de correo**
- Servicios de directorios.**

**Sus principales funciones son:**

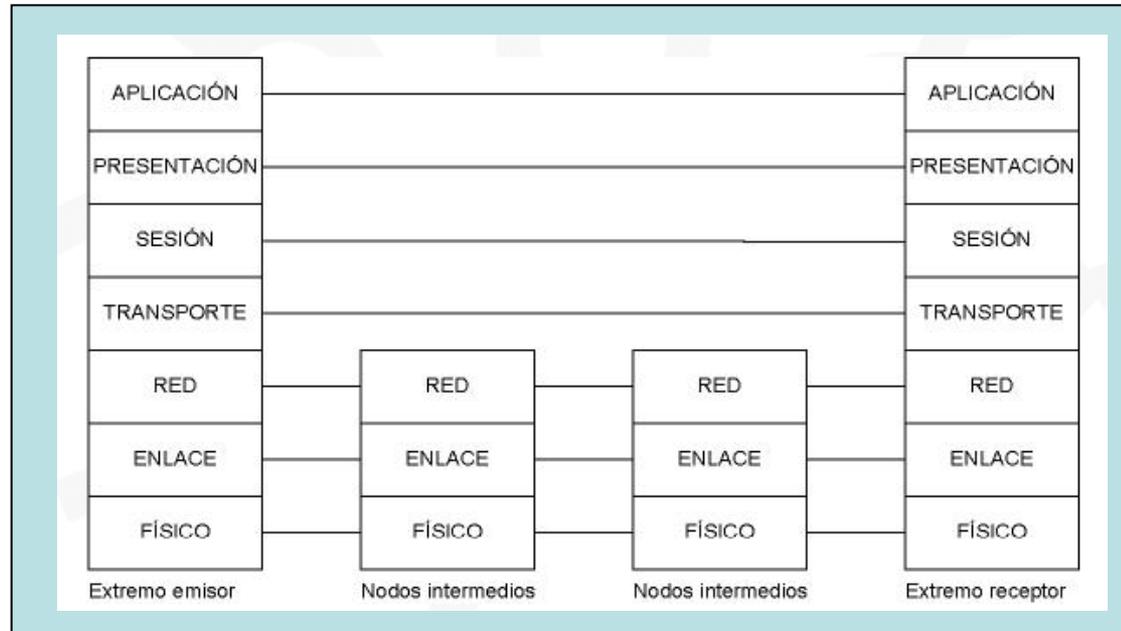
- Proporcionar comunicación entre dos procesos de aplicación, tales como: programas de aplicación de red, etc.**
- Proporcionar aspectos de comunicaciones para aplicaciones específicas entre usuarios de redes.**



## EN GENERAL:

Puede considerarse que las 7 capas del modelo OSI se encuentran agrupadas en 3 categorías:

- Las capas 1, 2 y 3 (Física, enlace de datos y de red), son las capas de soporte de la red.
- Las capas 5,6, y 7 (Sesión, presentación y aplicación) son las capas que dan soporte al usuario.
- La capa 4 (transporte) asegura una transmisión confiable punto a punto.

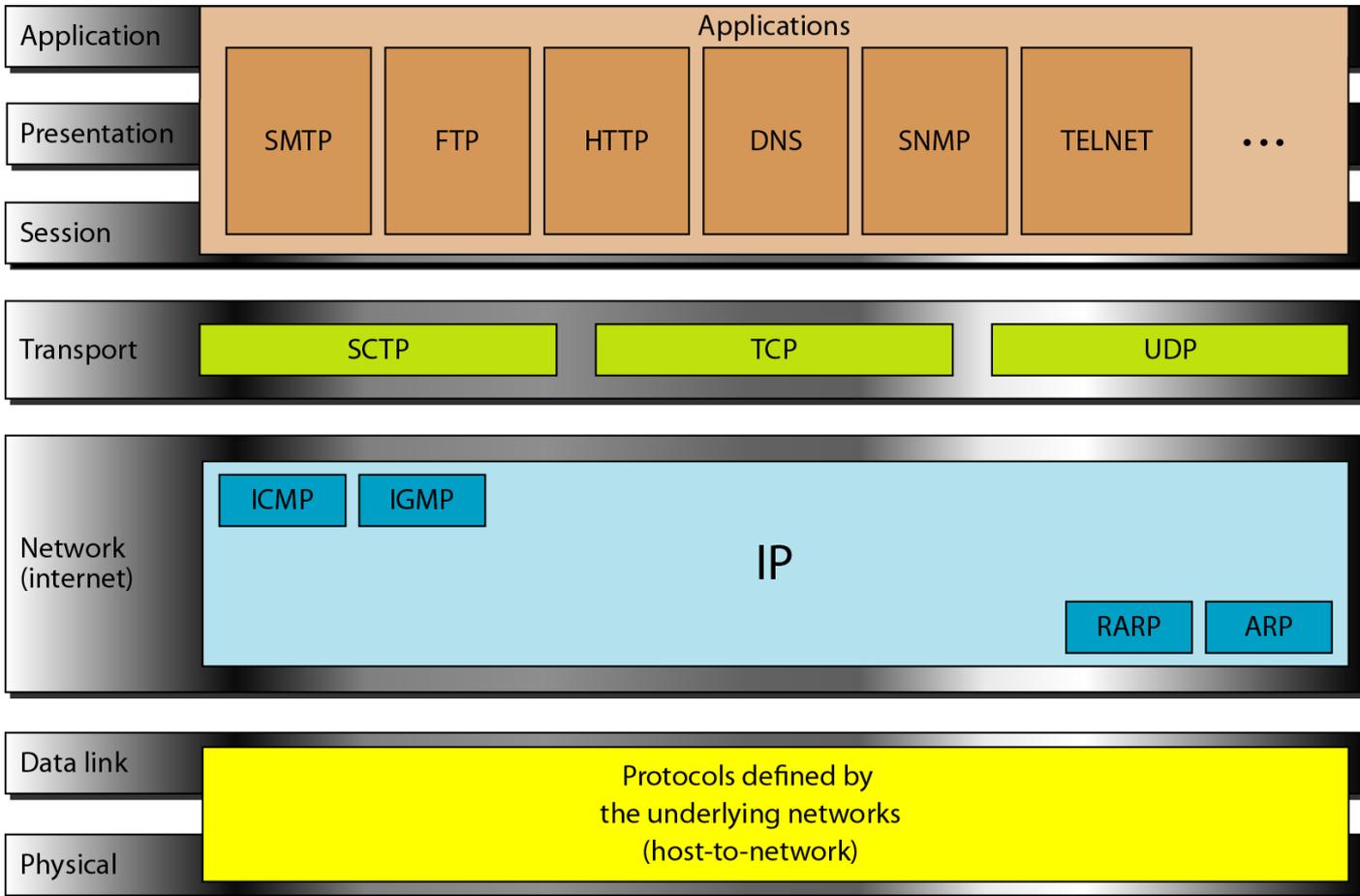




# Modelo de Internet.

4 Capas:

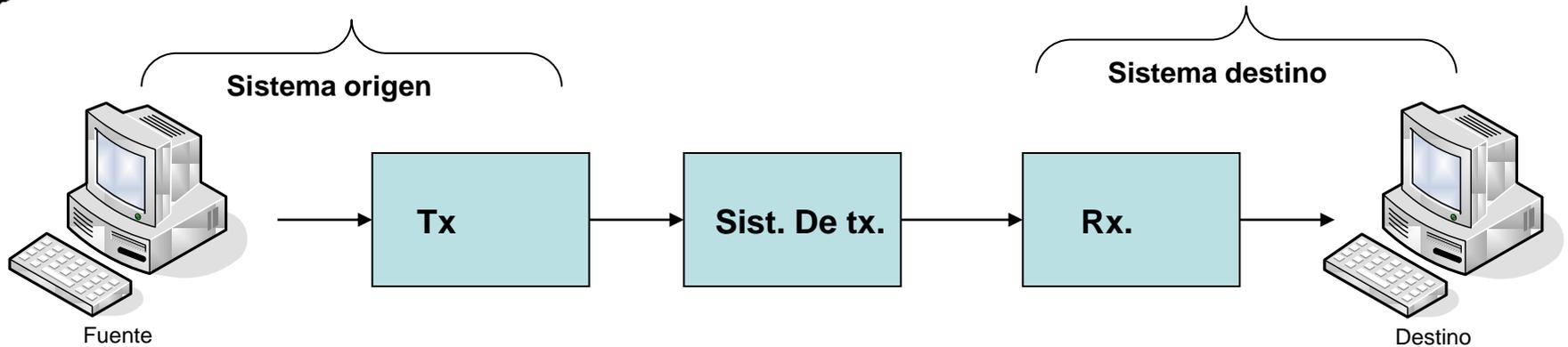
Acceso a la red, Internet Transporte y Aplicación



TCP/IP



***Una red de computadoras es un sistema de comunicaciones de datos que enlaza dos o más computadoras y dispositivos periféricos.***



- Generación de la señal
- Utilización del sistema de tx. (control de congestión)
- Implementación de la interfaz.
- Sincronización
- Gestión del intercambio
- Detección y corrección de errores

- Control de flujo
- Direccionamiento
- Encaminamiento
- Recuperación
- Formato de mensajes
- Seguridad
- Gestión de red



## **Objetivos principales de una red de computadoras:**

- 1. La información debe ser entregada de manera confiable y sin daños en los datos.**
- 2. La información debe entregarse de manera consistente.**
- 3. Los equipos que forman la red deben ser capaces de identificarse entre sí.**
- 4. Debe existir una manera estandarizada de nombrar e identificar las partes de la red.**



• ¿para que establecer una red de computadoras?

- **Compartición de archivos y programas**
- **Compartición de recursos de red**
- **Compartición de bases de datos**
- **Expansión económica de la PC**
- **Grupos de trabajo**
- **Correo electrónico**
- **Mejora de la estructura corporativa.**

# Clasificación de las redes por Escala



## LAN, (MAN), WAN

### •LAN (LOCAL AREA NETWORK):

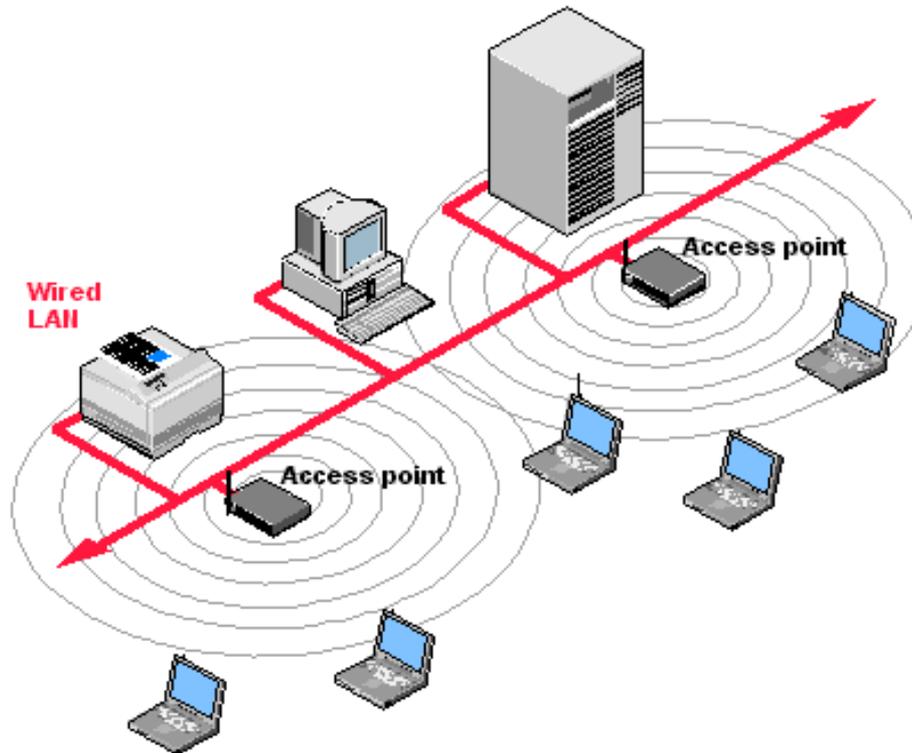
- Generalmente es una red privada. Se trata de una red que cubre una extensión reducida como una empresa, una universidad, un colegio, etc... No habrá por lo general dos computadoras que disten entre sí más de un kilómetro.

- Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información.

Generalmente utilizan un solo medio de transmisión y topología.



## LAN, WLAN



**Las redes LAN se pueden clasificar en dos categorías principales:**

**•Igual a igual**

**Cliente/servidor**

**Unidad I**



**El tipo de red que se implante debe depender de factores como:**

- **Tamaño de la organización**
- **Nivel de seguridad requerido**
- **Tipo de negocio**
- **Nivel de soporte administrativo disponible**
- **Cantidad de tráfico en la red**
- **Necesidades de los usuarios de la red**
- **Presupuesto disponible**

**Las redes igual a igual son una buena elección cuando:**

- **Hay menos de 10 usuarios**
- **Los usuarios están ubicados en la misma área**
- **La seguridad no es problema**
- **La organización y la red tendrán un crecimiento limitado en un futuro próximo.**

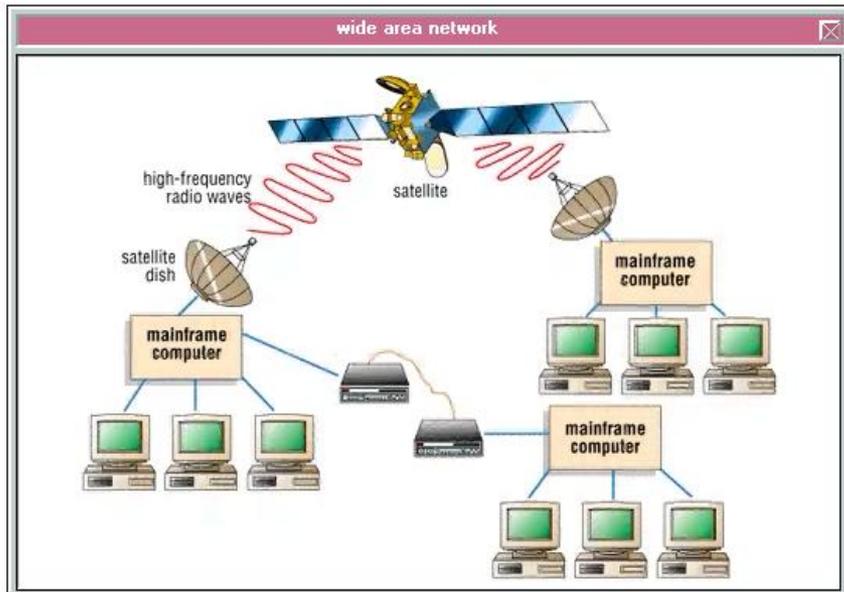
**Las redes cliente/servidor se han convertido en el modelo estándar de red, son apropiadas cuando hay más de 10 usuarios, se requiere mantener la seguridad y la integridad de la información, así como expansiones en la red.**

**Es posible tener múltiples servidores, incluyendo: de archivos, impresión, aplicación, de correo, de fax, de comunicación.**

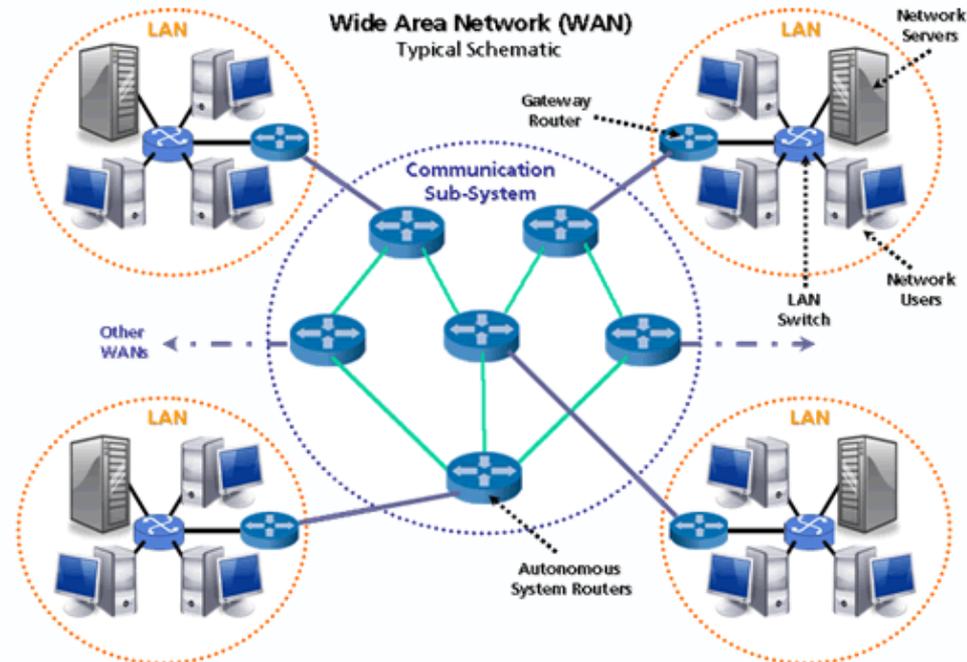
# WAN (WIDE AREA NETWORK)



Las redes de área extensa cubren grandes regiones geográficas como un país, un continente o incluso el mundo. Cable transoceánico o satélites se utilizan para enlazar puntos que distan grandes distancias entre sí. El mejor ejemplo es Internet.



Una WAN generalmente consiste en dos o mas LANs interconectadas.





## Las redes WAN pueden ser :

### Redes punto a punto:

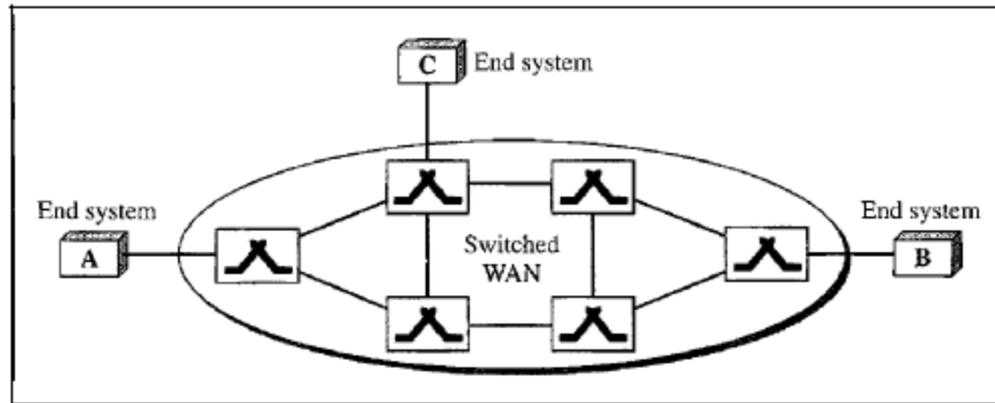
Redes Satelitales

Conexión ISP (Internet Service Provider)

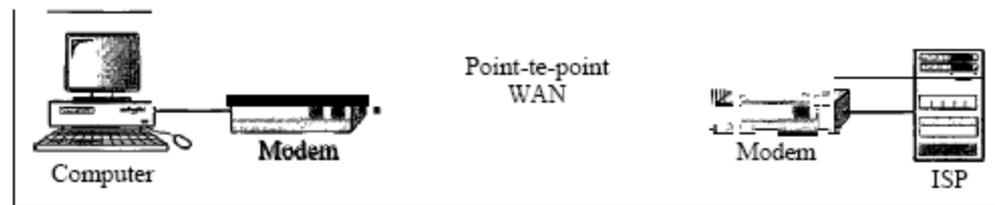
### Redes Conmutadas (switched)

Redes de conmutación de circuitos

Redes de conmutación de paquetes.



a. Switched WAN



b. Point-to-point WAN



**Conmutación se refiere a la transferencia de la unidad de información (datos)**

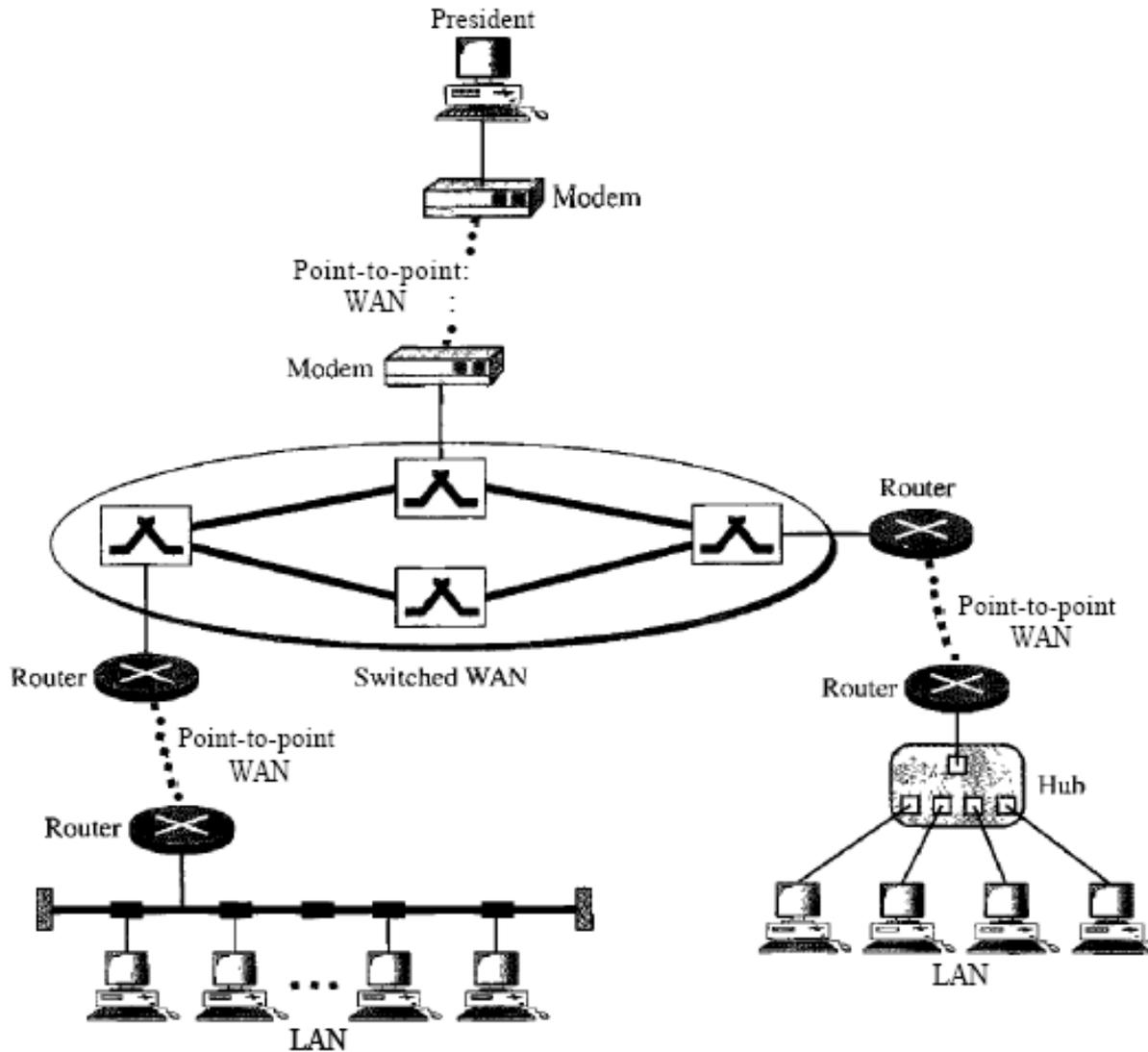
**-Conmutación de circuitos: Transferencia orientada a conexión.**

**-Conmutación de paquetes: Divide cada mensaje en varios paquetes (MTU) que pueden tomar diferentes caminos.**

Propiedad	Conmutación de circuitos	Conmutación de paquetes
Selección de la ruta	Estática	Dinámica
Reordenamiento posible	No	Si
Respuesta a fallas en la línea	Perdida de datos	Retransmisión
QoS	Garantizada	Depende de la red

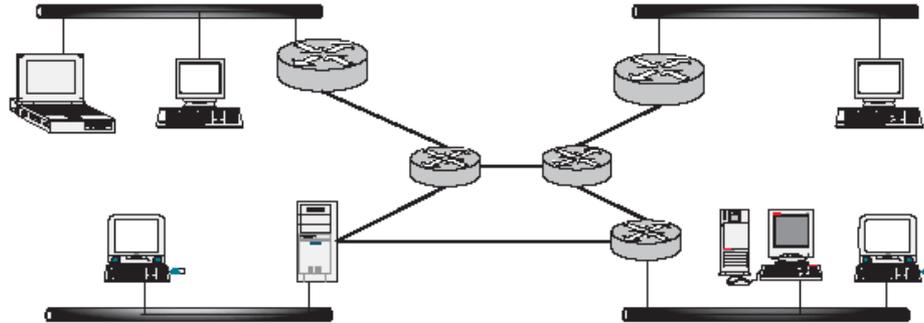


La diferencia de las LANs las WANs son heterogéneas.





# Las redes de computadoras requieren comunicación digital.



**Comunicación digital se refiere a cualquier proceso que transfiera información entre:**

- Un CPU a otro CPU
- Un CPU a cualquier periférico
- Un CPU a un Módem

**Los elementos requeridos para que pueda darse la comunicación digital son:**

- Computadora
- Software
- Adaptador de comunicaciones
- Medio de comunicación



**-El CPU de la computadora controla el proceso de comunicación completo.**

**-El software se encarga de la transferencia de información entre la memoria principal y el adaptador de comunicaciones, soportando diálogo, correo, transferencia de archivos, compartición de recursos y control.**

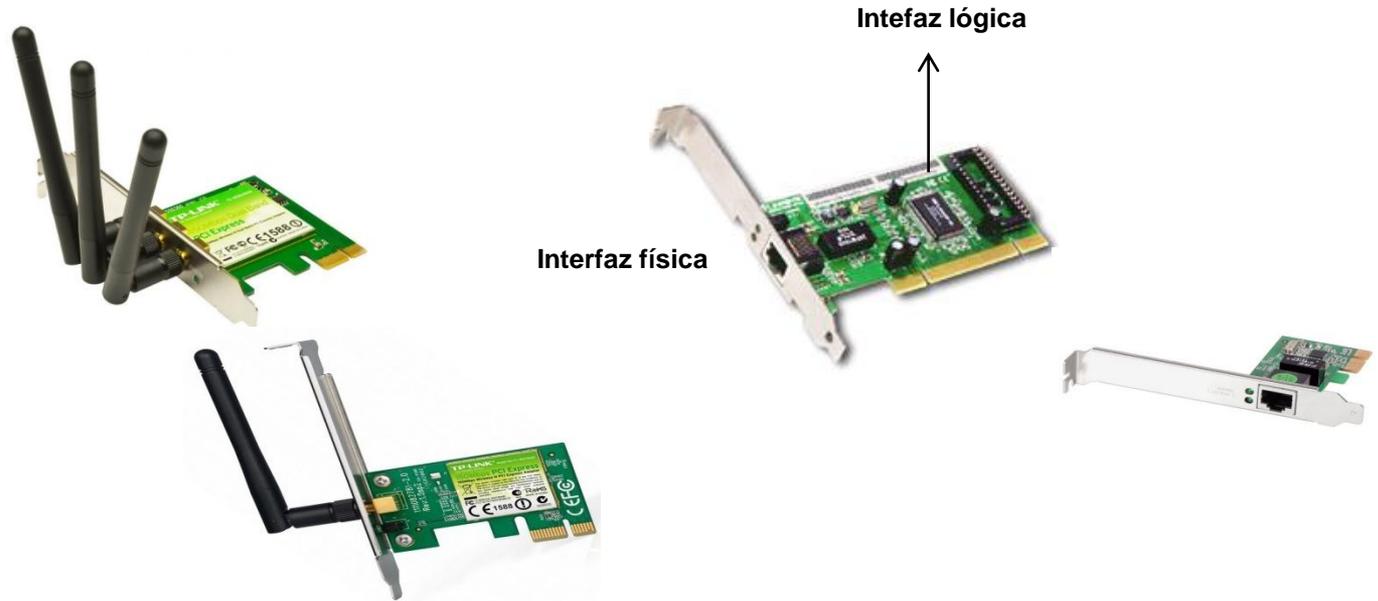
**-El medio de comunicación es el medio físico utilizado para transmitir información..**

**-El adaptador de comunicaciones formatea la información de manera adecuada para llevar a cabo la comunicación.**



## Elementos de un adaptador de comunicaciones:

- Interfaz física
- Interfaz lógica.



## Interfaz Física

es el método de conexiones mecánicas y eléctricas, debidamente estandarizadas que permite establecer la conexión física entre el adaptador de comunicaciones y el medio de comunicación. Se definen tres aspectos importantes de la misma:

- **Aspecto mecánico:** Define parámetros como: Geometría del conector y dimensiones del conector.
- **Aspecto eléctrico:** Define parámetros como: Número de líneas eléctricas útiles en el conector, disposición de las líneas, entre otros..
- **Aspecto funcional:** Describe la función de cada circuito eléctrico en la conexión especificando: Nombre de cada línea o circuito, número de cada línea y función de cada una.



# La interfaz lógica

Es software, apoyado en hardware, que determina completamente la operación del adaptador, ya que establece:

- **Técnica de transmisión (Banda base, banda ancha)**
- **Tipo de transmisión (Síncrona, asíncrona)**
- **Codificación (NRZ, RZ, BiFase, Diferenciales)**
- **Velocidad de transmisión (en base a la vel. De modulación y codificación)**
- **Modo de operación del medio de comunicación (Simplex, Half Duplex, Full Duplex)**
- **Método de acceso (Disciplina de comunicación).**



## **MEDIOS DE COMUNICACIÓN**

**El medio de comunicación es el canal o enlace físico, puede ser:**

- Alámbricos (Guiados)**
- Inalámbricos (No Guiados)**

**Ensayo.**



## **MEDIOS DE COMUNICACIÓN ALÁMBRICOS:**

**. Los tipos de cable más comunes en la transmisión de datos son:**

- Cables de cobre**
- Cables de fibra óptica**

**•Cable o alambre ?**

**-Un alambre es un filamento de material conductor, que puede tener diferentes diámetros o calibres,**

**-un cable es la reunión de varios alambres y otros elementos, integrados bajo una configuración específica.**

**Existen:**

- Cables multipares**
- Cables coaxiales**



Independientemente de su estructura, los cables presentan tres características importantes:

- *Características mecánicas*
- *Características eléctricas*
- *Características de transmisión.*

• **Características mecánicas:** Describen forma y geometría del conductor, propiedades mecánicas del material, etc. Entre ellas una característica importante es el diámetro del conductor, el cual establece un calibre estandarizado.

• **Características eléctricas: (Impedancia, capacitancia)**

- **Impedancia:** Es la suma de las contribuciones resistivas de cada una de las tres características: inductiva, capacitiva y resistiva del cable, que se oponen al paso de las señales. Se expresa en Ohms.

- **Capacitancia:** Es la capacidad medida por unidad de longitud de cable. Normalmente se expresa en picofarads/m



**Características de transmisión:** Describen la propagación de la señal eléctrica en un cable, se consideran:

**-Coeficiente de atenuación:** Es un factor constante por cable, que determina la cantidad de pérdida de la señal que existe en un cable por unidad de longitud. Se expresa en dB/m:

Con A = Atenuación del cable

L = Longitud del cable

$a=A/L$  es el coeficiente de atenuación.

**-Factor de propagación:** Es un numero fraccionario que representa el % de la velocidad de la luz con el que una señal se propagara en el cable. Es sensible a la frecuencia,

Si:

V = velocidad de propagación de la señal en el cable

C = Velocidad de la luz en el vacio

Entonces:

$K = v/c$  es el factor de propagación del cable.

**Ancho de banda:** Describe la capacidad de transmisión de un medio de comunicación, normalmente se expresa en Mhz.



## CABLE PAR TRENZADO.

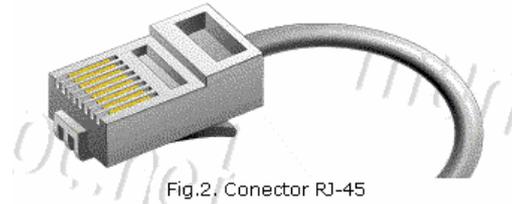
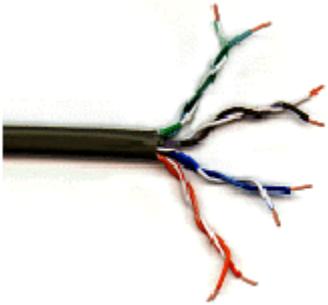


Fig.2, Conector RJ-45

**UTP** → unshielded twisted pair (sin blindaje)

**STP** → shielded twisted pair (con blindaje)

### -Características mecánicas (calibre):

- 22 AWG (diámetro = 0.640 mm) (American Wire Gauge)
- 24 AWG (diámetro = 0.510 mm)
- 26 AWG (diámetro = 0.404 mm)

### -Características eléctricas:

Impedancia: 100 ohms (UTP) y 150 ohms (STP)

Capacitancia: Cable grado de voz (60 a 115 pf/m) y cable grado de datos ( <60 pf/m)

-El coeficiente de atenuación de un cable multipar en promedio es del orden de 6 db/km.

-El factor de propagación de un cable multipar tiene valores aproximados a 0.66 por grado voz y 0.78 para grado datos.

-El ancho de banda de un cable multipar varia desde unos cuantos Mhz hasta 1000 Mhz.



La EIA/TIA (Electronic Industries Association/ Telecommunications Industries Association) en su norma 568 define las categorías de par trenzado:

- Categoría 1 Hilo telefónico trenzado de calidad de voz no adecuado para las transmisiones de datos. Velocidad de transmisión inferior a 1 Mbps.
- Categoría 2 Cable de par trenzado sin apantallar.Su velocidad de transmisión es de hasta 4 Mbps.
- Categoría 3 Velocidad de transmisión de 10 Mbps.Con este tipo de cables se implementa las redes Ethernet 10BaseT.
- Categoría 4 La velocidad de transmisión llega a 16 Mbps.
- Categoría 5 Puede transmitir datos hasta 100 Mbps.
- Categoría 6 / 6a Mejora la relacion señal a ruido que otras categorias,transmision hasta 10 Gbps
- Categoría 7 / 7a Soporta frecuencias de hasta 1000 MHz y transmisiones de hasta 40 Gbps.

*Los cables nivel 1 y 2 no son reconocidos en el estándar para cableado de redes.*



## Categoría

### Ancho de banda (MHz)

### Aplicaciones

### Notas

Categoría	Ancho de banda (MHz)	Aplicaciones	Notas
<a href="#">Cat. 1</a>		Líneas telefónicas y módem de banda ancha.	No descrito en las recomendaciones del EIA/TIA. No es adecuado para sistemas modernos.
<a href="#">Cat. 2</a>	4 CG CANDE	Cable para conexión de antiguos terminales como el <a href="#">IBM 3270</a> .	No descrito en las recomendaciones del EIA/TIA. No es adecuado para sistemas modernos.
<a href="#">Cat. 3</a>	16 MHz Clase C	10BASE-T and 100BASE-T4 <a href="#">Ethernet</a>	Descrito en la norma EIA/TIA-568. No es adecuado para transmisión de datos mayor a 16 Mbit/s.
<a href="#">Cat. 4</a>	20 MHz	16 Mbit/s <a href="#">Token Ring</a>	
<a href="#">Cat. 5</a>	100 MHz Clase D	10BASE-T y 100BASE-TX <a href="#">Ethernet</a>	
<a href="#">Cat. 5e</a>	100 MHz Clase D	100BASE-TX y 1000BASE-T <a href="#">Ethernet</a>	Mejora del cable de Categoría 5. En la práctica es como la categoría anterior pero con mejores normas de prueba. Es adecuado para <a href="#">Gigabit Ethernet</a>
<a href="#">Cat. 6</a>	250 MHz Clase E	1000BASE-T <a href="#">Ethernet</a>	Transmite a 1000Mbps. Cable más comúnmente instalado en Finlandia según la norma SFS-EN 50173-1.
<a href="#">Cat. 6a</a>	250 MHz (500MHz según otras fuentes) Clase E	10GBASE-T <a href="#">Ethernet</a>	
<a href="#">Cat. 7</a>	600 MHz Clase F		Cable U/FTP (sin blindaje) de 4 pares.
<a href="#">Cat. 7a</a>	1000 MHz Clase F	Para servicios de telefonía, <a href="#">Televisión por cable</a> y Ethernet 1000BASE-T en el mismo cable.	Cable S/FTP (pares blindados, cable blindado trenzado) de 4 pares. <b>Unidad en desarrollo.</b>



# CABLE COAXIAL.

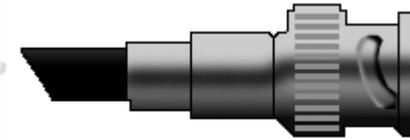
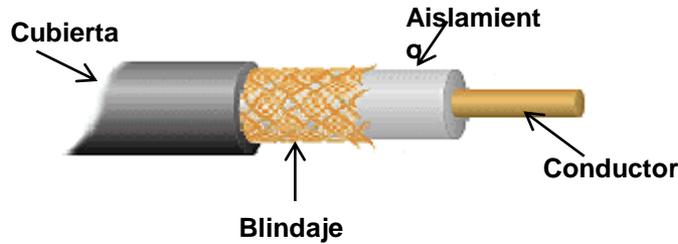


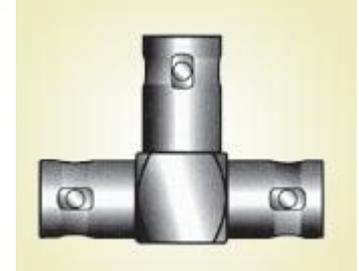
Fig.4, BNC connector

**Rango de Frecuencias:**  
**100kHz- 500MHz**

**RG → Radio Government**

**RG-8    RG-11    RG-59**

**RG-9    RG-58**



**-Características mecánicas:** Se describen por los diámetros de: Conductor central, del aislamiento y de la cubierta exterior:

•Cable coaxial delgado: Es un coaxial flexible con un grosor aproximado de 6 mm. Se conecta directamente a la tarjeta adaptadora. Calibre 20 AWG. Distancia: 185 mtrs.

•Cable coaxial grueso: Es un cable relativamente rígido de un diam. De 12 mm. Se denomina Ethernet estándar. Distancia: 500 mtrs. Calibre 12 AWG.

**-Características eléctricas:**

La impedancia es en promedio de 75.75 pf/m para coaxial grueso y de 84.84 pf/m para coaxial delgado.

**-Características de transmisión:** son muy sensibles al diseño del cable y a la elección de los materiales.

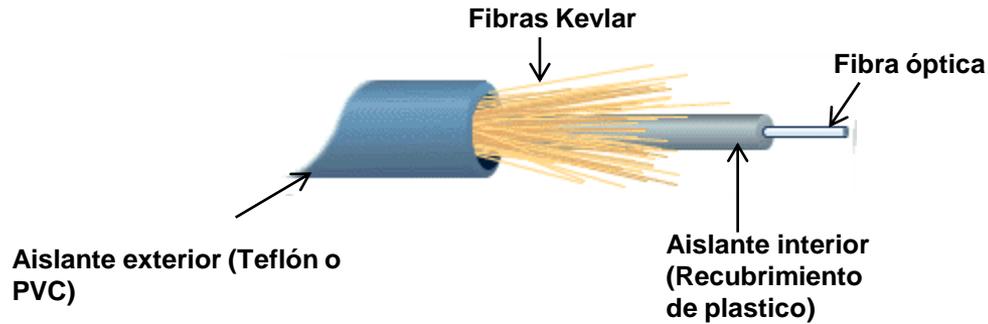
**Coefficiente de atenuación:** 11db/km/ grueso - 39 db/km delgado

**Factor de propagación:** 0.8/grueso - 0.66/delgado

**Ancho de banda:** 500 Mhz



## CABLES DE FIBRA ÓPTICA



La fibra consta de dos partes:

- Núcleo
- Revestimiento

Debiendo cumplir que:

$$n1 > n2$$

Conectores :ST, SC,FC



SC



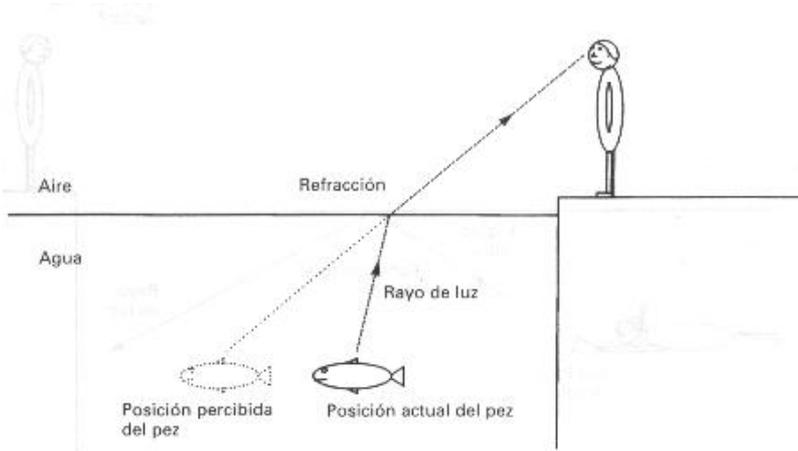
ST

- Alcance superior a los 10 km. sin repetidor
- Ancho de banda muy grande, superior a los 500 GHz-KM
- Velocidades de transmisión superior a 100 Mbps
- Baja atenuación  $\geq 0.16$  dB/km
- 100 % inmune a radiaciones electromagnéticas.
- Fácil de instalar
- Bajo peso
- Dimensiones reducidas
- Transmisiones altamente confiables
- Transmisiones altamente seguras.

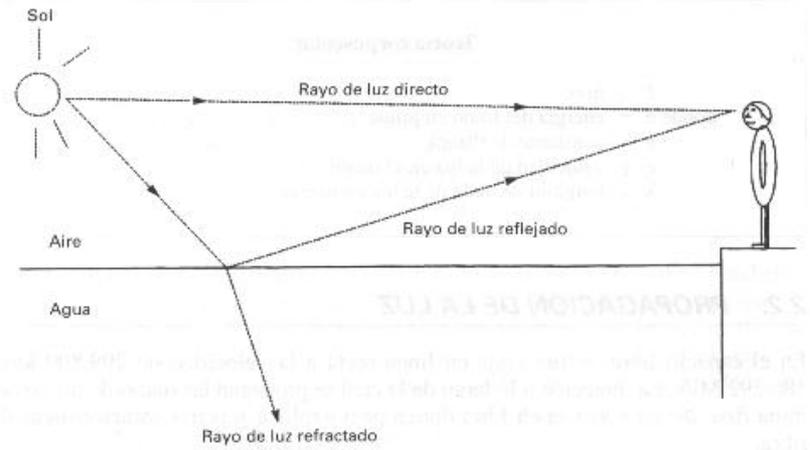


# CABLES DE FIBRA ÓPTICA

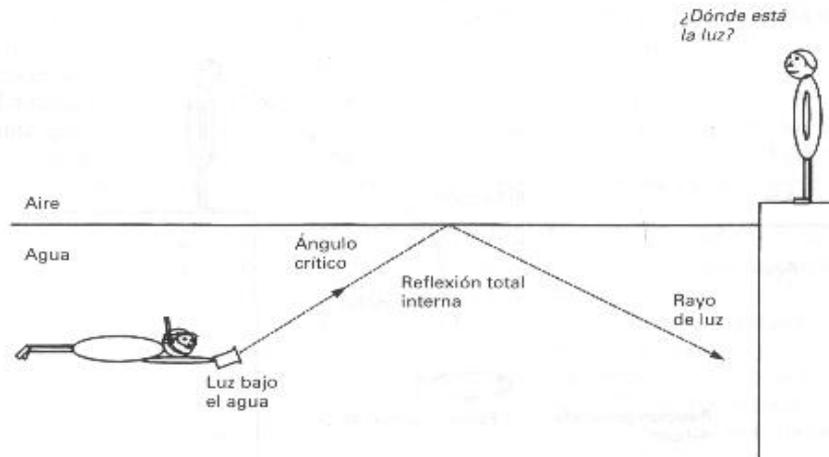
## Refracción



## Reflexión

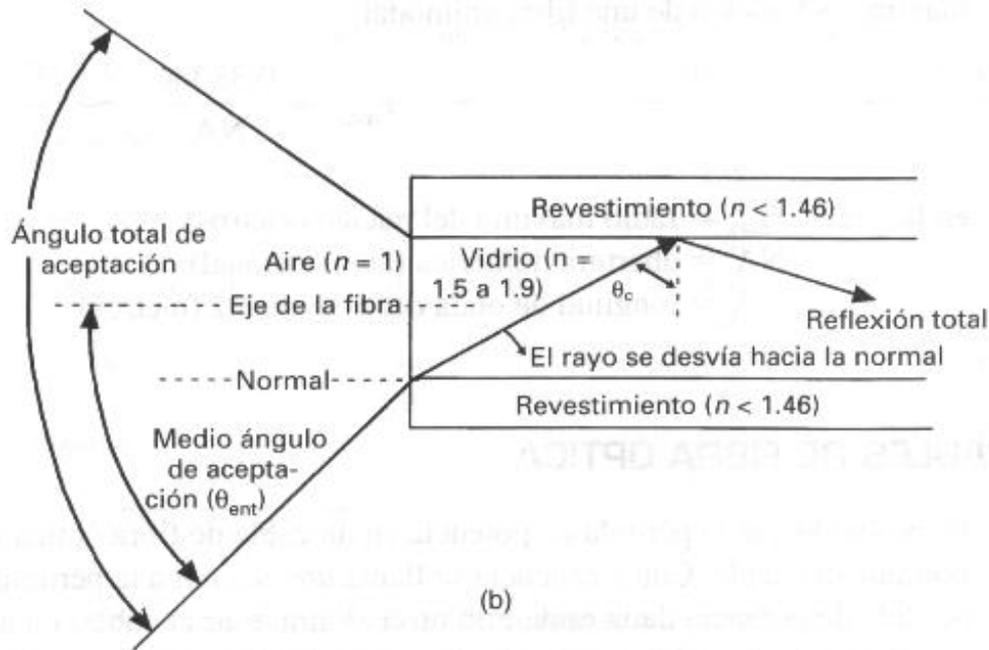
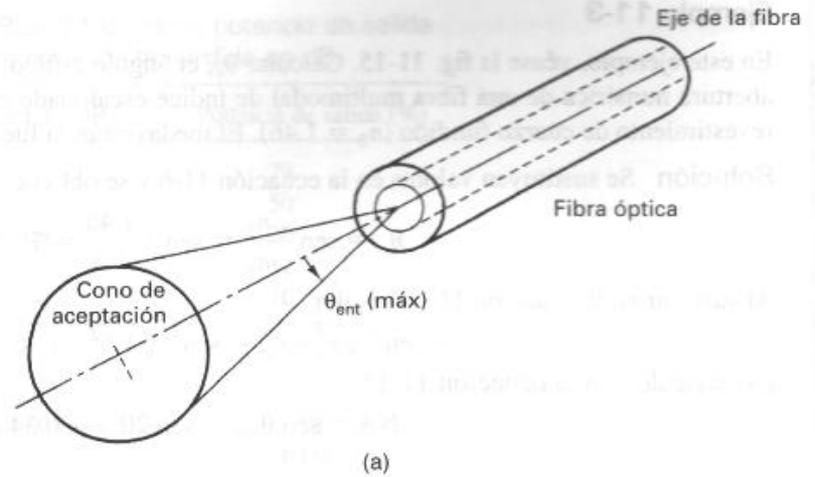
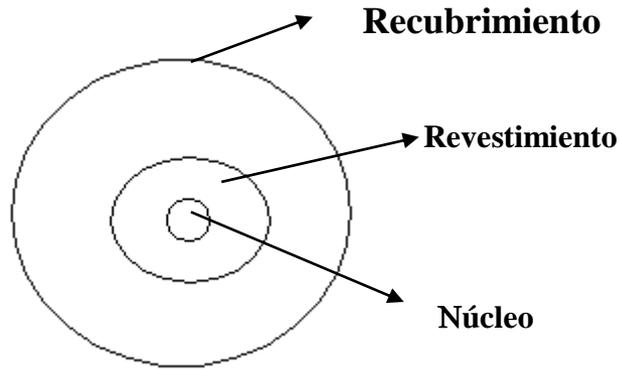


## Reflexión total





# CABLES DE FIBRA ÓPTICA



$$n_{nucleo} > n_{revestimiento}$$

[Video 1](#)

[Video 2](#)

Unidad I



## **MEDIOS DE COMUNICACIÓN INALÁMBRICOS:**

Las señales son normalmente difundidas en el aire y cualquiera que tenga un dispositivo capaz de recibirlas puede hacerlo.

Permiten establecer redes LAN, LAN extendidas y computación móvil. Utilizan básicamente 3 técnicas de transmisión:

❖ **Infrarrojos**

❖ **Ondas de radio**

❖ **Microondas**

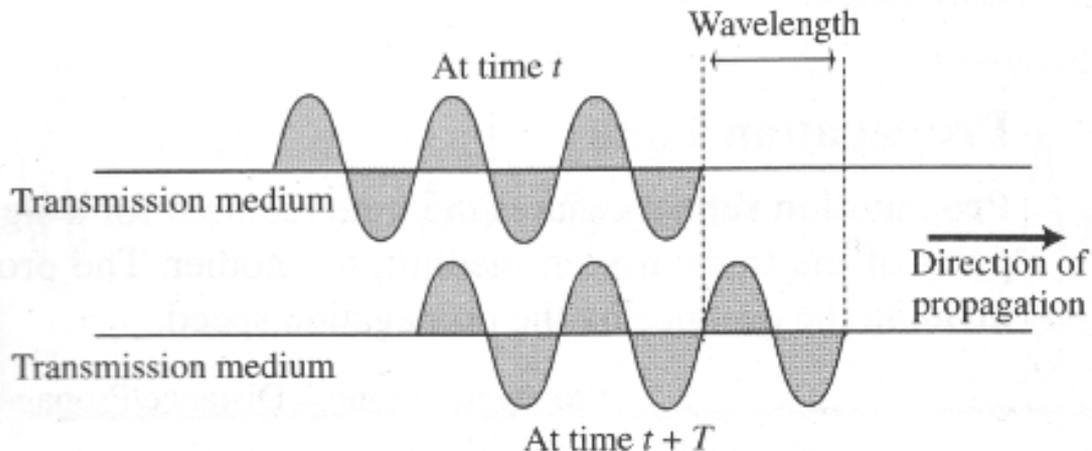
# Longitud de onda:



Es otra característica importante de las señales viajando a través de un medio de tx.

La longitud de onda une al periodo y la frecuencia de una señal sinusoidal a la velocidad de propagación del medio. Es decir, depende tanto de la frecuencia como del medio. La longitud de onda esta asociada con señales eléctricas, sin embargo es utilizada para caracterizar especialmente transmisiones de luz en fibra óptica.

Se define como la distancia que una señal puede viajar en un periodo.



Se calcula mediante :

Longitud de onda = Velocidad de propagación x periodo



Ya que la frecuencia es el inverso del periodo :  
Longitud de onda = velocidad de propagación / frecuencia.

De esta manera:

La velocidad de propagación de las señales electromagnéticas depende del medio y de la frecuencia de la señal. Por ejemplo, en el vacío, la luz es propagada a una velocidad de  $3 \times 10^8$  m/s.

La velocidad es menos en el aire y todavía menos en los cables.

La longitud de onda normalmente se mide en micrómetros o nanómetros, en lugar de metros.

$$\lambda = c/f \rightarrow \textit{velocidad de la luz/frecuencia}$$

$$\textit{Velocidad de la luz} \rightarrow 300,000,000 \text{ m/s}$$



**Ejemplo:**

**La longitud de onda de la luz infraroja: (Frecuencia =  $4 \times 10^{14}$ ) en el aire (en micrometros ) es:**

$$\lambda = \frac{c}{f} = ?$$

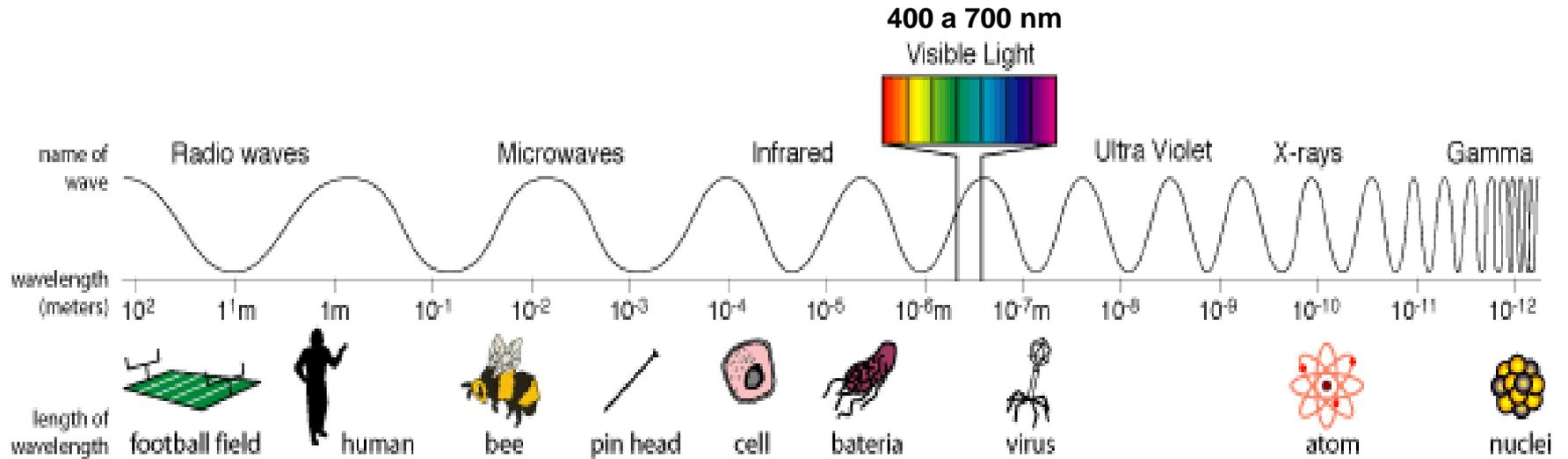
$$\lambda = \frac{c}{f} = \frac{3 \times 10^8}{4 \times 10^{14}} = 0.75 \times 10^{-6} \text{ m} = 0.75 \mu\text{m}$$



# Espectro electromagnético.

## Distribución del conjunto de ondas electromagnéticas.

A menor frecuencia mayor longitud de onda y viceversa.





**Infrarrojos:** Utilizan como transporte de las señales un haz de luz infrarroja. Permite la transmisión a altas velocidades debido a su gran ancho de banda, puede trabajar hasta a 10 Mbps.

- No pueden penetrar paredes (requieren vision directa)
- No hay interferencia entre sistemas
- No es posible usarlas en exteriores (los rayos solares contienen ondas infrarrojas)



## **Ondas de radio (radioenlace):**

**Requieren el uso de antenas omnidireccionales.**

**Las ondas de radio son útiles para transmisión multicast.  
Sus principales aplicaciones son: radio, televisión, teléfonos inalámbricos.**

## **Microondas:**

**Son señales electromagnéticas entre 1 y 300GHZ.**

**Las microondas son unidireccionales, esto significa que puede ser dirigida.**

**Las antenas receptora y emisora deben estar alineadas**

**Las antenas pueden alinearse sin provocar interferencias a otros sistemas.**

**Requieren línea de vista.**

**Sus principales aplicaciones son: Comunicacion unicast, teléfonos celulares, redes inalambricas.**

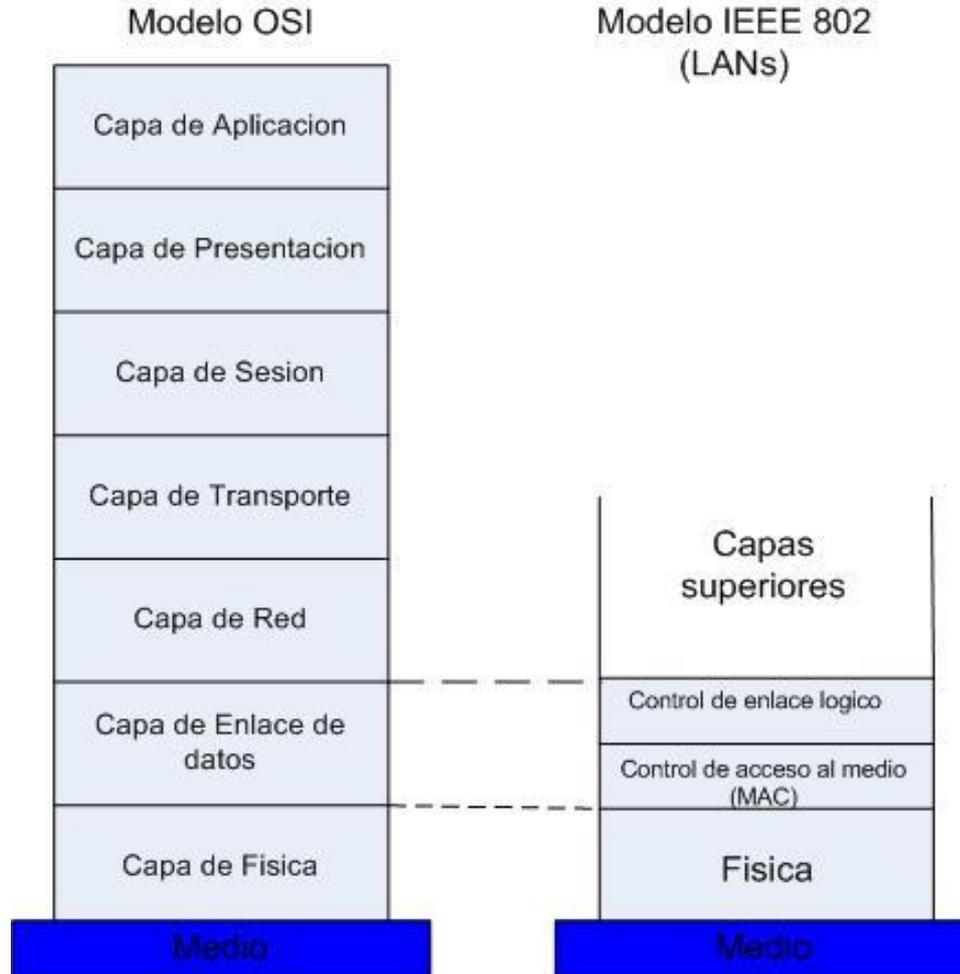


# Unidad 2.

## Redes de Área Local



Las especificaciones de las LANs están definidas en el estándar IEEE 802, corresponden a la capa física y la capa de enlace de datos del modelo OSI.





## **La capa física**

- **Codificación / decodificación de señales**
- **Sincronización**
- **Transmisión / recepción de bits**

## **La capa de enlace de datos**

- **Ensamblado/desensamblado de datos**
- **Campos de dirección**
- **Detección de errores**
- **Control de acceso al medio**



**La capa de enlace de datos Se divide en 2 subcapas.**

**a) Capa MAC. Control de acceso al medio. Determina la técnica de acceso al medio que utilizará el protocolo de red.**

**Existen técnicas: De contienda y ordenadas. Es decir, los protocolos de red pueden ser aleatorios o deterministas.**

**b) Capa LLC. Control de enlace lógico. Se encarga de las funciones de: Formación de bloques, control de flujo y control de errores.**



**Una red de área local se caracteriza por:**

- 1. Medio de Transmisión**
- 2. Modo de Transmisión**
- 3. Configuración de la Línea**
- 4. Topología.**
- 5. Método de acceso al medio**



## **Medios de Transmisión: Medios guiados, no guiados.**

### **Medios guiados (alambricos)**

**Proporcionan un conductor de un dispositivo al otro:**

- Cable par trenzado
- Cable Coaxial.
- Fibra Óptica

### **Medios no guiados (inalámbricos)**

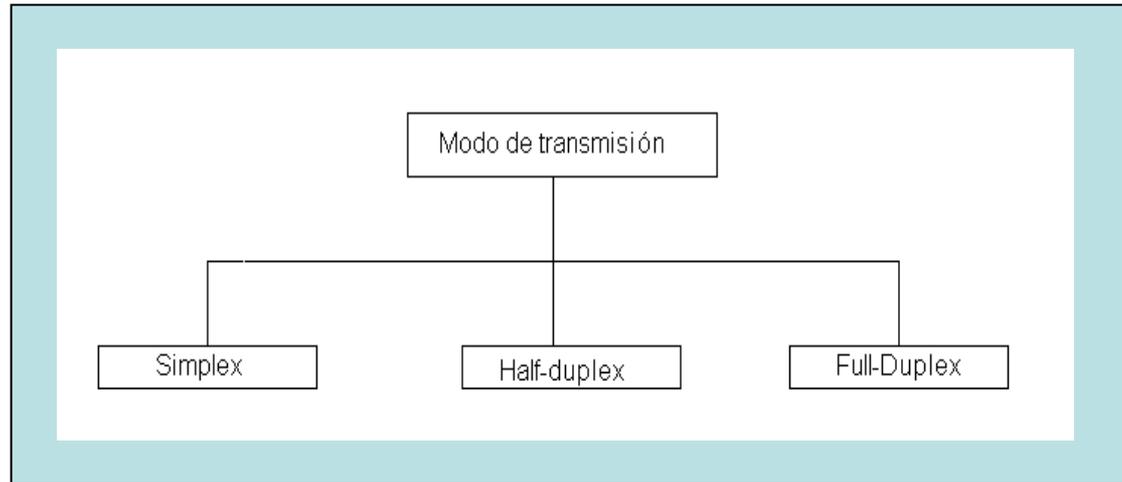
**Transportan ondas electromagnéticas sin usar un conductor físico.**

- Ondas de radio
- Infrarrojas
- Laser.



## Modo de Transmisión

Define la dirección del flujo de las señales entre dos dispositivos enlazados.



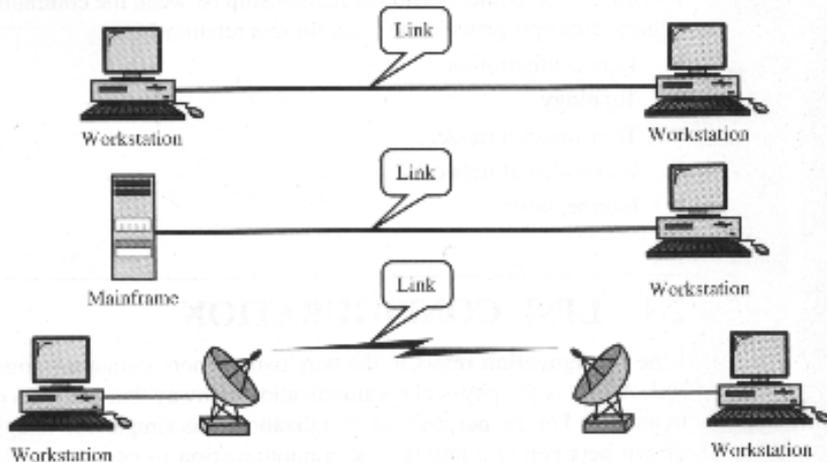


## Configuración de la línea.

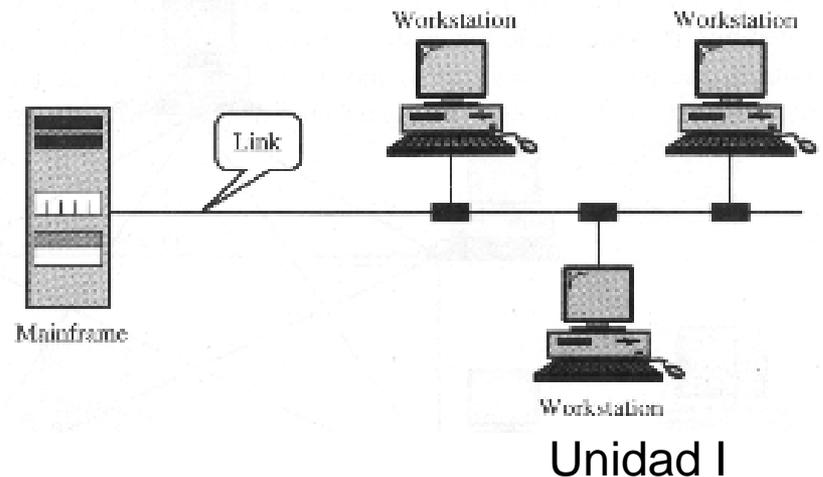
Se refiere a la forma en que dos o mas dispositivos que se comunican se conectan al enlace.

El enlace es el medio de comunicación físico.

### •Punto a punto



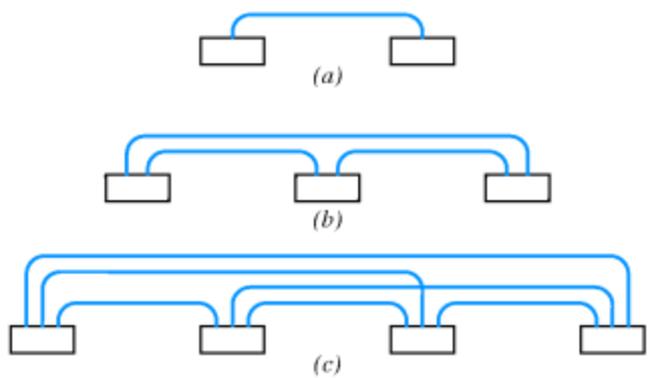
### •Difusion (Multipunto)



# Conexión punto a punto

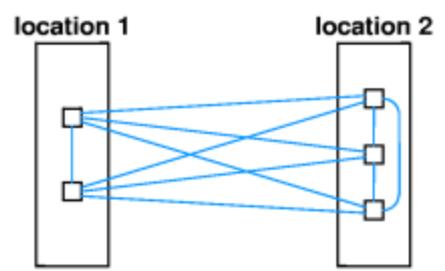


En una conexión punto a punto el numero de cables requerido aumenta conforme aumenta el numero de computadoras.



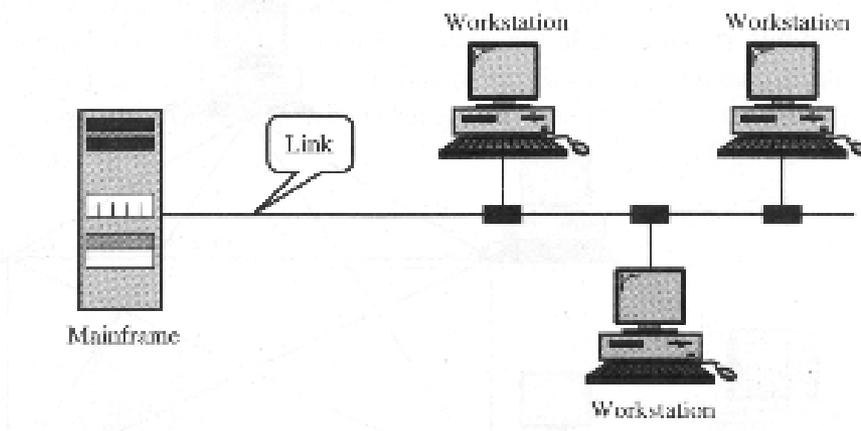
Para N computadoras se requiere:

conexiones =  $\frac{(n^2 - n)}{2}$



Conexiones entre dispositivos pueden ser prohibitivas.

Agregar una nueva computadora requiere agregar N-1 conexiones.



**Permiten hacer un mejor uso del medio y disminuir el número de conexión.**

**Para compartir el medio se requiere establecer:**

- Método de acceso al medio**
- Topología**



# Topología

**Se refiere a la forma en que esta diseñada la red.**

**Puede referirse al diseño lógico o físico de la red.**

**Es la representación geométrica de la relación entre todos los enlaces y los dispositivos que los enlazan entre si ( denominados nodos).**

**Las topologías describen como están interconectados los dispositivos de una red, pero no indica su posición física.**

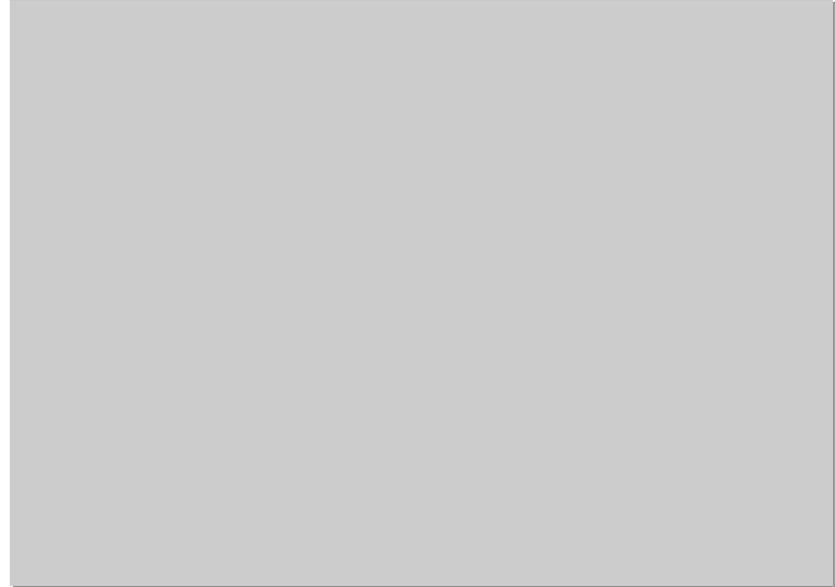
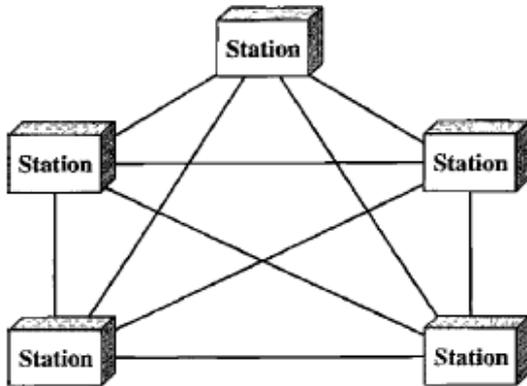
**Las principales son:**

- Malla
- Estrella
- Arbol
- Bus
- Anillo



# Topología en Malla

Cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo.





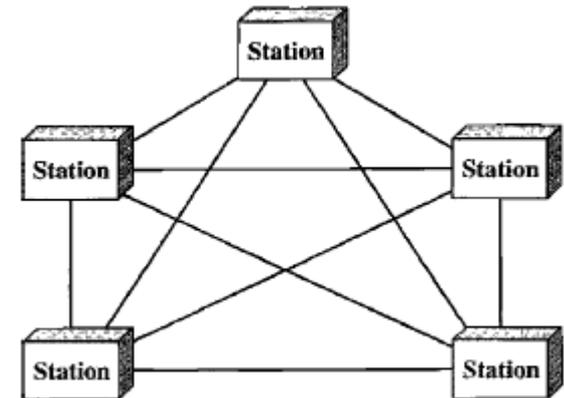
## Ventajas y desventajas

### Ventajas :

- Los enlaces no son compartidos.
- Si un enlace falla el resto de la red sigue funcionando.
- Privacidad y seguridad.
- Fácil localización de fallas.

### Desventajas:

- La cantidad de cables y puertos E/S requeridos.
- Instalación y reconfiguración de red complicada
- Extremadamente cara

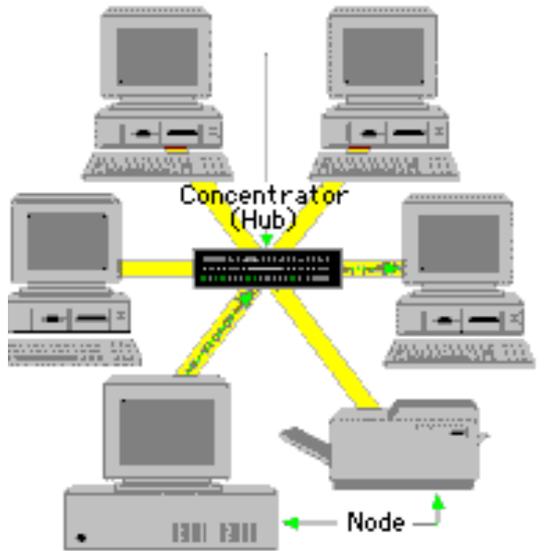




## Topología en Estrella.

Es una conexión en la que se utiliza un medio de comunicación pasivo, y en el cual, el control de acceso al medio esta centralizado por el nodo o dispositivo central.

Cada dispositivo solamente tiene un enlace punto a punto dedicado con el controlador central. Los nodos no se conectan directamente entre si.





Unidad I

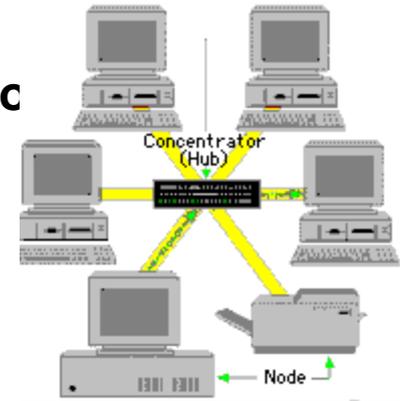


## Ventajas y Desventajas

### Ventajas

Gran facilidad de instalación.

- Posibilidad de desconectar elementos de red sin causar problemas.
- Facilidad para la detección de fallo y su reparación.
- Los nodos no requieren gran capacidad, sólo el nodo central.



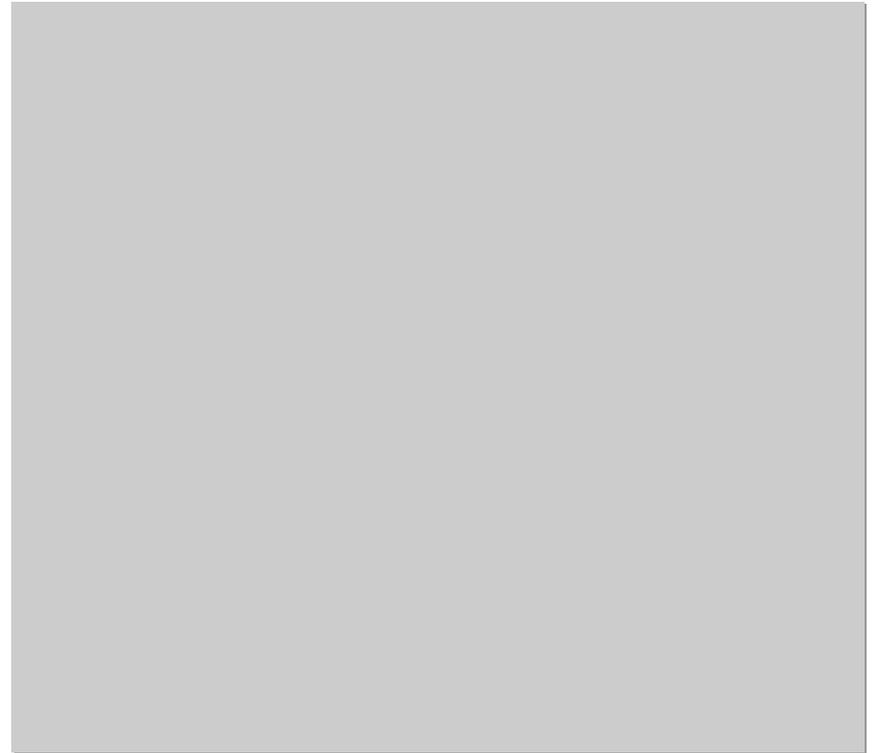
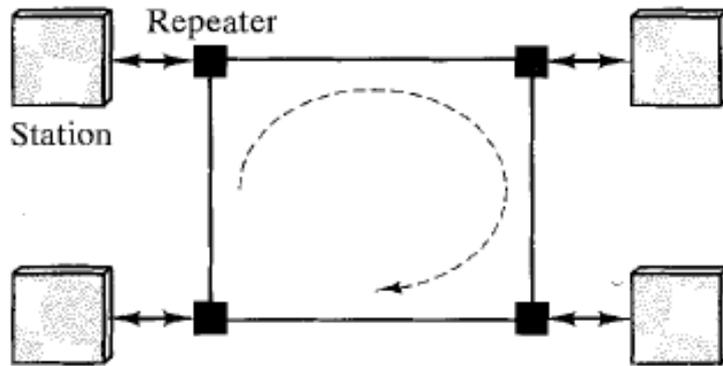
### Desventajas

- Un fallo en el concentrador provoca el aislamiento de todos los nodos a él conectados.
- Se requieren hubs o concentradores
- Cubre muy poca distancia (100 mts con par trenzado, 600m con cable coaxial)



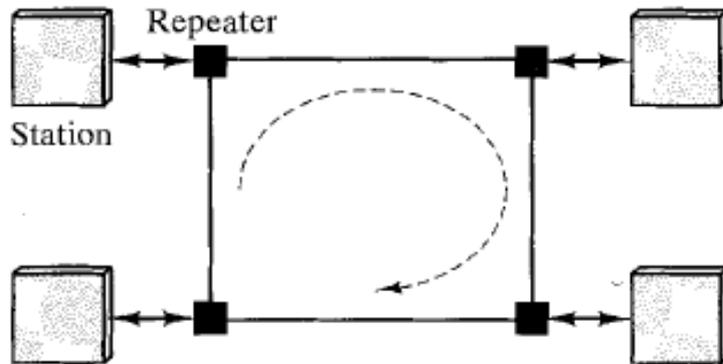
# Topología en Anillo

Cada dispositivo tiene una línea de conexión dedicada solamente con los dispositivos que están a los lados.





# Topología en Anillo



## Ventajas:

- Instalación y mantenimiento sencillo
- Pueden cubrirse distancias mayores ya que se emplean repetidores.

## Desventajas:

Si un nodo falla, se puede interrumpir toda la red.

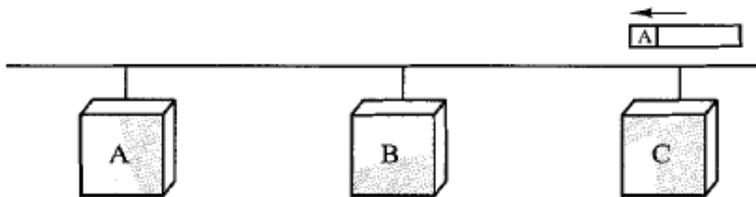
Se requiere interrumpir el funcionamiento de la red para incorporar nuevos nodos.



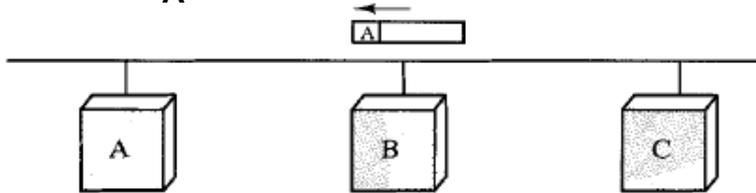
# Topología en BUS

La topología en bus establece una conexión multipunto.

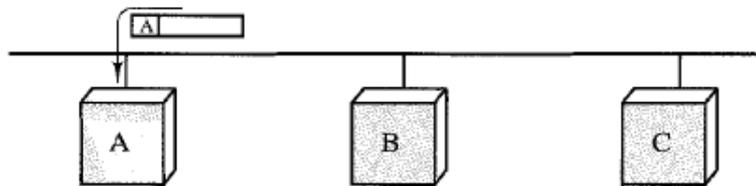
Los nodos se conectan a un medio de comunicación común denominado cable troncal o bus, mediante un cable denominado derivación.



C transmite un marco dirigido a A



B recibe e ignora el marco



A copia el marco y lo deja pasar



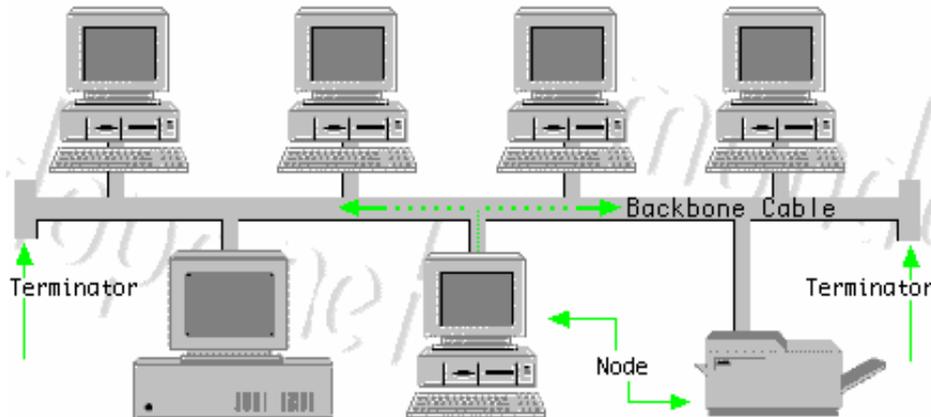
Debido a que la señal se debilita existe un limite para la distancia y el numero de nodos.



## Topología en BUS

Una topología en bus requiere el uso de:

- **Cable troncal o bus:** Es el medio al que están conectados todos los nodos y por el que pasa toda la información.
- **Terminador:** Dispositivo de 50 ohms que elimina automáticamente la señal de los extremos.



La transmisión es bidireccional. Todas las estaciones de trabajo reciben simultáneamente el mensaje enviado, aunque solo es procesado por aquella a la que va dirigido.

La técnica de acceso al medio debe ser adecuada para evitar:

-Colisiones

-Que una estación monopolice la red.



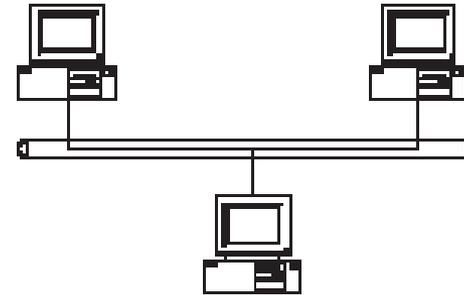
## Ventajas y Desventajas

### Ventajas

- Facilidad de implementación y crecimiento.
- Económica.
- Simplicidad en la arquitectura.

### Desventajas

- Toda la red se caería si hubiera una ruptura en el cable principal.
- Se requieren terminadores.
- Es difícil detectar el origen de un problema cuando toda la red falla.
- No se debe utilizar como única solución en un gran edificio.
- El tiempo de respuesta es sensible al número de nodos en la red, al nivel de tráfico y a las aplicaciones

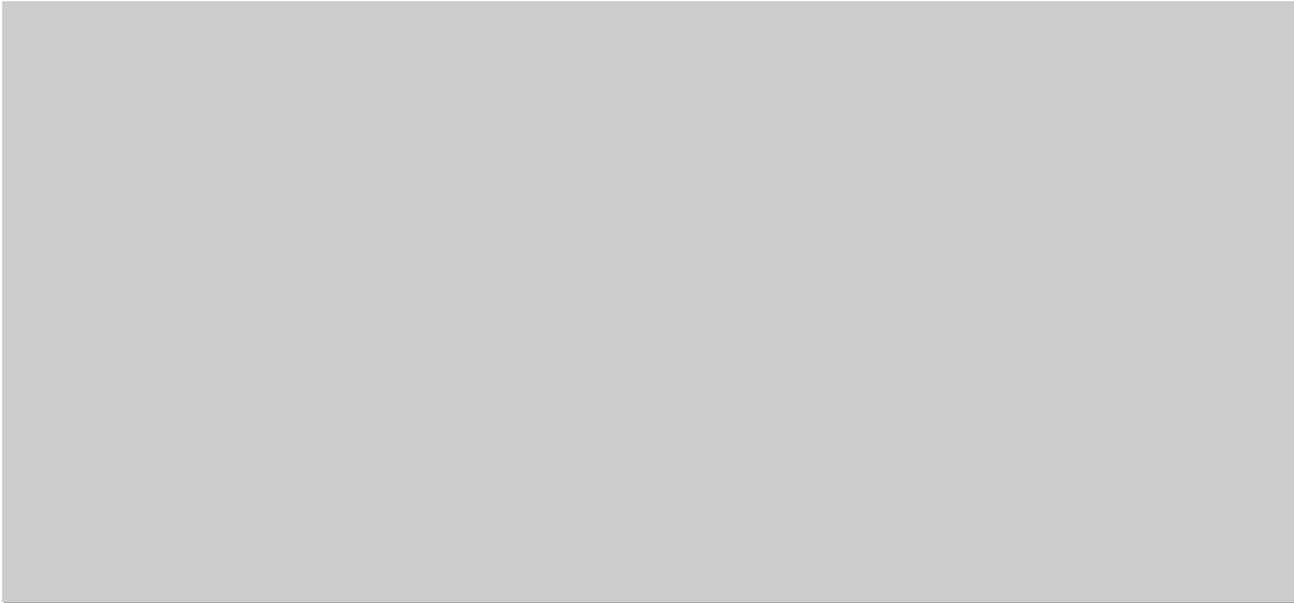




## Topología en árbol

**La topología en árbol es una variante de la de estrella.**

**La topología de árbol combina características de la topología de estrella con la BUS. Consiste en un conjunto de subredes estrella conectadas a un BUS. Esta topología facilita el crecimiento de la red.**





# Topología en árbol

## VENTAJAS:

**El Hub central al retransmitir las señales amplifica la potencia e incrementa la distancia a la que puede viajar la señal.**

**Permite conectar mas dispositivos.**

**Permite priorizar las comunicaciones de distintas computadoras.**

**Se permite conectar más dispositivos gracias a la inclusión de concentradores secundarios.**

**Permite priorizar y aislar las comunicaciones de distintas computadoras.**

.

## DESVENTAJAS:

**Se requiere más cable.**

**La medida de cada segmento esta determinada por el tipo de cable utilizado.**

**Si se viene abajo el segmento principal todo el segmento se viene abajo con él.**

**Es más difícil su configuración.**



## Topología híbrida

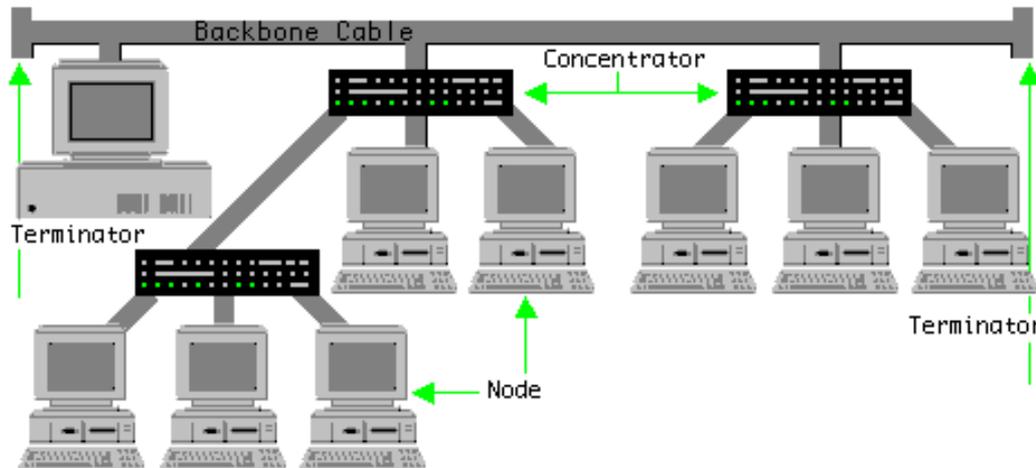
A menudo, una red combina varias topologías mediante subredes enlazadas entre si para formar una topología mayor.





## Ejemplo: Estrella-Bus

Consiste en un conjunto de subredes estrella conectadas a un bus. Esta topología facilita el crecimiento de la red.

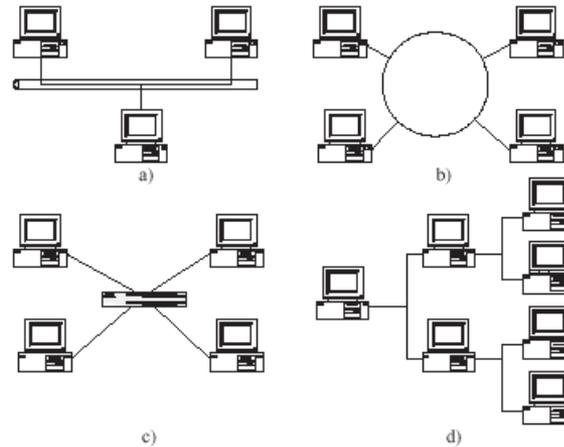


**Si un equipo falla no se afecta el resto de la red**

**Si un concentrador deja de funcionar todos los equipos conectados a el dejaran de funcionar**



# Existen estándares definidos para cada topología



Topologías Típicas de una LAN. a) Bus b) Anillo c) Estrella d) Árbol.

Topología	Cableado	Protocolo
Bus	Coaxial Par Trenzado Fibra óptica	Ethernet LocalTalk
Estrella	Par trenzado Fibra óptica	Ethernet LocalTalk
Estrella en Anillo	Par trenzado	Token Ring
Arbol	Coaxial Par trenzado Fibra óptica	Ethernet



**La selección de una topología tendrá impacto sobre:**

- **El tipo de equipo necesario**
- **Capacidades del equipo**
- **Crecimiento de la red**
- **Formas de administrar la red**

**Es importante diseñar la red antes de hacer cualquier adquisición de equipo.**



## Cuestionario topologias



## Método de Acceso al medio

Un método de acceso es una técnica de control de acceso al medio que establece las reglas que indican como un nodo de red puede hacer uso del medio de comunicación para transmitir su información.

Se clasifican en base a su forma de operación en:

### •CONTIENDA:

Ejemp: Los métodos de acceso múltiple con detección de la portadora

- Con detección de colisiones
- Con prevención de colisiones

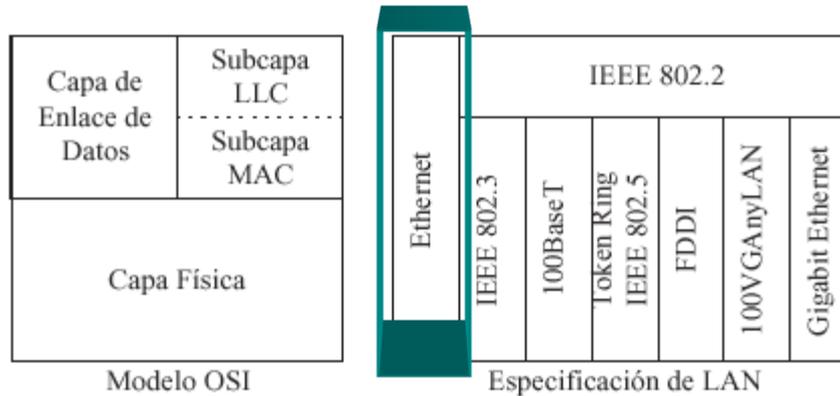
### •ORDENADOS:

Ejemp:El método de paso de testigo.



# PROTOCOLOS DE REDES DE ÁREA LOCAL

Existen diferentes protocolos que definen LANs en base a sus características: Topologías, medios de transmisión, modo de transmisión, configuración de línea y técnica de acceso al medio.



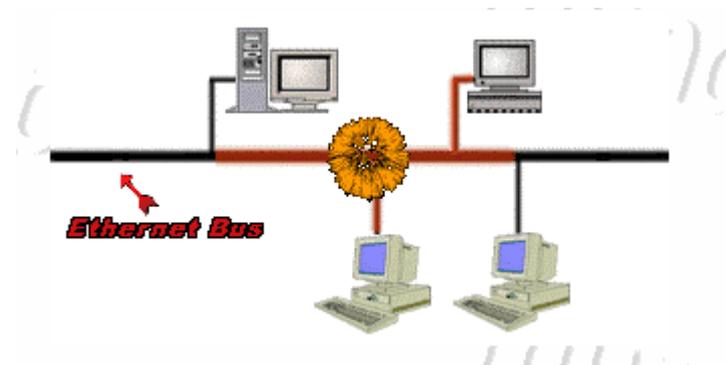
Relación entre el modelo OSI y los protocolos LAN



## •802.3 / ETHERNET

### •**ETHERNET**

- Desarrollada por Xerox en 1976.
- En 1985 las redes Ethernet de Xerox se convierten en 802.3, el cual esta basado en el protocolo Ethernet pero presenta múltiples opciones en el nivel físico.
- Define una LAN con topología en bus
- Protocolo MAC CSMA/CD



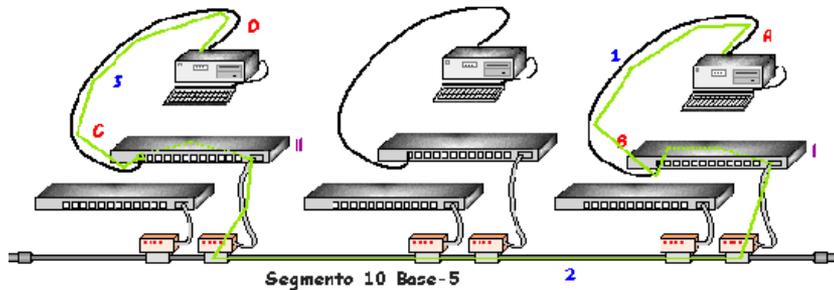
<b>Velocidad de Transmisión</b>	<b>10 Mbps</b>
<b>Distancia máxima de enlace</b>	<b>2.5 km</b>
<b>Número máximo de nodos</b>	<b>1024</b>
<b>Longitud máxima por segmento</b>	<b>500 m</b>
<b>Número máximo de segmentos</b>	<b>5</b>
<b>Número máximo de repetidores</b>	<b>4</b>
<b>Técnica de acceso al medio</b>	<b>CSMA/CD</b>
<b>Medio de transmisión</b>	<b>Cable coaxial grueso</b>



## •REPETIDORES.

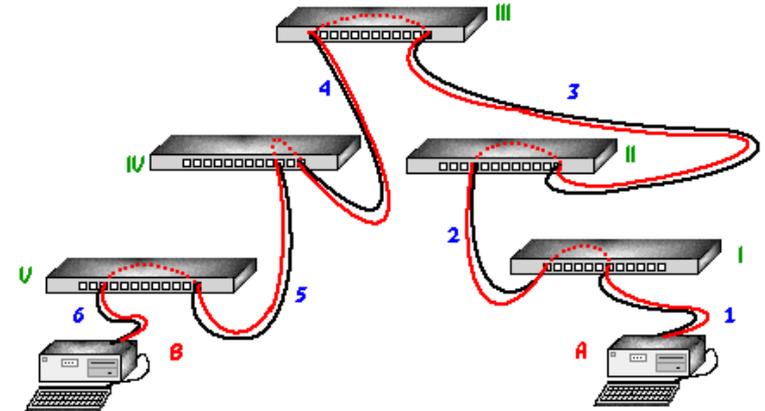
Prolongan la longitud de la red uniendo dos segmentos, incluso con diferentes tipos de cableado.

La regla **5-4-3** limita el uso de repetidores y dice que *entre dos equipos de la red no podrá haber más de 4 repetidores y 5 segmentos de cable. Igualmente sólo 3 segmentos pueden tener conectados dispositivos que no sean los propios repetidores, es decir, 2 de los 5 segmentos sólo pueden ser empleados para la interconexión entre repetidores.*



Correcto

Entre A y D hay 3 segmentos y 2 repetidores.



incorrecto

Unidad I



La información es enviada en tramas o marcos, determinadas en la capa de enlace de datos.

### FORMATO DE TRAMA ETHERNET ORIGINAL:

Bytes:

8

6

6

2

de 46 a 1500

4



Señala el comienzo de la trama.  
Consigue la sincronización de bit y de paquete en recepción  
El preámbulo se transmite incluso cuando se detectan colisiones.  
No se utiliza campo de fin de paquete, este se detecta por no escuchar portadora.

Contiene 1 y 0's alternados

Permite identificar el formato de datos enviados y determinar como deben ser procesados en recepción

El paquete mínimo permitido es de 512 bits (no se considera el preámbulo)

**Tarea:**  
Hacer una presentación sobre CRC  
Verificación de redundancia cíclica



# Campos de dirección: Dirección Física / Dirección MAC

**6 B**

**6B**

Dirección destino	Dirección fuente
-------------------	------------------

La dirección destino especifica la estación o estaciones a las que va dirigido el paquete, con las siguientes opciones:

Si el primer bit es:

**0**

El destinatario será:

única estación

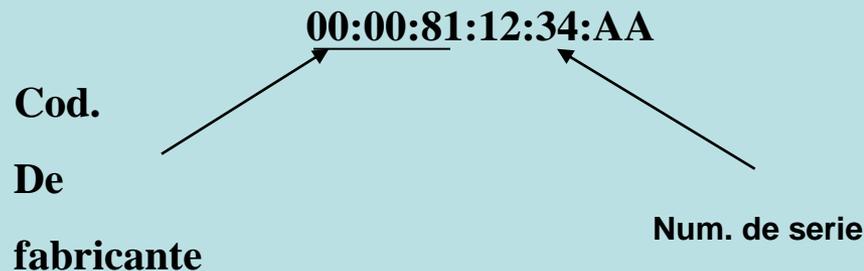
**1**

varias estaciones (multicast)

Todos los bits en 1

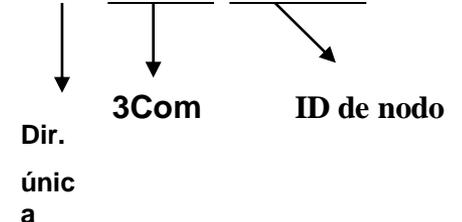
todas las estaciones (broadcast)

## FORMATOS DE DIRECCIONES MAC:



## Ejemplo:

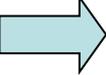
**02608C010203**



Unidad I



## **CONTROL DE ACCESO AL MEDIO (MAC).**

**Técnica de Contienda- Acceso Aleatorio**  **Colisiones**

**Ethernet utiliza la técnica:**

**Carrier Sense Multiple Access / Collision Detection**

**Acceso Múltiple con sensado de portadora /  
Detección de colisiones**

**CSMA / CD**

**DCTAR**

**Unidad I**

# TEORÍA DE OPERACIÓN DE ETHERNET.



**Utiliza un canal de comunicación compartido (Ether)  
Para adquirir el canal la estación sigue el siguiente procedimiento:**

- 1. Comprueba si la red esta ocupada (Sensado de portadora)**
- 2. Detiene la transmisión del paquete si el ether esta ocupado**
- 3. Cuando detecta la disponibilidad del canal la estación empieza a transmitir**
- 4. Durante la transmisión se mantiene en escucha del canal**
- 5. En el caso de una colisión la estación transmisora se retrae y aborta la transmisión del paquete**
- 6. La estación envía una ráfaga corta de bits a todas las estaciones indicando la existencia de una colisión (jam).**
- 7. Se establece un intervalo de tiempo de espera**
- 8. Se implementa un algoritmo de retransmisión.**
- 9. Si no existe colisión se envía el paquete completo.**

**En una transmisión exitosa, las estaciones solo aceptan paquetes dirigidos a ellas y descartan los equivocados.**



## ALGORITMO DE RETRANSMISIÓN:

- El proceso de retransmisión tiene como objetivo:
  1. Programar una transmisión rápidamente para acceder el paquete y mantener el uso del canal.

Ethernet emplea una técnica de retardos aleatorios denominada *algoritmo de contención binario exponencial truncado (TBEB, Truncated Binary Exponential Back-off)*

Este algoritmo calcula un retardo de tiempo después de una retransmisión.

Después de una colisión, el objetivo es obtener períodos de retardo que reprogramen cada estación a puntos cuantificados en tiempo, llamados ranuras de tiempo de retransmisión (RST, Retransmission Slot Time).

Los tiempos de retardo son discretos siendo su unidad la RST, según la especificación Ethernet esta RST debe ser de  $51.2 \mu\text{s}$ , el cual se considera el tiempo máximo para detectar una colisión, divididos de la siguiente manera:

$46.4 \mu\text{s}$  -→ Tiempo de circulación (round trip)

$4.8 \mu\text{s}$  -→ Señal de refuerzo de colisión (jam)



•Las ranuras de tiempo deben ser cortas, pero mayores o iguales que un intervalo de colisión para evitar sucesivas colisiones.

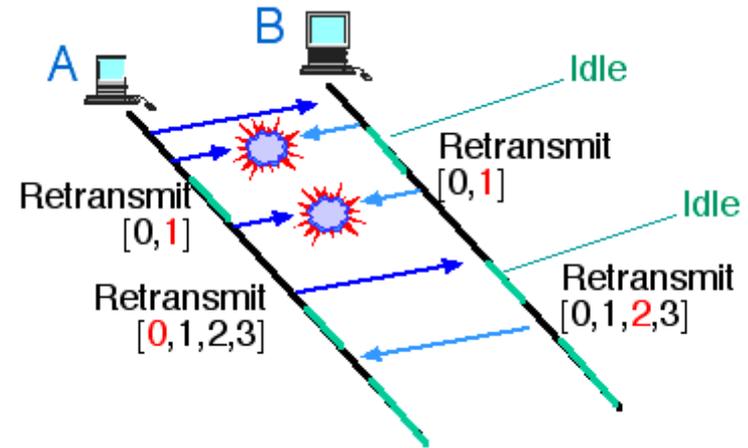
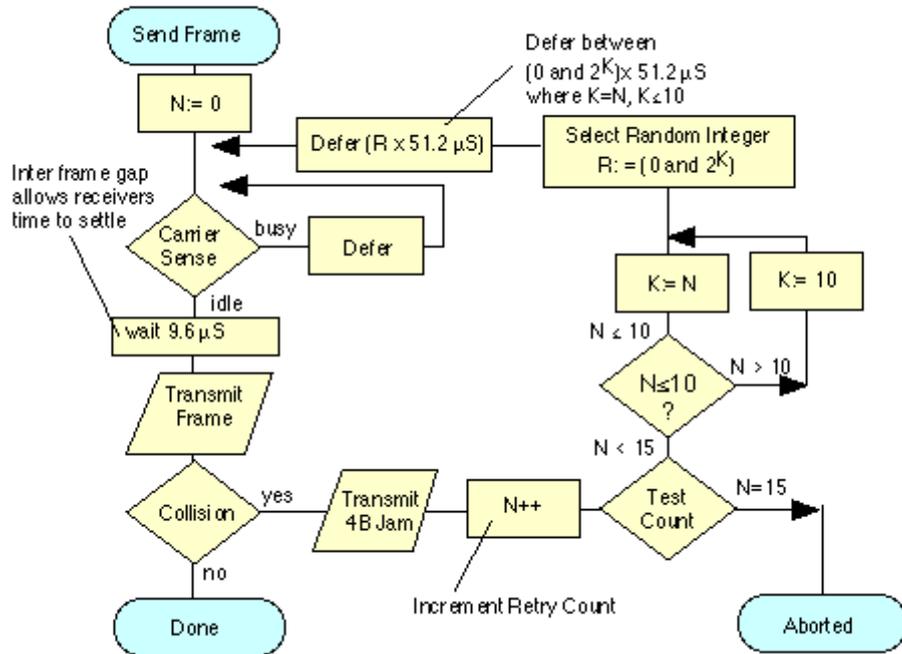
•El tiempo de retardo de transmisión es igual al producto de la RST por un entero positivo, obtenido en base a una distribución aleatoria uniforme en un cierto intervalo.

•El intervalo se duplica si existen colisiones sucesivas, los períodos cortos utilizados en TBEB se incrementan rápidamente conforme aumentan los intentos de retransmisión.

•Después de 15 intentos se aborta la política de retransmisión y se manda hacia niveles superiores una señal de error.



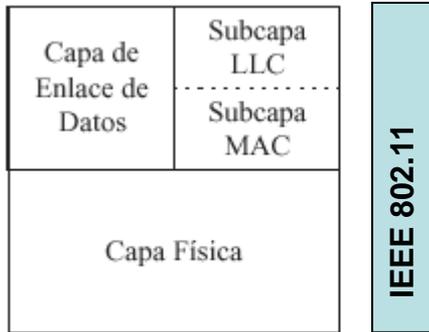
# Algoritmo de retransmisión





# PROTOCOLOS DE REDES DE ÁREA LOCAL

## LAN'S INALÁMBRICAS



Modelo OSI



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: 3 Mbps



### •Bluetooth

Radiofrecuencia

Velocidad: 433.9 Kbps aprox.



### •El estándar 802.11

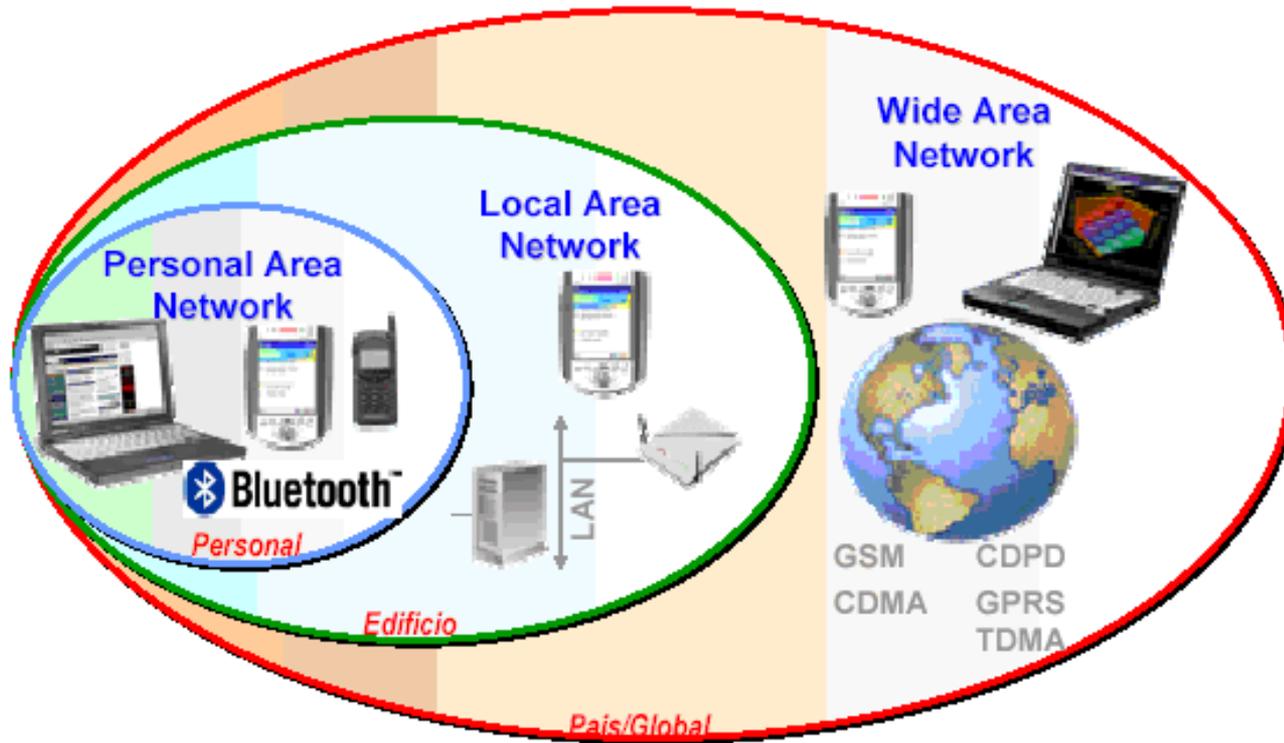
Velocidad: 2-100 Mbps

Reconocido por IEEE





# TECNOLOGÍAS INALÁMBRICAS





## APLICACIONES DE LAN's INALÁMBRICAS

- Redes pequeñas donde instalar cable resulta más complicado.
- Necesidad de movilidad por parte del usuario (comerciantes, hospitales, etc.)
- Necesidad de eliminar el cableado por estética.
- Comunicación en lugares remotos donde cablear resulta poco viable.

**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.

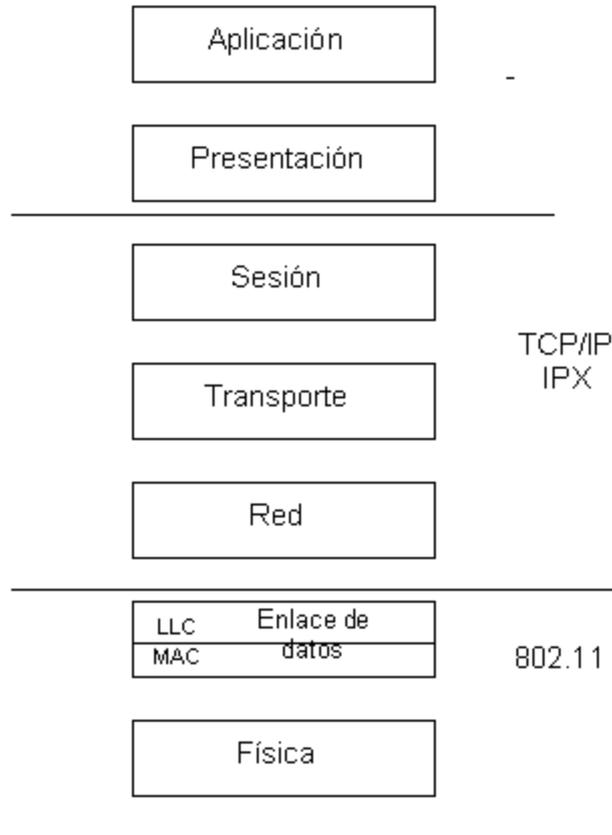


Las principales diferencias entre 802.11 y los estándares de LAN con medios acotados (802.3 ), es que se deben considerar los siguientes aspectos:

- **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





# NIVEL FISICO 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:

### Topología ad-hoc o IBSS (BSS independiente)

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

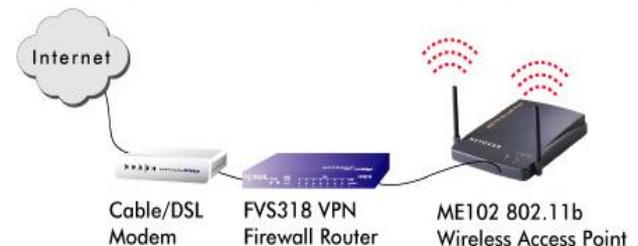


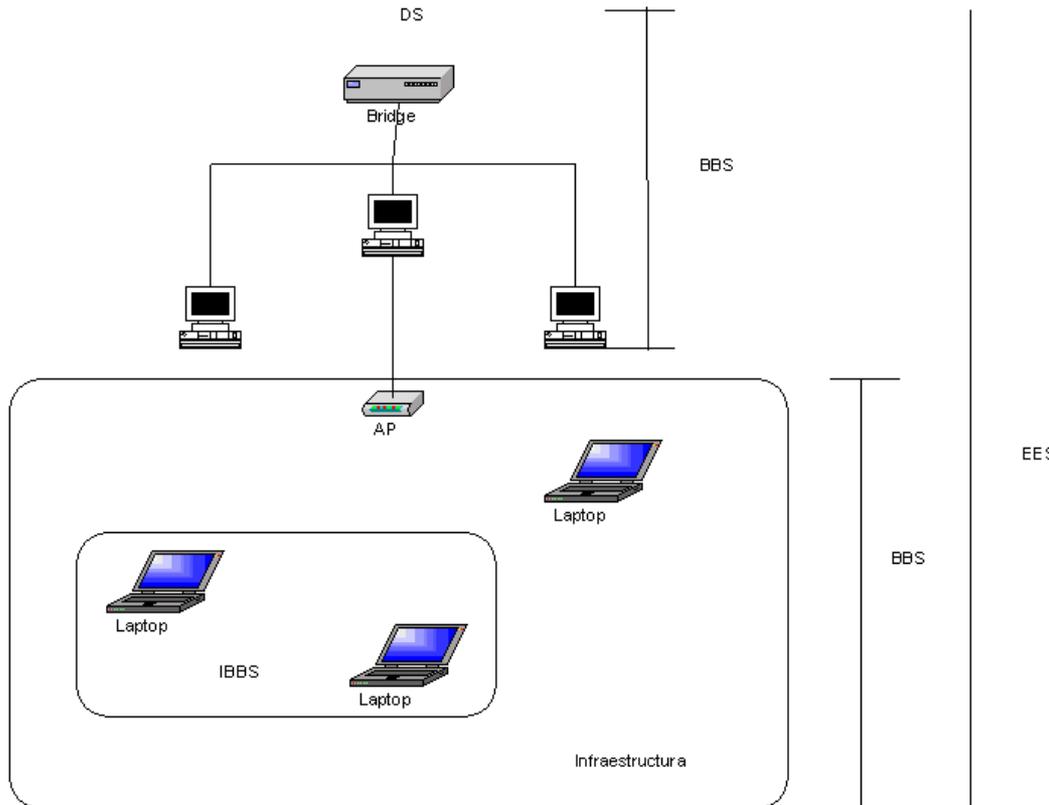
Generalmente cubre un área muy limitada y suele utilizarse para grupos colaborativos, juegos, transferencia de archivos y comunicaciones rápidas, en general.

### 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 BSS 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 número ilimitado de AP.





Debido a que una red con topología de infraestructura puede tener cualquier número de AP, puede por lo tanto tener un número 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 sí.

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



## Capa física 802.11

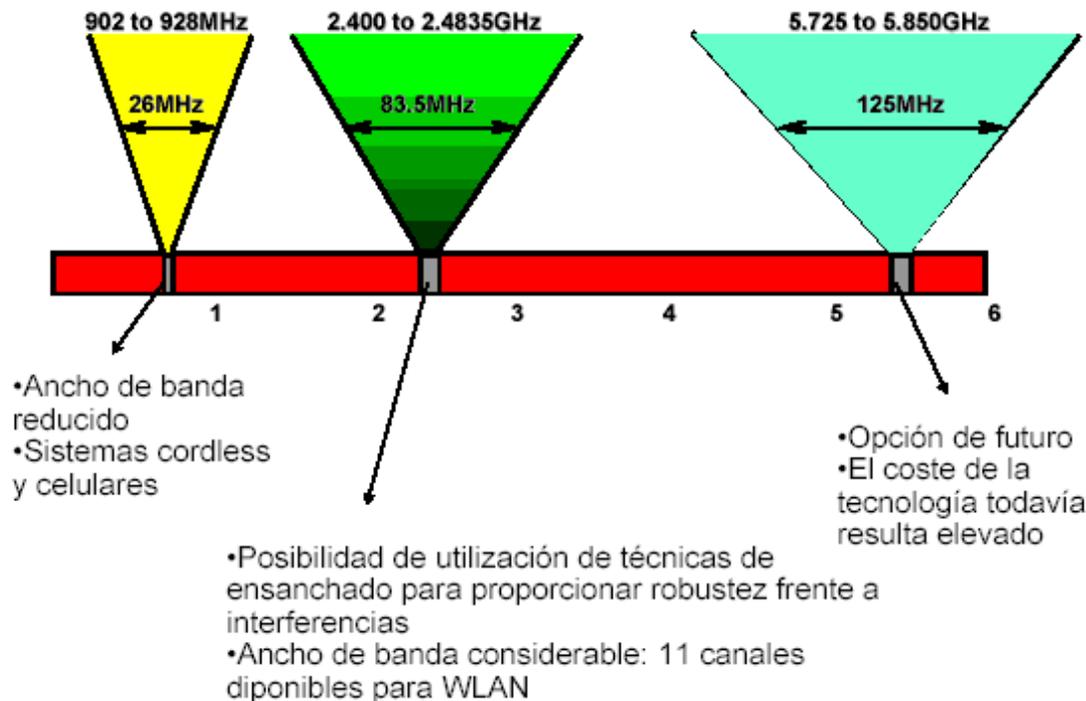
FHSS (Espectro extendido de salto de frecuencia )

-DSSS (Espectro extendido de secuencia directa )

-OFDM (Multicanalización por división de frecuencias ortogonales)

-MIMO

-MU MIMO



← Disponibilidad de espectro

Lectura Tarea



- **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 será el aumento en la señal original, esto hace que sea más fácil recuperar información en caso que se presenten errores.**

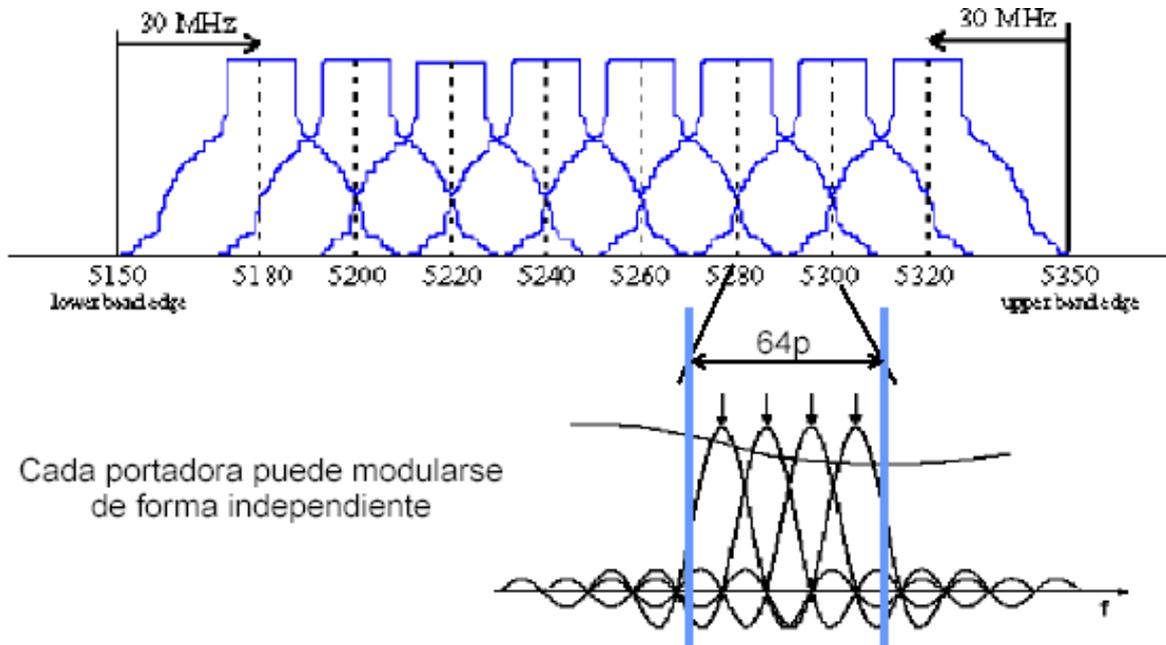
**Para poder leer la información el receptor y el emisor deben conocer el chip utilizado.**



# 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



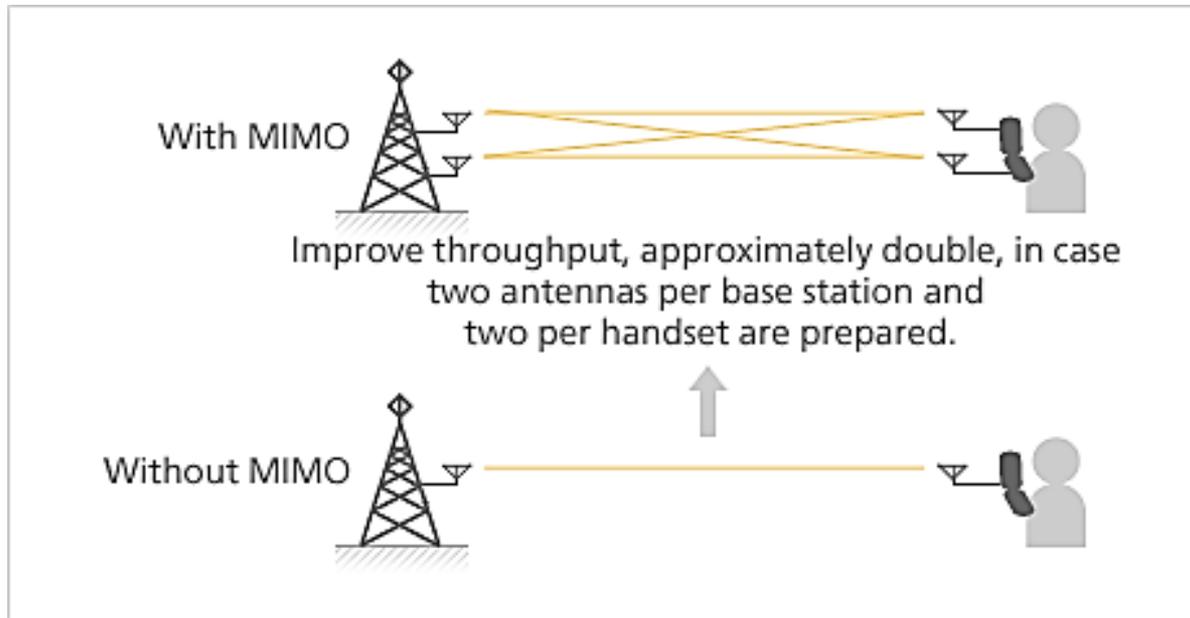
Utiliza 52 portadoras de datos en un canal con tiempos de guardas entre ellas de 400 ns



# MIMO

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

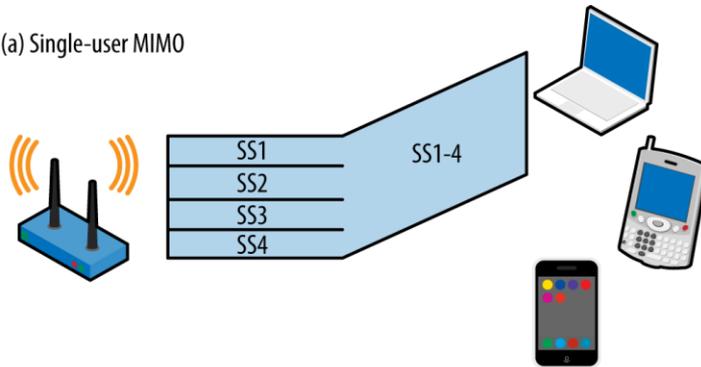
**MIMO aprovecha fenómenos físicos como la propagación multicamino para incrementar la tasa de transmisión y reducir la tasa de error. Aumenta la eficiencia espectral de un sistema de comunicación inalámbrica por medio de la utilización del dominio espacial (antenas físicamente separadas).**





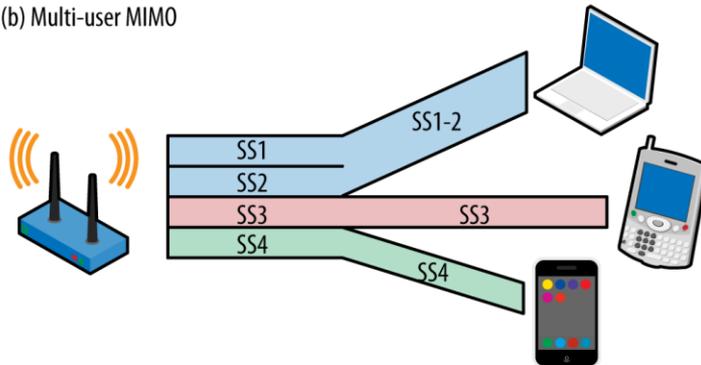
# MU MIMO (MIMO Multiusuario)

(a) Single-user MIMO



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

(b) Multi-user MIMO



[Video:](#)



## **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.**

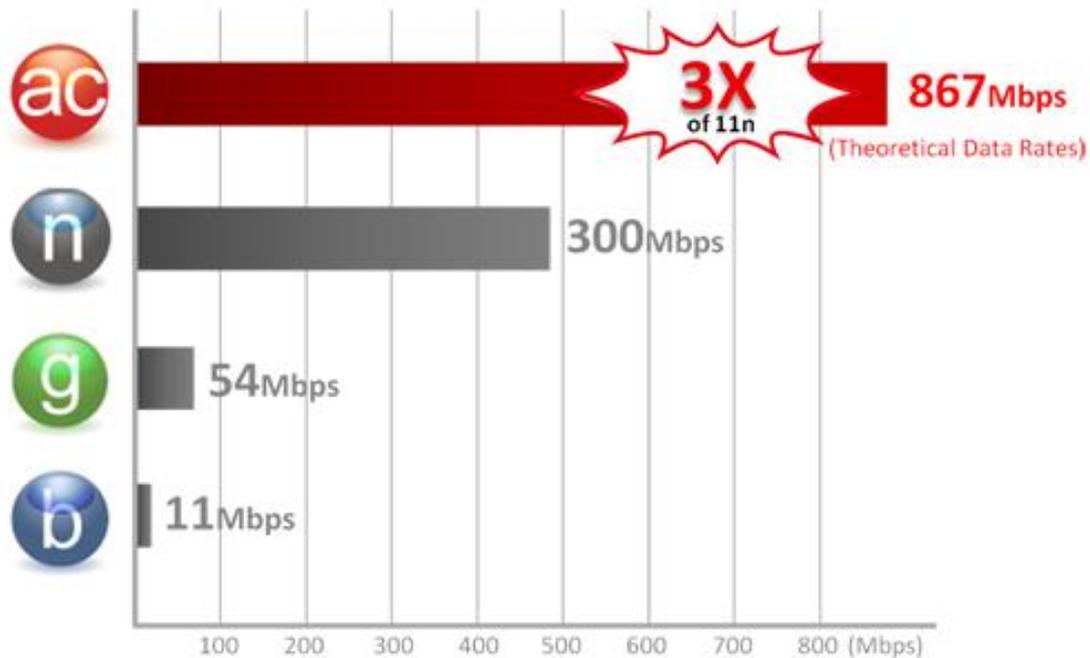
**802.11ac. Banda de 5 Ghz, Utiliza Multi User-MIMO (MU-MIMO) y mas canales incluidos incluidas las bandas de 80 y 160 MHZ Equipos de hasta 8 antenas, velocidades de 1Gbps**



## The Evolution of Wi-Fi



### Maximum Speed: Next Generation 802.11ac vs. 802.11n



\*As of January 2013.



## **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 codificación OFDM (Orthogonal Frequency Division Multiplexing)**

### **802.11b:**

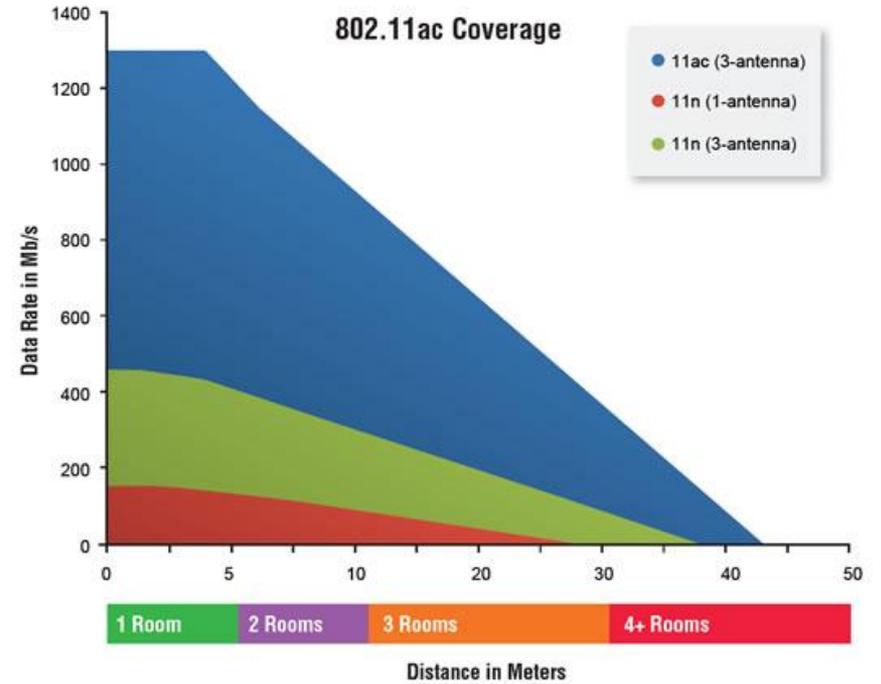
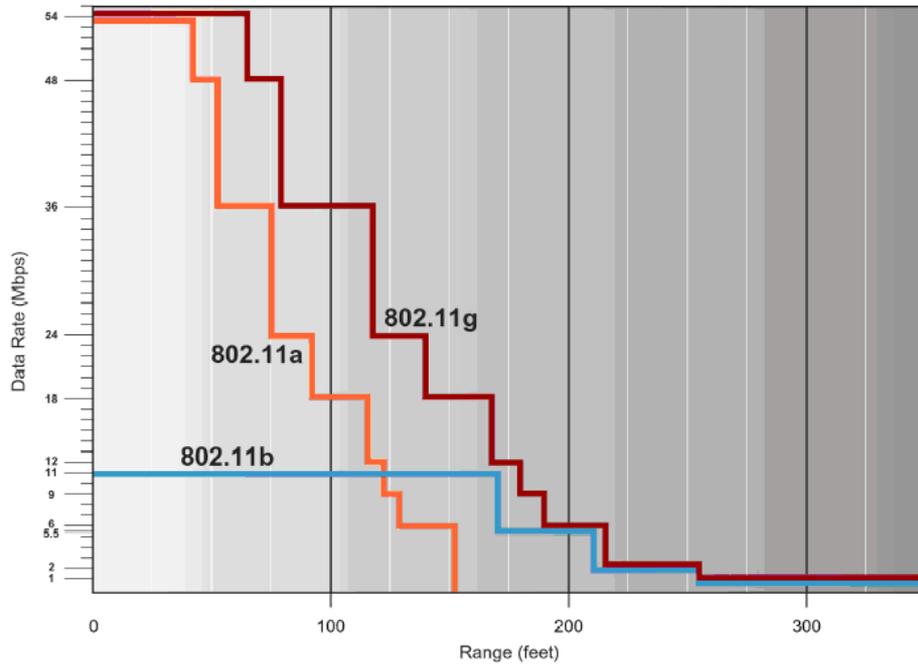
**11 Mbps, 32 usuarios por AP. Opera en la banda de 2.4 GHz. Alta compatibilidad. Requiere menos energía eléctrica. Excelente alcance. También se conoce como WiFi. Utiliza DSSS**

### **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.**



Fuente: Broadcom

100 pies -> 30 mts aprox



## 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:**

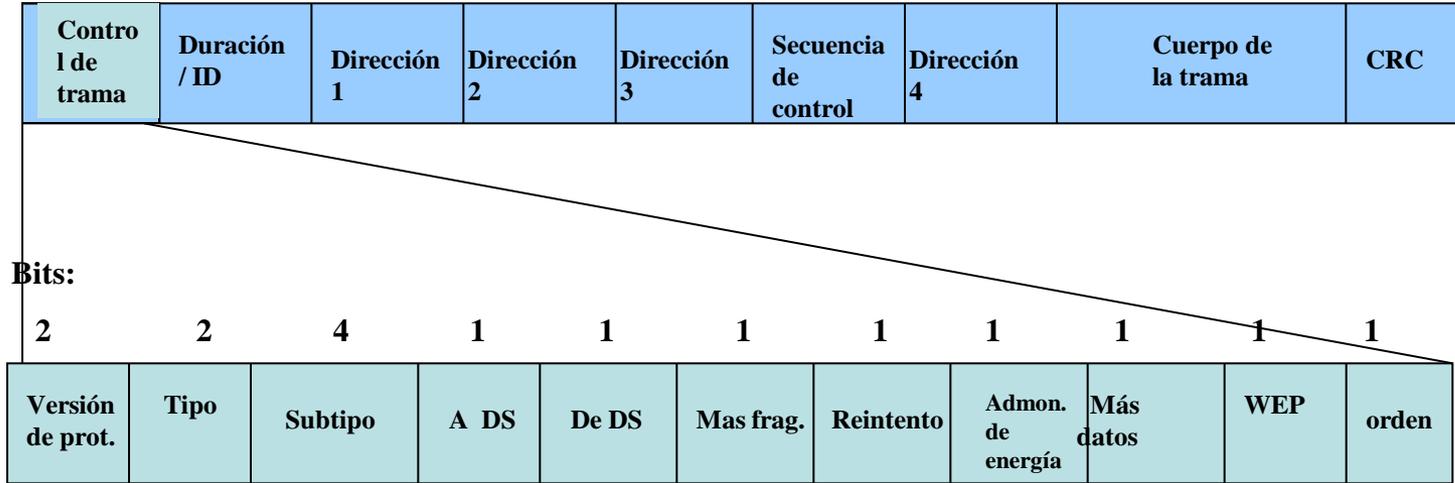
- De datos: Utilizadas para transmitir datos de los niveles superiores entre estaciones**
- De control: Utilizadas para regular el acceso al medio de la red y para reconocer las tramas de datos transmitidas.**
- De administración: Utilizadas para intercambiar información de administración de la red y realizar funciones de autenticación.**



# Trama 802.11

Bytes:

2            2            6            6            6            2            6            0-2312            4



•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:

2	2	6	6	6	2	6	0-2312	4
Control de trama	Duración / ID	Dirección 1	Dirección 2	Dirección 3	Secuencia de control	Dirección 4	Cuerpo de la trama	CRC

- 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 reensamblarlos 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

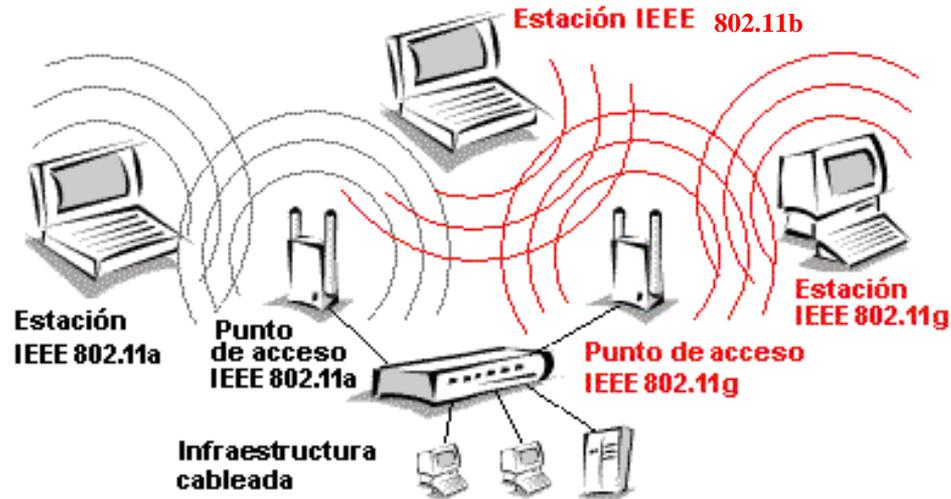
Al DS	Del DS	Función	Valor de la Dirección 1	Valor de la Dirección 2	Valor de la Dirección 3	Valor de la Dirección 4
0	0	Tramas de datos intercambiado por estaciones del mismo IBSS y todas las tramas de control y de administración	DA	SA	BSSID	No usado
1	0	Tramas de datos transmitidas al DS	DA	BSSID	SA	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.

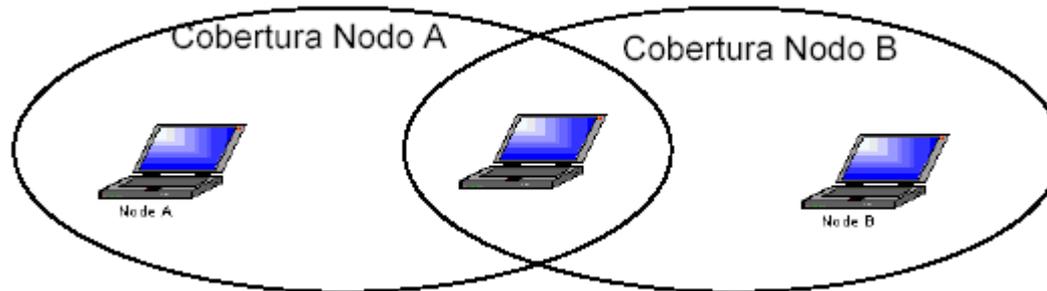




## Control de acceso al medio.

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)

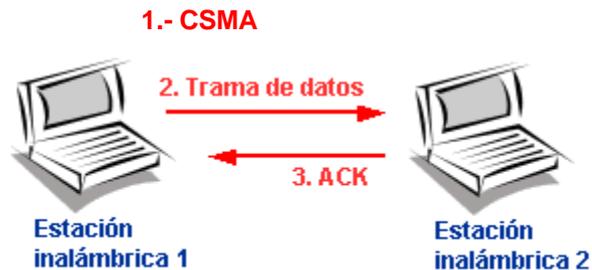
1.- CSMA



## Lectura CSMA/CA



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



- 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 envía un ACK (trama de control) para indicar que se recibió la información sin errores (checa el CRC)

- Si el canal está 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.

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



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



Estación 1

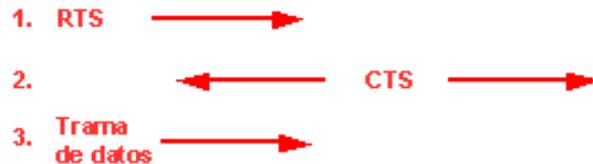
Estación 2

Estación 3

RTS: Request to send

CTS: Clear to Send

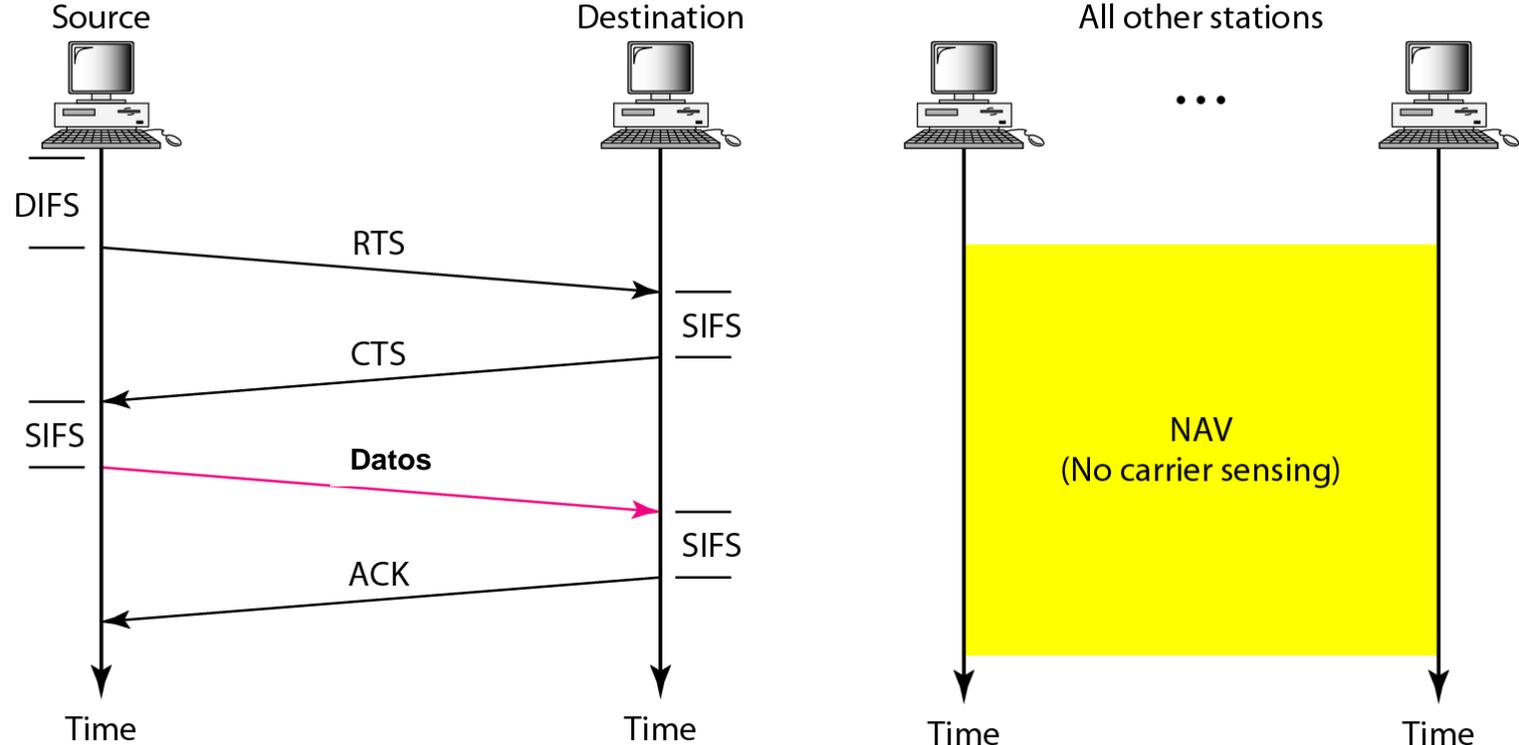
Ambos banderas son colocadas en el campo Duración/ID



Debido a que este mecanismo aumenta el tráfico, su utilización es opcional y puede administrarse con la utilidad del equipo. Así 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 (Distributed 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 III.

## Protocolos de Interconexión de Redes

- **Protocolos de Internet**



## *Modelo de Interconexion de sistemas abiertos (Open Systems Interconnection model)*



- Desarrollado en 1984 por la ISO
- Provee un modelo abstracto para la implementación de redes de computadoras.
- Divide las tareas requeridas para la transmisión de la información entre computadoras en 7 grupos de tareas
- Cada grupo de tarea consiste en una capa.

•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 de Internet



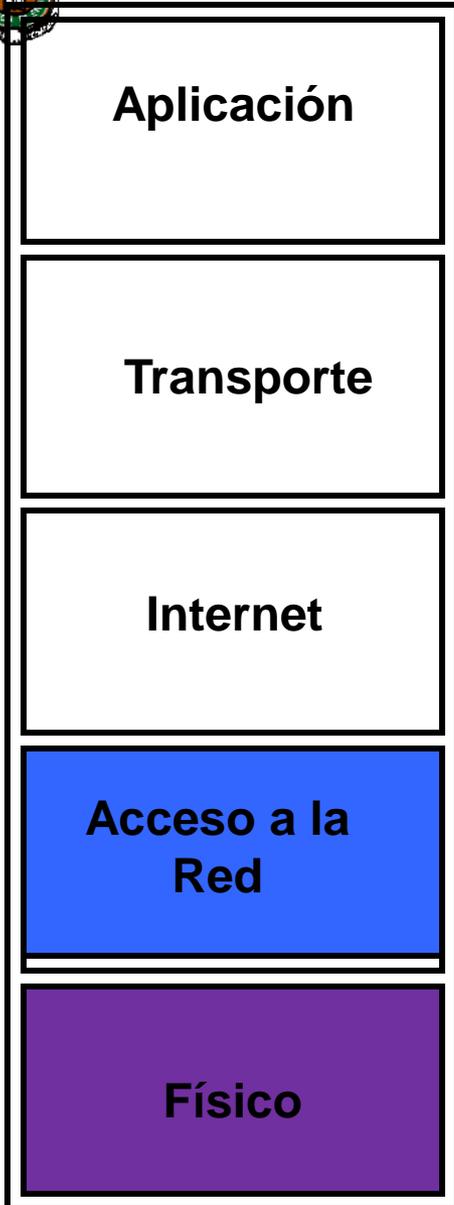
- El modelo de Internet es la arquitectura adoptada para la interconexión de sistemas, también conocido como arquitectura de protocolos TCP/IP.

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

## Historia

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

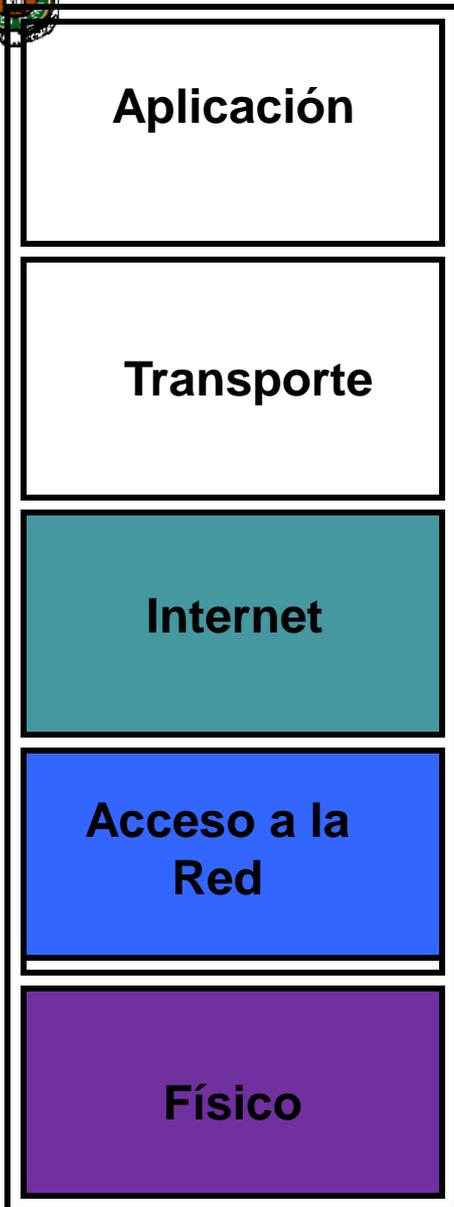
- Las dos ultimas capas muchas veces se unen en una sola: Acceso a la Red.



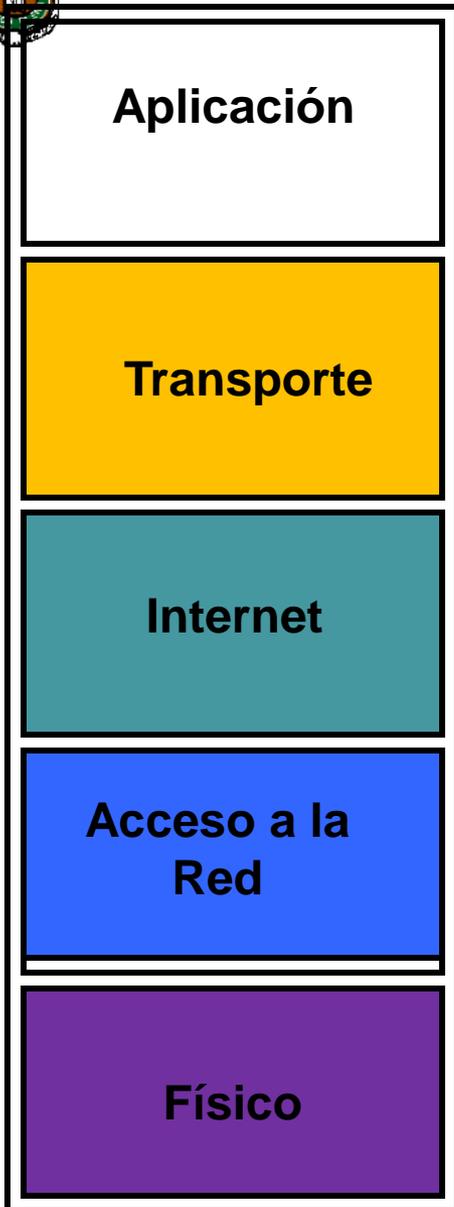
- La capa física se encarga únicamente del hardware: Cables, enlaces satelitales, interfaces de red, dispositivos de interconexión.
- Codificación y modulación si necesaria se llevan a cabo en esta capa.

**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**

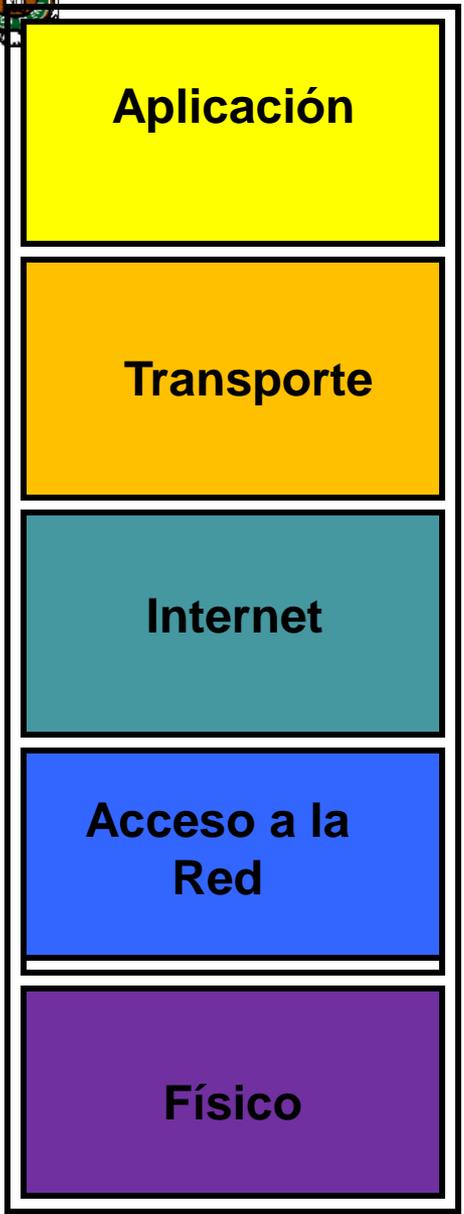
**Ethernet existe en las capas Física y de Acceso a la red – Su hardware en la capa física y la técnica de Acceso en la capa de Acceso a la red.**



- 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 Transmission Protocol), Diseñado para la transmisión de telefonía por Internet.

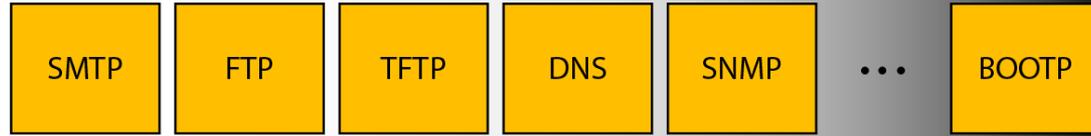


- Esta capa incluye funciones de las capas de sesión, presentación y aplicación del modelo OSI.
- Provee comunicación y capacidades de red a una aplicación
- Ejemplos:
  - Telnet
  - FTP
  - HTTP (Hyper Text Transfer Protocol)
  - SMTP (Simple Mail Transfer Protocol)



# Modelo de Internet → Protocolos TCP/ IP

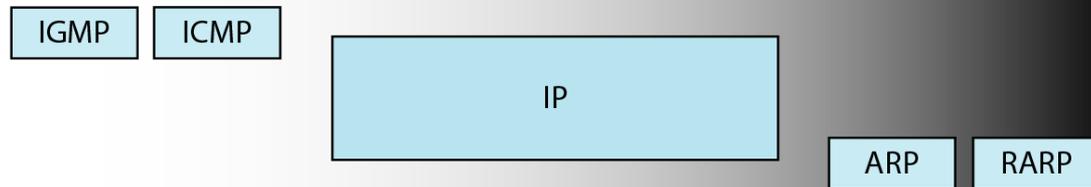
**Capa de Aplicación**



**Capa de Transporte**



**Capa de Internet**



**Capa de Acceso a la Red**



**Capa Física**



## Protocolos de Capa de Internet:

IP → IPv4, IPv6



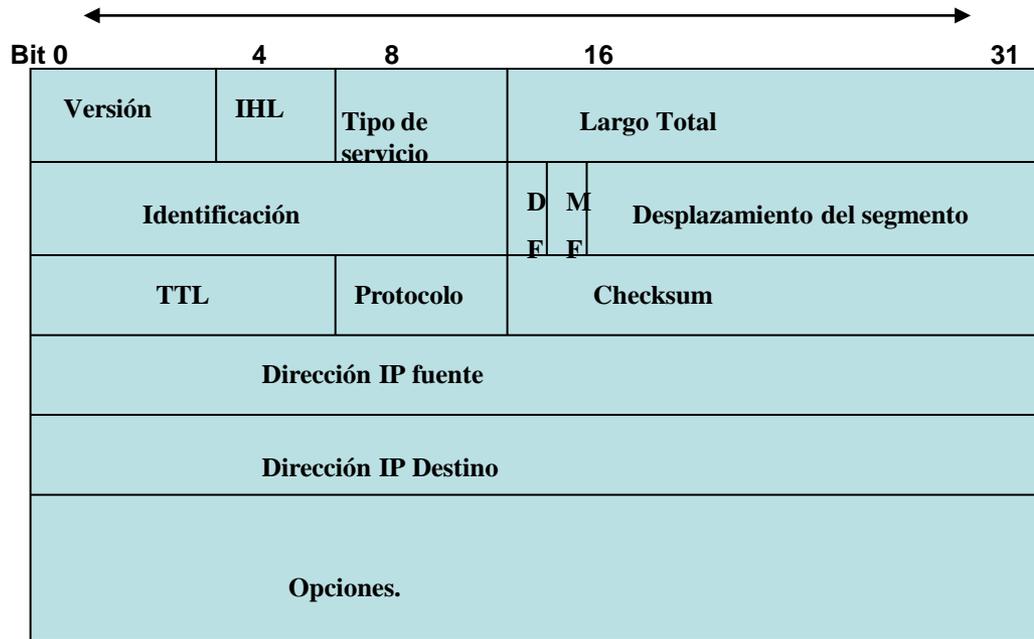
## PROCOLO IP (Internet Protocol)

- Se encarga del enrutamiento a través de Internet.
- Versiones IPv4- IPv6
- Servicio no orientado a conexión
- Servicio de mejor esfuerzo
- Datagramas de longitud variable, transportados independientemente:



**Max. 65,535 octetos**

# Encabezado IP



Puede variar entre 20 a 60 bytes

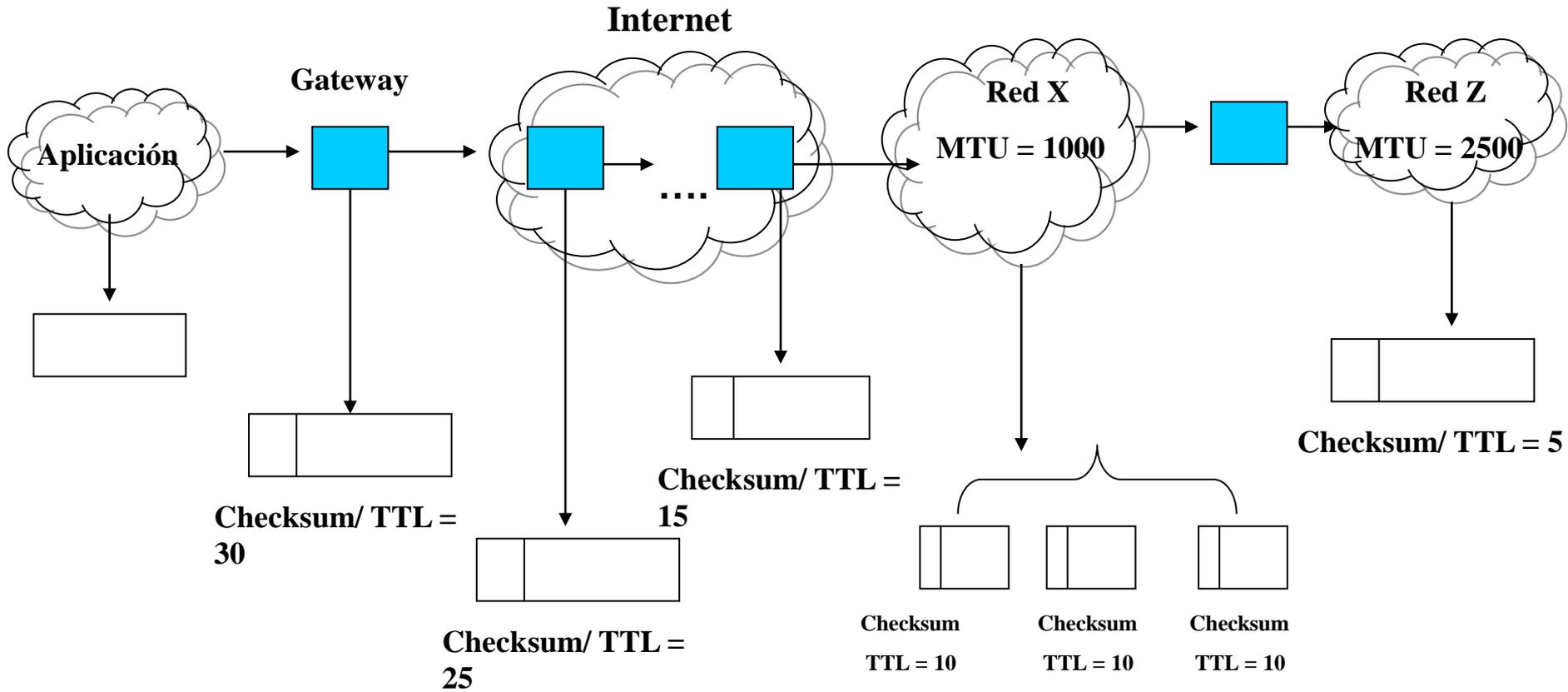
DCTAR

- **Versión (4 bits)** :Indica el número de versión del protocolo
- **Longitud de la cabecera de Internet (IHL, 4 bits)**
- **Servicios(8 bits)**: Parámetros como seguridad, prioridad, y retardo)
- **Largo o longitud total (16 bits).**
- **Identificación (16 bits)** : Identifica de forma única el datagrama
- **Indicadores: (DF : No fragmentar /Don't Fragment, MF :Mas fragmentos/ More Fragment)**
- **Desplazamiento (13 bits)**, posición del fragmento dentro del datagrama.

- **Tiempo de vida (TTL, 8 bits)**. Especifica el tiempo en segundos que un datagrama puede permanecer en la red (de 15 a 30 seg.)
- **Protocolo (8 bits)**: Identifica al protocolo de transporte.
- **Checksum (16 bits)**. Solo se aplica a los campos del encabezado.
- **Dirección de origen y destino (32 bits)**: Direcciones IP
- **Opciones**: opciones solicitadas por el usuario como son: registro de tiempo, seguridad, enrutamiento estricto u holgado)
- **Relleno** : Asegura que el datagrama sea múltiplo de 32
- **Datos**: Debe tener una longitud múltiplo de 8, maximo de 65535 octetos.



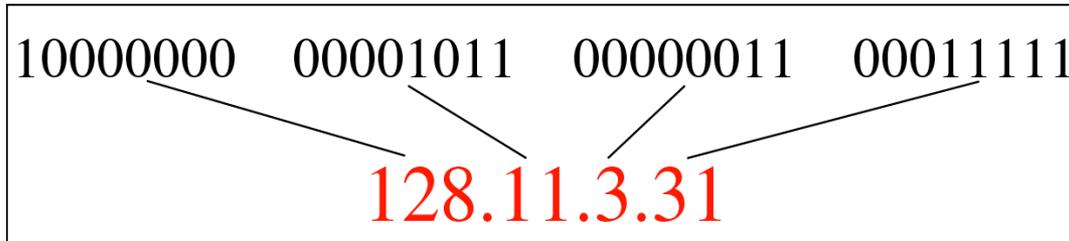
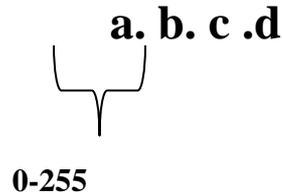
# LA VIDA DE UN DATAGRAMA





# DIRECCIONES IP

Las direcciones IP se forman de 4 bytes (32 bits):



Las direcciones IP se manejan como números binarios pero pueden ser representadas en notación decimal

Las direcciones IP permiten un enrutamiento global

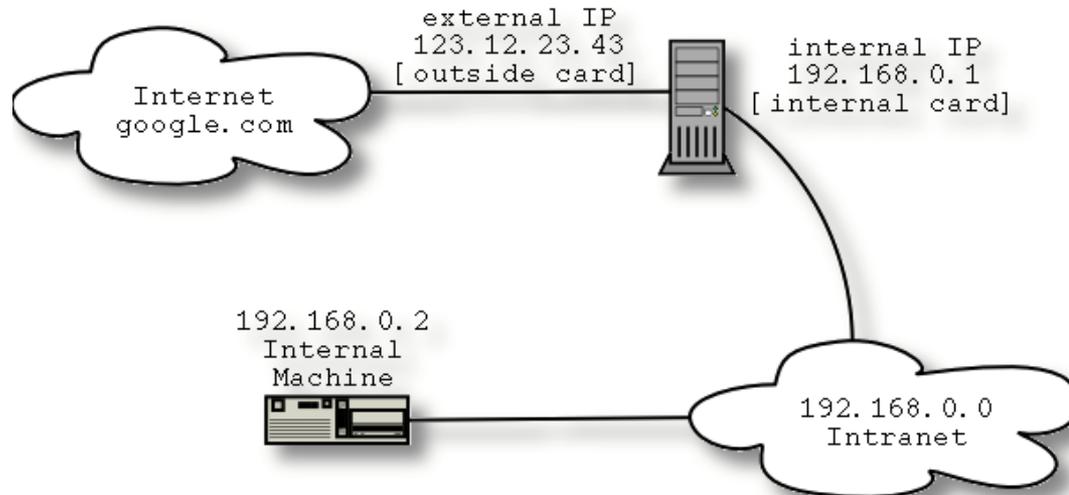
Cada dirección publica es única.

Existen  $2^{32} = 4.294.967.296$  (Mas de 4 billones) de direcciones distintas



## Hay 4 tipos de direcciones IP:

- **Públicas:** Son únicas y son visibles en todo internet.
- **Privadas:** Son visibles sólo dentro de su propia red, dentro de la cual deben ser únicas.
- **Estáticas:** Un servidor o estación siempre accederá a la red con la misma dirección.
- **Dinámicas:** Es posible que cada vez que una estación accede a la red lo haga con una dirección distinta.





## Estructura de las direcciones IP



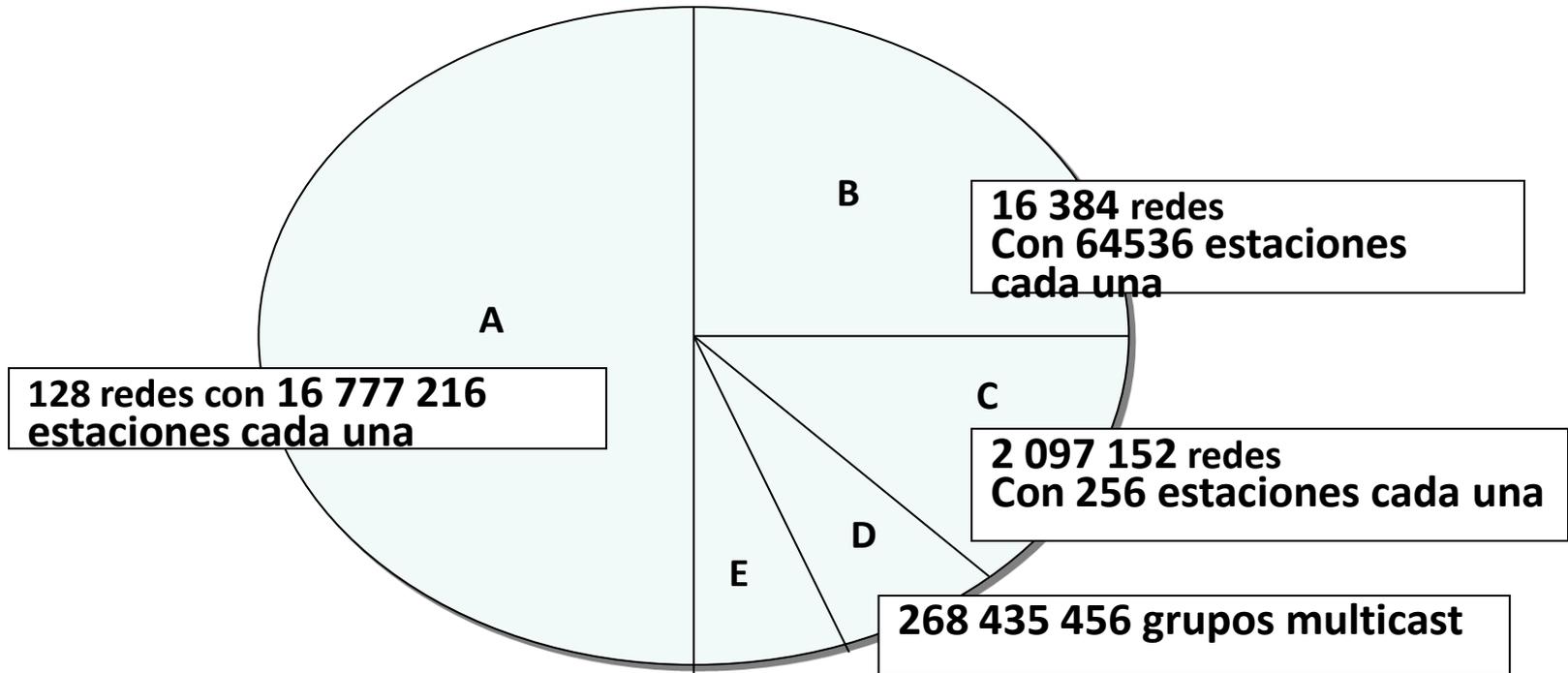
- **Una direccion IP tiene dos objetivos:**
  1. Identificar de manera unica la estacion
  2. Identificar la ubicacion de la estacion
- **Por esto, una direccion IP tiene dos partes**
  - Red (prefix, netid)
  - Estacion (suffix, hostid)
- **La red identifica la red en la que la estacion esta trabajando.**
- **La estacion identifica esa estacion de manera unica en la red**
- **Red y Estacion identifican a una estacion de manera unica en Internet.**

# Clases de direcciones IP



Las direcciones IP han sido clasificadas en 5 Clases

	Byte 1	Byte 2	Byte 3	Byte 4	
Clase A	0	red	estacion		0.0.0.0-127.0.0.0
Clase B	10	red	estacion		128.0.0.0-191.0.0.0
Clase C	110	red		estacion	192.0.0.0-223.0.0.0
Clase D	1110 Direccion Multicast				224.0.0.0-239.0.0.0
Clase E	1111 Reservada para uso futuro				240.0.0.0-255.0.0.0





## Utilidades de las clases IP

**CLASE A:** Redes grandes con muchas máquinas. Se tienen 7 bits para el número de redes y 24 restantes para el número de estaciones. Se caracterizan por tener un 0 en el primer bit.

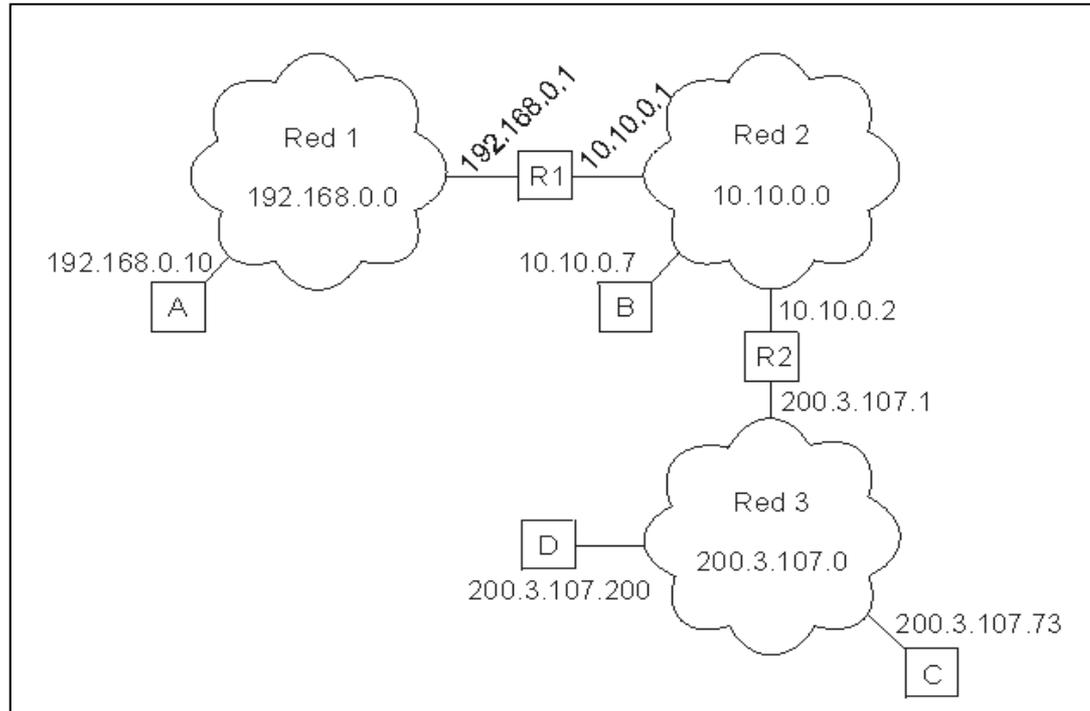
**CLASE B:** Estas direcciones tienen el primer bit en 1 y el siguiente en 0. El campo de red ocupa los 14 bits siguientes y el de servidores (host) los 16 restantes. Se utilizan para redes de tamaño medio.

**CLASE C:** Organizaciones pequeñas con un número pequeño de estaciones. Los primeros 3 bits son 110. El campo de red ocupa los siguientes 21 bits y los 8 restantes son para las estaciones.

**CLASE D:** Los primeros 4 bits son 1111. Se utiliza para definir grupos multicast. El grupo queda definido por los 28 bits siguientes.



## Asignación de direcciones IP



Host	Dirección física	Dirección IP	Red
A	00-60-52-0B-B7-7D	192.168.0.10	Red 1
R1	00-E0-4C-AB-9A-FF	192.168.0.1	
B	A3-BB-05-17-29-D0	10.10.0.1	Red 2
	00-E0-4C-33-79-AF	10.10.0.7	
R2	B2-42-52-12-37-BE	10.10.0.2	
	00-E0-89-AB-12-92	200.3.107.1	Red 3
C	A3-BB-08-10-DA-DB	200.3.107.73	
D	B2-AB-31-07-12-93	200.3.107.200	



## Direcciones IP especiales y reservadas

### No todas las direcciones IP pueden utilizarse

#### Rango reservado para direcciones privadas

Clase	Rango
A	10.0.0.0
B	172.16.0.0
C	192.168.0.0 - 192.168.255.0

#### Direcciones que no pueden asignarse

Dir.	Uso
255.255.255.255	Indica broadcast o difusión en la propia red
0.0.0.0	Identifica a la estación actual. Sólo puede utilizarse como dirección de origen.
127.0.0.1	Se utiliza como prueba de respuesta. Los paquetes son regresados a la misma dirección de origen.



## Otras direcciones que no pueden utilizarse....

Bits de red	Bits de estaciones	Uso
Todos 0	Estaciones correspondientes	Envia paquetes a cualquier estación dentro de la red, aunque no se conozca la dirección de red. Ejemplo: 0.0.1.1 Envía información a la estación 1.1 de ésta red.
Red correspondiente	Todos 0	Sólo se utiliza para especificar rutas y no puede usarse como dirección destino o dirección origen. Ejemplo: 157.74.21.0 identifica una ruta de red.
Red correspondiente	Todos 1	Dirección de difusión o broadcast a la red indicada. Ejemplo: 192.168.1.255 envía información a todas las estaciones de la red 192.168.1.0

**En base a las dos últimas restricciones siempre hay 2 direcciones que no pueden utilizarse para definir estaciones: La primera que corresponde a la dirección de red y la última que corresponde a la dirección de difusión (Broadcast)**



## Máscara de subred

Es una dirección especial asignada a cada clase de red, utilizada para separar la parte de red de la parte de estaciones.

La dirección de red se obtiene haciendo un AND de la dirección IP con la dirección de la máscara de subred.

Clase	Formato (r=red, h=host)	Número de redes	Número de hosts por red	Rango de direcciones de redes	Máscara de subred
A	r.h.h.h	128	16.777.214	0.0.0.0 - 127.0.0.0	255.0.0.0
B	r.r.h.h	16.384	65.534	128.0.0.0 - 191.255.0.0	255.255.0.0
C	r.r.r.h	2.097.152	254	192.0.0.0 - 223.255.255.0	255.255.255.0
D	grupo	-	-	224.0.0.0 - 239.255.255.255	-
E	no válidas	-	-	240.0.0.0 - 255.255.255.255	-



**Supongamos una red con mascara 255.255.0.0 en la que tenemos una estación con dirección 148.120.33.110. Si expresamos esta dirección en binario.**

```
148.120.33.110 10010100.01111000.00100001.01101110 (dirección de una máquina)
255.255.0.0    11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.120.0.0    10010100.01111000.00000000.00000000 (dirección de su subred)
<-----RED-----> <-----HOST----->
```



La dirección de difusión puede obtenerse haciendo un OR de la dirección IP con el NOT de la máscara.

**Ejemplo:**

**Para la dirección y máscara : 148.120.33.110**

**Mascara: 255.255.0.0    not(mascara) = 0.0.255.255**

**En binario:**

**Dir IP . 148.120.33.110    10010100.01111000.00100001.01101110**

**or**

**Not (mascara):                    00000000.00000000.11111111.11111111**

---

**10010100.01111000.11111111.11111111**

**En decimal:                    148.120.255.255 -> Dirección de difusión**

**Es el equivalente de colocar en 1 todos los bits correspondientes a las estaciones.**



## División en subredes

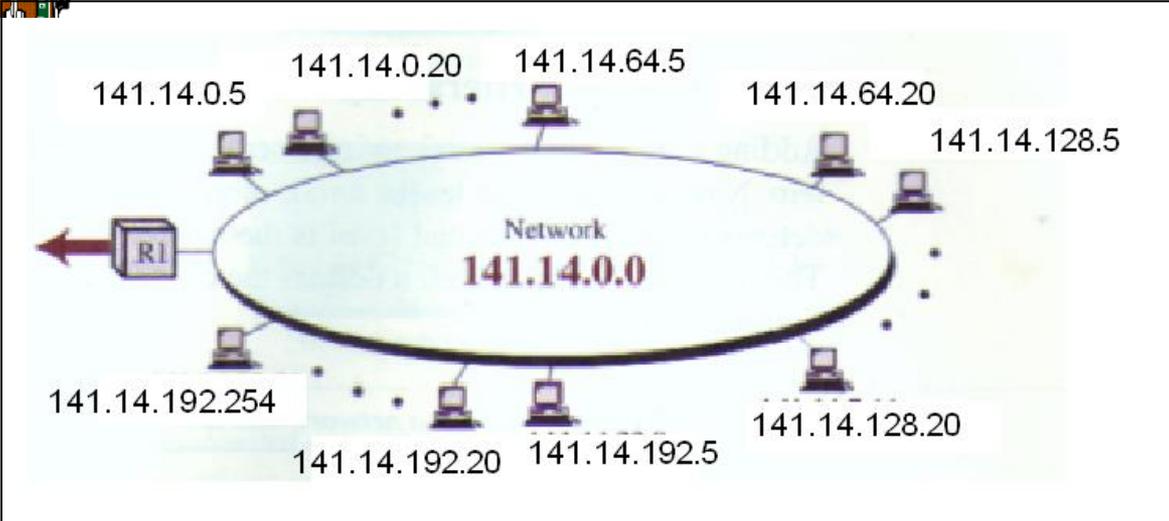
Debido a que una empresa puede requerir dividir su espacio asignado en subredes, la máscara puede modificarse para obtener subredes.

Máscara de subred	Binario	Número de subredes	Núm. de hosts por subred	Ejemplos de subredes (x=a.b.c por ejemplo, 192.168.1)
255.255.255.0	00000000	1	254	x.0
255.255.255.128	10000000	2	126	x.0, x.128
255.255.255.192	11000000	4	62	x.0, x.64, x.128, x.192
255.255.255.224	11100000	8	30	x.0, x.32, x.64, x.96, x.128, ...
255.255.255.240	11110000	16	14	x.0, x.16, x.32, x.48, x.64, ...
255.255.255.248	11111000	32	6	x.0, x.8, x.16, x.24, x.32, x.40, ...
255.255.255.252	11111100	64	2	x.0, x.4, x.8, x.12, x.16, x.20, ...
255.255.255.254	11111110	128	0	ninguna posible
255.255.255.255	11111111	256	0	ninguna posible

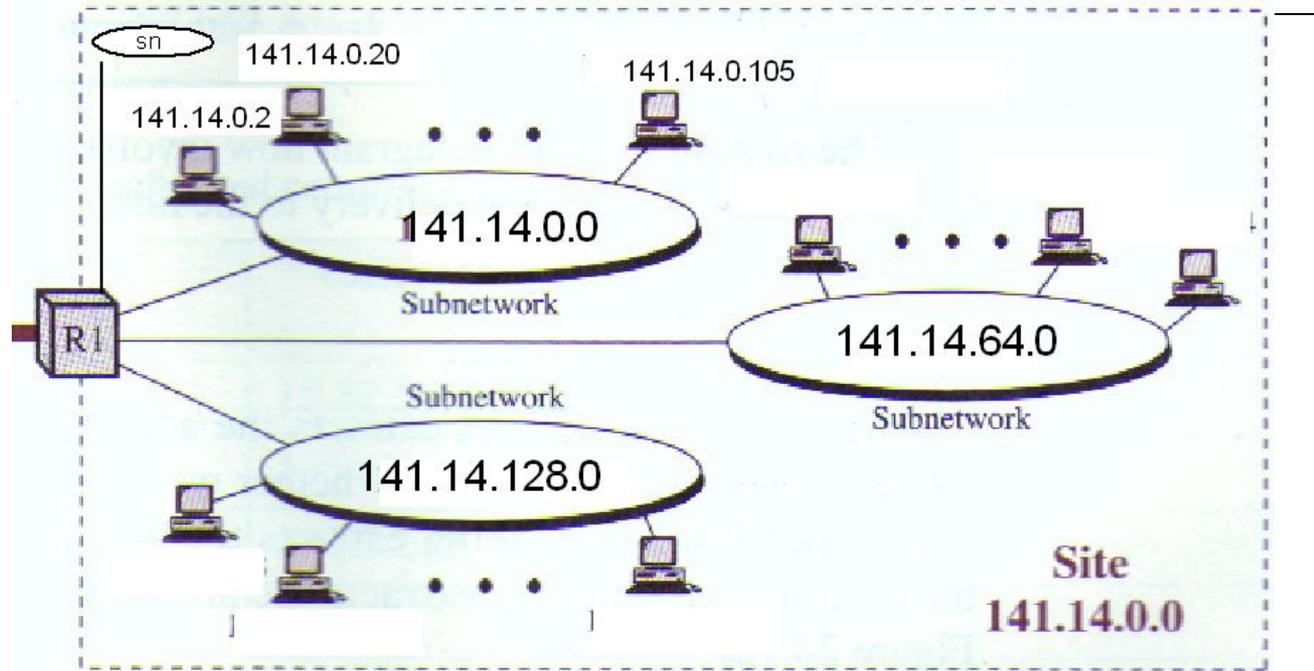
Ejerc.



# EXPANSIÓN EN SUBREDES



Una sola red (2 niveles)



1 red y 4 subredes (3 niveles)



Encontrar la dirección de subred utilizando la mascara puede realizarse mediante:

- 1.- Los bytes de la dirección IP que se correspondan con 255 en la mascara serán repetidos en la dirección de subred.
- 2.- Los bytes de la dirección IP que se correspondan con 0 en la mascara cambian a 0 en la dirección de subred.
- 3.- Para el resto de los bytes se utiliza el operador AND

**Ejemplo:**

**Encontrar la dirección de subred para:**

**Dirección IP: 45.123.21.8**

**Mascara: 255.192.0.0**

**Convertir a binario para realizar el AND:**

**123 → 01111011**

**192 → 11000000**

**01000000**

**→ 64**

**La dirección de subred es: 45.64.0.0**



Encontrar la dirección de difusión o broadcast utilizando la mascara puede realizarse mediante:

- 1.- Obtener el complemento de la mascara de subred (NOT)
- 2.- Los valores que coincidan con 0's pasan igual en la dirección de difusión.
- 3.- Los valores que coincidan con todos 1's (255) se convierten en 255
- 4.- Para el resto de los bytes se utiliza el operador OR

**Ejemplo:**

Encontrar la dirección de subred para:

Dirección IP: 45.123.21.8

Mascara: 255.192.0.0

Not(mask): 0.63.255.255

1) Not de la mascara: 0.63.255.255

Convertir a binario para realizar el OR:

123 → 01111011

63 → 00111111

01111111 → 127

La dirección de subred es: 45.127.255.255



**Ejemplo:**

**Obtener la clase, dirección de red y de difusión de la siguiente dirección IP en base a su mascara:**

**213.23.47.37 / 255.255.255.240**

**La clase: Inicia con 213 → Clase C**

**Para obtener dirección de subred:**

**37 → 00100101 AND**

**240 → 11110000**

**Dirección de subred: 213.23.47.32**

**00100000 → 32**

**La dirección de difusión es un OR con el NOT de la mascara:**

**240 → 11110000 NOT (240) → 00001111**

**37 → 00100101 OR**

**240' → 00001111**

**Dirección de difusión: 213.23.47.47**

**00101111 → 47**



Las direcciones que se asignan a las estaciones de una subred se obtienen después de haber calculado la dirección de red y broadcast. Estas direcciones se podrán asignar dentro de un rango permitido por la cantidad de direcciones disponibles entre la dirección de la primera y la última estación posibles de asignar.

**Ejemplo:**

Para la dirección IP y máscara: **200.16.2.160/255.255.255.192**

Dirección de red:

La dirección IP: **200. 16. 2. 10100000 AND**

Mascara: **255.255.255.11000000**

Dirección de red: **200.16. 2. 10000000 → 200.16.2.128**

Dirección de difusión

Not(mascara) **0.0.0.00111111 = 0.0.0.63**

Dirección IP : **200.16.2. 10100000 OR**

Not mascara **0. 0. 0. 00111111**

Dirección de difusión: **200.16.2. 10111111 → 200.16.2.191**

Dirección para la primer estación será: **200.16.2.129**

Dirección para la última estación será: **200.16.2.190**

**NOTA:**

1	1	1	1	1	1	1	1
2 <sup>7</sup>	2 <sup>6</sup>	2 <sup>5</sup>	2 <sup>4</sup>	2 <sup>3</sup>	2 <sup>2</sup>	2 <sup>1</sup>	2 <sup>0</sup>
128	64	32	16	8	4	2	1



## EJEMPLO:

A una empresa se le asigna la dirección IP 205.16.74.0. La empresa desea tener 4 subredes a partir de esta dirección. Determinar:

- a) Clase de la dirección.
- b) Máscara de subred requerida
- c) Las 4 direcciones de las subredes
- d) Número de estaciones por subred
- e) Número total de estaciones

a) Se trata de una dirección clase C

b) La máscara de subred de clase C es 255.255.255.0, pero se desea tener 4 subredes por lo que se requieren 2 bits más, de manera que la máscara es 255.255.255.192

c) Las 4 direcciones serán:

205.16.74.0

205.16.74.64

205.16.74.128

205.16.74.192

d) Se tienen 6 bits restantes para las estaciones, por lo que es posible tener:

$2^6 - 2 = 64 - 2 = 62$  estaciones por red

e) El número total de estaciones posibles es:  $62 \times 4 = 248$

rede  
s



**1) En base a la dir IP y mascara dada**

**Determinar :**

**a)la dirección de red**

**b) la dirección de difusión para las siguientes**

**c)la dirección de la primera estación**

**d) La dirección de la ultima estación**

**215.33.109.216/255.255.255.224**



## **Ejercicio 2**

**A una empresa se le asigna la dirección IP 215.143.120.43 La empresa desea tener 8 subredes a partir de esta dirección. Determinar:**

- a) Clase de la dirección.**
- b) Máscara de subred requerida**
- c) Las 8 direcciones de las subredes**
- d) Número de estaciones por subred**
- e) Número total de estaciones**



En base a la dir IP y mascara dada

Determinar :

a) la direccion de red

b) la dirección de difusión para las siguientes

c) la direccion de la primera estacion

d) La direccion de la ultima estacion

**215.33.109.216/255.255.255.224**

a)

AND	1 1 0 1 1 0 0 0 (216)
	<u>1 1 1 0 0 0 0 0</u> (224)
	1 1 0 0 0 0 0 0 (192)

Red: 215.33.109.192

b)

OR	1 1 0 1 1 0 0 0 (216)
	<u>0 0 0 1 1 1 1 1</u> (32)
	1 1 0 1 1 1 1 0 1 (223)

Difusion: 215.33.109.223

c)	<b>215.33.109.193</b>
d)	<b>215.33.109.222</b>



## Ejercicio 2

A una empresa se le asigna la dirección IP 215.143.120.43 La empresa desea tener 8 subredes a partir de esta dirección. Determinar:

- a) Clase de la dirección.
- b) Máscara de subred requerida
- c) Las 8 direcciones de las subredes
- d) Número de estaciones por subred
- e) Número total de estaciones

a) Se trata de una dirección clase C

b) 255.255.255.224

c) Las 8 direcciones serán:

215.143.120.0

215.143.120.32

215.143.120.64

215.143.120.96

215.143.120.128

215.143.120.160

215.143.120.196

215.143.120.224

d) Se tienen 5 bits restantes para las estaciones, por lo que es posible tener:

$2^5 - 2 = 32 - 2 = 30$  estaciones por red

e) El número total de estaciones posibles es:  $30 \times 8 = 240$

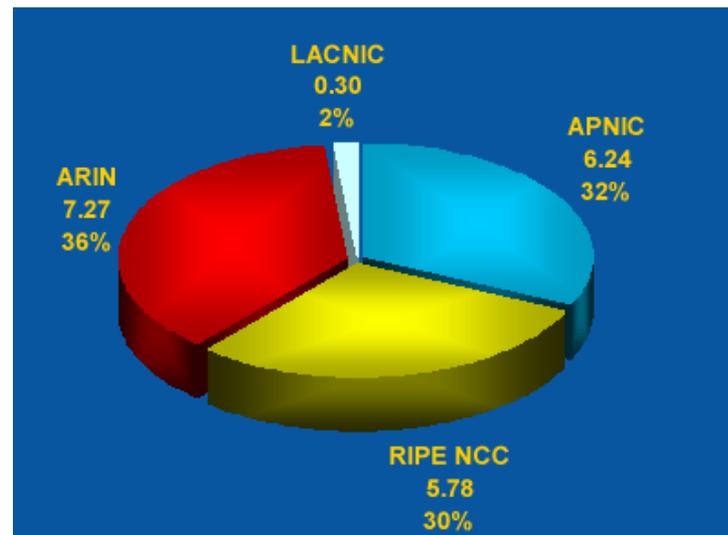


## **PROBLEMAS Y DEFICIENCIAS DE IPv4**

- **IPv4 fue publicado en 1981 (hace más de 20 años!!). RFC 791**
- **La capacidad de direcciones IP únicas es de más de 4 billones.**
- **Se han asignado todas las direcciones IPv4 disponibles**
- **El crecimiento de los usuarios de Internet ha sido exponencial!. Sin direcciones IP no es posible conectarse a Internet.**
- **Las tablas de enrutamiento han crecido de manera alarmante con el aumento de los usuarios.**
- **No cumple con los requerimientos de Calidad de Servicios, Movilidad y seguridad que demandan las aplicaciones recientes.**



Direcciones IPv4 asignadas por región hasta octubre del 2003.



En México:

[https://www.iar.mx/jsf/static\\_content/services/resources\\_request/payments/paymentsHowMuch.jsf](https://www.iar.mx/jsf/static_content/services/resources_request/payments/paymentsHowMuch.jsf)



## ¿Porque cambiar el protocolo IPv4?

- Permitir un mejor manejo de diferentes tipos de servicio
- Mayor seguridad
- Menor procesamiento en los enrutadores.
- Establecer un conjunto de direcciones que no se agoten en un futuro cercano

## ¿Que ofrece IPv6?

- Publicado en 1998. RFC 2460
- Encabezado IP más eficiente con extensiones para aplicaciones y opciones
- No utiliza suma de verificación en el encabezado
- Seguridad incorporada para autenticación y encriptación.
- Prevención de fragmentación intermedia de datagramas.
- Direcciones de red de 128 bits (16 bytes),

esto es, se tienen :

**340,282,366,920,938,463,463,374,607,431,768,211,456**  
(340 sextillones)  
**Direcciones distintas!**



## Características IPv6

IPv6 ha sido considerado una evolución positiva de la Internet global actual.

Incorpora tecnologías basadas en IPv4 y además las integra en un todo único con las nuevas características de IPv6.

Algunas de estas características importantes incorporadas a la Internet de la nueva generación son:

- Descubrimiento del vecindario (neighbor discovery)
- Autoconfiguración
- Movilidad
- Seguridad
- Calidad de servicio

Todos estos son elementos importantes en el Internet actual



## **DESCUBRIMIENTO DEL VECINDARIO (Neighbor discovery, ND)**

**Esta característica importante de IPv6 consiste en un conjunto de mensajes y procesos que determinan las relaciones entre los nodos vecinos.**

*ND se utiliza por los nodos para descubrir:*

- **Enrutadores vecinos,**
- **Direcciones, prefijos de direcciones y otros parámetros de configuración**

*ND se utiliza por enrutadores para:*

- **Anunciar su presencia, parametros de configuración de nodos, y prefijos de direcciones.**
- **Informar a los nodos sobre las mejores rutas para enviar sus paquetes.**

**ND consiste en el mecanismo con el cual un nodo que se incorpora a la red, descubre la presencia de otros en su mismo enlace, para determinar sus direcciones, localizar enrutadores y mantener información de conectividad.**



## **Autoconfiguración.**

**Las direcciones IPv6 son significativamente más complejas que las direcciones IPv4, por lo tanto, una de las metas de las características de IPv6 es reducir el número de veces que estas direcciones tengan que ser configuradas.**

**Además, la utilización exitosa de otros mecanismos como DHCP ha probado el gran valor de la asignación dinámica de direcciones IP.**

**IPv6 ofrece dos tipos de autoconfiguración automática:**

- Sin intervención (stateless)**
- Predeterminada (stateful)**

**La autoconfiguración es la base para la característica de Movilidad de IPv6**



## **Autoconfiguración sin Intervención (Stateless)**

**En una LAN, los nodos deben ser capaces de configurarse con una dirección de enlace local automáticamente, y utilizar estas direcciones para comunicarse entre si.**

## **Autoconfiguración predeterminada (Stateful)**

**Este mecanismo de autoconfiguración esta basado en el nuevo protocolo llamado DHCPv6.**

**DHCPv6 provee a los clientes (nodos IPv6) la información de configuración almacenada en el servidor, entre los que se encuentran direcciones IPv6 y otros parámetros.**

**DHCPv6 se basa en el concepto cliente-servidor y además introduce el concepto de relay (Un nodo que opera como intermediario entre el nodo y el servidor), así como el concepto de agente, el cual puede ser el servidor o el relay.**

**DHCPv6 se basa en el protocolo de transporte UDP.**



← 32 bits

### 3.1 Encabezado IPv6

Versión	Prioridad	Etiqueta de flujo	
Longitud de carga útil		Siguiente encabezado	Límite de saltos
Dirección IP fuente (128 bits)			
Dirección IP Destino (128 bits)			

**Versión (4 bits):** Toma el valor 6 en este caso.

**Prioridad(8 bits):** Determina el tipo de tráfico para asignarle prioridad en la transmisión. Del 0 al 7 indica poca sensibilidad al tiempo. Del 8 al 15 indica mayor prioridad del tráfico.

**Etiqueta de flujo (20 bits)** Identifica los paquetes que pertenecen a una sesión entre dos servidores. Es usado generalmente para una determinada QoS y acelera el paso de datagramas en la red.

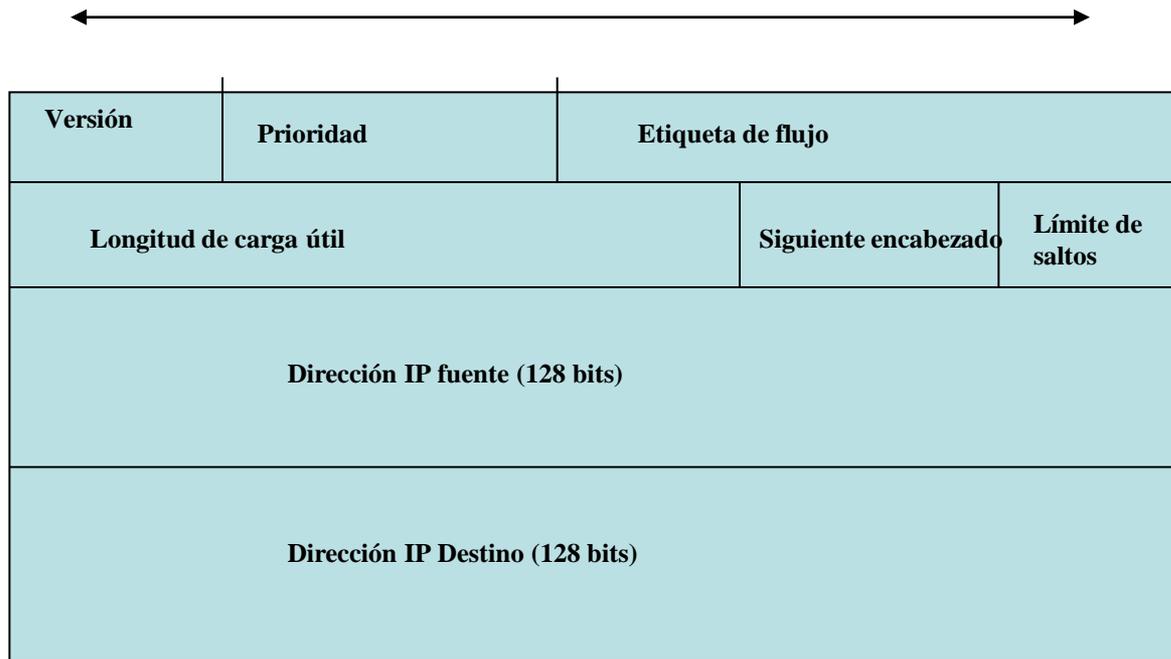
**Longitud de carga útil (16 bits):** Especifica la longitud total del datagrama en bytes (Maximo 65635)

**Siguiente encabezado( 8 bits):** Se utiliza para indicar cual encabezado sigue a IP, si lo hay, de no ser así indica el protocolo de transporte que se utiliza.

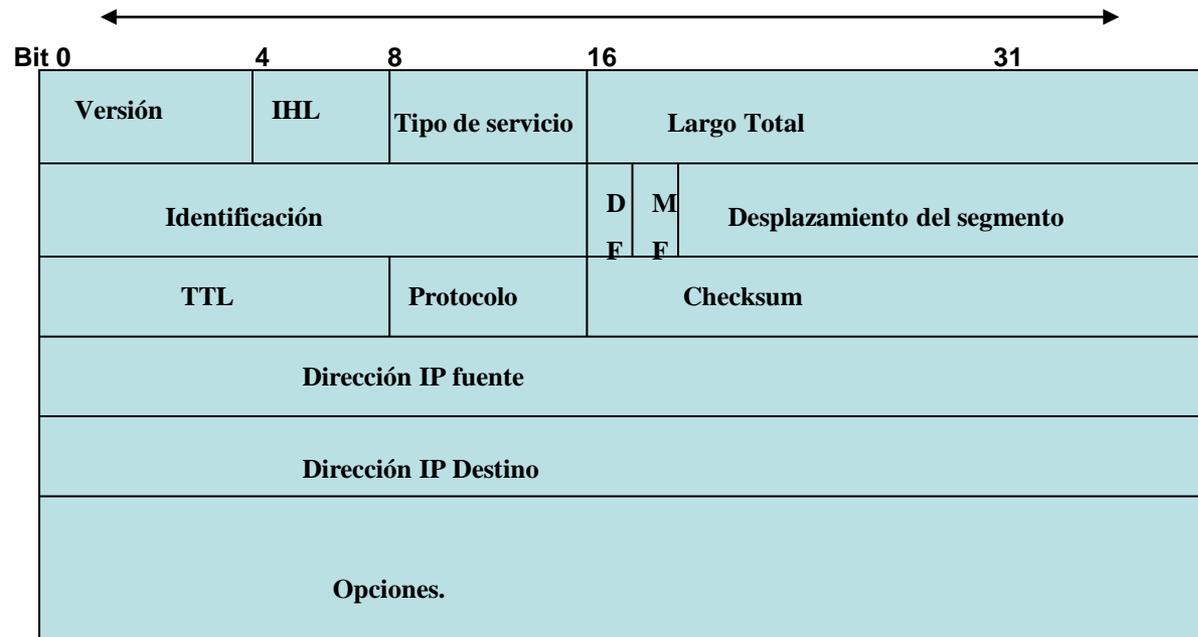
**Limite de saltos (8 bits):** Equivale al TTL en IPv4, determina el número de saltos que puede viajar el datagrama. Cada dispositivo de interconexión lo disminuye en 1.



# IPv6

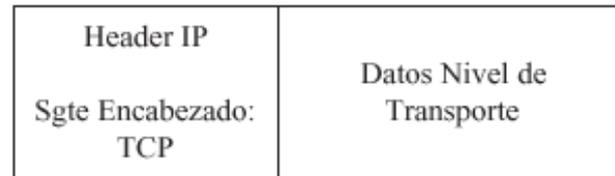


# IPv4

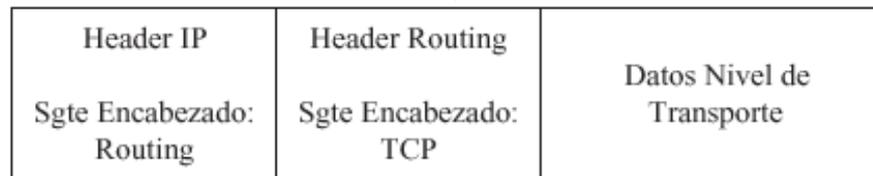




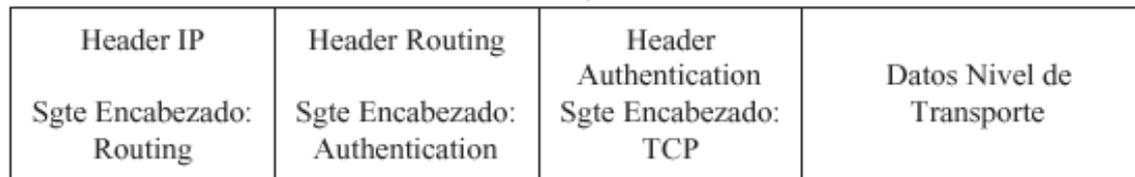
- Salto a salto:** La información del datagrama debe ser examinada por todos los dispositivos de interconexión.
- De enrutamiento o encaminamiento:** Se utiliza cuando la estación transmisora desea controlar el enrutamiento del datagrama.
- De fragmentación:** Permite a una estación fragmentar un datagrama en partes más pequeñas.
- De autenticación:** Se utiliza para asegurar que no se hizo ninguna alteración del contenido del datagrama que se origina en la estación fuente.
- De Encriptación:** Se utiliza para incorporar algún algoritmo de encriptación de la información



a)



b)



c)

### Encabezados opcionales de un paquete IPv6

a) Sin opciones, b) Una opción c) Dos opciones



Cabecera siguiente	Reservado	Desplazamiento del fragmento	Res	M
<b>Identificación</b>				

**Cabecera de Fragmentación**

0	8	16	31
Cabecera siguiente	0	Num. de dirección	Dirección siguiente
<b>Dirección [1]</b>			
<b>Dirección [2]</b>			

**Cabecera de Enrutamiento**



### 3.2 DIRECCIONES IPv6

**Unidistribución  
(Unicast)**



•A una única PC (locales o globales)

**Cualquier difusión  
(AnyCast)**



Sólo son asignadas a Enrutadores, con el mismo formato que las direcciones unicast.

**Multidistribución  
(Multicast)**



Direcciones multicast  
Ejemplo:  
FF01:0:0:0:0:0:101

**Ejemplos:**

Unicast local: fe80::212:34ff:fe12:3456

**Ejemplo dirección IPv6 global:**

2001:0000:0000:0000:0000:0123:44B7:CDEF o

2001::123:44B7:CDEF

**Todas las direcciones IPv6:**

- Son autoconfigurables
- Cada interfaz puede tener varias direcciones asignadas



## Existen tres maneras de representar una dirección IPv6:

1) 8 grupos de 16 bits: x:x:x:x:x:x:x:x en notación hexadecimal.

Ejemplo: fedc:ba98:7654: 3210:fedc:ba98:7654:3210

2) Utilizando el separador de cadenas de ceros ‘::’, el cual se usará una sola vez en la dirección.

Ejemplo: La dirección 1080:0000:0000:0000:8000:0000:200C:417a puede representarse como:

1080::8000:0000:200c:417a,

Los grupos de 16 ceros pueden también representarse como un solo cero, en tal caso la dirección anterior sería:

1080::8000:0:200c:417a

y es posible eliminar ceros iniciales en un conjunto de 16 bits, pero no ceros finales:

Ejemplo: 1080:0000:0000:0000:8000:8000:200c:417a NO puede representarse como

1080::8:8:200c:417a, ya que esta dirección sería el equivalente a tener:

1080::0008:0008:200c:417a



**3) Al utilizar direcciones IPv4 en una dirección IPv6 es posible mezclar valores hexadecimales y decimales cambiando los 2 puntos por puntos.**

**Ejemplo: 0000::129.144.52.38**



**NICAST:**

# Formatos de Direcciones IPv6



En hex  
2

Define la agencia que ha registrado la direccion:

**INTERNIC (ARIN) America**

**RIPNIC: En Europa**

**APNIC: En Asia**

Identifica al proveedor de Acceso a Internet (ISP)

Cuando una organizacion se suscribe a Internet a traves de un proveedor se le asigna un ID de suscriptor.

**Dirección unidistribución global basada en proveedor.**

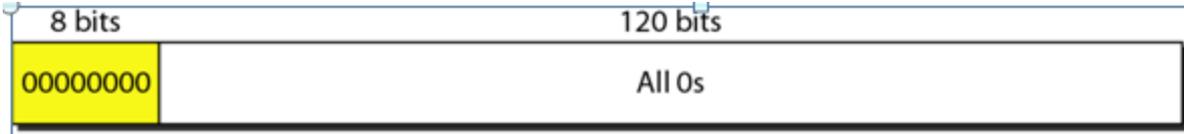
**Se asigna a estaciones conectadas directamente a Internet:**

**2001::123:44B7:CDEF**

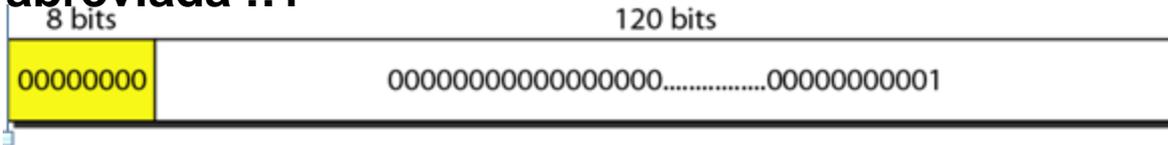


# Direcciones Reservadas

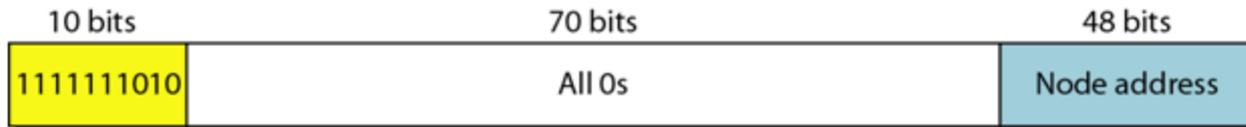
a) Ausencia de dirección, abreviada ::



b) Loopback para enviarse paquetes a si mismo, abreviada ::1



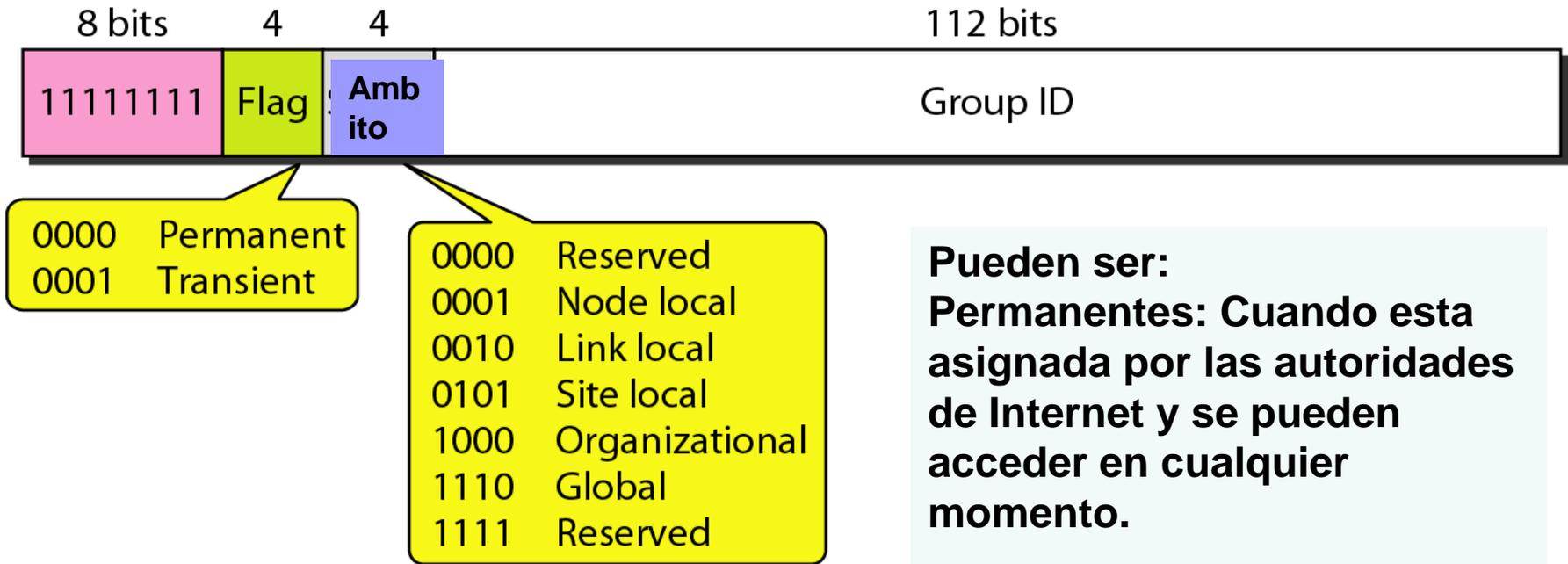
c) De enlace local, dirección privada solo valida en una subred aislada abreviada fe80::dirnodo





## Dirección Multicast

Siempre inician con ff00:: o ff01::



**Pueden ser:**  
**Permanentes:** Cuando esta asignada por las autoridades de Internet y se pueden acceder en cualquier momento.

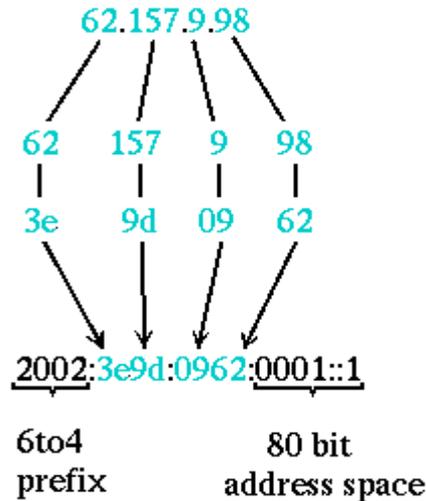
**Transitorias:** Se usan temporalmente, por ejemplo para una videoconferencia.



Además existen otros tipos de direcciones de unidistribución agregables globales :

❖ De prueba 6Bone: inician con: 3ffe,  
Ejemplo: 3FFE:8070:1027::2/64

❖ 6to4: tienen el formato: 2002::/16, son direcciones compatibles con IPv4  
Ejemplo:



Dirección 6to4:  
2002:3e9d:0962::1

❖ Asignadas por un proveedor: comienzan con 2001

Ejemplo: 2001::123:44B7:CDEF