

TEMA 1

Introducción

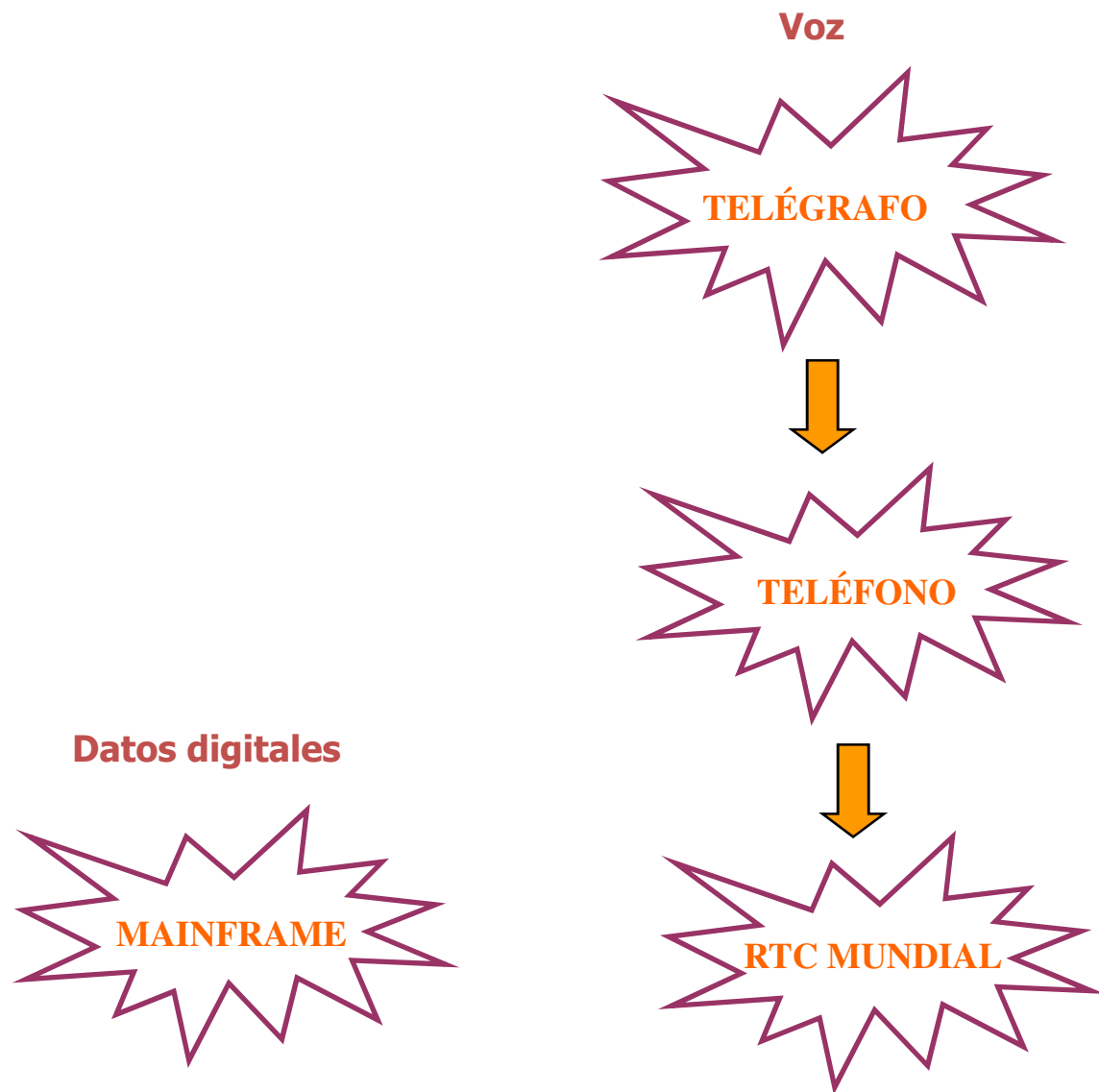
1.1 Evolución histórica de las redes de comunicaciones

Mediados siglo XIX

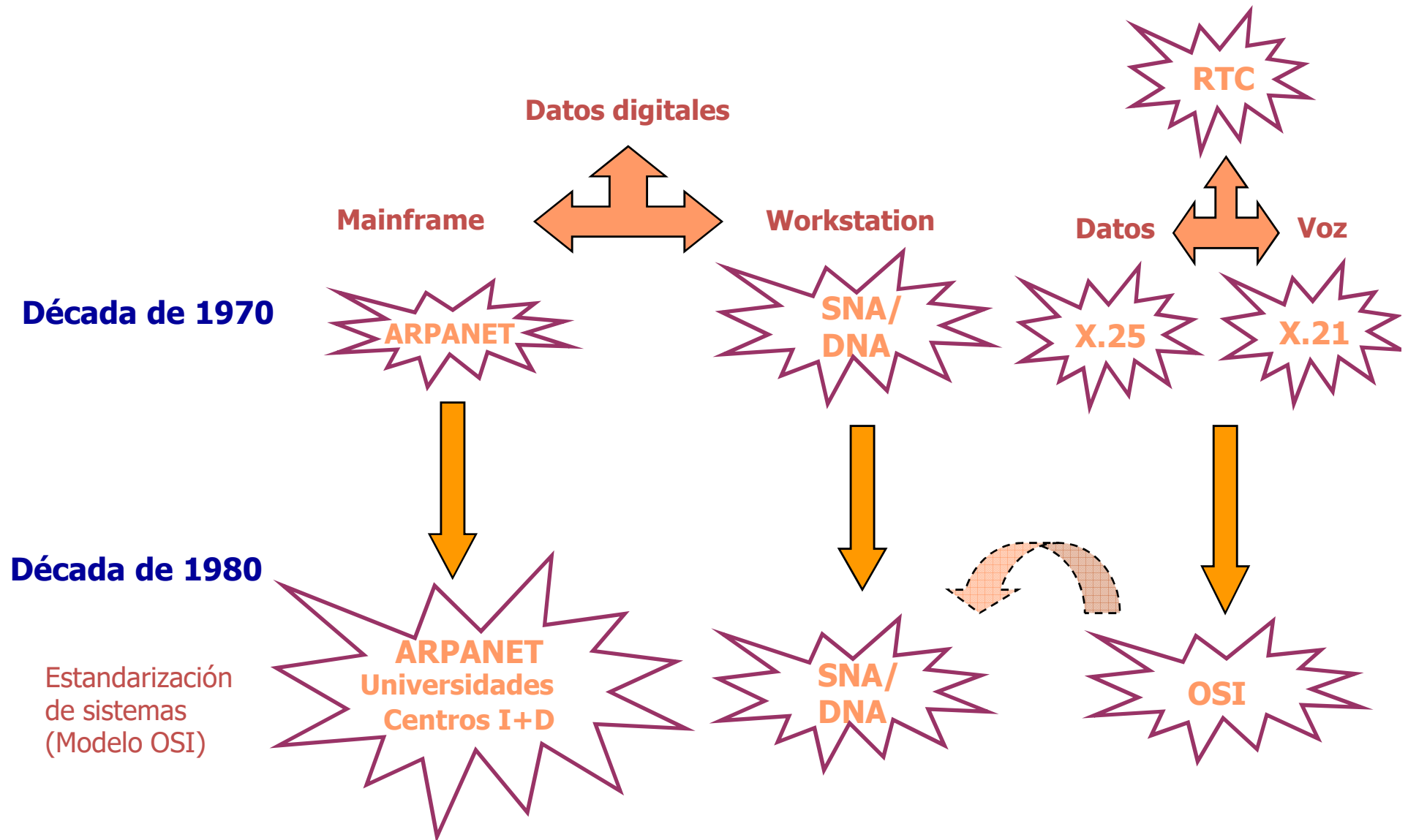
Finales siglo XIX

Década de 1950

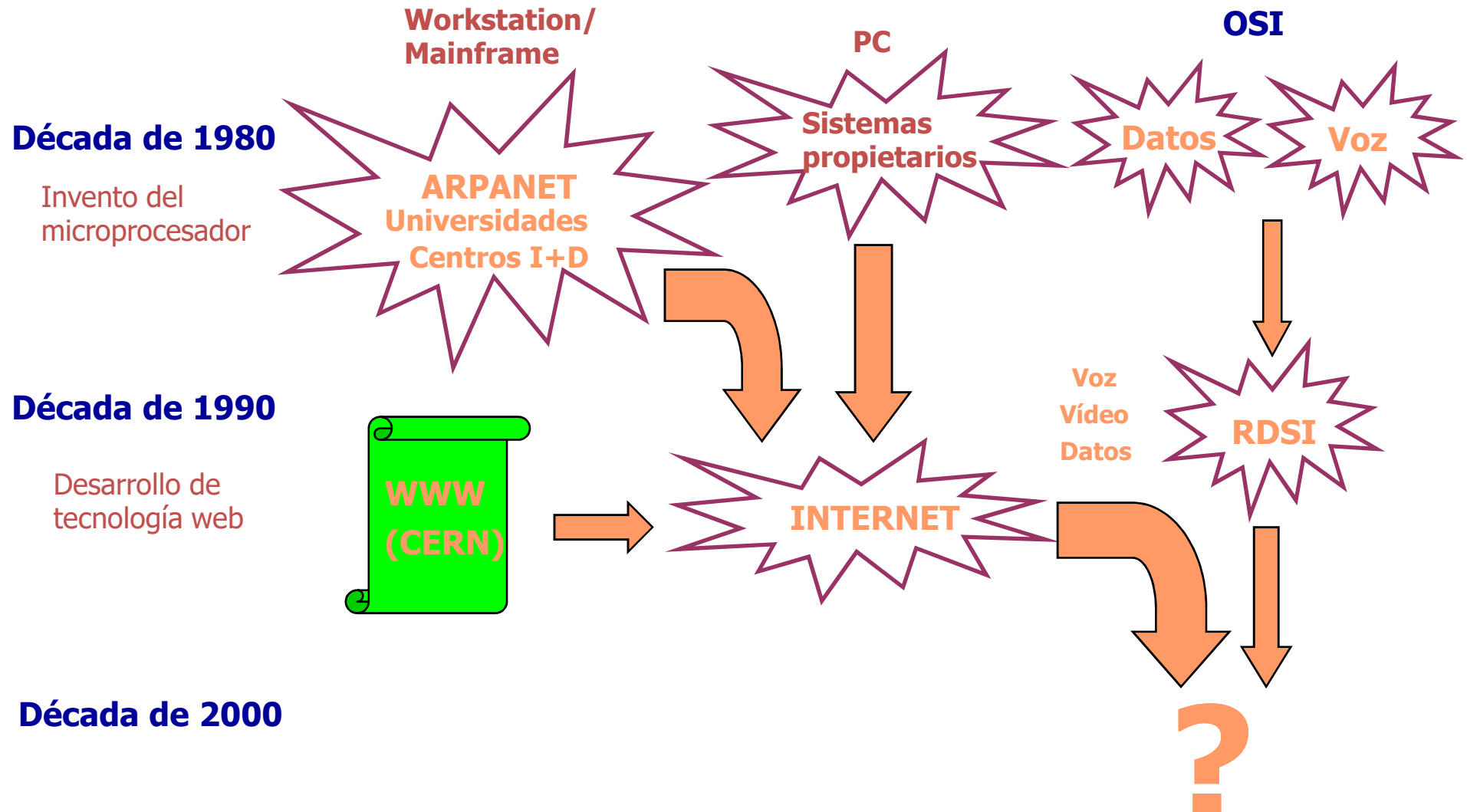
Electrónica digital



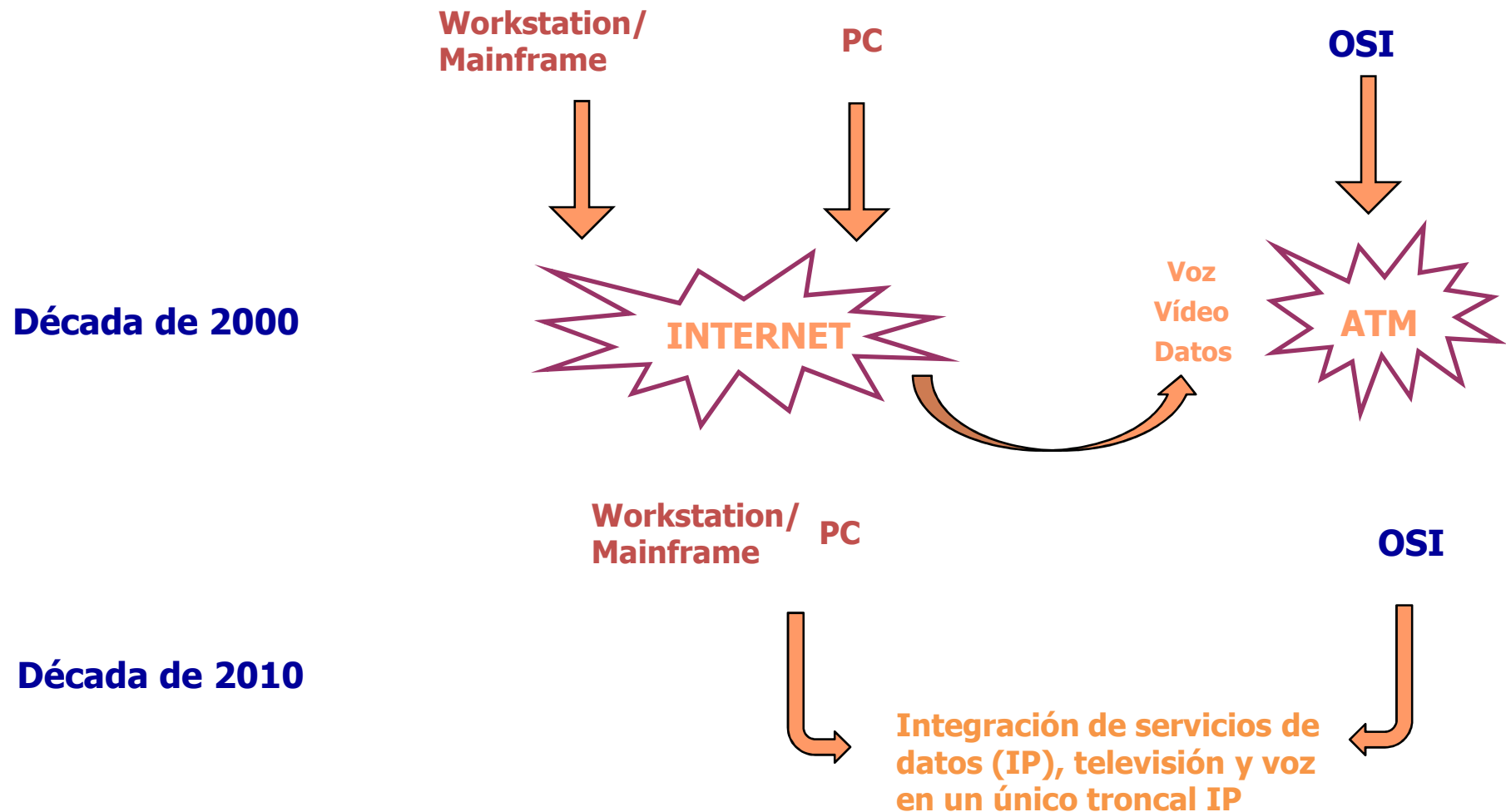
1.1 Evolución histórica de las redes de comunicaciones



1.1 Evolución histórica de las redes de comunicaciones



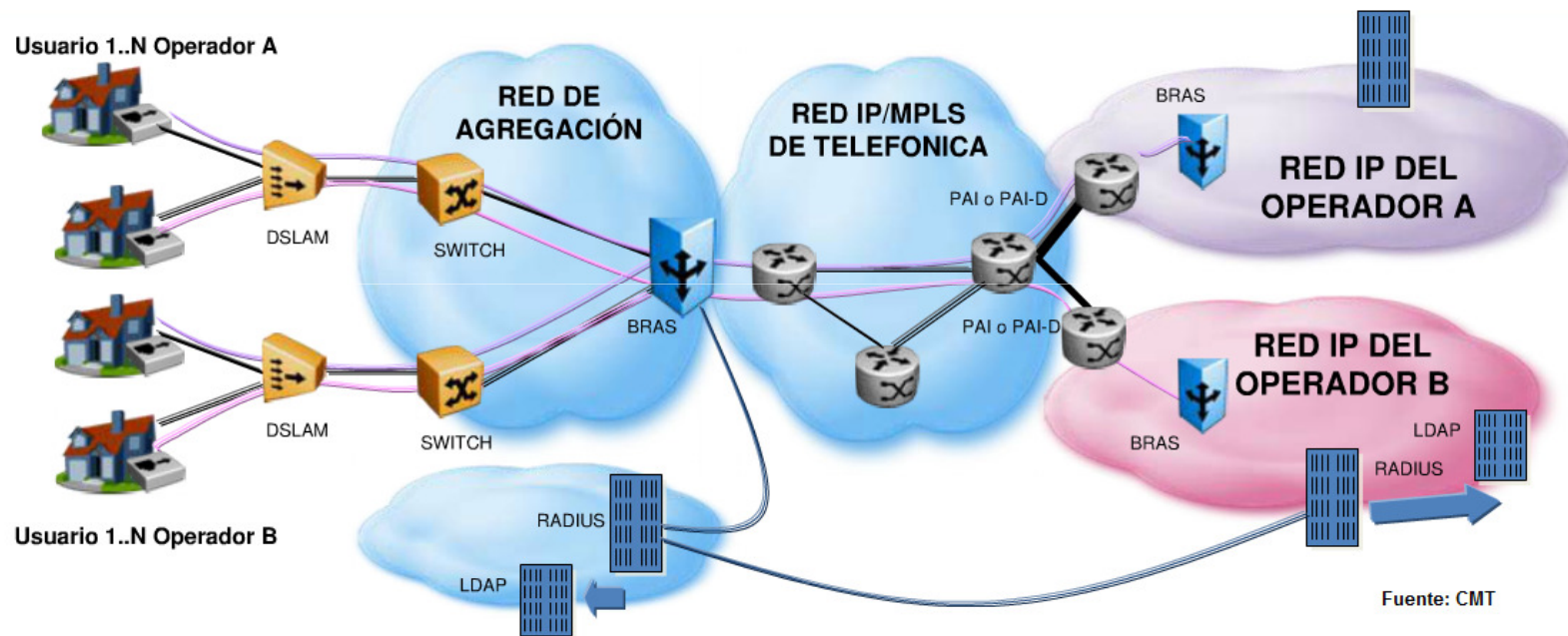
1.1 Evolución histórica de las redes de comunicaciones



1.1 Evolución histórica de las redes de comunicaciones

Década de 2010

Comunicaciones orientadas al servicio, basadas en una arquitectura con Redes de Acceso, Redes de Agregación y Redes Troncales



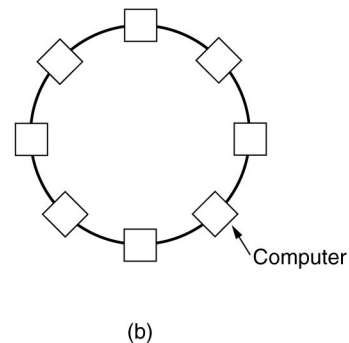
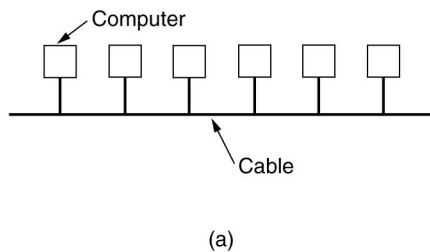
1.2 Fundamentos tecnológicos de las redes de comunicaciones

Clasificación por tipo de interconexión entre las estaciones

Redes de difusión

Redes punto a punto

Redes de difusión

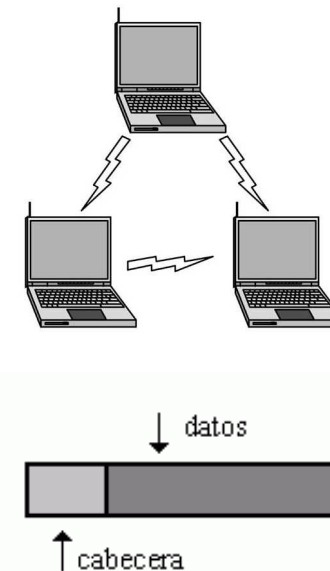


Uso compartido del medio físico por un conjunto de estaciones

La fragmentación en paquetes permite un reparto del uso del medio y reenvíos pequeños en caso de errores.

- **Direccionamiento físico:** n bits para identificar 2^n estaciones en la red
- **Dirección de difusión:** difusión de información a todas las estaciones de la red.

Ejemplo: n bits con valor 1



1.2 Fundamentos tecnológicos de las redes de comunicaciones

- **Dirección de multidifusión:** difusión de información a un grupo de estaciones de la red.

El primer bit de la dirección especifica si es una dirección de multidifusión

$$b_0 \ b_1 \ b_2 \ b_3 \ b_4 \dots b_{n-1} \left\{ \begin{array}{l} b_0 = 0 \text{ dirección de estación } (2^{n-1}) \\ b_0 = 1 \text{ dirección de grupo } (2^{n-1}) \end{array} \right.$$

Existen dos direcciones reservadas que no se emplean para identificar ni estaciones ni grupos de estaciones

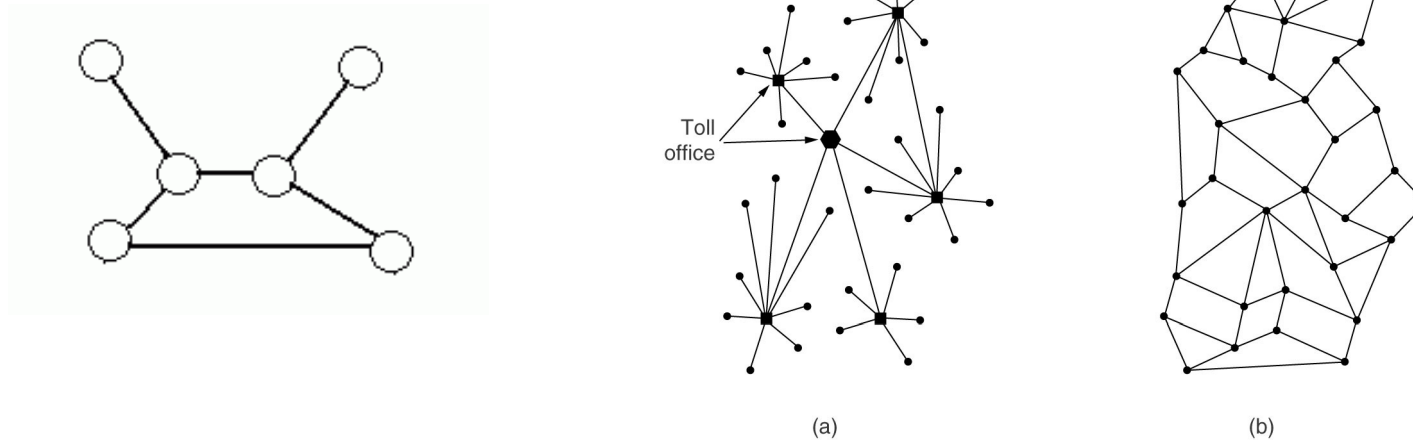
11111111.....11  **Dirección de difusión de la red**

00000000.....00  **Dirección reservada (en algunas redes es la de difusión)**

1.2 Fundamentos tecnológicos de las redes de comunicaciones

Redes punto a punto

Establecimiento de enlace físicos entre pares de nodos de la red.



- El direccionamiento físico es insuficiente para el envío de información entre estaciones
- Necesidad de conocer la estructura de la red y de cómo enviar la información a través de nodos intermedios => Algoritmos de encaminamiento
- Tolerancia a fallos por redundancia de conexiones => alto coste económico de cableado

1.2 Fundamentos tecnológicos de las redes de comunicaciones

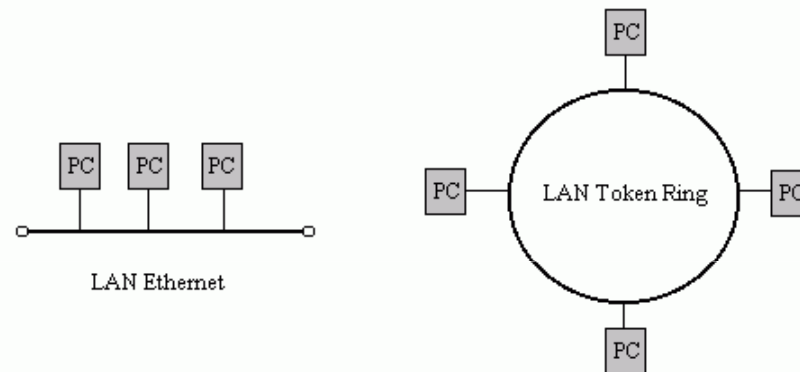
Clasificación por la escala geográfica de la red

Redes LAN (Local Area Network)

Redes MAN (Metropolitan Area Network)

Redes WAN (Wide Area Network)

Redes LAN - Redes de área local



- **Extensión geográfica de una sala, edificio o hasta campus (< 10 Km)**

- **LAN \Leftrightarrow tecnología de difusión**

Baja tasa de error en el medio físico

Alta velocidad de transferencia (10 Mbps - 10 Gbps)

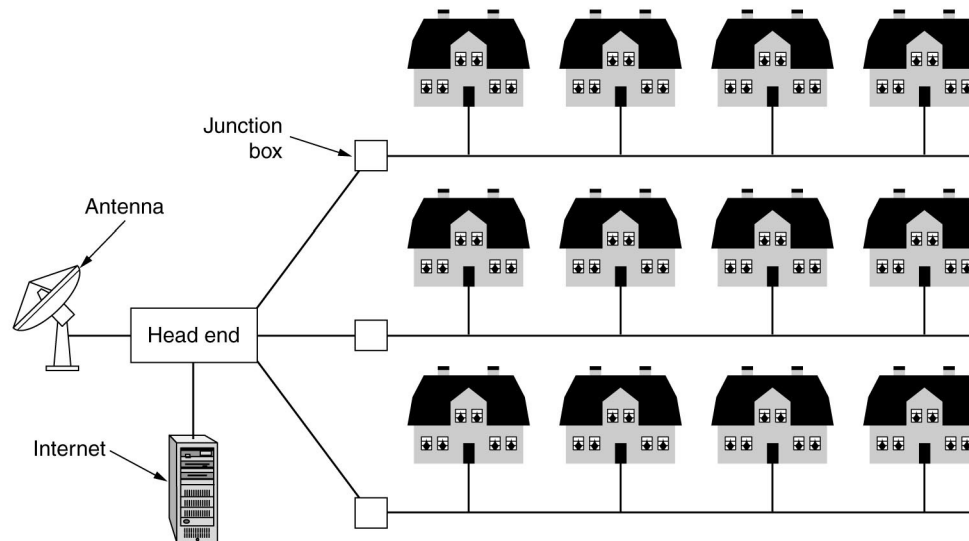
Bajo coste de cableado

Colisiones en el medio físico

1.2 Fundamentos tecnológicos de las redes de comunicaciones

Redes MAN - Redes de área metropolitana

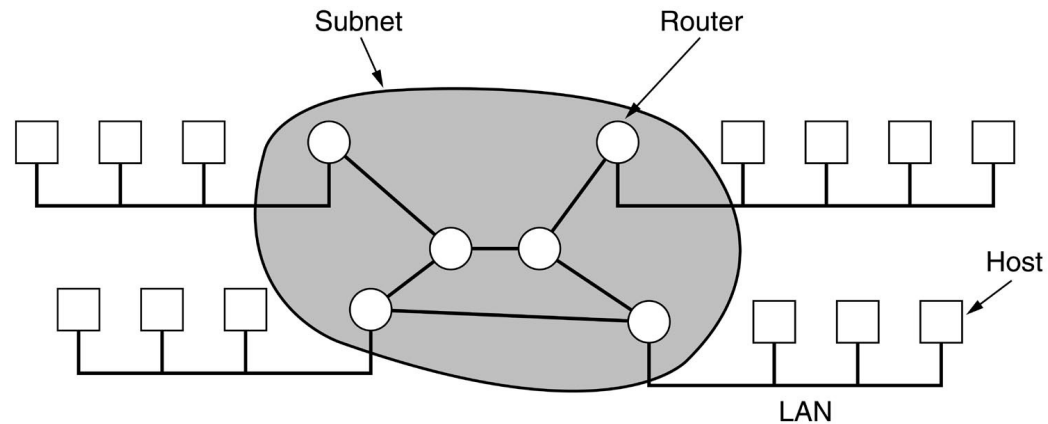
- Extensión geográfica de una ciudad
- MAN \Leftrightarrow tecnología de difusión y punto a punto (cable coaxial y fibra óptica)



**Alta velocidad de
transmisión
(100 Mbps - 1 Gbps)**

1.2 Fundamentos tecnológicos de las redes de comunicaciones

Redes WAN - Redes de área extendida



- Extensión geográfica de un país o continente

- WAN \Leftrightarrow tecnología punto a punto

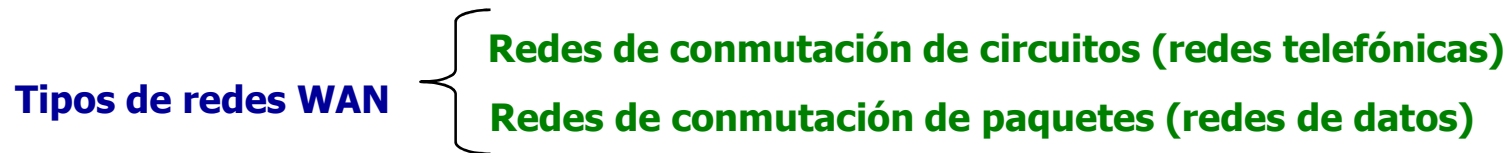
Encaminamiento de la información

Tasa de error en el medio físico mayor que en LAN

Velocidad de transferencia elevada (cientos de Gbps)

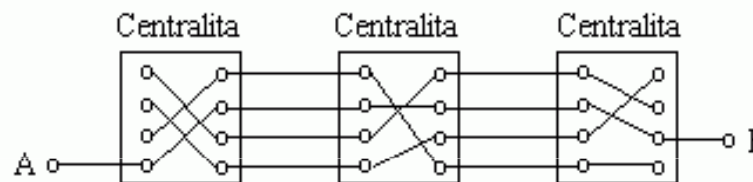
Coste de cableado elevado

1.2 Fundamentos tecnológicos de las redes de comunicaciones



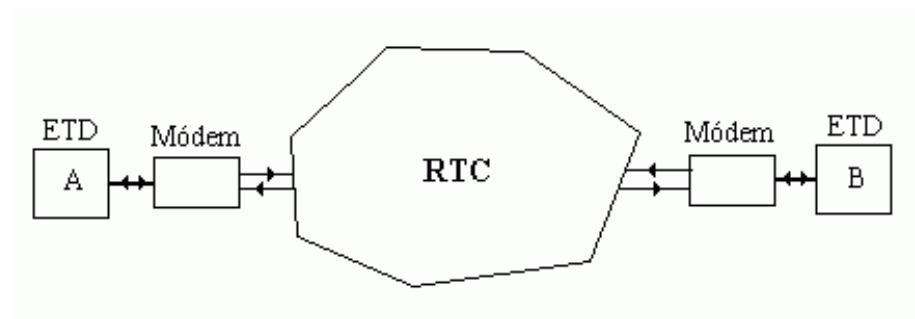
Redes de conmutación de circuitos

- Establecimiento de caminos físicos fijos en la red para cada comunicación



Saturación: falta de disponibilidad de circuitos en una centralita

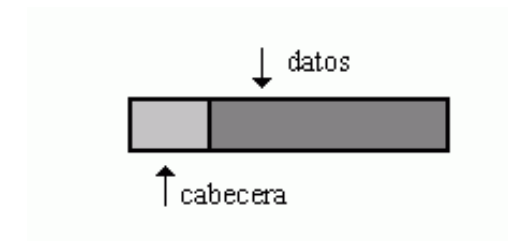
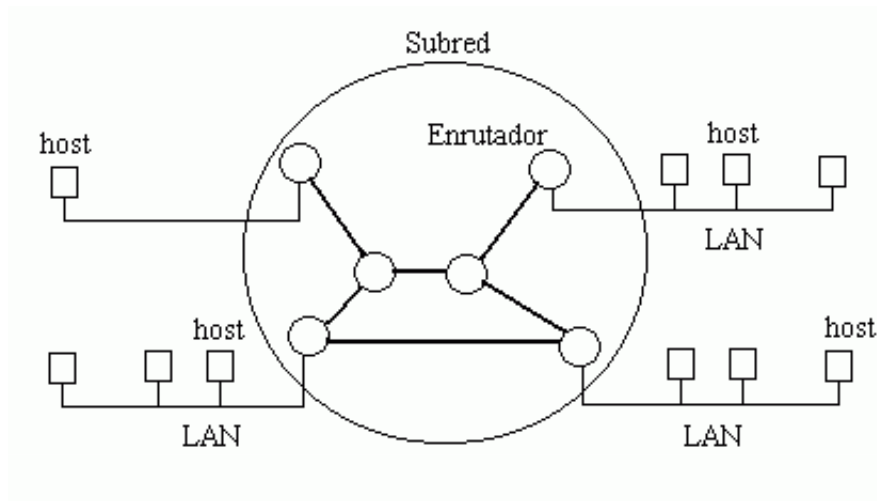
- Transmisión de datos en la red telefónica conmutada (RTC)



Velocidad de transferencia (V.90)
57600 bps

1.2 Fundamentos tecnológicos de las redes de comunicaciones

Redes de conmutación de paquetes



- **Router o encaminador:**

Dispositivo que determina el camino que los paquetes de información siguen en la red

- **Subred (Troncal):**

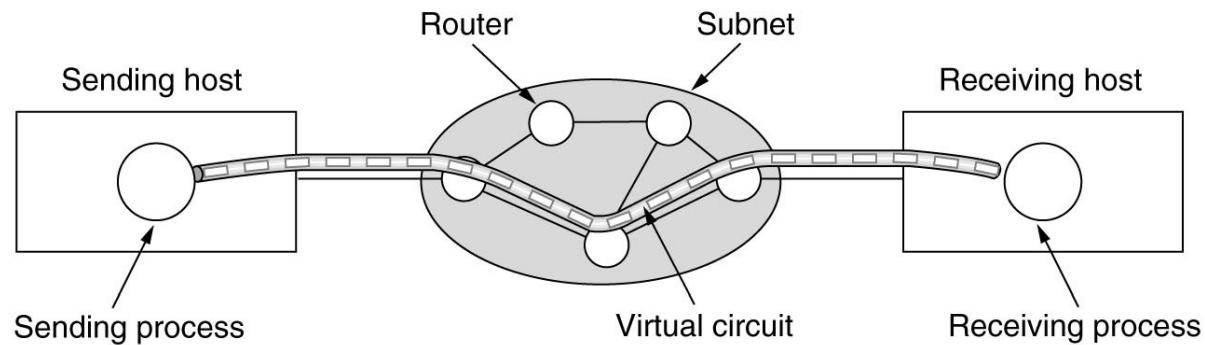
Conjunto de nodos encaminadores y líneas punto a punto que conforman la red

- **Congestión:** falta de recursos computacionales para el encaminamiento de los paquetes de información, produciéndose ralentización en el envío de información

1.2 Fundamentos tecnológicos de las redes de comunicaciones

Determinación de caminos en una red de conmutación de paquetes

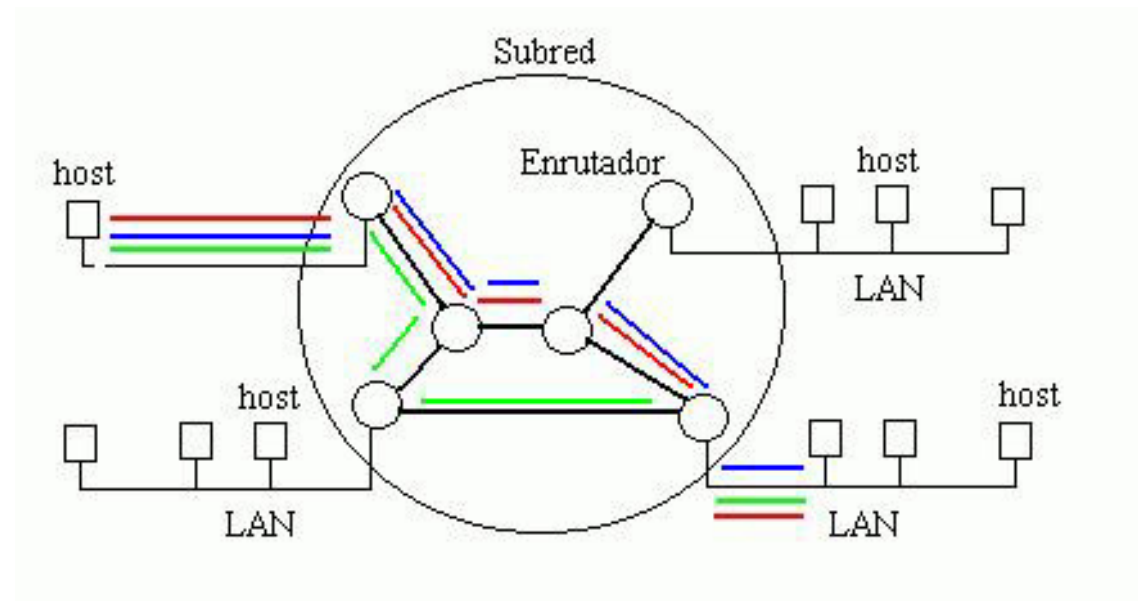
Conmutación de paquetes con circuitos virtuales



- **Establecimiento del circuito virtual (id. de circuito virtual)**
- **Transferencia de paquetes de datos** **C.V. permanentes/no permanentes**
- **Liberación del circuito virtual**
- **Intercambio de datos fiable**
- **Control de los recursos disponibles para una comunicación**

1.2 Fundamentos tecnológicos de las redes de comunicaciones

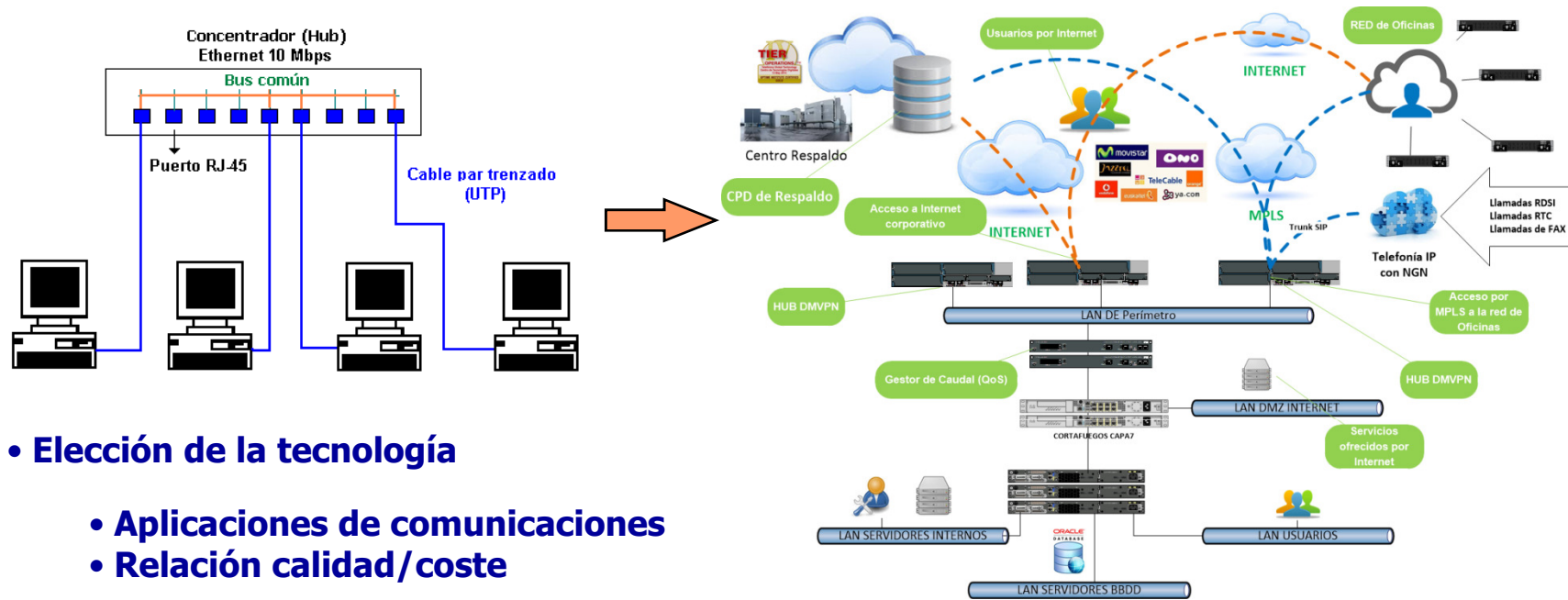
Conmutación de paquetes con datagramas



- Decisión del siguiente salto para cada paquete en cada nodo (dirección origen y destino en la cabecera del paquete)
- No existen caminos preestablecidos, poco control de la congestión
- Tolerancia a fallos
- Comunicación no fiable (control de errores en los extremos)

1.3 Diseño y planificación de redes de computadores

Topología de un red de computadores corporativa (organismo privado)



- Elección de la tecnología
 - Aplicaciones de comunicaciones
 - Relación calidad/coste
 - Planificación del direccionamiento
 - Tamaño de la red
 - Coste del encaminamiento
 - Seguridad
 - Autenticación
 - Autorización
 - Accountig (monitorización)
-
- Diagrama de una red de datos:
- En el centro: **CORTAFUEGOS CAPA7** (Rack de servidores).
 - Debajo: **ORACLE DATABASE** y **LAN SERVIDORES BBDD** (Servidor de base de datos).
 - A la izquierda: **LAN SERVIDORES INTERNOS** (Grupo de servidores).
 - A la derecha: **LAN USUARIOS** (Grupo de usuarios).
 - En la esquina superior derecha: **Servicios ofrecidos por Internet** (Recuadro verde).
- Calidad de servicio (QoS)
 - Reparto de la velocidad de transferencia
Servicio: web, ftp, pop3
Equipo

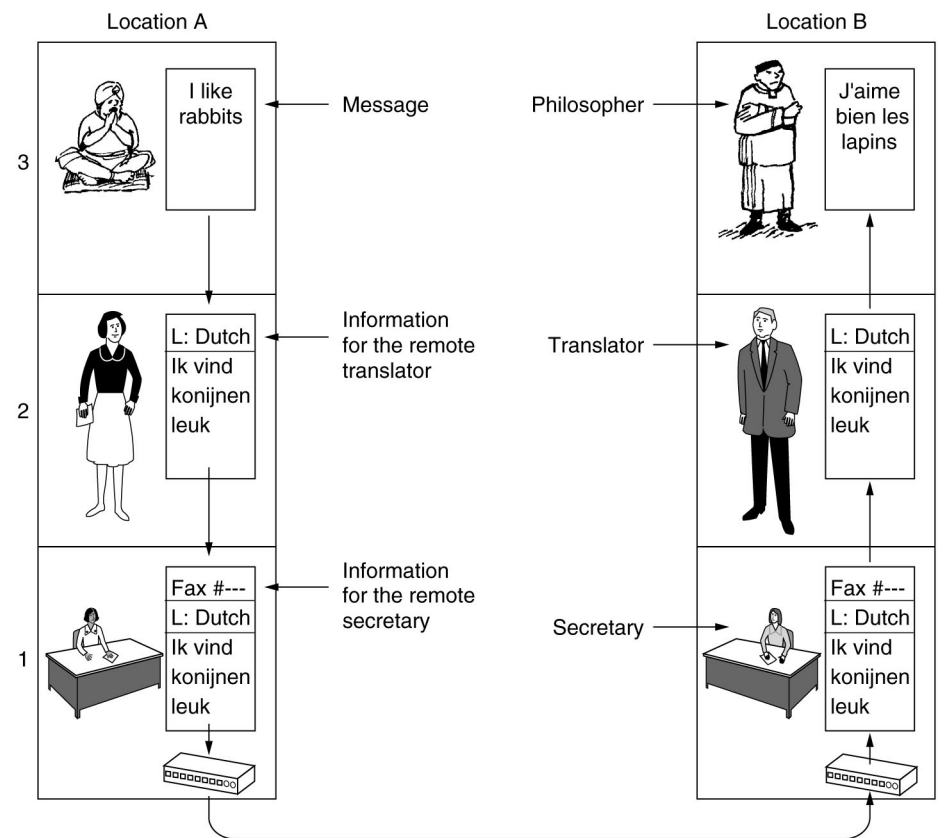
TEMA 2

ARQUITECTURA DE RED

2.1 Modelo de capas

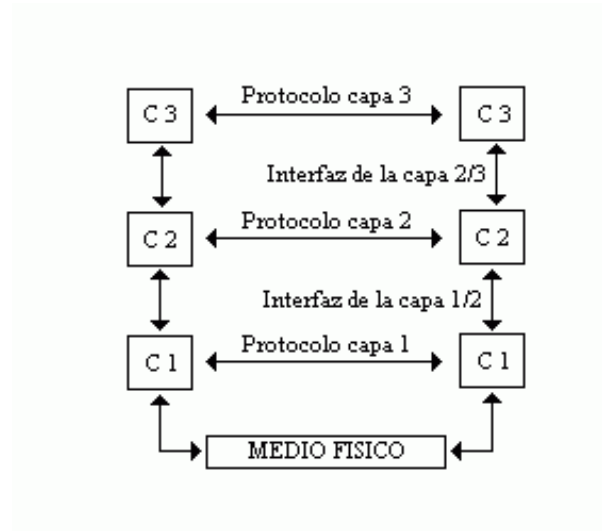
Arquitectura de red

Conjunto de protocolos perfectamente definidos e implementados que caracterizan cómo se realiza el intercambio de información en una red de comunicaciones



2.1 Modelo de capas

Modelo de capas



Capa o nivel de una arquitectura de red: Cada uno de los niveles de abstracción definidos en la comunicación.

Entidades pares: Las instancias de una capa en cada extremo de la comunicación.

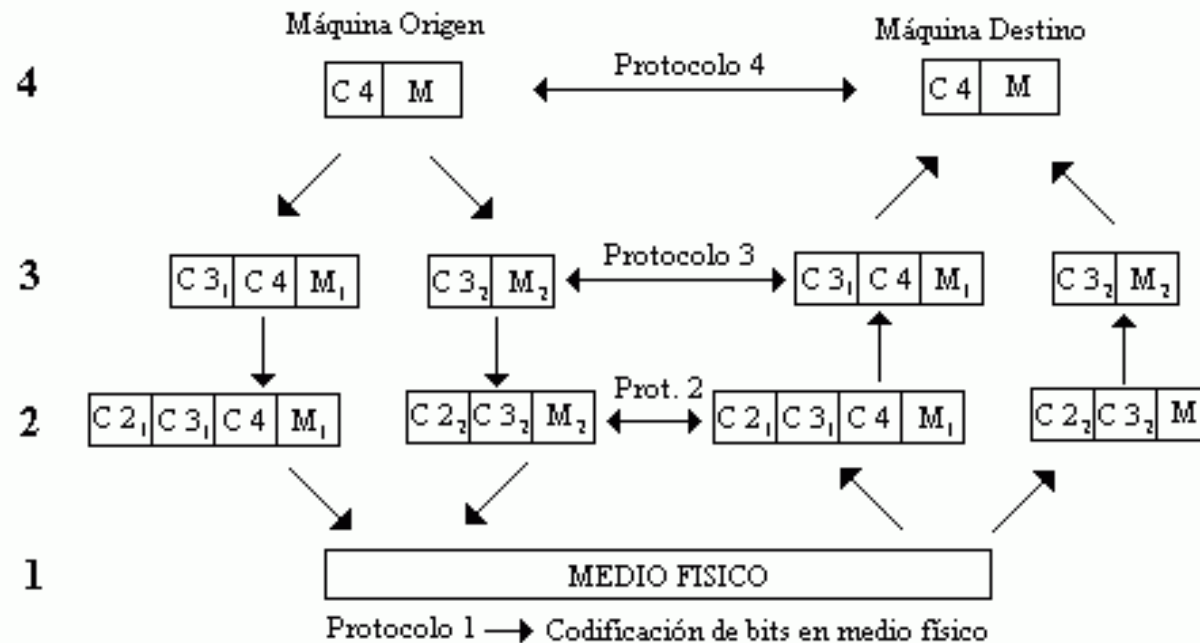
Protocolo: Conjunto de normas para la comunicación entre entidades pares

Servicios: Conjunto de funciones que una capa ofrece a su capa superior

Interfaz: Conjunto de normas para la comunicación entre capas adyacentes

2.1 Modelo de capas

Ejemplo de arquitectura de red



Protocolo 4: Definición del tipo de mensaje a intercambiar: e-mail, página web, fichero, etc.

Protocolo 3: Fragmentación del mensaje en trozos para evitar el retardo debido a errores.

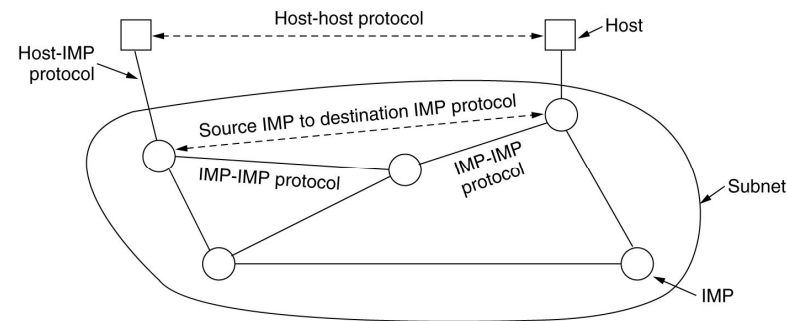
Protocolo 2: Identificación del destinatario del mensaje en la red.

Protocolo 1: Codificación de los bits en señales eléctricas.

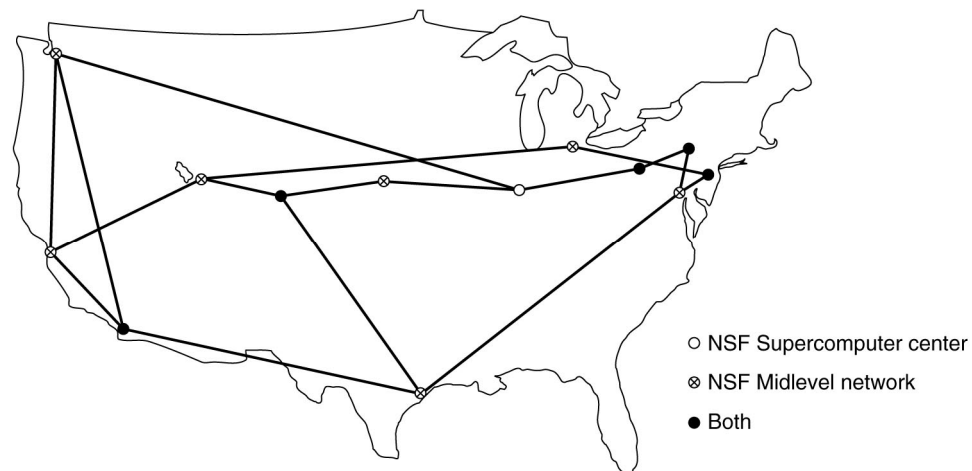
2.2 Modelo de Arquitectura TCP/IP (Internet)

El origen y desarrollo de Internet

Década de 1970: ARPANET. Red militar (DoD) en EEUU con objetivos de defensa.



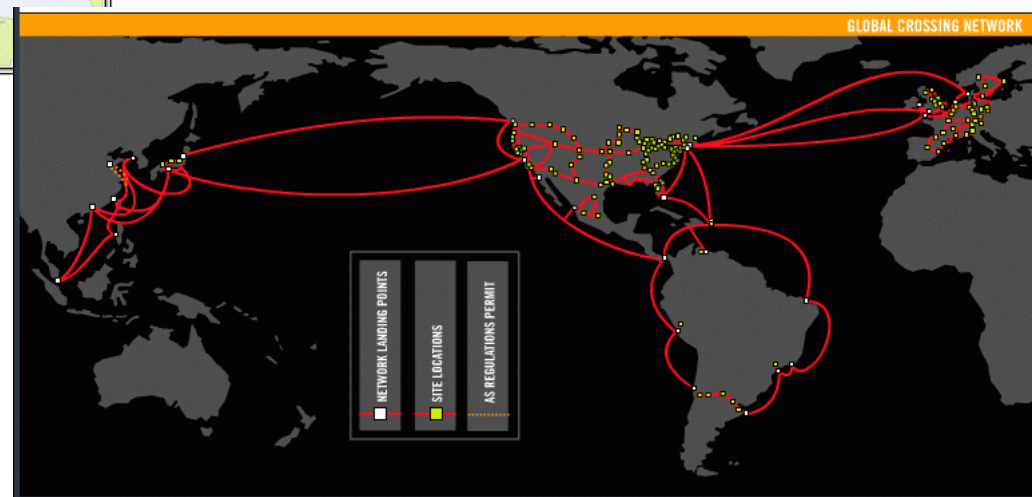
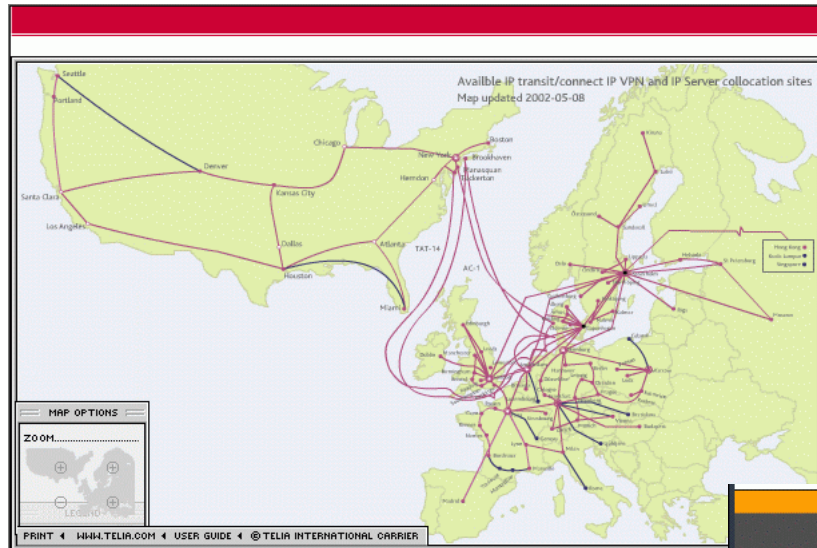
Década de 1980: ARPANET/MILNET. Separación en red de investigación y militar. Expansión de ARPANET en Universidades y centros de investigación EEUU y Europa. Unix de Berkeley.



2.2 Modelo de Arquitectura TCP/IP (Internet)

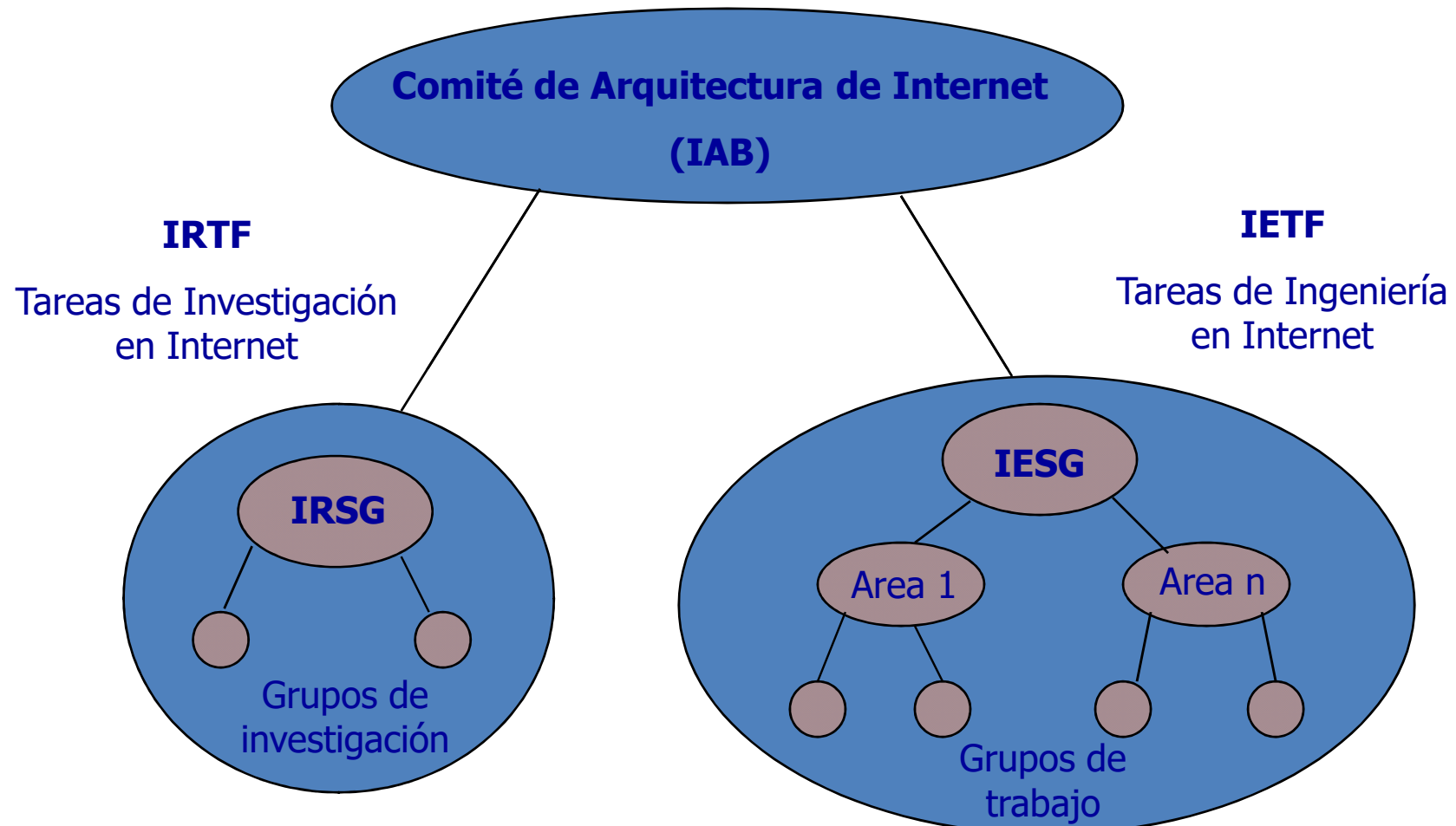
El origen y desarrollo de Internet

Década 1990: Expansión de ARPANET en empresas de todo el mundo: conexión a Internet o adopción de protocolos de Internet.



El origen y desarrollo de Internet

Estructura organizativa en Internet

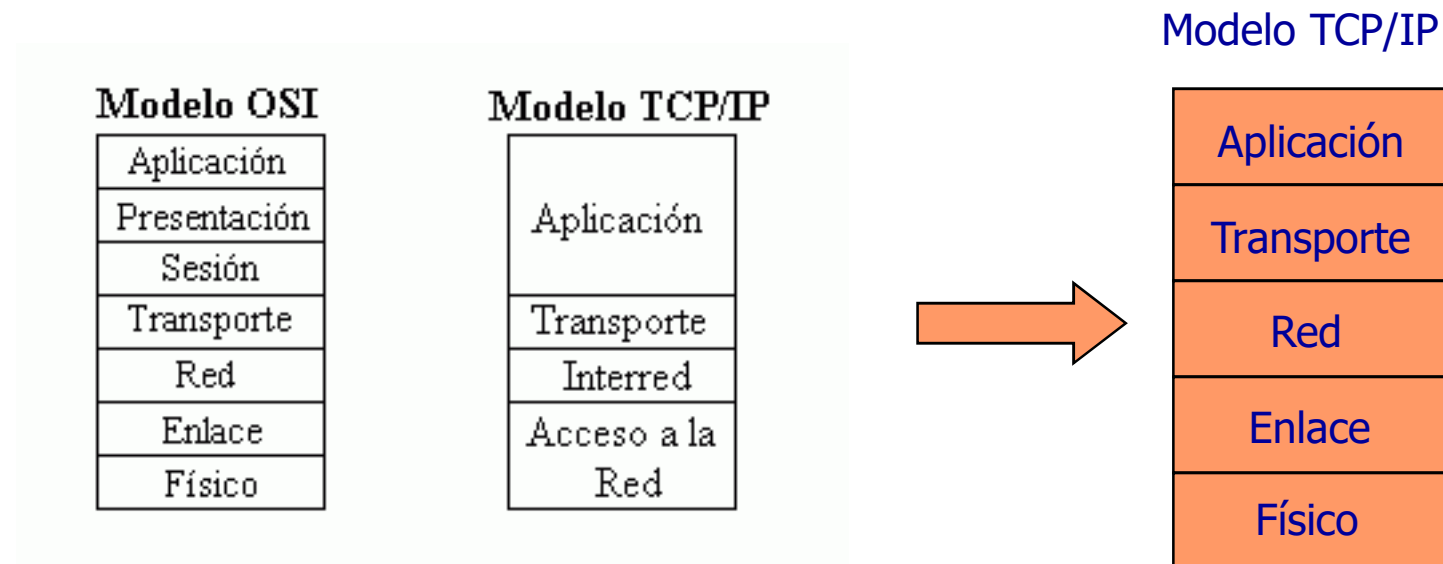


RFC: Request for comments

2.2 Modelo de Arquitectura TCP/IP (Internet)

Modelo de capas de TCP/IP

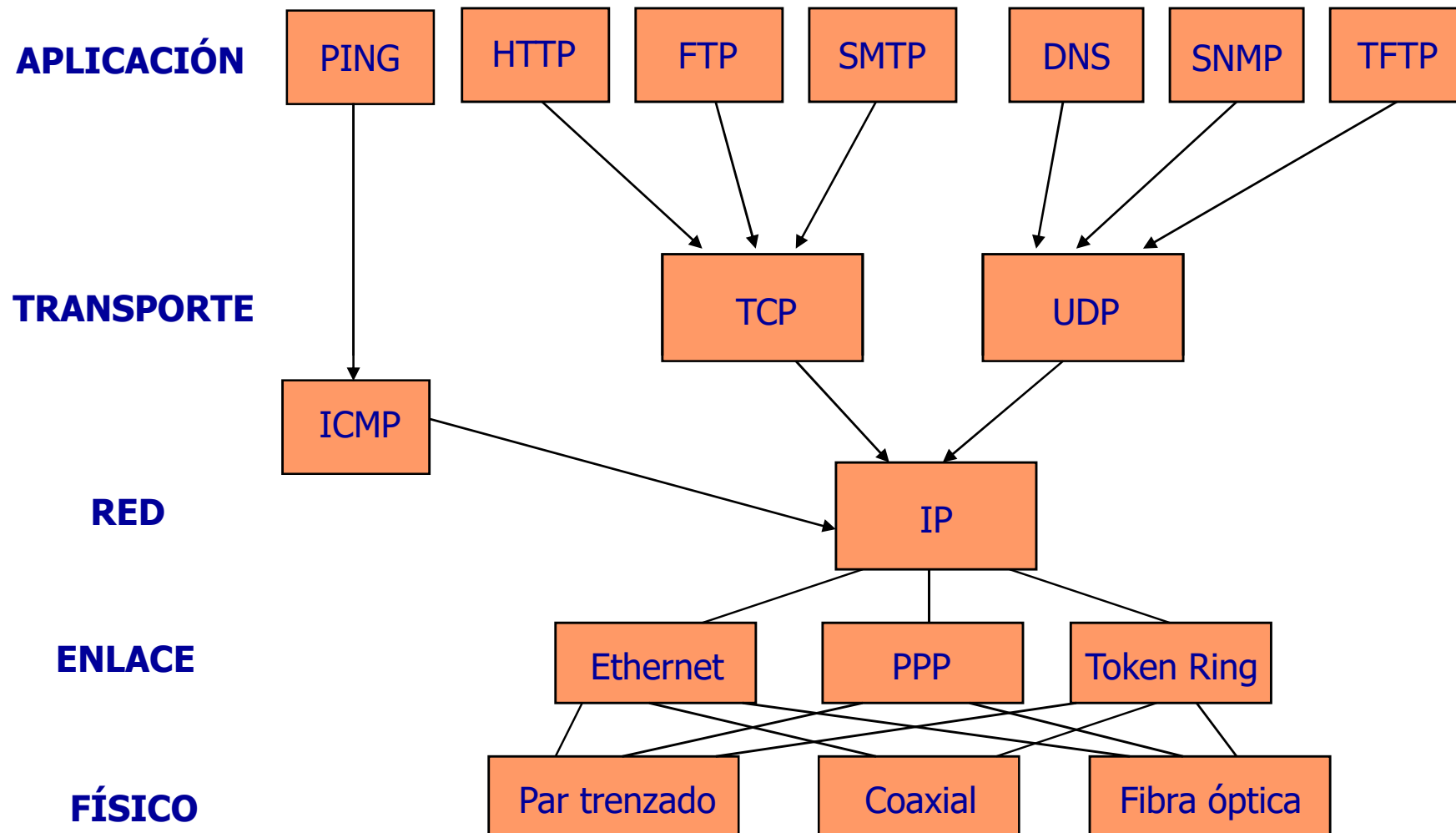
Aplicación	Capa de aplicación: Define el conjunto de aplicaciones que ofrece Internet para la comunicación.
Transporte	Capa de transporte: Permite el control de la comunicación extremo a extremo en Internet.
Interred (Red)	Capa de interred (red): Permite el encaminamiento de paquetes de información entre dos equipos de la red.
Acceso a la red	Capa de acceso al medio: Permite el envío de un paquete procedente de la capa de red (paquete IP) a través de un medio físico de comunicación



2.2 Modelo de Arquitectura TCP/IP (Internet)

Modelo de capas de TCP/IP

Protocolos de la arquitectura TCP/IP



2.2 Modelo de Arquitectura TCP/IP (Internet)

Modelo de capas de TCP/IP

Capa Física

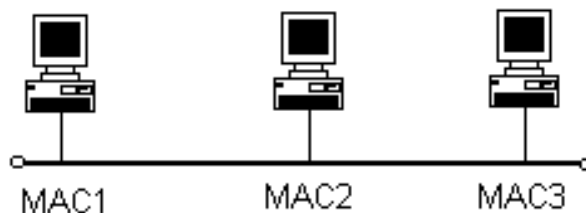
- Especificación de los medios físicos empleados en la comunicación
- Especificación de la señalización de la información en el medio físico

Ejemplo: cables pares trenzados, cable coaxial, fibra óptica

Capa de Enlace

- Especificación de los mecanismos para el intercambio de información en un medio físico

Ejemplo: Ethernet



2.2 Modelo de Arquitectura TCP/IP (Internet)

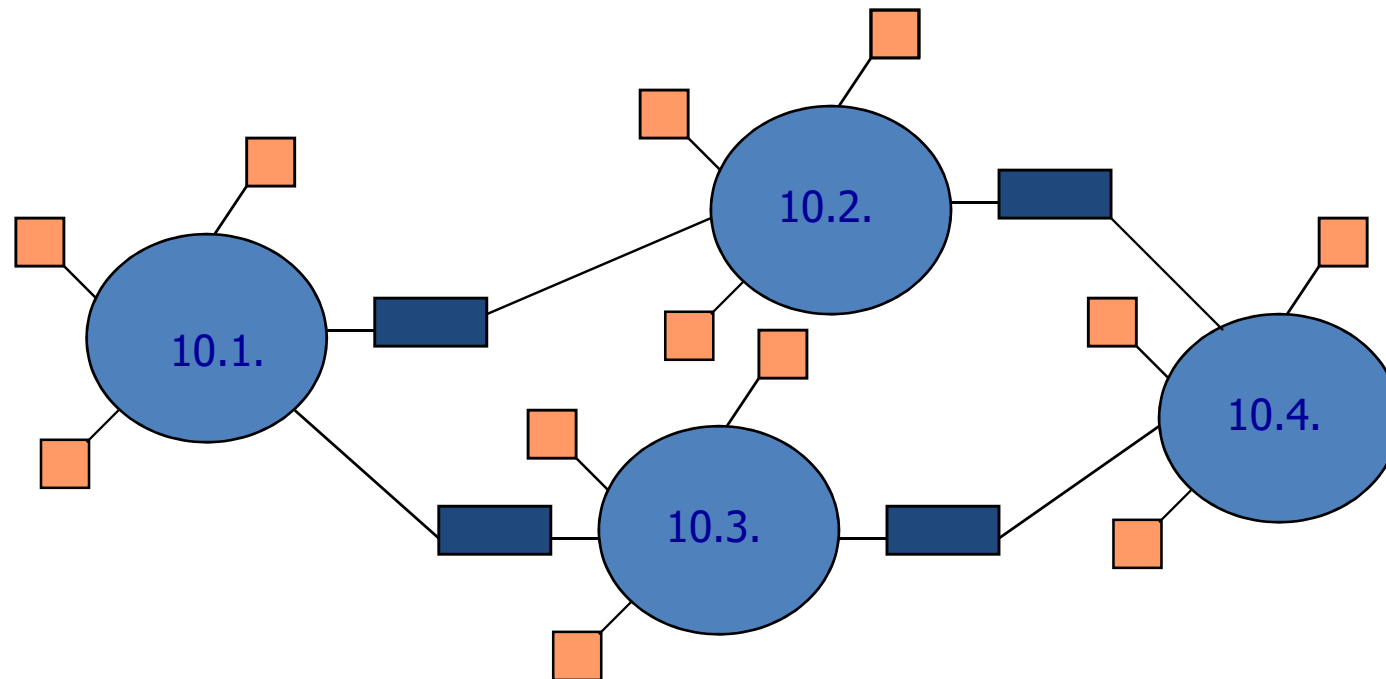
Modelo de capas de TCP/IP

Capa de red. Protocolo IP

- Identificación de equipos en una red formada por la interconexión de redes (Internet)
- Encaminamiento de paquetes en la red (Internet)

Direccionamiento IP

- Identificador de 32 bits \longrightarrow X . X . X . X \longrightarrow 0-255 . 0-255 . 0-255 . 0-255



2.2 Modelo de Arquitectura TCP/IP (Internet)

Modelo de capas de TCP/IP

- Dirección IP 192.168.17.23

¿ Identificador de red ?  Máscara de red de una red IP

Valor de 32 bits (X.X.X.X)  11111111..1000000000000000

Máscara de red = 255.255.255.0  192.168.17.23 pertenece a la red 192.168.17.

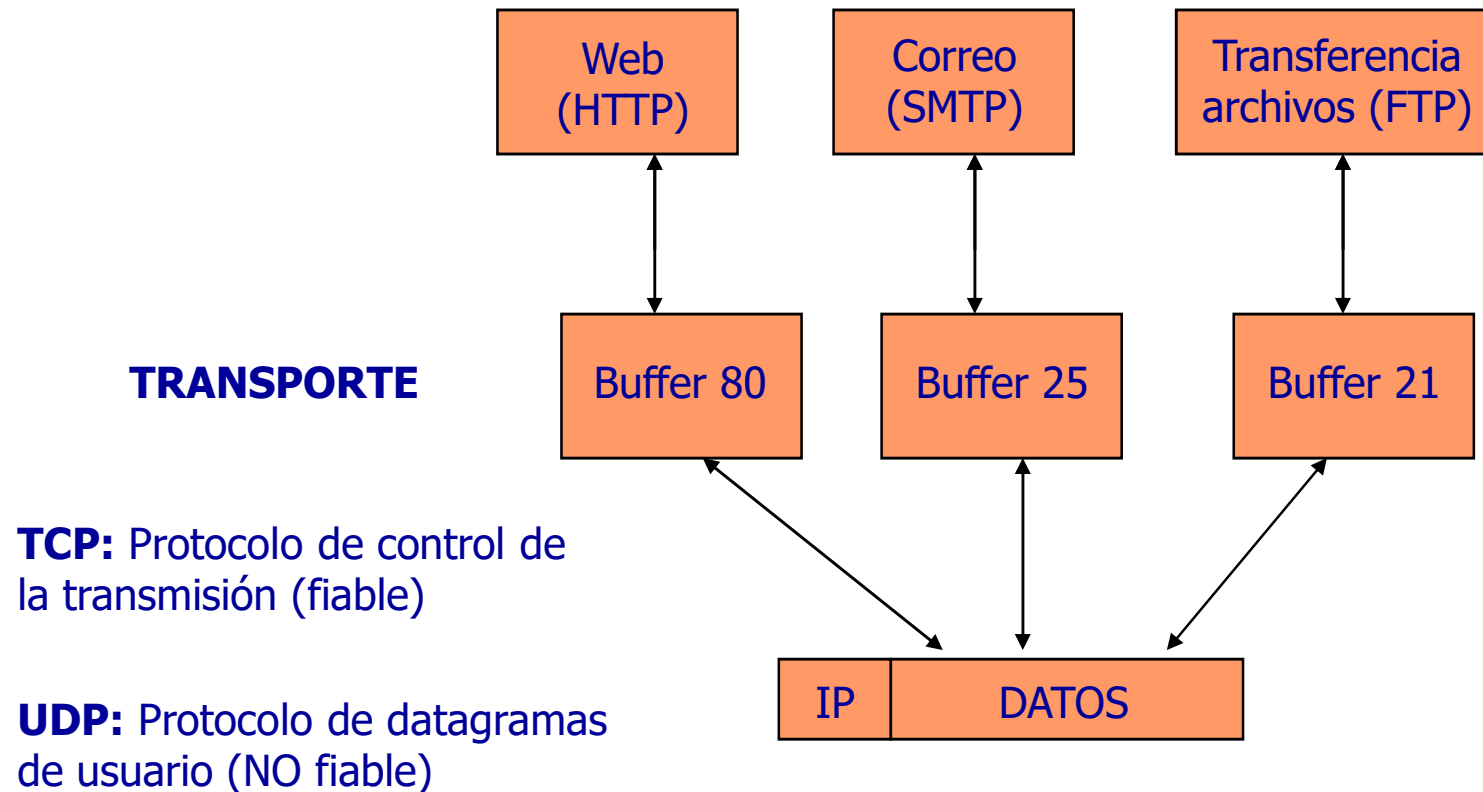
192.168.17.	{	192.168.17.0	Dirección de red
		192.168.17.1	
		192.168.17.2	
		
		
		192.168.17.255	Dirección de broadcast

2.2 Modelo de Arquitectura TCP/IP (Internet)

Modelo de capas de TCP/IP

Capa de transporte. Protocolos TCP y UDP

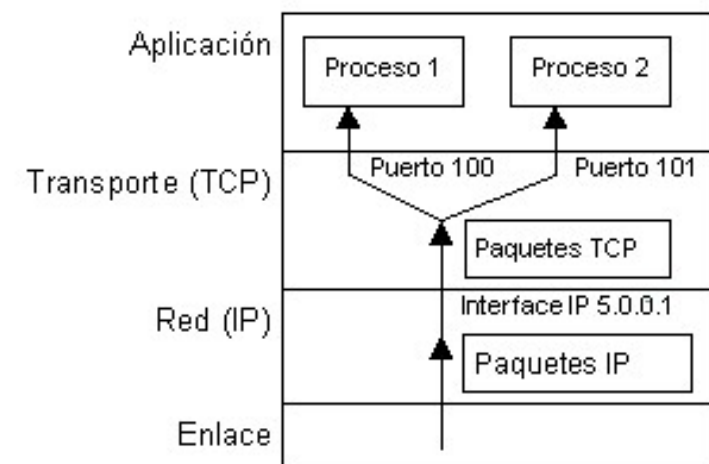
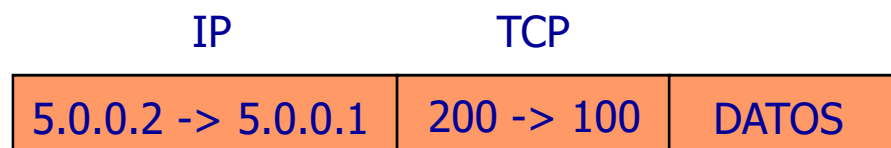
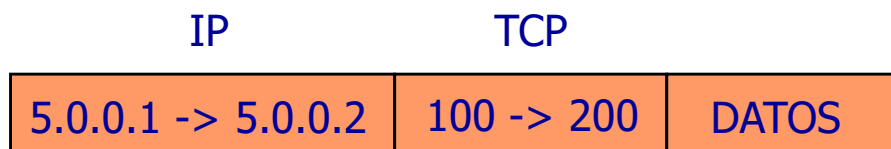
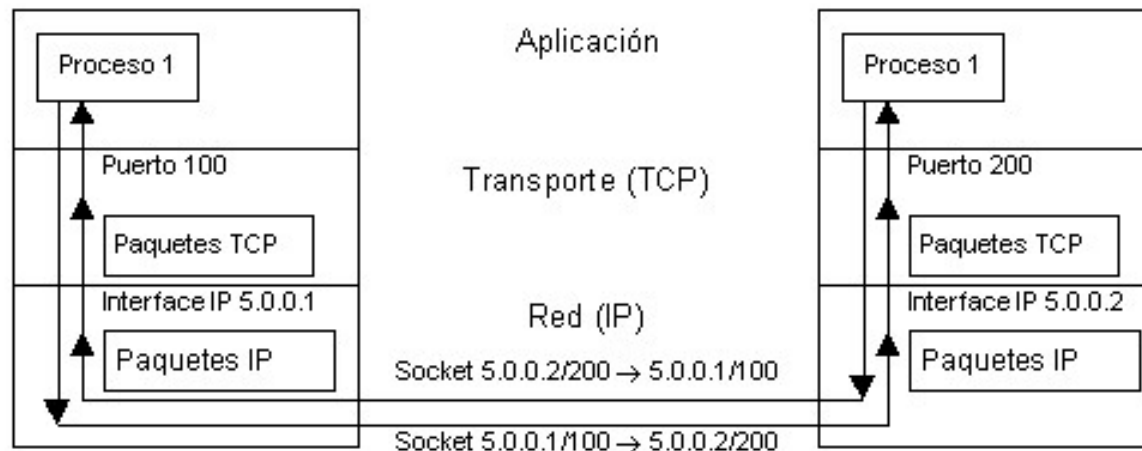
- Interfaz entre la capa de aplicación y red para la gestión de comunicaciones extremo a extremo (conexiones) entre equipos de Internet.



2.2 Modelo de Arquitectura TCP/IP (Internet)

Modelo de capas de TCP/IP

Gestión de conexiones. Sockets



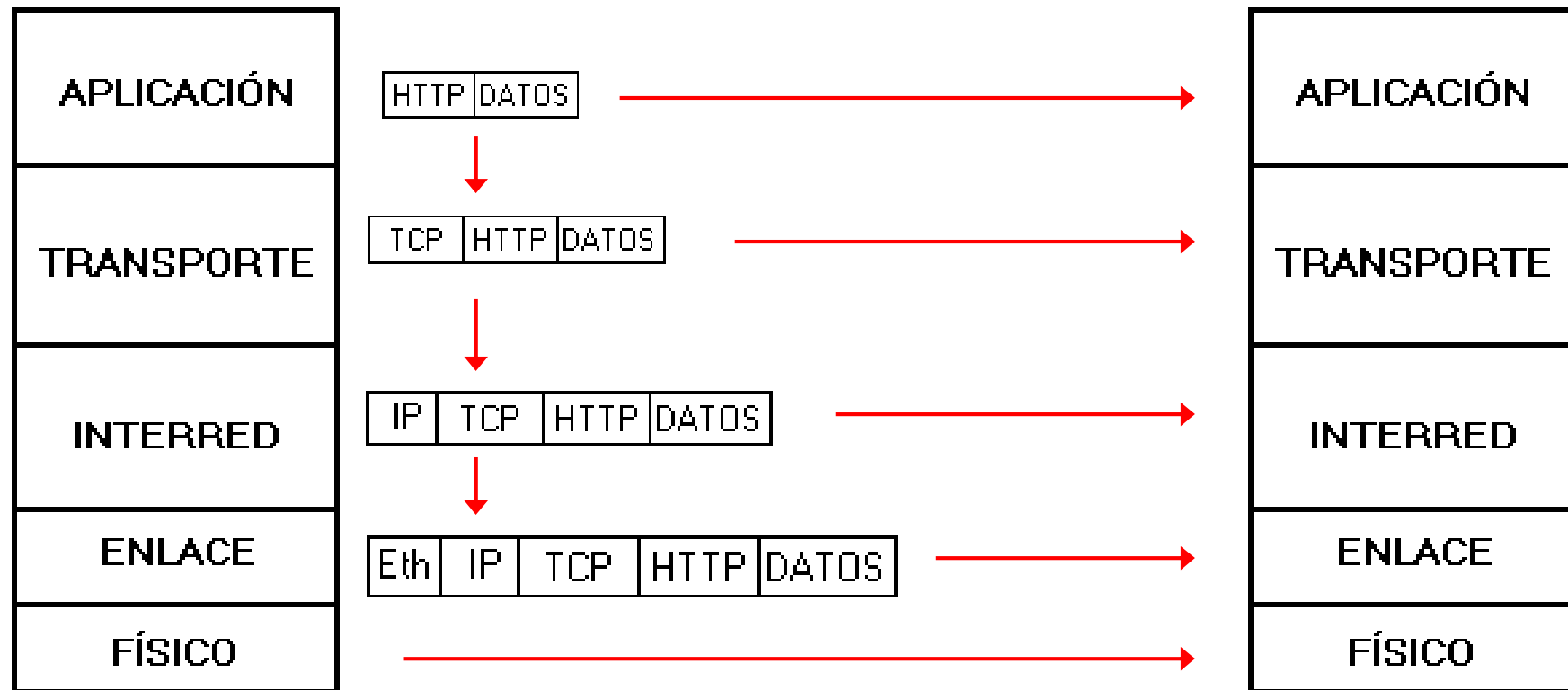
2.2 Modelo de Arquitectura TCP/IP (Internet)

Modelo de capas de TCP/IP

Capa de aplicación. Protocolo HTTP

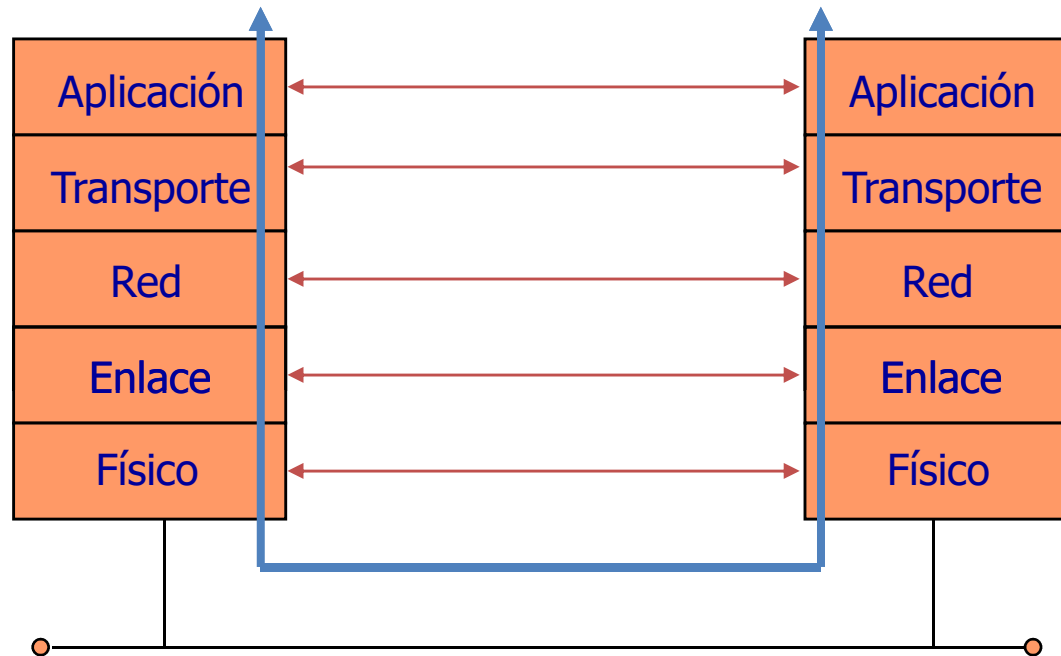
Cliente navegador

Servidor web



2.3 Interconexión de redes

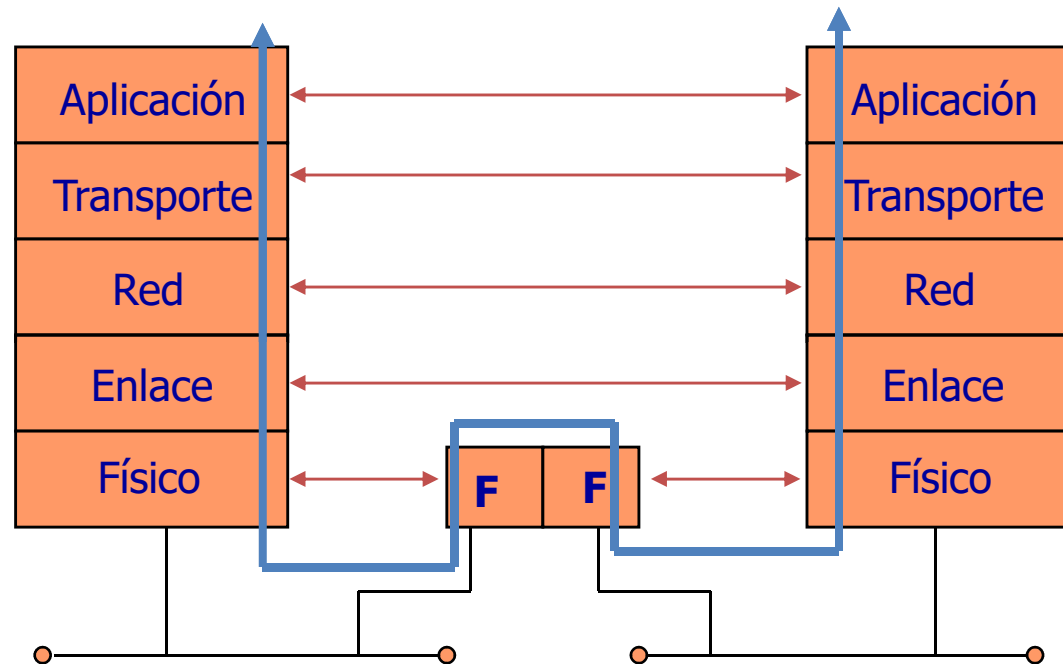
Modelo de comunicación entre capas en una red



En base a este modelo de comunicación, se puede estudiar la necesidad de diferentes tipos de dispositivos para interconectar diferentes segmentos físicos de red.

2.3 Interconexión de redes

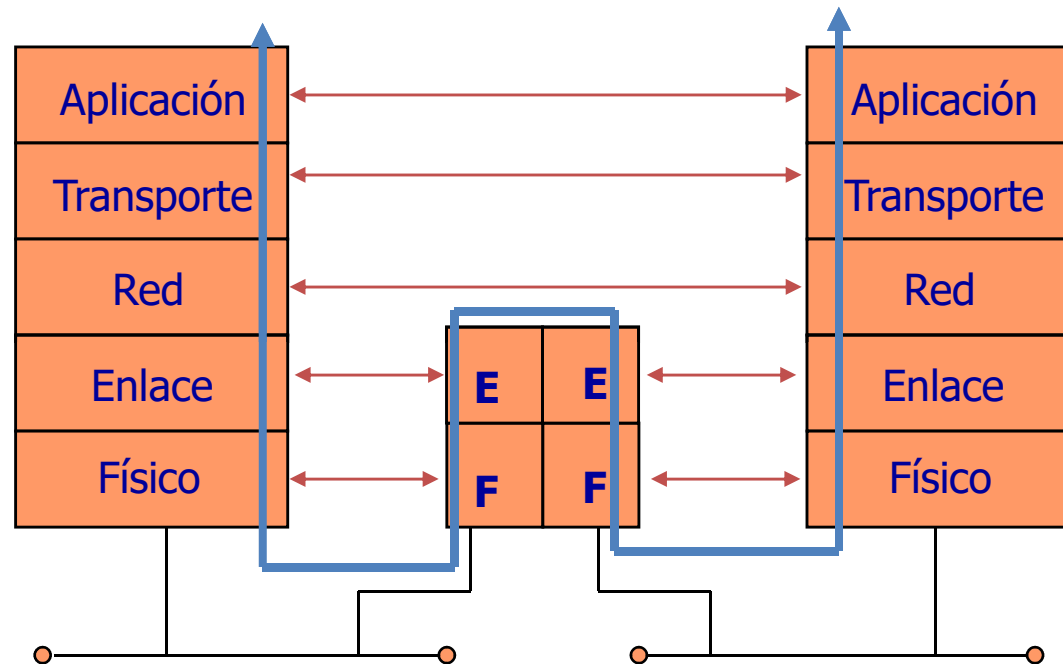
Interconexión de redes a nivel físico. Repetidor (Repeater)



Dispositivo sencillo y económico que proporciona muy poco rendimiento y situaciones de colisiones permanentes.

2.3 Interconexión de redes

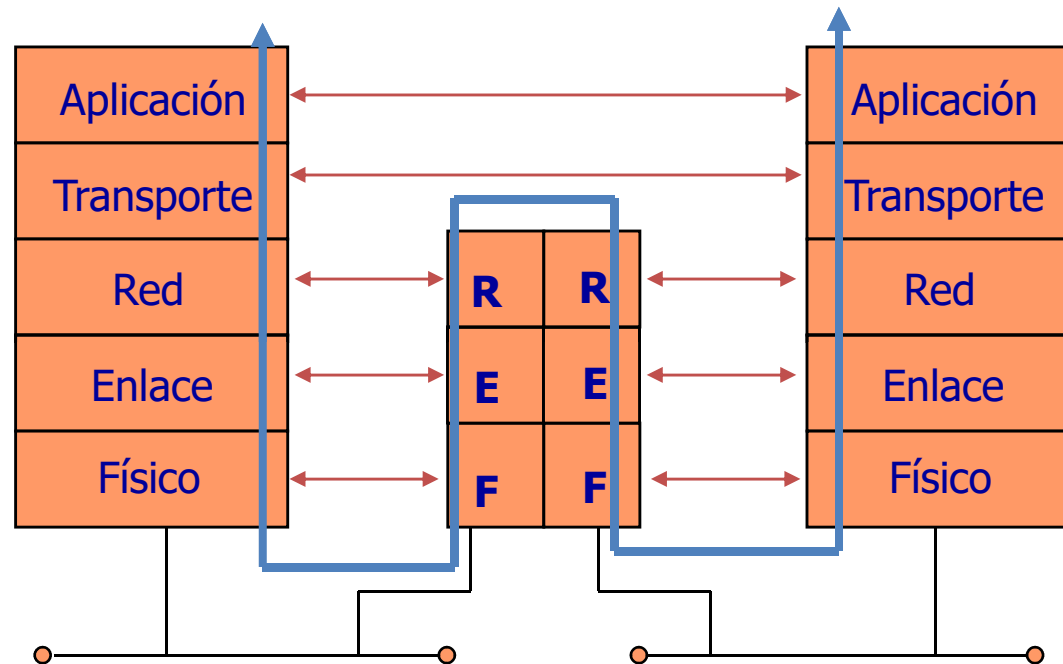
Interconexión de redes a nivel de enlace. Puente (Bridge)



Dispositivo que presenta un buen rendimiento al evitar transmisiones innecesarias. Limitado en cuanto a los tipos de redes a interconectar.

2.3 Interconexión de redes

Interconexión de redes a nivel de red. Encaminador (Router)



Dispositivo con rendimiento de interconexión menor que los puentes, pero aplicable para la interconexión de cualesquiera segmentos de red que soporten un protocolo de red común (IP).

2.4 Modelado de protocolos. Máquinas de estado finito (MEF)

Especificación de un protocolo

Definición: Conjunto de reglas de utilización de las primitivas de servicio suministradas por el nivel inferior para la comunicación a nivel horizontal

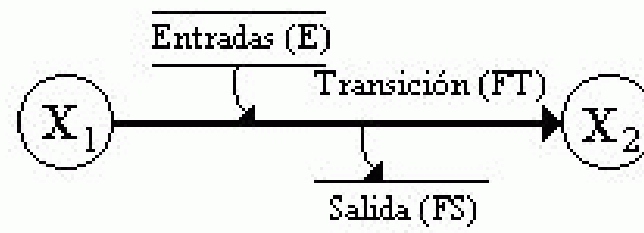
Elementos de una máquina de estado finito

Estados: Descripción de las situaciones de funcionamiento del protocolo

Entradas: Eventos que provocan cambios en el estado del protocolo

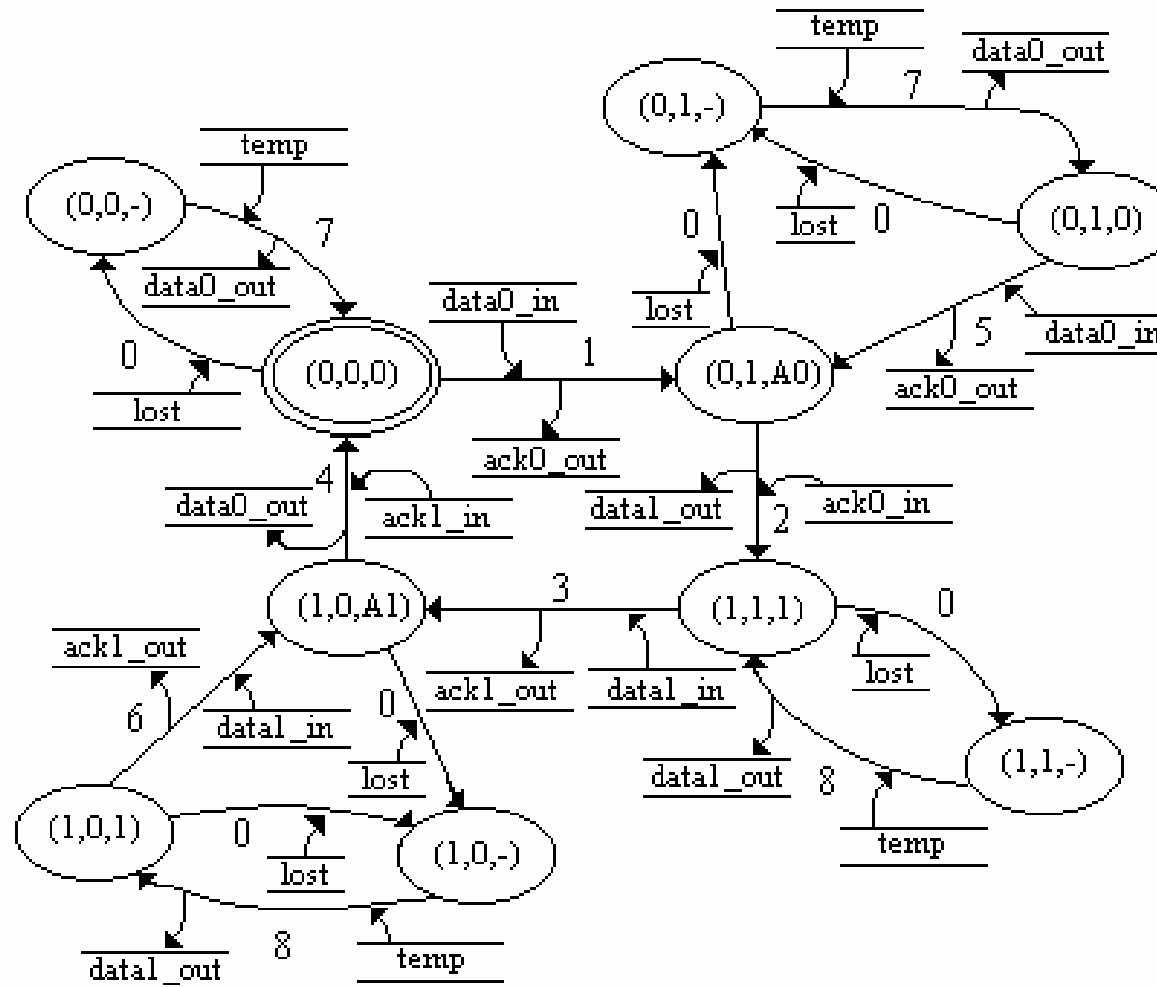
Salidas: Acciones como consecuencia de cambios en el estado del protocolo

Transición: Proceso por el cual un protocolo cambia de un estado de funcionamiento a otro.



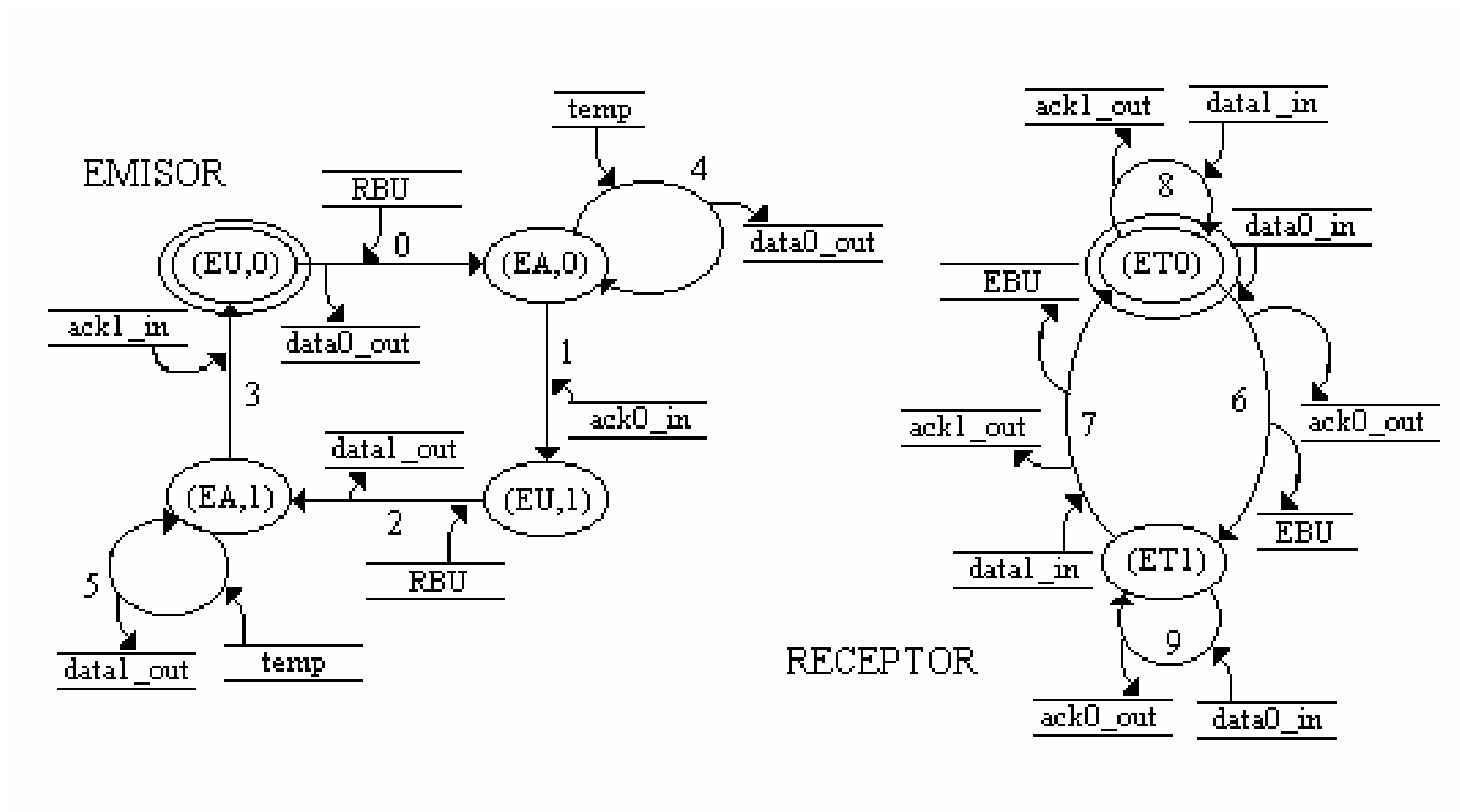
2.4 Modelado de protocolos. Máquinas de estado finito (MEF)

Ejemplo de protocolo: Protocolo unilateral de parada y espera



2.4 Modelado de protocolos. Máquinas de estado finito (MEF)

Ejemplo de protocolo: Protocolo bilateral de parada y espera



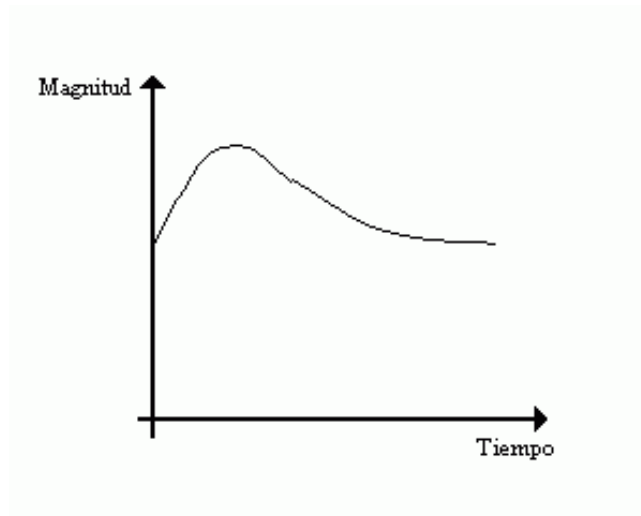
TEMA 3

NIVEL FÍSICO

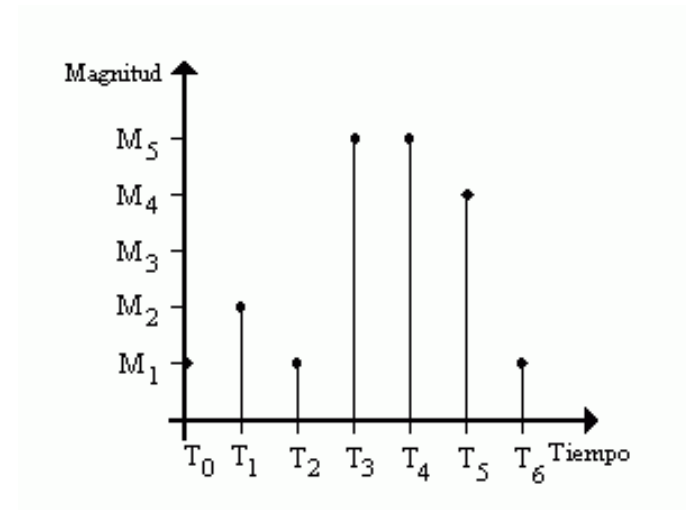
3.2 Transmisión de una señal de datos.

Tipos de señales

Señal analógica



Señal digital



3.2 Transmisión de una señal de datos.

Análisis de señales con series de Fourier

$$f(t) = a_0 + \sum_{n=1}^{\infty} a_n \cdot \cos(2\pi n f_0 t) + \sum_{n=1}^{\infty} b_n \cdot \sin(2\pi n f_0 t)$$

$T = \text{Periodo de la señal } f(t)$
 $f_0 = \frac{1}{T} = \text{Frecuencia de la señal } f(t)$

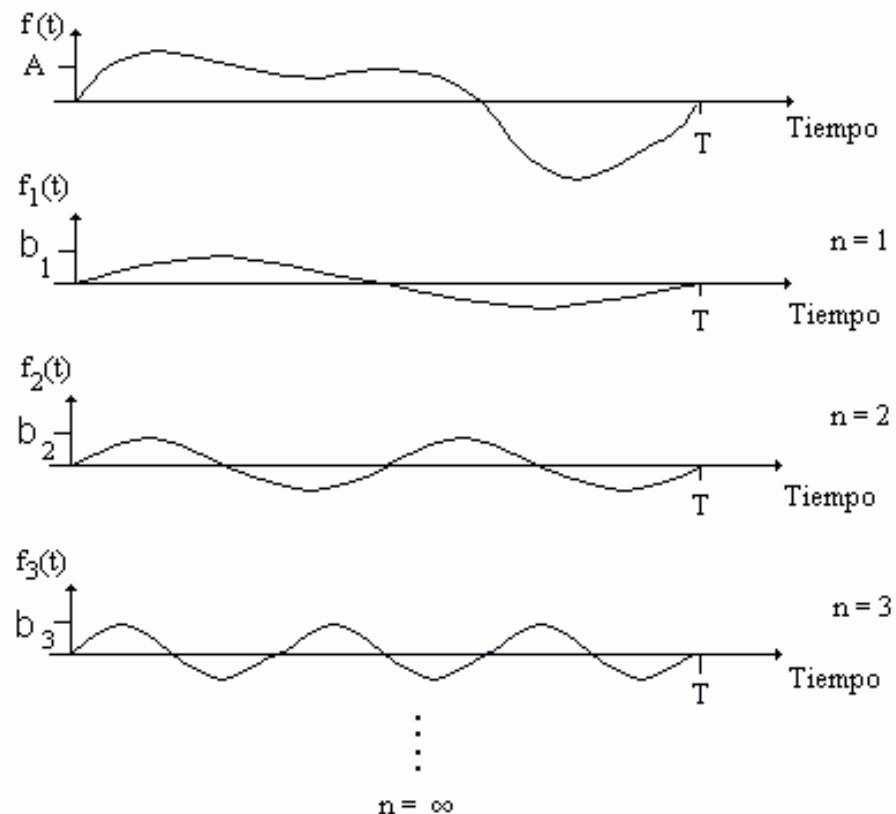
$$a_n = \frac{2}{T} \int_0^T f(t) \cos(2\pi n f_0 t) dt \quad n = 1, 2, 3, \dots$$

$$b_n = \frac{2}{T} \int_0^T f(t) \sin(2\pi n f_0 t) dt \quad n = 1, 2, 3, \dots$$

Armónico de orden n :

Par de funciones cos y sen
de frecuencias $n f_0$ y
amplitudes a_n y b_n .

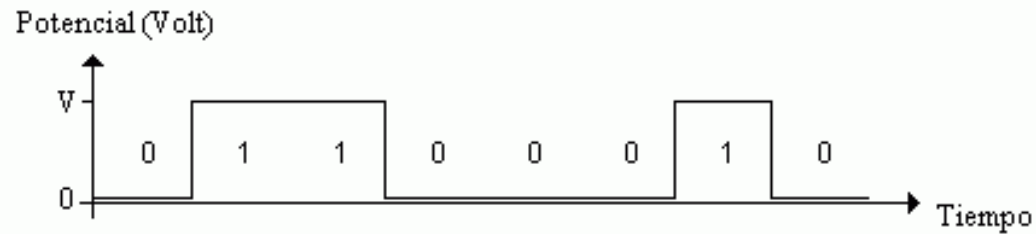
Una señal está compuesta por
la suma de infinitos armónicos.



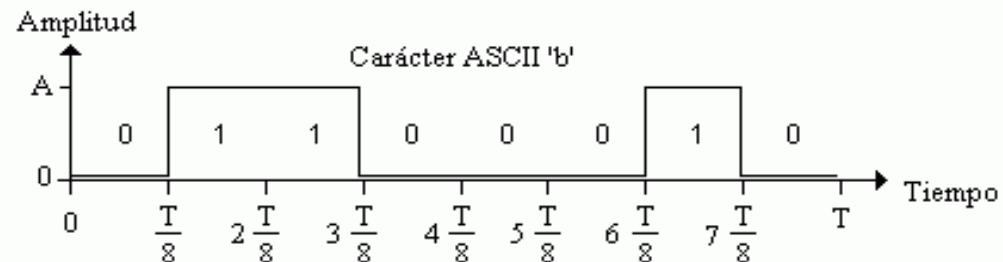
3.2 Transmisión de una señal de datos.

Análisis de señales con series de Fourier

Señal analógica de pulsos



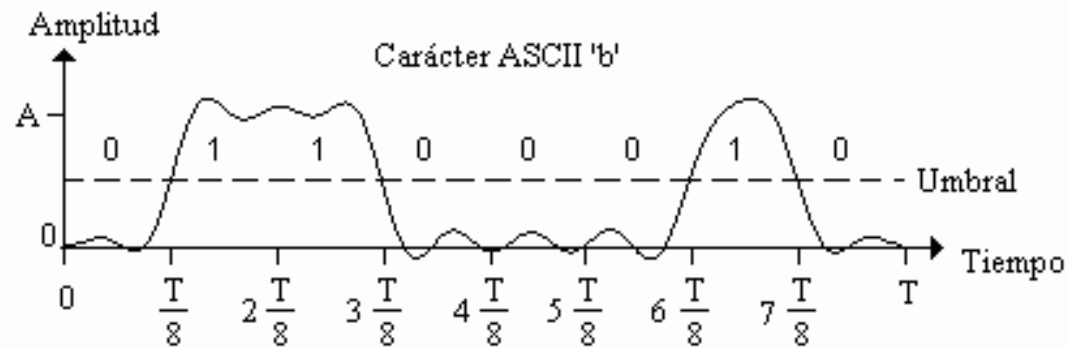
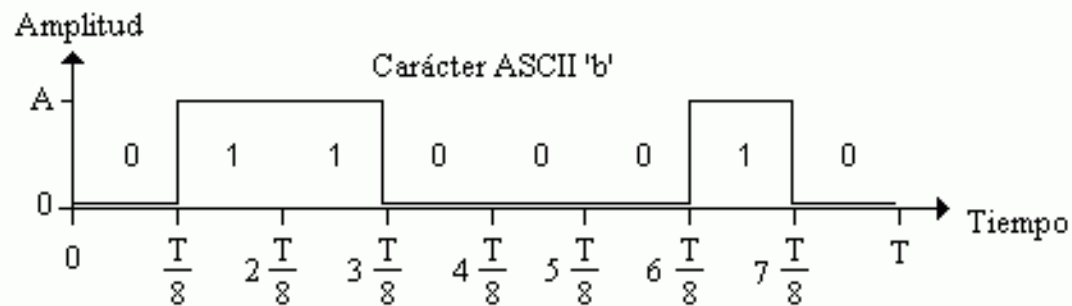
Señal periódica asociada a la transmisión secuencial de un carácter ASCII



3.2 Transmisión de una señal de datos.

Análisis de señales con series de Fourier

Reconstrucción de la señal empleando los 10 primeros armónicos



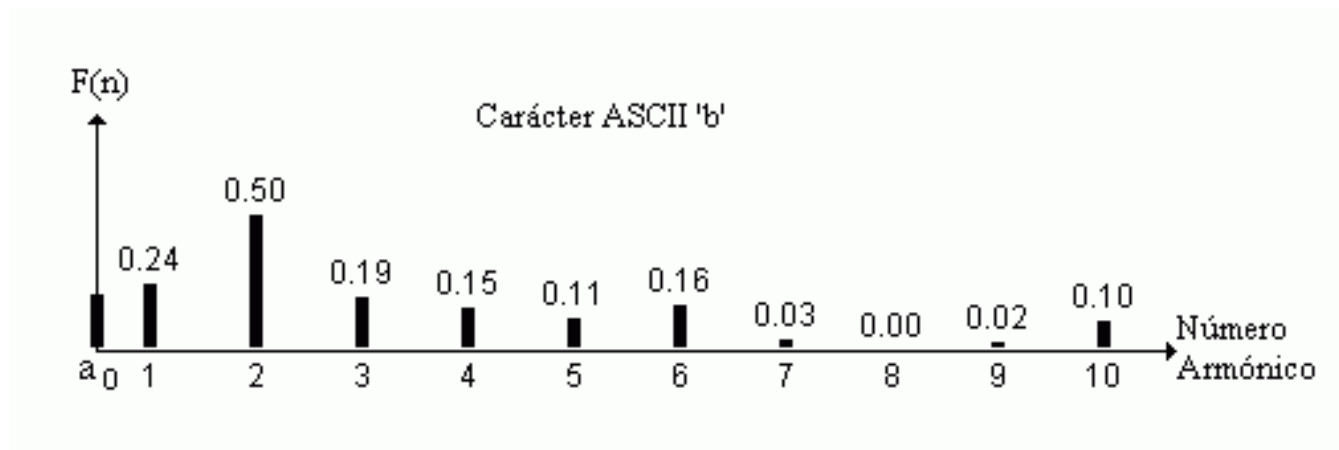
3.2 Transmisión de una señal de datos.

Análisis de señales con series de Fourier

Espectro de potencia de una señal

$$F_n = \sqrt{a_n^2 + b_n^2}$$

Valor medio de la contribución en amplitud de un armónico a la reconstrucción de la señal



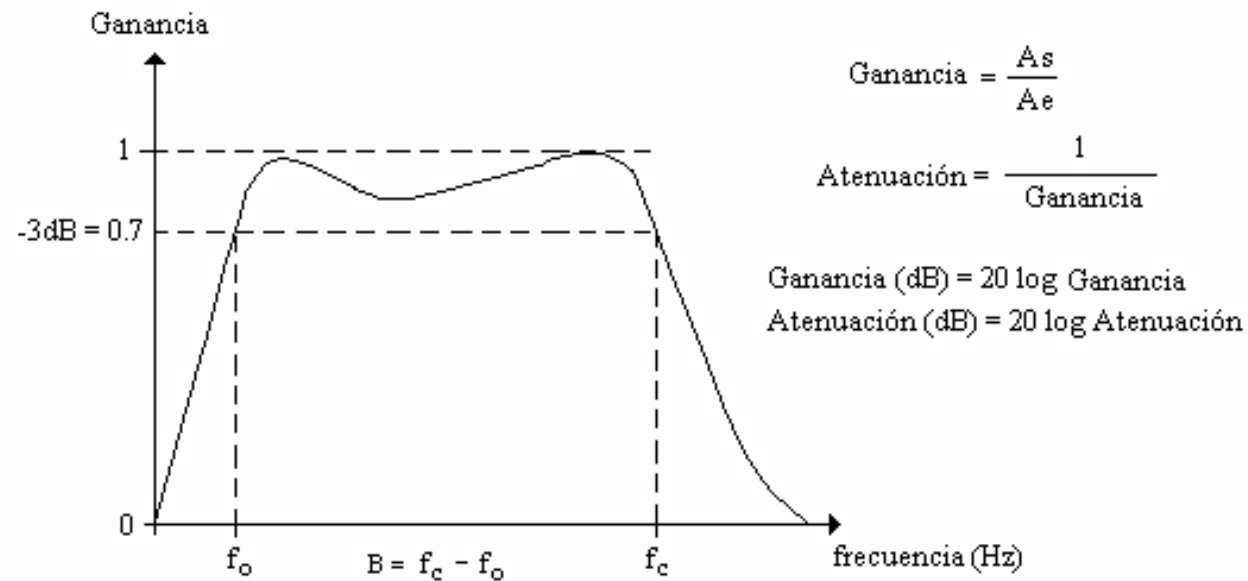
3.2 Transmisión de una señal de datos.

Ancho de banda de un medio físico (B)

Un medio físico es capaz de transmitir los armónicos o componentes frecuenciales de una señal que tengan una frecuencia dentro de un rango determinado.

$$B = f_c - f_0 \text{ Hz (Hertzios)}$$

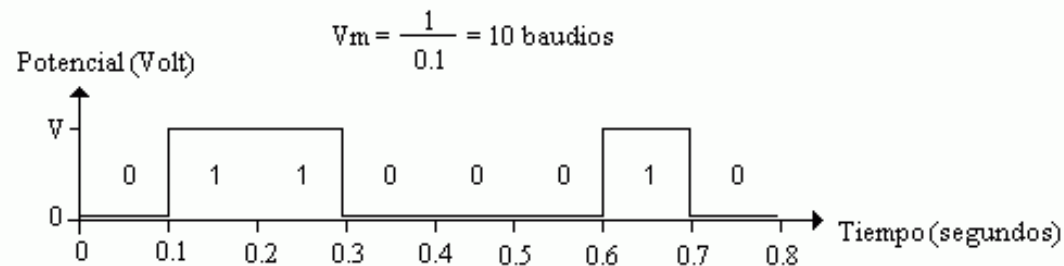
Simulador



3.2 Transmisión de una señal de datos.

Velocidad de modulación (V_m)

Número de veces por unidad de tiempo que la magnitud física de una señal puede variar su valor. Unidad de velocidad de modulación: baudio (bd)



$$v_t = \frac{8 \text{ bits}}{0.8 \text{ seg}} = 10 \text{ bps}$$

Velocidad de transmisión en un medio físico (V_t)

Número de bits transmitidos por unidad de tiempo en un medio físico.

Unidad de V_t : bps (bits por segundo)

1000 bps \Leftrightarrow 1 Kbps

1000 Kbps \Leftrightarrow 1 Mbps

1000 Mbps \Leftrightarrow 1 Gbps

Unidad de V_t : Bps (bytes por segundo)

1024 Bps \Leftrightarrow 1 KBps

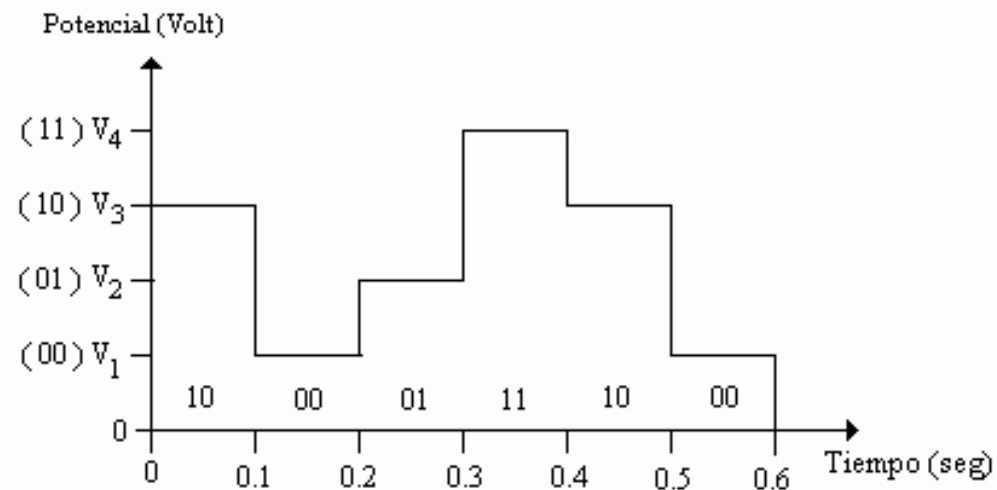
1024 KBps \Leftrightarrow 1 MBps

1024 MBps \Leftrightarrow 1 GBps

3.2 Transmisión de una señal de datos.

Relación entre V_t y V_m

$$V_t = V_m \cdot \log_2 n \quad n = \text{número de niveles de la señal de pulsos}$$



$$V_t = \frac{12 \text{ bits}}{0.6 \text{ seg}} = 20 \text{ bps} \quad V_t = \frac{1 \text{ cambio}}{0.1 \text{ seg}} \log_2 4 = 20 \text{ bps}$$

3.2 Transmisión de una señal de datos.

Relación entre B, Vt y número de armónicos transmitidos en un medio

Sea n el número de armónicos de una señal que son transmitidos por un medio, f_0 la frecuencia fundamental de la señal periódica transmitida y B el ancho de banda del medio. Entonces,

$$n \cdot f_0 \leq B \quad (1)$$

Si se transmite una señal periódica consistente en la repetición de 8 bits en un tiempo de T segundos, entonces

$$V_t = \frac{8}{T} = 8 \frac{1}{T} = 8f_0 \text{ bps} \quad \text{luego} \quad f_0 = \frac{V_t}{8} \text{ Hz} \quad (2)$$

Sustituyendo (2) en (1) obtenemos:

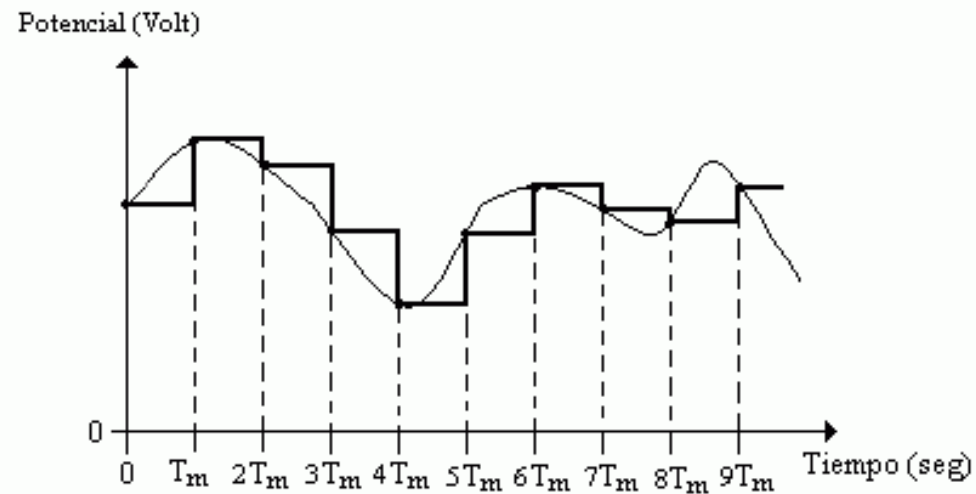
$$n \cdot \frac{V_t}{8} \leq B$$

Simulador

3.2 Transmisión de una señal de datos.

Teorema de Nyquist

Reconstrucción de señales empleando un muestreador

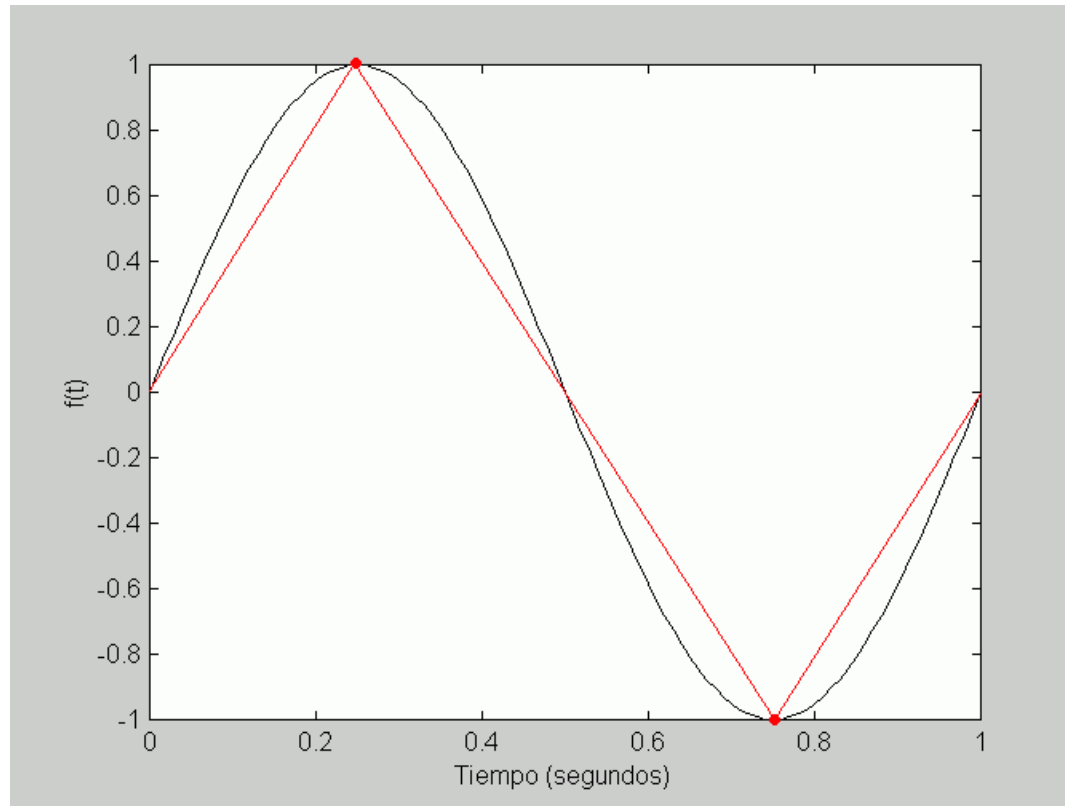


$$\begin{aligned} f_m &= \text{frecuencia de muestreo} \\ T_m &= \text{periodo de muestreo} \end{aligned} \quad f_m = \frac{1}{T_m}$$

3.2 Transmisión de una señal de datos.

Teorema de Nyquist

Representación de la función $f(t) = A \cdot \sin(2\pi t)$ donde $A=1$ y $T= 1$ seg ($f_0 = 1$ Hz)



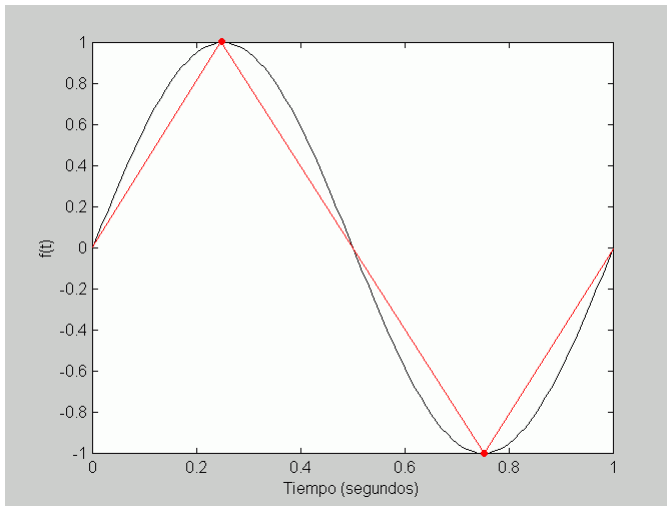
Para recuperar una función seno (o coseno) se necesitan como mínimo dos puntos en cada periodo de la señal. Luego $T_m = 0.5$ segundos y $f_m = 2 \text{ Hz} = 2 f_0$.

3.2 Transmisión de una señal de datos.

Teorema de Nyquist

Si un medio físico tienen un ancho de banda B , entonces es cierto que:

La frecuencia del armónico de mayor frecuencia de la señal transmitido por el medio físico tendrá una frecuencia de B Hz



$$f_m = 2B \text{ Hz}$$

La velocidad de modulación para una señal de pulsos es el número de veces por unidad de tiempo en que se detectan cambios.

$$V_{m(max)} = \frac{1}{T_m} = f_m = 2B \text{ baudios}$$

Ejemplo: Transmisión de pulsos en RTC

$$B = 4000 \text{ Hz} \Rightarrow$$

$$V_{t(max)} = 2 \cdot 4000 \cdot \log_2 2 = 8000 \text{ bps}$$

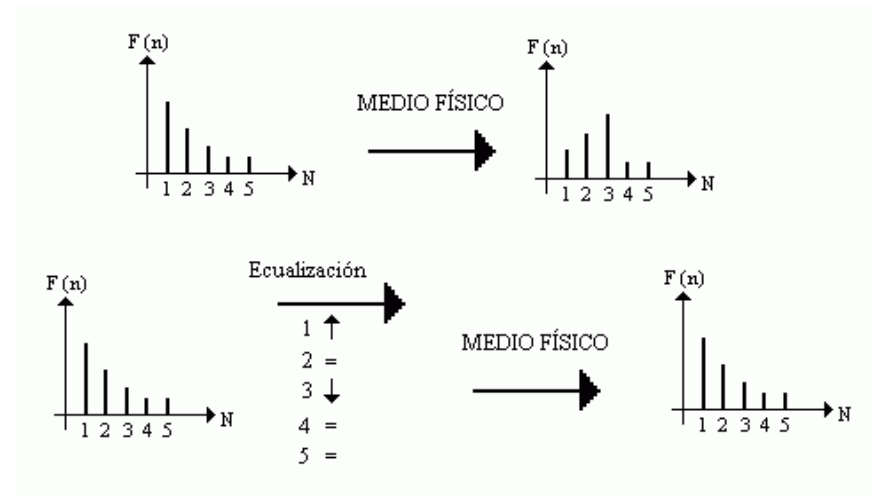
$$V_{t(max)} = V_m \log_2 n = 2B \log_2 n \text{ bps} \quad \longrightarrow$$

n = Número de niveles de la señal

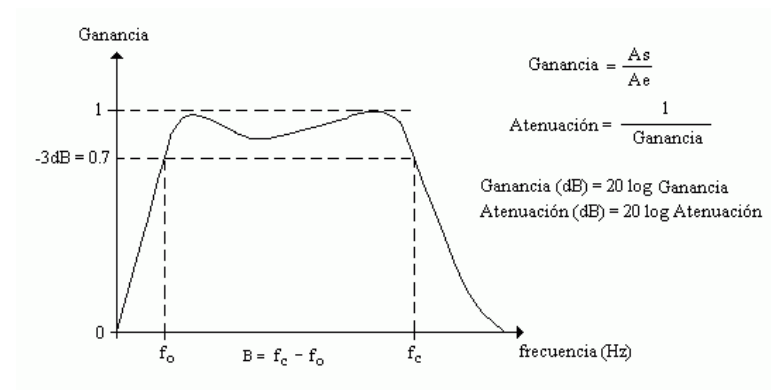
3.2 Transmisión de una señal de datos.

Distorsión en el medio de transmisión

1. Atenuación



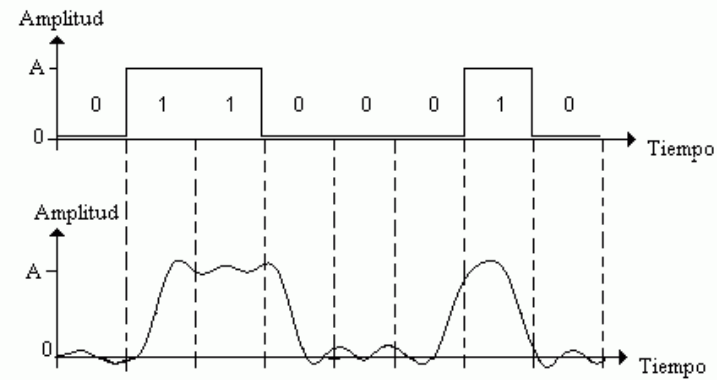
2. Ancho de banda



3.2 Transmisión de una señal de datos.

Distorsión en el medio de transmisión

3. Distorsión de retardo



4. Ruido



3.2 Transmisión de una señal de datos.

Ruido en el medio. Teorema de Shannon



Ruido de fondo en un medio físico

$$\text{Relación señal-ruido (signal to noise ratio)} = 10\log_{10}\left(\frac{P_s}{P_n}\right) \text{ dB (decibelios)}$$

Teorema de Shannon

Velocidad máxima de transmisión en un medio físico (independientemente del número de niveles de la señal) con una relación señal ruido en el medio.

$$V_{t(max)} = B\log_2\left(1 + \frac{P_s}{P_n}\right) \text{ bps}$$

3.2 Transmisión de una señal de datos.

Ruido en el medio. Teorema de Shannon

Ejemplo: Velocidad máxima de transmisión en la RTC con una relación señal ruido de 30 dB.

$$V_{t(max)} = 4000 \log_2 \left(1 + \frac{P_s}{P_n} \right) \text{ bps}$$

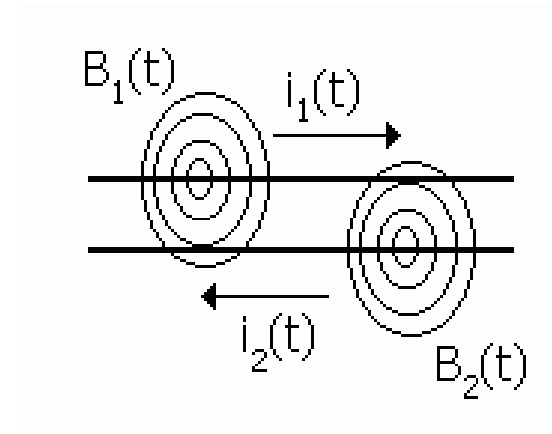
$$30 \text{ dB} = 10 \log_{10} \left(\frac{P_s}{P_n} \right) \Rightarrow \log_{10} \left(\frac{P_s}{P_n} \right) = \frac{30}{10} = 3 \quad \frac{P_s}{P_n} = 10^3 = 1000$$

$$V_{t(max)} = 4000 \log_2 (1 + 1000) = 4000 \frac{\log_{10}(1001)}{\log_{10} 2} = 39868.91 \text{ bps}$$

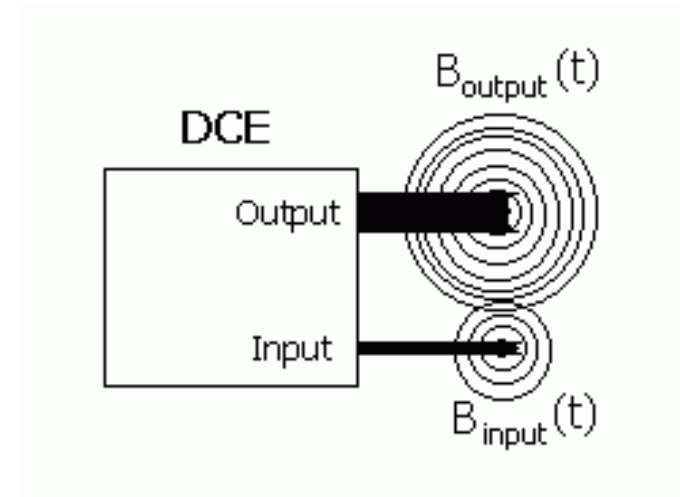
3.2 Transmisión de una señal de datos.

Tipos de ruido según la naturaleza de su origen

1. Ruido cruzado (crosstalk) o diafonía →



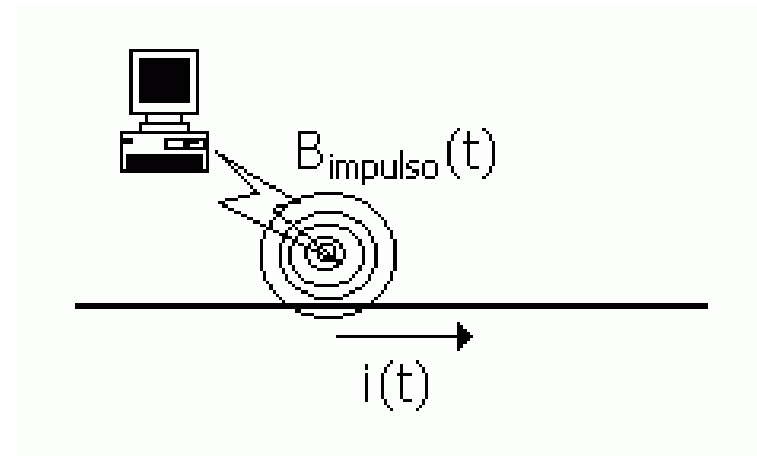
2. Autoacoplamiento →



3.2 Transmisión de una señal de datos.

Tipos de ruido según la naturaleza de su origen

3. Ruido de impulso



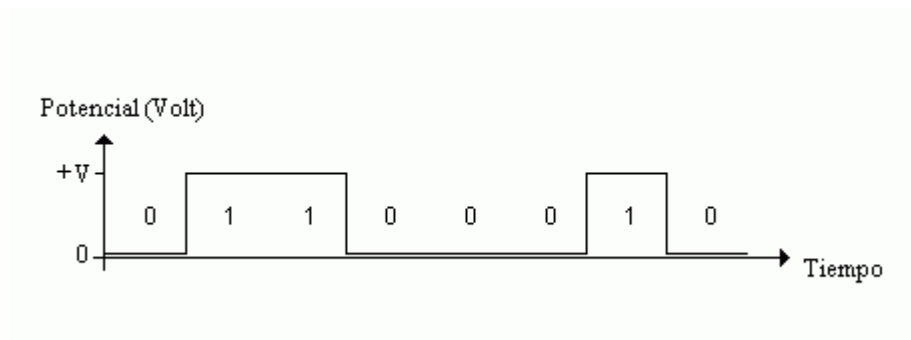
3.3 Señalización en banda base

Transmisión de la señal de información directamente al medio físico: transmisión de una señal de pulsos con información binaria.

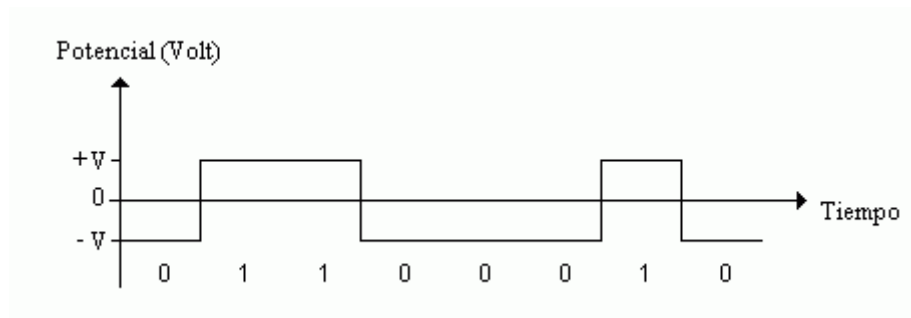
Codificación binaria

Cada valor lógico de la señal de información tiene asignado un nivel de tensión eléctrica (valor de la magnitud física).

CODIFICACIÓN BINARIA SIN RETORNO A CERO



UNIPOLAR

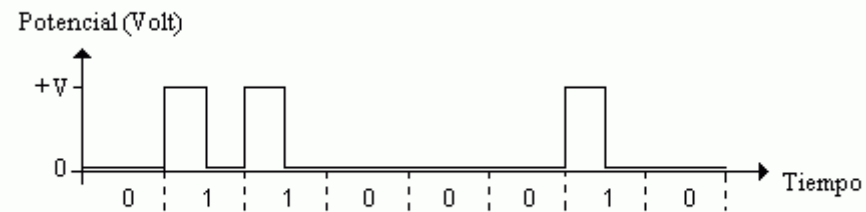


BIPOLAR

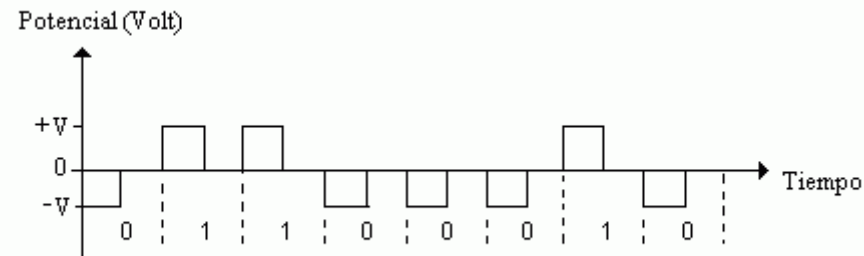
3.3 Señalización en banda base

Codificación binaria

CODIFICACIÓN BINARIA CON RETORNO A CERO



UNIPOLAR

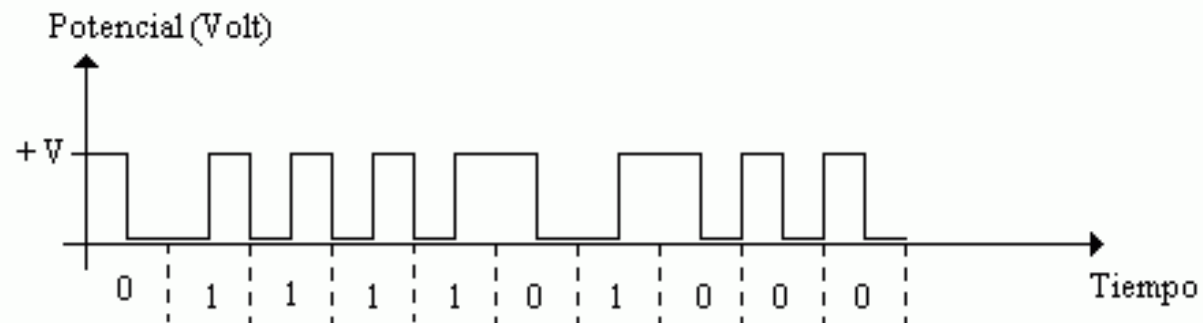


BIPOLAR

3.3 Señalización en banda base

Codificación Manchester

Cada valor lógico de la señal de información tiene asignado un tipo de transición en el cambio del valor de la tensión eléctrica (valor de la magnitud física).



3.4 Señalización en banda modulada

La señal de información a transmitir sufre un proceso de adaptación antes de su transmisión al medio físico.

Existen tres tipos de señales en la transmisión en banda modulada:

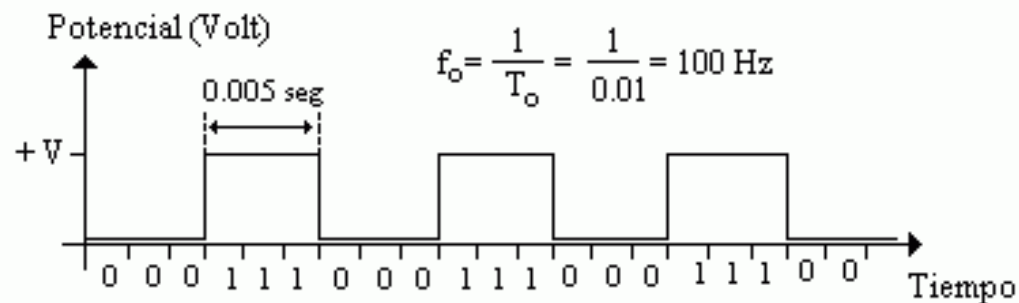
- Señal moduladora: señal de información a transmitir.
- Señal portadora: señal con unas características que permite su transmisión por el medio físico.
- Señal modulada: señal portadora transmitida en el medio modificada en función de las características de la señal moduladora.

3.4 Señalización en banda modulada

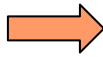
Modulación

Incorporación de la información de una señal **moduladora** en una señal **portadora** que puede ser transmitida de forma adecuada por un medio físico.

Ejemplo: Transmisión de una señal de pulsos por la red telefónica conmutada (RTC).



Componentes frecuenciales de la señal (armónicos): 100 Hz, 200 Hz, 300 Hz, 400 Hz...

Ancho de banda de RTC: 400 Hz - 4400 Hz  ¡¡¡ LA SEÑAL NO PUEDE SER TRANSMITIDA !!!

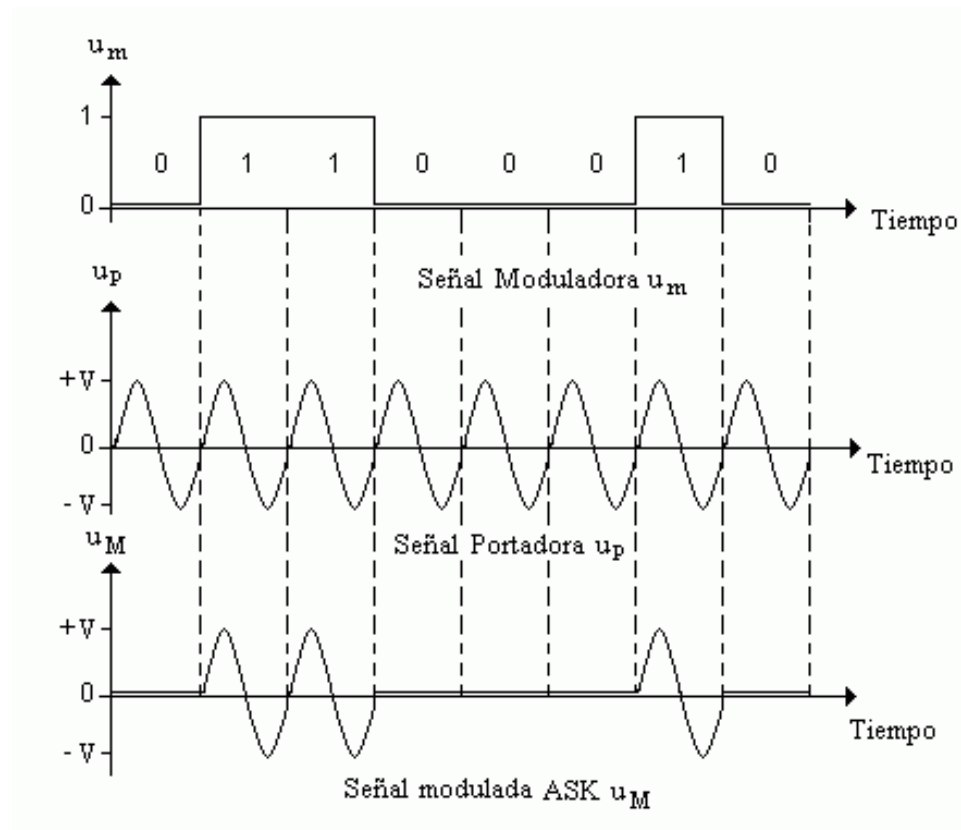
3.4 Señalización en banda modulada

Modulación analógica

Señal moduladora: DIGITAL (Señal de pulsos con información binaria)

Señal portadora: ANALÓGICA (Señales periódicas senoidales)

1. Modulación por cambio en amplitud (ASK - Amplitude shift keying)

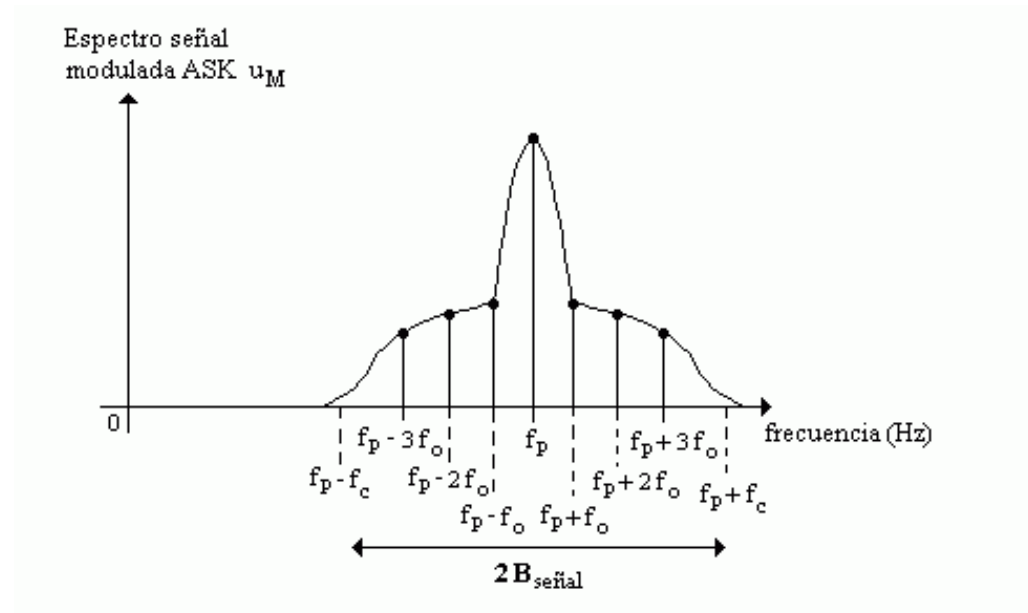
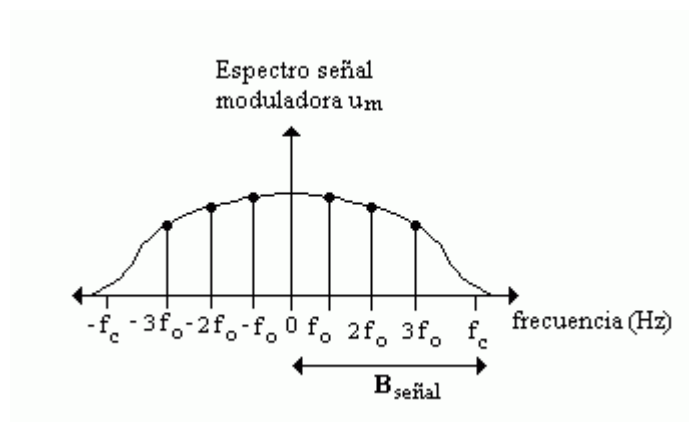


3.4 Señalización en banda modulada

Modulación analógica

1. Modulación por cambio en amplitud (ASK - Amplitude shift keying)

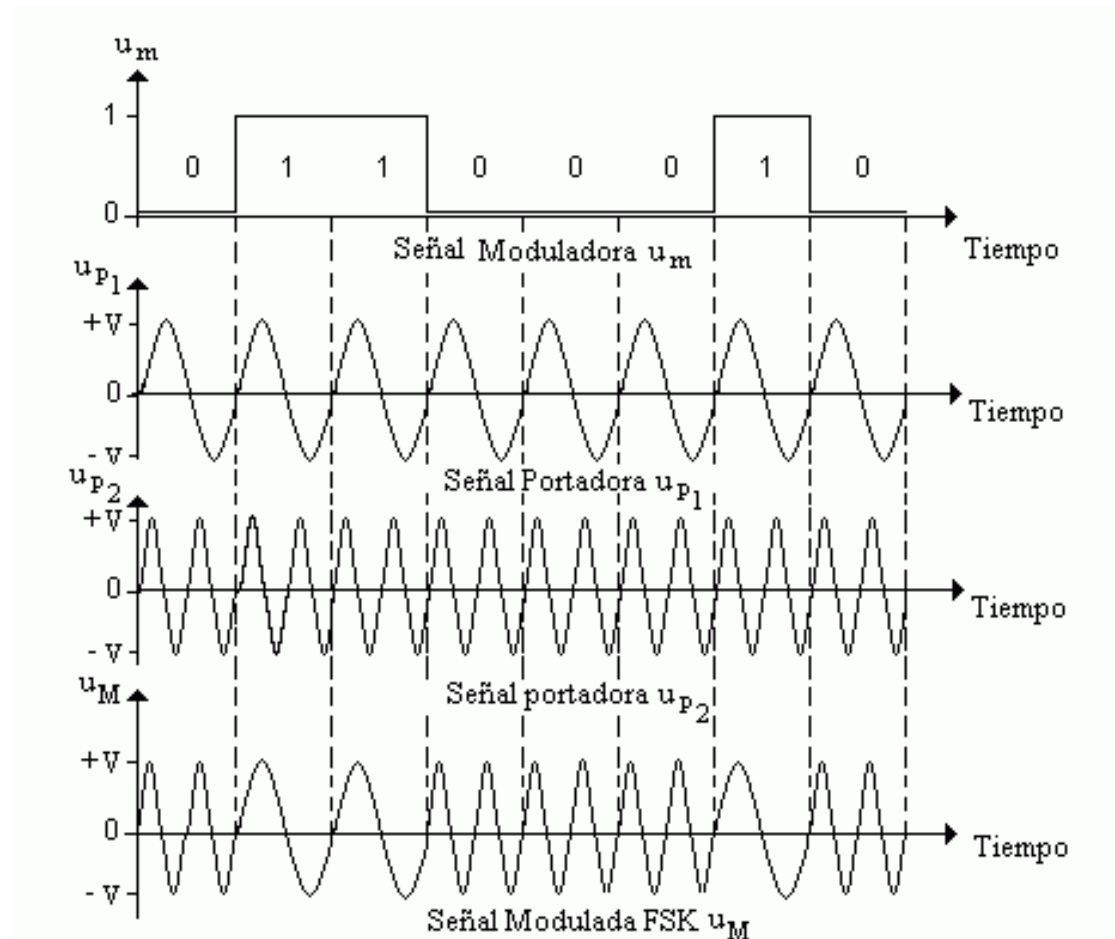
Espectro de potencia de la señal moduladora y modulada



3.4 Señalización en banda modulada

Modulación analógica

2. Modulación por cambio en frecuencia (FSK - Frequency shift keying)

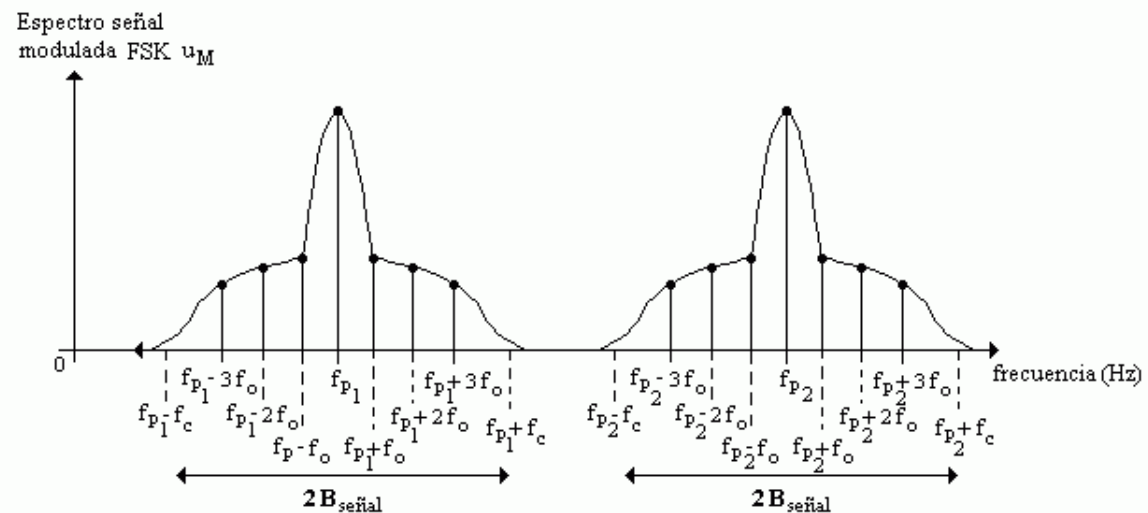
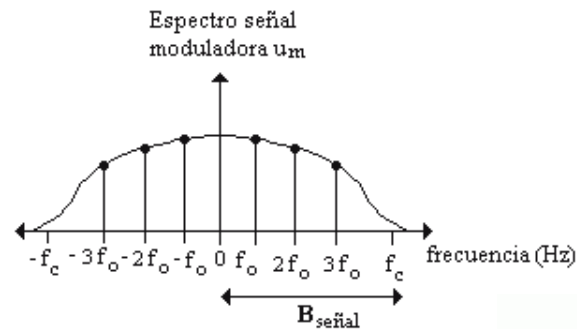


3.4 Señalización en banda modulada

Modulación analógica

2. Modulación por cambio en frecuencia (FSK - Frequency shift keying)

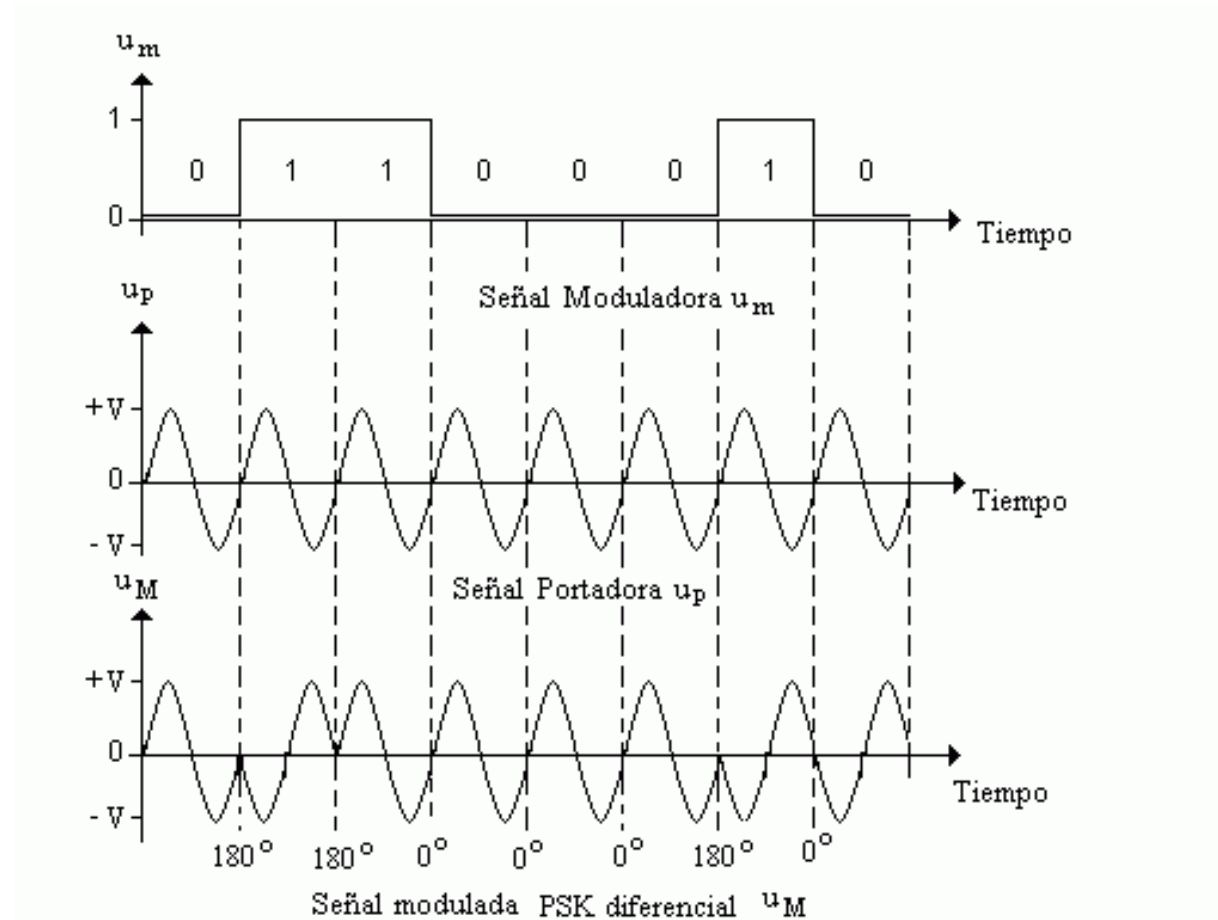
Espectro de potencia de la señal moduladora y modulada



3.4 Señalización en banda modulada

Modulación analógica

3. Modulación por cambio en fase (PSK - Phase shift keying)

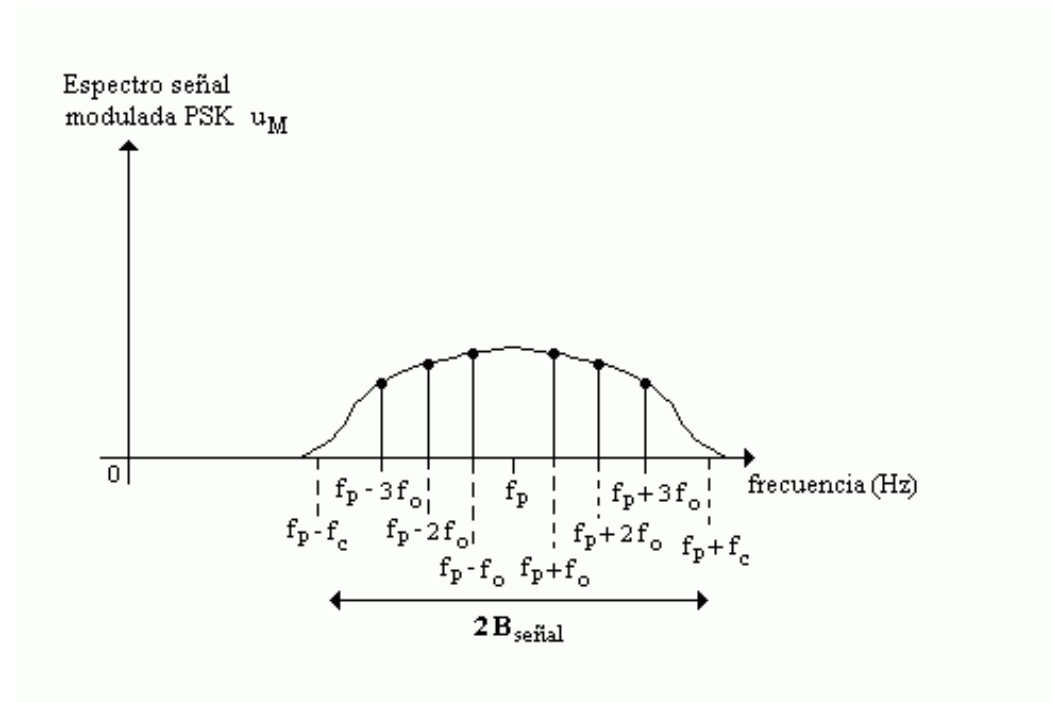
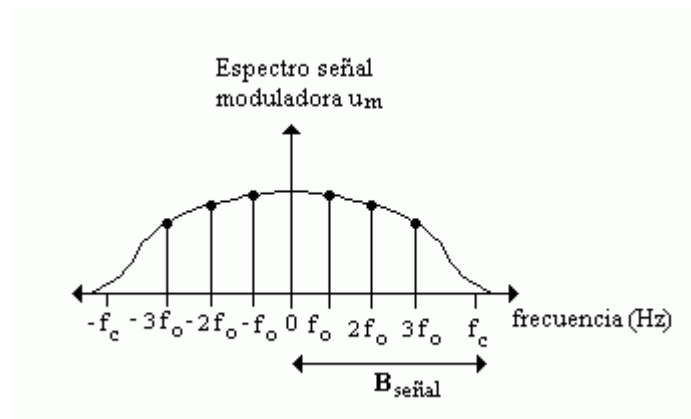


3.4 Señalización en banda modulada

Modulación analógica

3. Modulación por cambio en fase (PSK - Phase shift keying)

Espectro de potencia de la señal moduladora y modulada

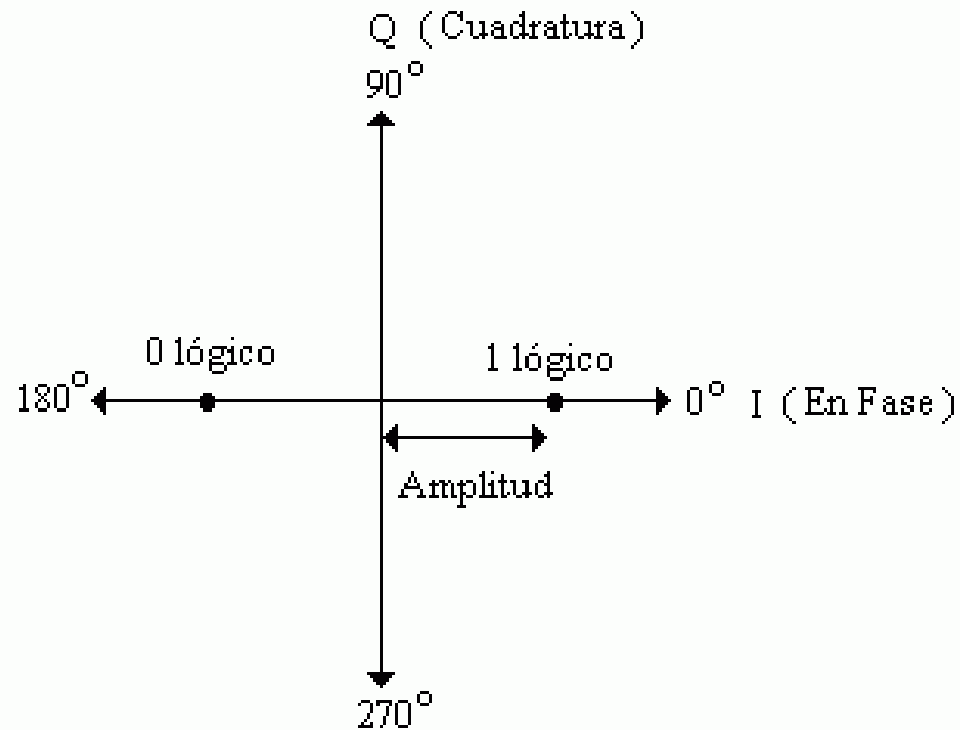


3.4 Señalización en banda modulada

Modulación analógica

4. Métodos de modulación de múltiples niveles

Diagrama de fase

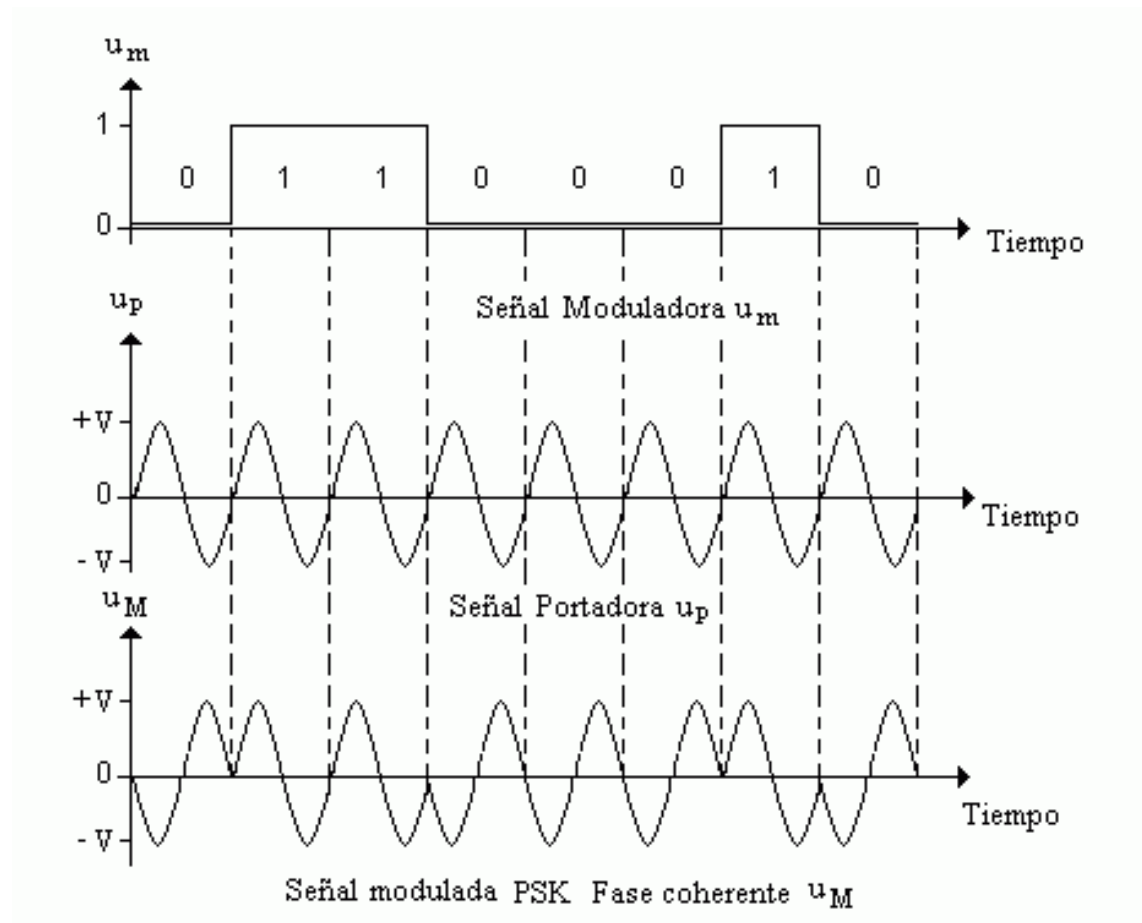


3.4 Señalización en banda modulada

Modulación analógica

4. Métodos de modulación de múltiples niveles

Modulación PSK de fase coherente

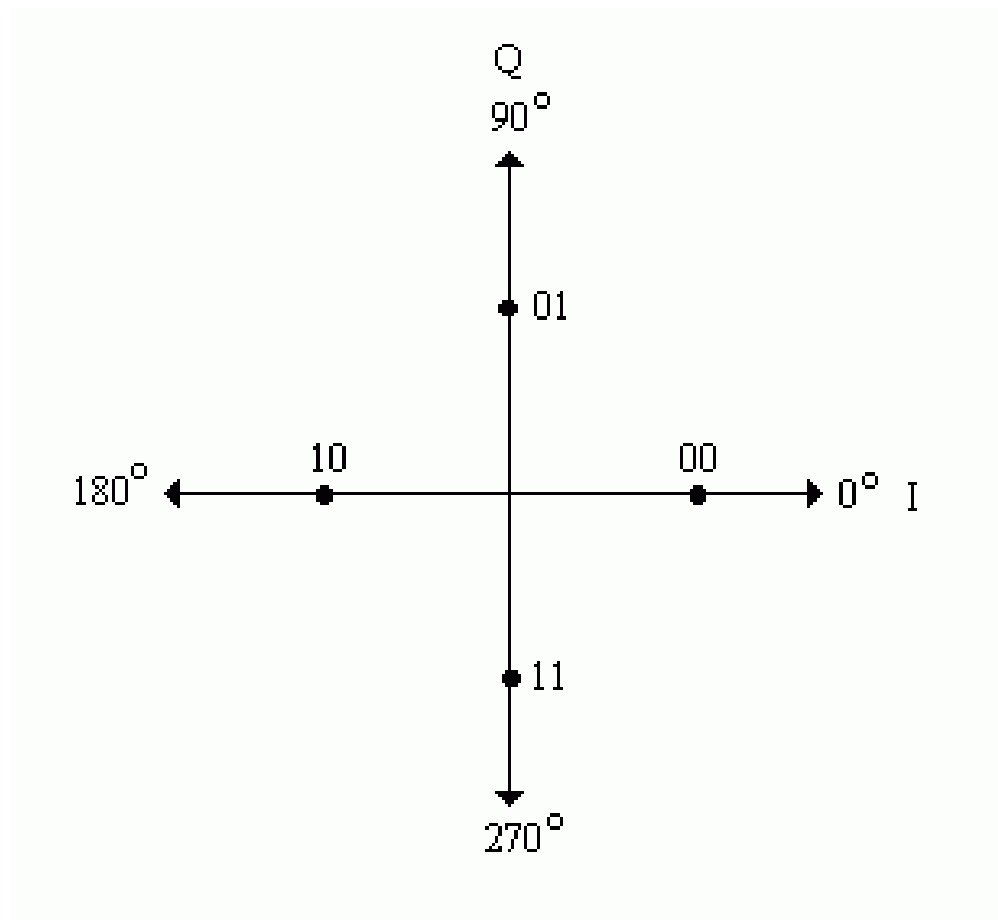


3.4 Señalización en banda modulada

Modulación analógica

4. Métodos de modulación de múltiples niveles

Diagrama de fase de la modulación QPSK

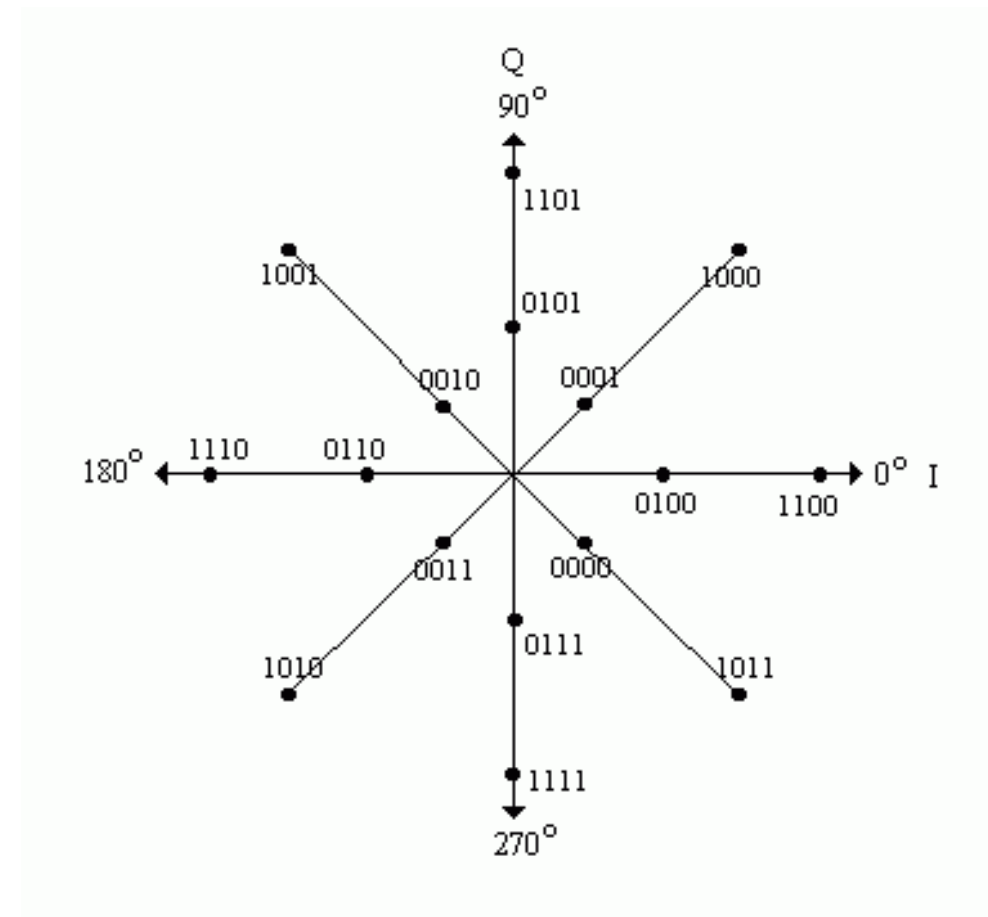


3.4 Señalización en banda modulada

Modulación analógica

4. Métodos de modulación de múltiples niveles

Diagrama de fase de la modulación QAM



3.4 Señalización en banda modulada

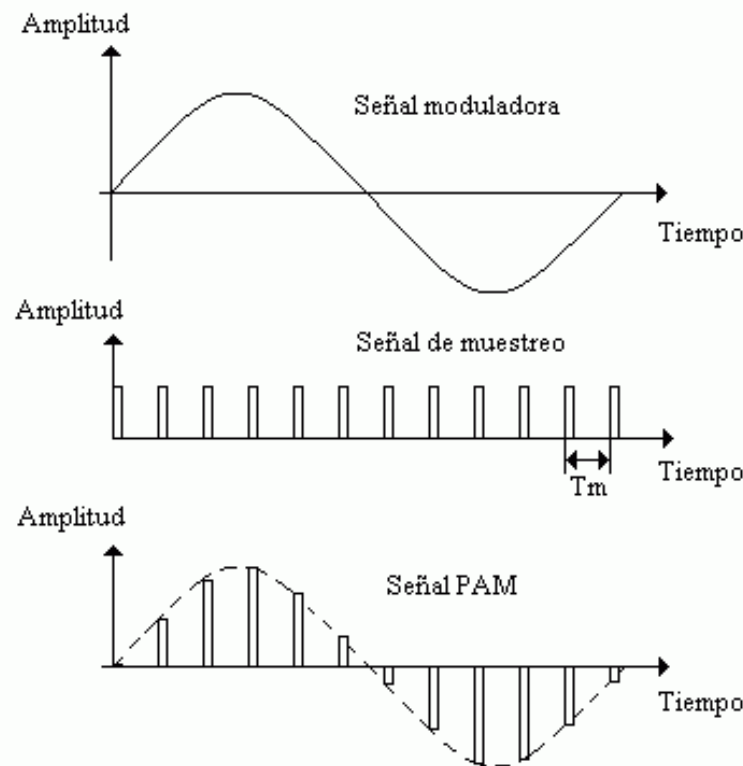
Modulación digital

Señal moduladora: ANALÓGICA (Señales periódicas senoidales)

Señal portadora: DIGITAL (Señal de pulsos)

Ejemplo: Transmisión de voz empleando señales de pulsos (RDSI)

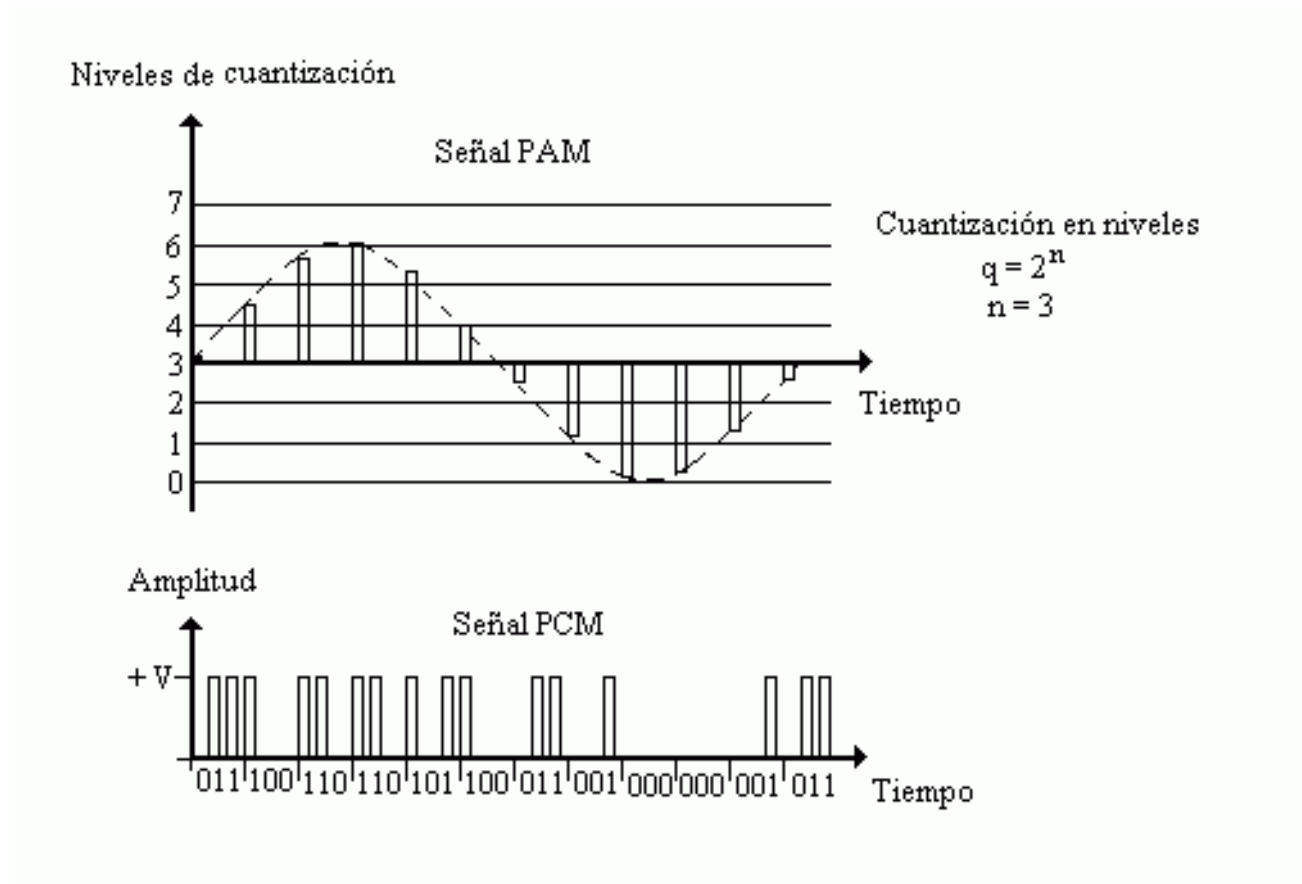
Modulación por código de pulsos (PCM - Pulse code modulation)



$$f_m = 2B_{señal}$$

3.4 Señalización en banda modulada

Modulación digital



q = número de niveles de cuantización

n = número de bits de codificación para los niveles q

$$V_{t-digital} = \frac{n}{T_{m-señal}} = n \cdot f_{m-señal} = n \cdot 2B_{señal} \text{ bps}$$

3.4 Señalización en banda modulada

Modulación digital

¿ Es posible modular cualquier señal analógica con PCM ?

Dado un número de bits de codificación n :

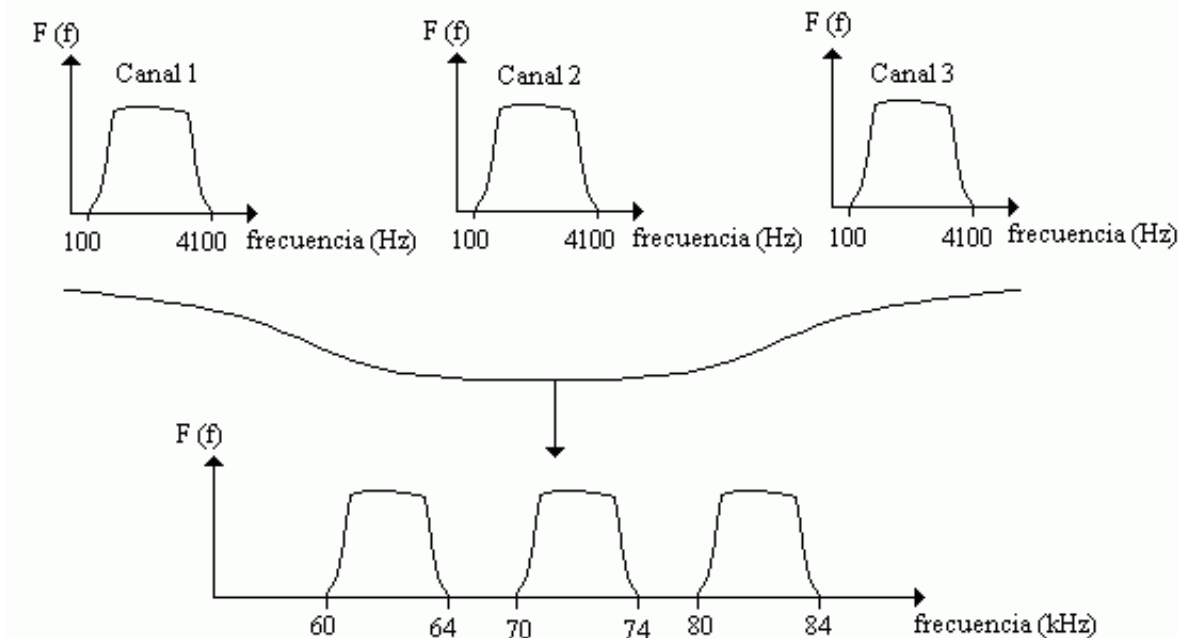
$$T_{m-digital} = \frac{T_{m-señal}}{n} \longrightarrow f_{m-digital} = \frac{1}{T_{m-digital}} = \frac{n}{T_{m-señal}} = \frac{n}{\frac{1}{2B_{señal}}} = n \cdot 2 \cdot B_{señal} \text{ Hz}$$

$$f_{m-digital} \leq 2B_{digital} \longrightarrow n \cdot 2 \cdot B_{señal} \leq 2B_{digital} \longrightarrow n \leq \frac{B_{digital}}{B_{señal}}$$

3.5 Multiplexión

Multiplexión por división de frecuencias (FDM)

Reparto de un medio físico entre varias fuentes de información asignando una zona del ancho de banda a cada fuente.



$$B_{medio} = n \cdot (B_{canal} + \Delta B) \text{ Hz}$$

n = número de canales a multiplexar

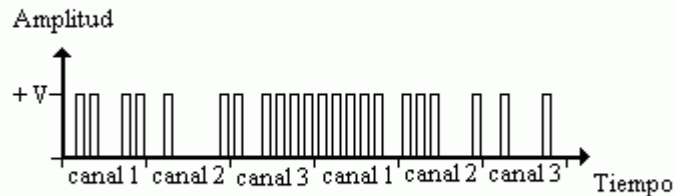
3.5 Multiplexión

Multiplexión por división en el tiempo (TDM)

Reparto de un medio físico entre varias fuentes de información asignando un tiempo de uso del medio a cada fuente.

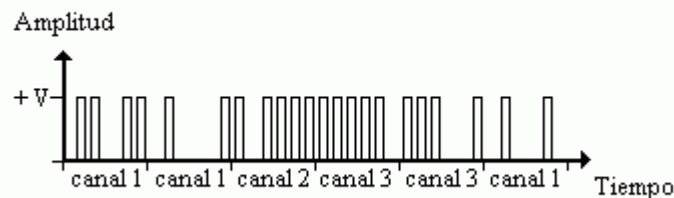
1. TDM síncrona

Cada fuente tiene asignada una misma posición temporal periódica en el uso del medio de transmisión.



2. TDM estadística

Cada fuente no tiene asignada una misma posición temporal periódica en el uso del medio de transmisión.



3.5 Multiplexión

Multiplexión por división en el tiempo (TDM)

Ejemplo de TDM síncrona: multiplexión de canales digitales de voz en RDSI

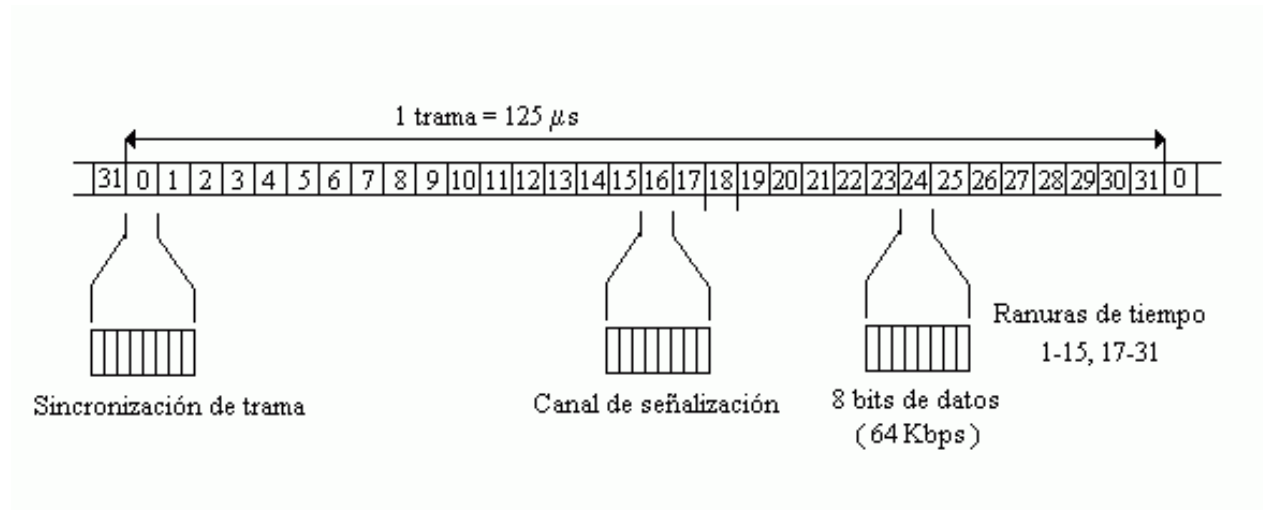
Digitalización PCM de un canal de voz (4000 Hz)

$$f_m = 2B_{voz} = 2 \cdot 4000 = 8000 \text{ Hz}$$
$$T_m = \frac{1}{f_m} = 125 \mu\text{seg}$$

➡

$$V_{t \text{ canal de voz}} = \frac{8}{T_m} = \frac{8}{125 \mu\text{seg}} = 64000 \text{ bps}$$

Normativa Europa



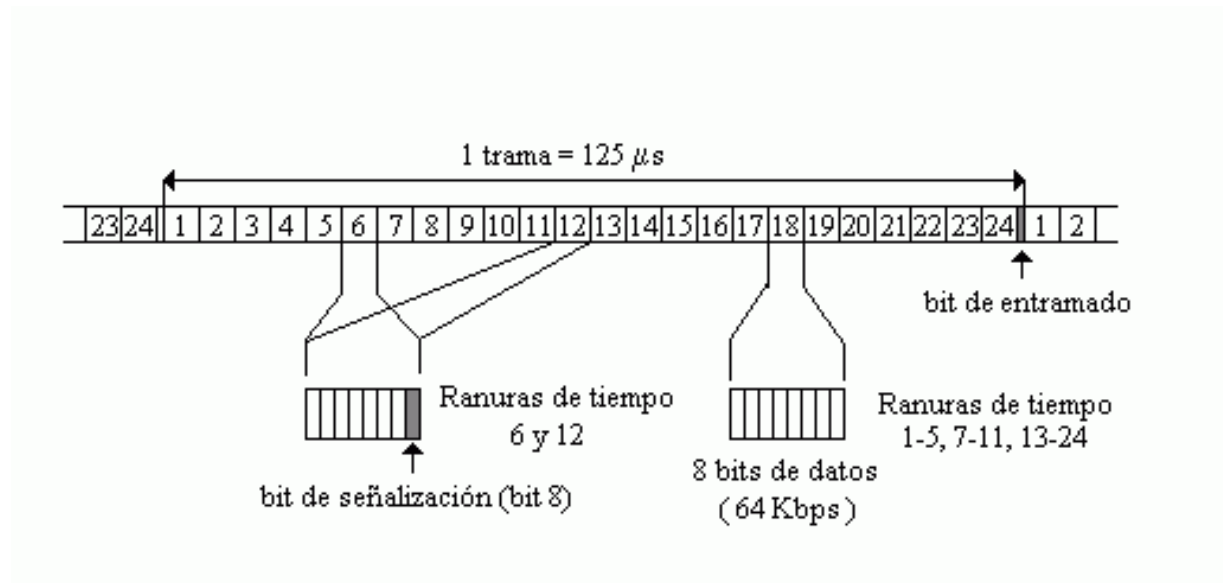
$$V_{t \text{ canal multiplexado}} = \frac{32 \cdot 8}{125 \mu\text{sec}} = 2.048 \text{ Mbps}$$

3.5 Multiplexión

Multiplexión por división en el tiempo (TDM)

Ejemplo de TDM síncrona: multiplexión de canales digitales de voz en RDSI

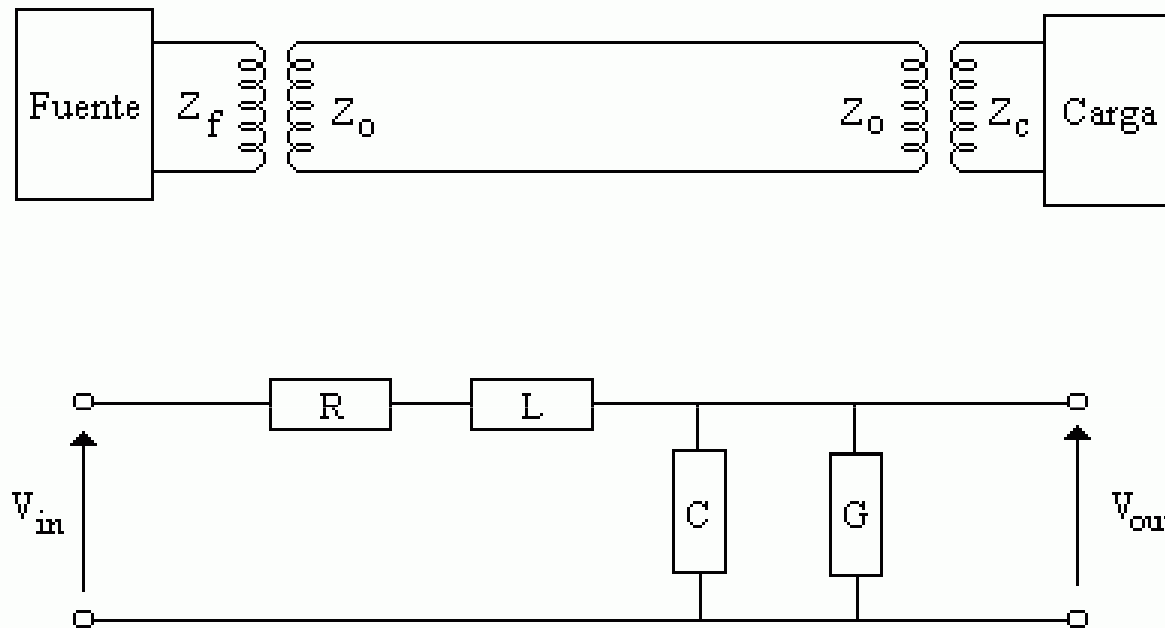
Normativa EEUU-Japón



$$V_{t \text{ canal multiplexado}} = \frac{24 \cdot 8 + 1}{125 \mu \text{sec}} = 1.544 \text{ Mbps}$$

3.6 Medios de transmisión

Modelo de parámetros distribuidos de un cable eléctrico



1. Para evitar reflejos en la propagación de la señal

$$Z_c = Z_0 \quad \text{Ej. Ethernet: } Z_0 = 50 \, \Omega$$

2. Para conseguir una atenuación mínima en la propagación de la señal

$$RC = GL$$

3.6 Medios de transmisión

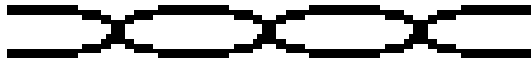
Cable par paralelo



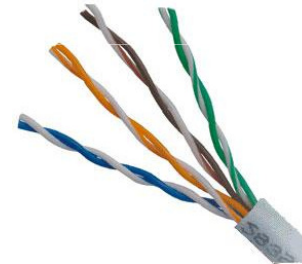
$V_t \leq 20$ Kbps, distancia máxima 50 m

Comunicaciones DTE - DCE

Cable par trenzado no blindado (UTP – *Unshielded Twisted Pair*)



Reduce el ruido cruzado o diafonía



Tipos de cable UTP

Categoría 3

$V_t \leq 30$ Mbps, distancia máxima 100 m

Categoría 5

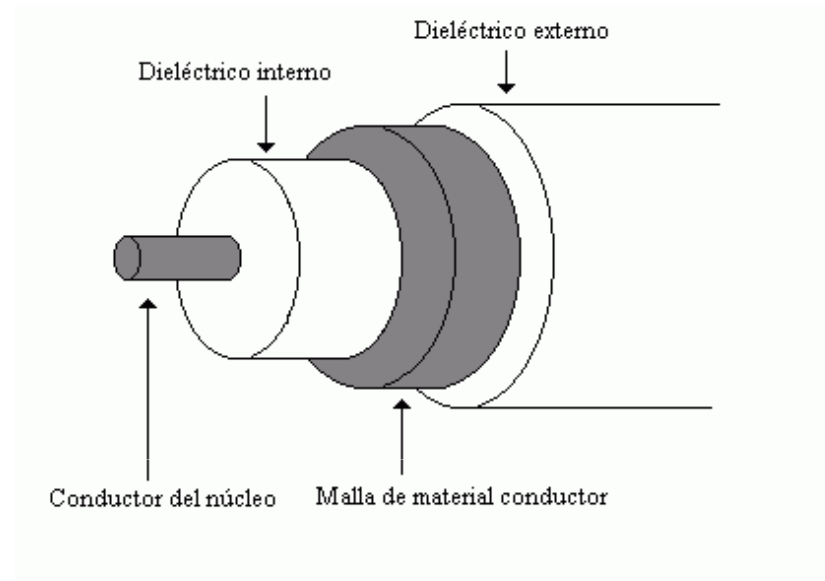
$V_t \leq 100$ Mbps, distancia máxima 100 m

Categoría 6

$V_t \leq 1000$ Mbps, distancia máxima 100 m

3.6 Medios de transmisión

Cable coaxial



La malla conductora evita las interferencias de campos eléctricos externos al cable, elimina el ruido de impulso.

Esta propiedad se aplica en los cables pares trenzados para conseguir mejorar sus prestaciones, obteniendo el denominado **cable STP** (*Shielded Twisted Pair*).



$V_t \leq 1000$ Mbps, distancia máxima 100 m

3.6 Medios de transmisión

Cable coaxial

Tipos de cable coaxial

Cable coaxial 50 Ω

- Transmisión en banda base (Manchester).
- Redes LAN (sustituido por pares trenzados).
- Velocidad de 10 Mbps a distancia de 100 m. para cable coaxial fino.
- Velocidad de 10 Mbps a distancia de 500 m. Para cable coaxial grueso.

Cable coaxial 75 Ω

- Transmisión en banda modulada.
- Multiplexión en frecuencia de múltiples canales (transmisión *broadband* - 300 MHz).
- Televisión analógica/digital por cable.

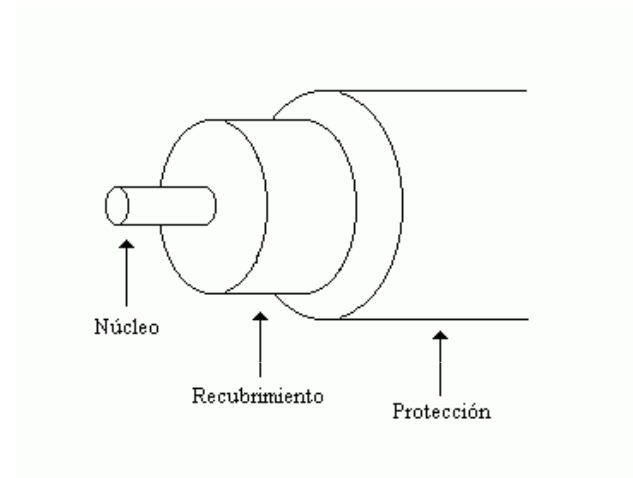
3.6 Medios de transmisión

Fibra óptica

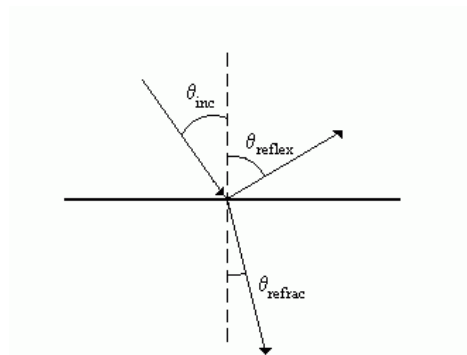
Medio que permite el confinamiento y propagación de un haz de luz.

Estructura

Núcleo de cristal de sílice rodeado de un recubrimiento de silicona. Dispone de una capa externa como protección hecha de poliuretano.



Modelo de propagación



La propagación de la luz entre dos medios distintos distorsiona la trayectoria del haz, produciéndose una refracción o reflexión.

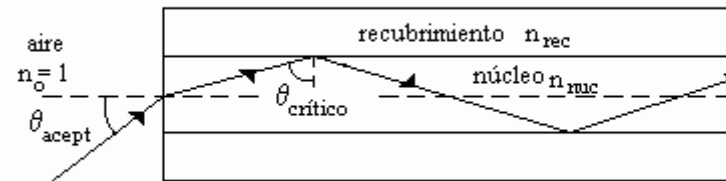
Índice de refracción de un medio $n = \frac{v_c}{v_n}$

Ley de Snell $n_1 \sen \vartheta_{inc} = n_2 \sen \vartheta_{refrac}$

3.6 Medios de transmisión

Fibra óptica

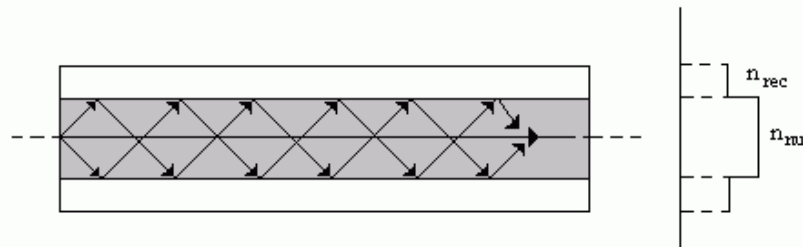
Modelo de propagación



$$\vartheta_{\text{crítico}} = \arcsen \frac{n_{\text{rec}}}{n_{\text{nuc}}}$$

Tipos de fibra óptica

A) Fibra multimodo o de índice de salto. Existen múltiples haces que se propagan en la fibra, desfasándose temporalmente debido a los diferentes recorridos ópticos, y provocando distorsiones (dilatación) en los pulsos del haz (**dispersión intermodal**).

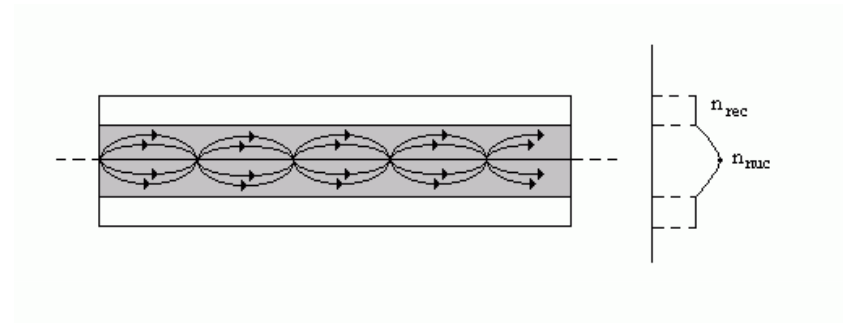


3.6 Medios de transmisión

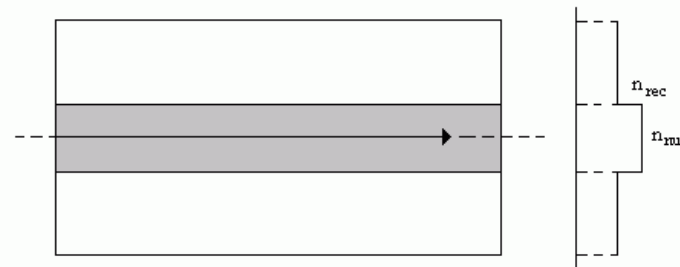
Fibra óptica

Tipos de fibra óptica

B) Fibra de índice gradual. El índice de refracción variable en el núcleo permite compensar el efecto de la dispersión intermodal.



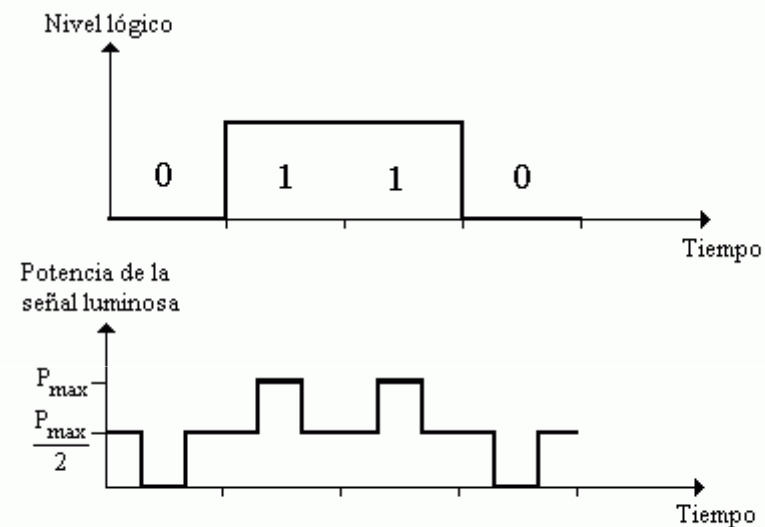
C) Fibra monomodo. Un núcleo de diámetro muy reducido ($< 10 \mu\text{m}$) permite la propagación de un único haz en paralelo al eje de la fibra. No existe dispersión intermodal, pero las diferentes longitudes de onda del haz producen una distorsión en el pulso denominada **dispersión intramodal**.



3.6 Medios de transmisión

Fibra óptica

Velocidad de transmisión



TIPO DE FIBRA	ANCHO DE BANDA (Hz/Km)
Multimodo	20 MHz/Km
Índice gradual	500 - 1000 MHz/Km
Monomodo	1 - 10 GHz/Km

Tecnología de multiplexión de longitudes de onda  **Vt de 100 Gbps a varios Km**

3.6 Medios de transmisión

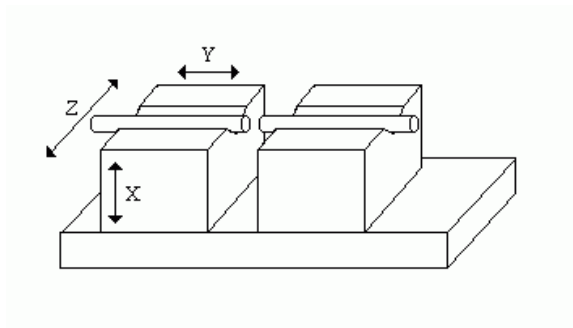
Fibra óptica

Dispositivos luminosos. Conexión de fibras óptica

Dispositivos emisores	Diodo emisor de infrarrojos (IRED)	$T_{comm} \approx 20 \eta seg$ $\Delta\lambda \approx 40 \eta m$
	Diodo láser	$T_{comm} \approx 1 \eta seg$ $\Delta\lambda \approx 2 \eta m$
Dispositivos receptores	Fotodiodo semiconductor en avalancha (APD)	

Conexiones de fibra

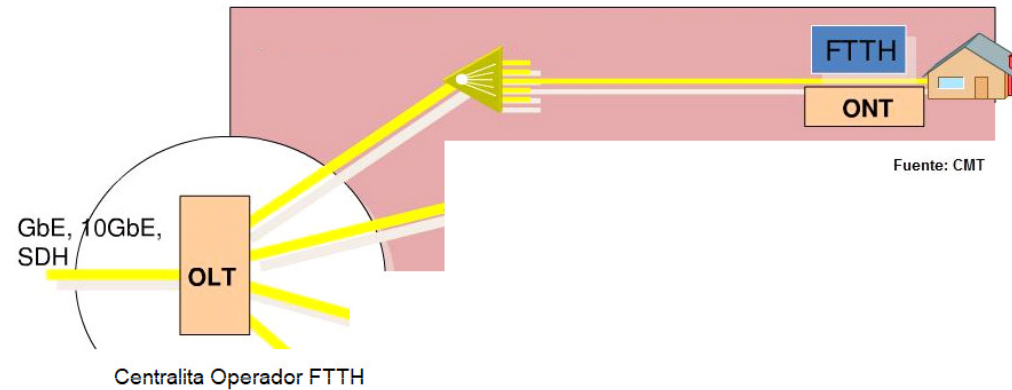
Las uniones de cables de fibra óptica (debido a cortes) precisa de un dispositivo de alineamiento y fusión de las fibras: fusionadora.



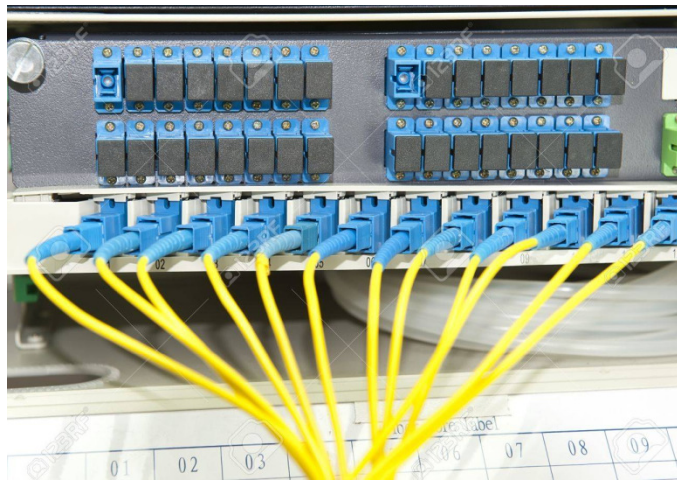
3.6 Medios de transmisión

Fibra óptica

Aplicaciones



Trazados de fibra óptica al hogar (FTTH) con fibras monomodo y velocidades de 2 Gbps y 20 km.

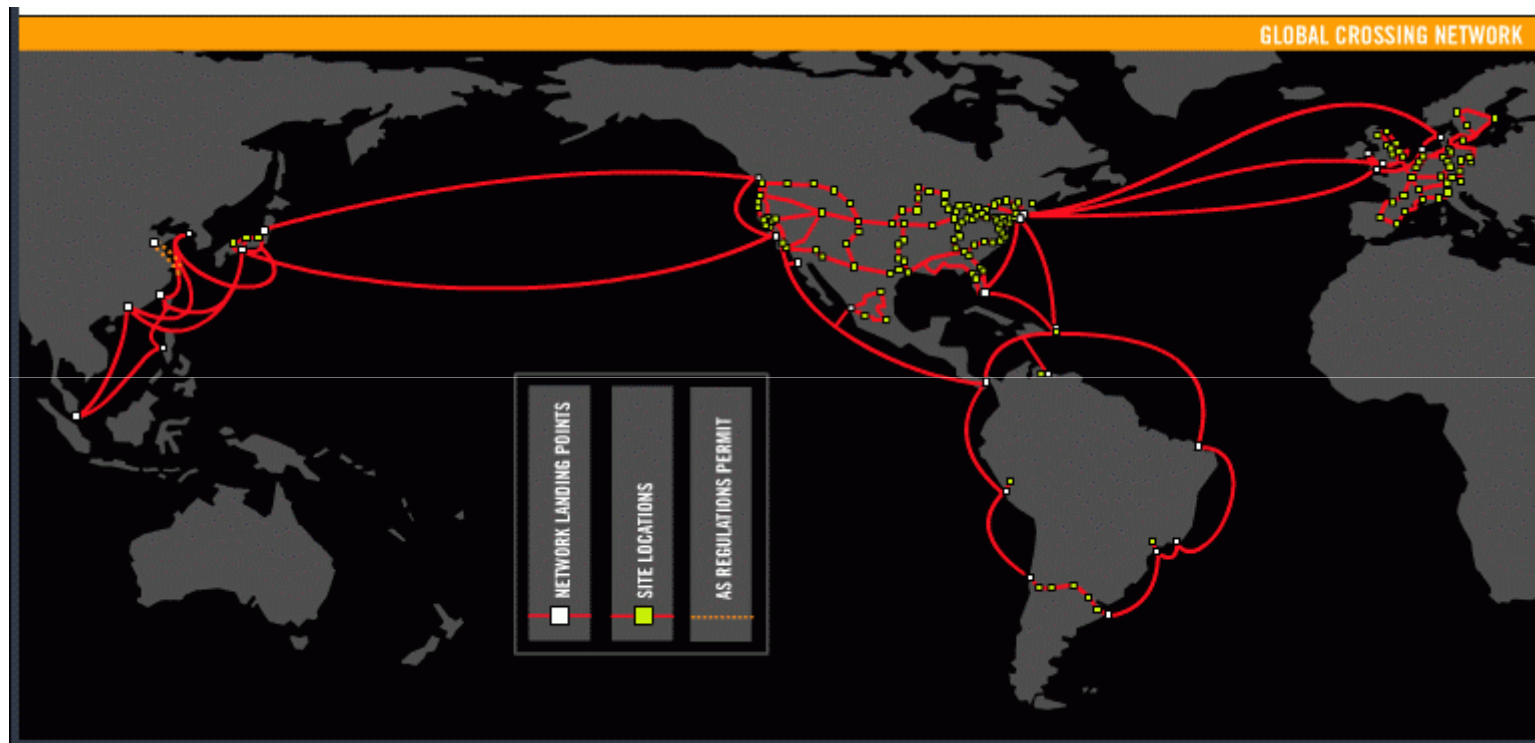


Redes LAN Ethernet Fibra óptica

3.6 Medios de transmisión

Fibra óptica

Aplicaciones



Enlaces nacionales e internacionales

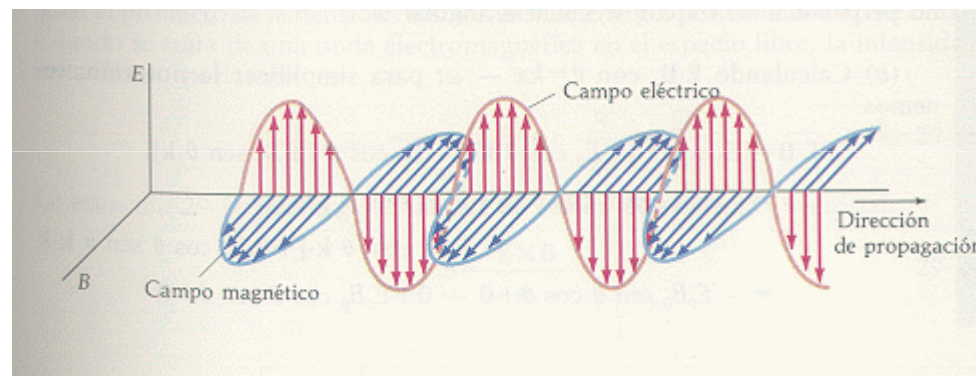
3.6 Medios de transmisión

Ondas electromagnéticas

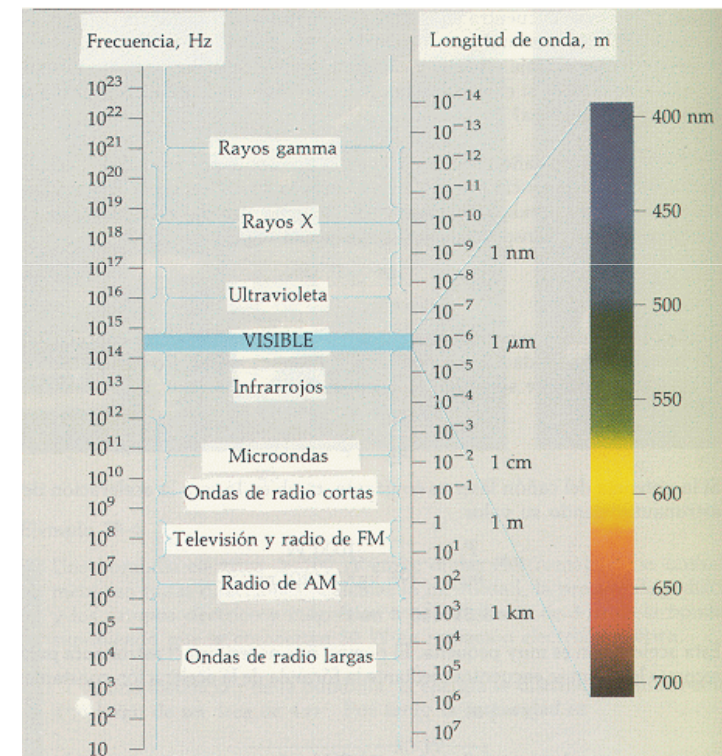
La radiación electromagnética es un mecanismo de transmisión de energía que presenta las propiedades de una onda.

Esta onda es susceptible de incorporar información empleando mecanismos de modulación (ASK, PSK, FSK).

Espectro electromagnético



$$f(s^{-1} = Hz) = \frac{c(m/s)}{\lambda(m)}$$



3.6 Medios de transmisión

Ondas electromagnéticas

Espectro de radiocomunicación

El espectro de radiocomunicación es el conjunto de frecuencias de radiación electromagnética que se han definido para incorporar información y se emplean en los sistemas de comunicaciones.

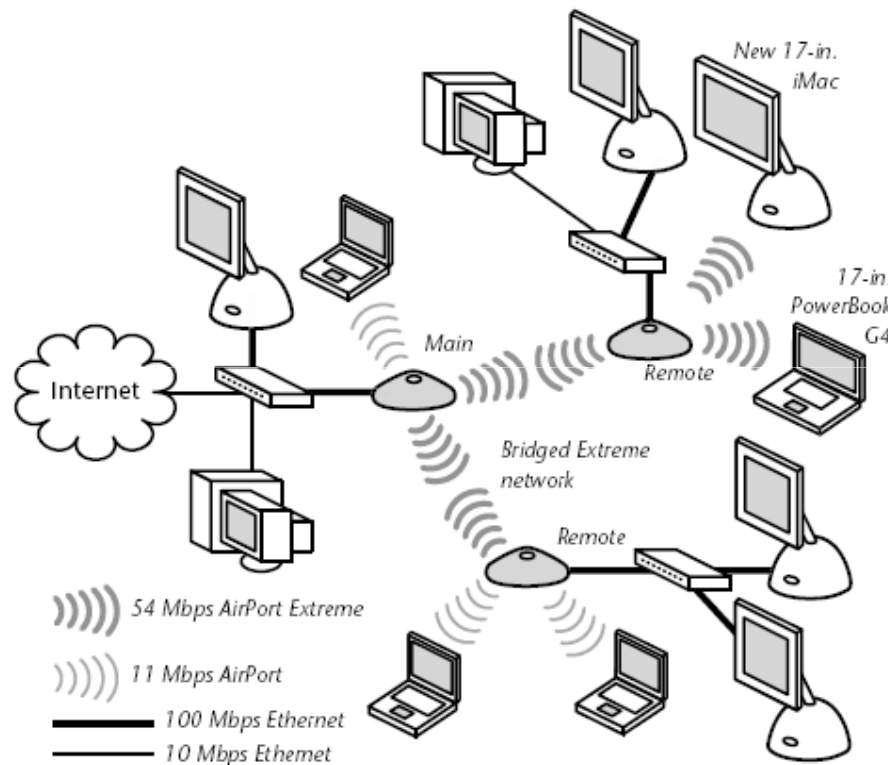
Esta elección es por motivos energéticos (coste de generación reducido), salud (radiación inmune a los seres vivos) y propiedades de propagación (atravesar obstáculos, largas distancias, etc.).

Banda	Frecuencia	Aplicaciones
VLF	< 30 KHz	Audio
LF	30 KHz - 300 KHz	Marítima
MF	300 KHz - 3 MHz	Radio AM
HF	3 MHz - 30 MHz	
VHF	30 MHz - 300 MHz	Radio FM, TV, Radar
UHF	300 MHz - 3 GHz	Radar, TV, Microondas
SHF	3 GHz - 30 GHz	Satélite, Microondas, Radar
EHF	30 GHz - 300 GHz	Radar, Infrarrojo
SEHF	300 GHz - 3000 GHz	Infrarrojo

3.6 Medios de transmisión

Ondas electromagnéticas

Aplicaciones: Redes inalámbricas



Red inalámbrica de infraestructura



Punto de acceso (AP): Dispositivo puente entre LAN de cable y LAN inalámbrica.

Normativa IEEE 802.11g

Frecuencia portadora: 2.4 GHz. 54 Mbps.

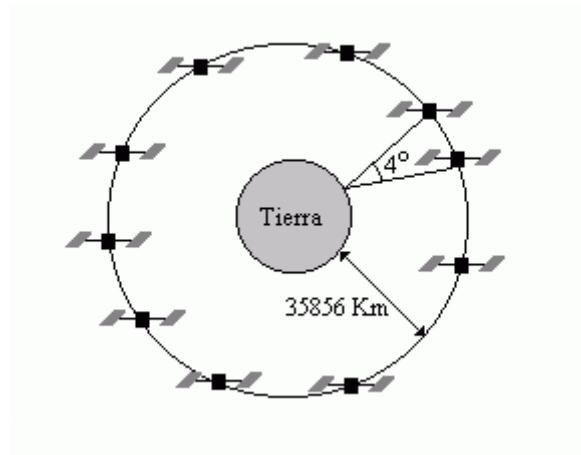
Normativa IEEE 802.11n

Frecuencia portadora: 2.4 y 5 GHz. 600 Mbps.

3.6 Medios de transmisión

Ondas electromagnéticas

Aplicaciones: Comunicación satelital.



Satélites geoestacionarios (órbitas a 35856 km de la tierra) : cobertura permanente de una zona geográfica.

Satélites no-geoestacionarios (órbitas inferiores a 35856 km): cobertura NO permanente de amplias zonas geográficas.

Transmisión analógica con modulación

Frecuencias de portadoras:

Banda C (4 - 8 GHz) Banda Ku (12 - 18) GHz

Banda Ka (27 - 40 GHz)

Aplicaciones:

- Multidifusión: TV vía satélite.
- Telefonía: Iridium, Inmarsat, Thuraya.
- Transmisión de datos: Mecanismo alternativo (de respaldo) cuando no es posible la fibra óptica (más barato).
- Servicios de acceso a Internet por satélite: <http://www.hispasat.com>

Transponder: dispositivo emisor/receptor a bordo de un satélite

Ancho de banda en 1 transponder: 36 - 70 Mhz -> 50 - 100 Mbps.

Varios transponders y varios haces de ondas -> Gbps de capacidad por satélite.

TEMA 4

NIVEL DE ENLACE

4.1 Servicios y funciones del nivel de enlace

Función genérica del nivel de enlace: comunicación libre de errores en un medio físico.



Fragmentación de paquetes
Numeración de paquetes
Reconocimiento de la información
Reenvío de paquetes erróneos
Control del flujo

4.1 Servicios y funciones del nivel de enlace

Tipos de servicios ofrecidos al nivel superior (nivel de red)

1 Servicio sin conexión y sin reconocimiento

- Medios físicos con baja tasa de error
- Más importante el retardo que la fiabilidad

2 Servicio sin conexión y con reconocimiento

- Medios físicos con tasa de error considerable
- Sólo confirmación del envío de información

3 Servicio con conexión y con reconocimiento

- Medios físicos con tasa de error considerable
- Control del flujo: ordenación de paquetes y reenvío correcto

4.1 Servicios y funciones del nivel de enlace

Funciones del nivel de enlace

A) Delimitación de tramas	Identificación del inicio y fin de un paquete
B) Direccionamiento	Identificación de los extremos de la comunicación en un medio físico
C) Control de errores	Asegura una transmisión sin errores debidos al medio físico
D) Control del flujo	Control del flujo de tramas entre emisor y receptor para evitar saturaciones, reenvíos incorrectos, etc.

4.1 Servicios y funciones del nivel de enlace

Formato de una trama de nivel de enlace



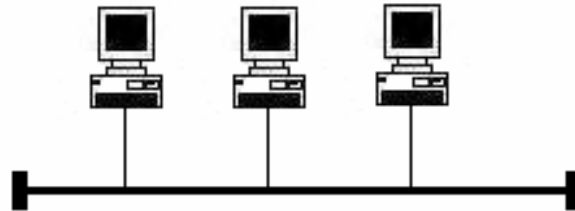
Formato de la trama Ethernet



4.1 Servicios y funciones del nivel de enlace

Direccionamiento

Objetivo: Identificar los elementos que intercambian tramas de nivel de enlace en un medio físico.



El mecanismo de direccionamiento consiste en asignar secuencias de bits únicas a cada estación. La cantidad de bits (b) asociados a una dirección nos indica el rango de direccionamiento.

Para $b=5$, tendríamos 2^5 estaciones, identificadas desde la secuencia 00000 a la 11111.

Tipos

Implícito	No es necesario especificar las estaciones origen y destino que intercambian tramas. Ej: línea punto a punto.
Explícito	Es necesario especificar las estaciones origen y destino que intercambian tramas. Ej: Ethernet.

4.1 Servicios y funciones del nivel de enlace

Control de errores

FCS (*Frame Check Sequence*): Secuencia de verificación de trama (SVT)

Conjunto reducido de datos que suele añadirse en la cola de un paquete de enlace y que permite determinar si la información del paquete ha sufrido algún error.

Dependiendo del tipo de información en la FCS se distingue entre:

A) Códigos de detección de error

Procedimientos que determinan un valor de FCS que permite detectar si el paquete de nivel de enlace presenta algún bit erróneo, pero no puede identificarlo.

B) Códigos de corrección de error

Procedimientos que determinan un valor de FCS que permite detectar si el paquete de nivel de enlace presenta algún bit erróneo e identificarlo, por lo que la trama puede ser corregida en el receptor.

Estos procedimientos no se emplean en los sistemas de comunicaciones actuales, pues el retardo en el reenvío de un paquete que ha sufrido un error es muy inferior al tiempo de cómputo para identificar los bits erróneos.

(Como excepción, los sistemas de comunicación en sondas de exploración del sistema solar, donde los retardos son muy elevados, del orden de horas).

4.1 Servicios y funciones del nivel de enlace

Control de errores

Detección de errores por paridad de bits de datos

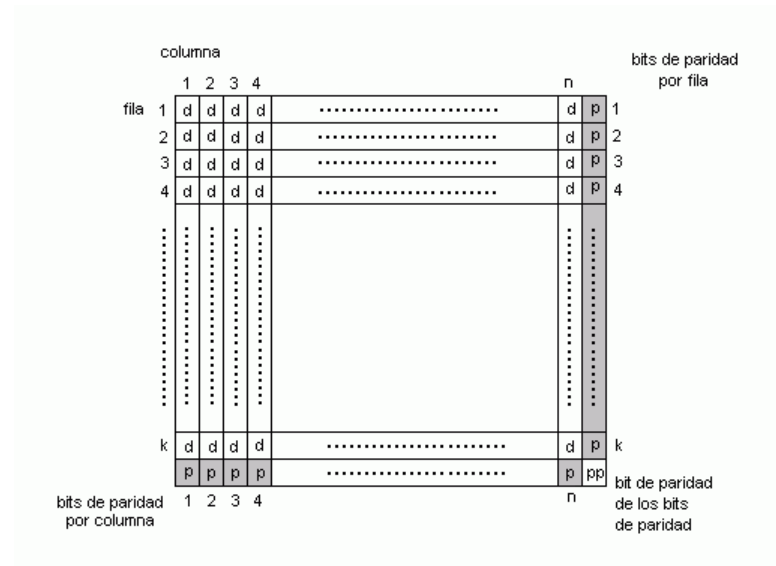
1. Paridad de los bits de datos

Bits de datos	Bit de paridad	Paridad par	00100101 1
00100101	P		00100101 0

Permiten detectar si en el paquete hay errores en un número impar de bits (1,3,5,etc).

2. Paridad por filas y columnas

Permiten detectar si en el paquete hay errores en 2 bits y un número impar de bits (1,3,5, etc).



En general, los sistemas de detección de errores por paridad incorporan mucha información redundante, en comparación con otros sistemas.

4.1 Servicios y funciones del nivel de enlace

Control de errores

Detección de errores por Códigos de Redundancia Cíclica (CRC)

Asocia un bloque de datos a un polinomio en x , determinando la SVT mediante operaciones y propiedades de polinomios.

$$\mathbf{11101110 \text{ (8 bits)} \rightarrow 1 \cdot x^7 + 1 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 0 \cdot x^0}$$
$$x^7 + x^6 + x^5 + x^3 + x^2 + x$$

Propiedad de la división

$D(x)$ = Polinomio asociado a los datos a transmitir

$G(x)$ = Polinomio generador

$T(x)$ = Polinomio asociado a los datos transmitidos por el emisor

$$\begin{array}{r|l} D(x) & G(x) \\ \hline R(x) & C(x) \end{array}$$

$$T(x) = D(x) - R(x)$$

El receptor realiza la operación división de la secuencia recibida entre el mismo polinomio generador, analizando el resto.

Si $T(x) \% G(x) = 0$ Transmisión correcta

Si $T(x) \% G(x) \neq 0$ Transmisión incorrecta

4.1 Servicios y funciones del nivel de enlace

Control de errores

Detección de errores por Códigos de Redundancia Cíclica (CRC)

La elección del polinomio generador se realiza para cumplir con las propiedades de detección de errores más adecuadas. Dado un polinomio generador de grado r , es posible detectar errores en 2 bits, un número impar de bits y errores en ráfaga (bits erróneos consecutivos) de longitud menor que r .

Polinomios generadores $G(x)$

$$\text{CRC-12} \quad G(x) = x^{12} + x^{11} + x^3 + x + 1$$

$$\text{CRC-16} \quad G(x) = x^{16} + x^{15} + x^2 + 1$$

$$\text{CRC-32} \quad G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

División de polinomios para el cálculo del CRC

$$\begin{array}{r} D(x) \cdot x^r \quad \overline{) \quad G(x)} \\ R(x) \quad C(x) \end{array}$$

$r = \text{grado de } G(x)$

$$T(x) = D(x) \cdot x^r - R(x)$$

La operación resta es la operación XOR

4.1 Servicios y funciones del nivel de enlace

Control de errores

Detección de errores por Códigos de Redundancia Cíclica (CRC)

Ejemplo

$$D(x) = 1101011011 \quad G(x) = x^4 + x + 1 \quad r = 4 \quad D(x) x^r = 11010110110000$$

$$\begin{array}{r} \overline{11010110110000} \\ \oplus 10011 \\ \hline 010011 \\ \oplus 10011 \\ \hline 000001 \\ \oplus 00000 \\ \hline 000010 \\ \oplus 00000 \\ \hline 000101 \\ \oplus 00000 \\ \hline 001011 \\ \oplus 00000 \\ \hline 010110 \\ \oplus 10011 \\ \hline 001010 \\ \oplus 00000 \\ \hline 010100 \\ \oplus 10011 \\ \hline 001110 \\ \oplus 00000 \\ \hline 01110 \\ \hline R(x) \end{array}$$

$$T(x) = D(x) \cdot x^r - R(x)$$

$$\begin{array}{r} 11010110110000 \\ \oplus 00000000001110 \\ \hline 11010110111110 \end{array}$$

$$T(x) = D(x) R(x)$$

$R(x)$ es la FCS incluida en la trama de enlace

4.2 Algoritmos de control del flujo

Objetivos

La funcionalidad del control del flujo en el nivel de enlace tiene como objetivos:

- Controlar el envío y recepción correcto de los paquetes de nivel enlace

- Controlar la sincronización del emisor y receptor de datos

- Evitar congestiones en el envío de información del emisor al receptor

Para llevar a cabo estas funcionalidades se suelen emplear dos protocolos diferentes para el control del flujo

Protocolos de parada y espera

Protocolos de ventana deslizante

La funcionalidad de control del flujo se puede realizar a nivel de enlace (protocolos de control del medio físico) o nivel de transporte (protocolos de control de la comunicación extremo a extremo, como TCP).

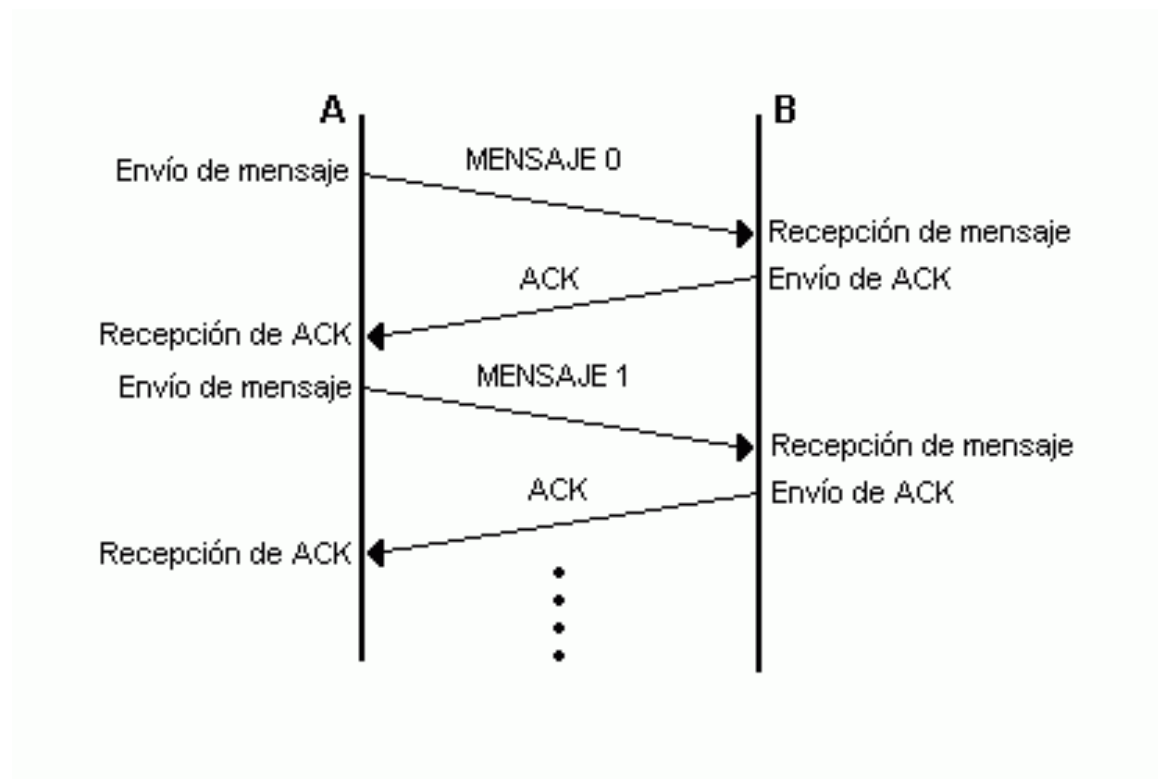
4.2 Algoritmos de control del flujo

Protocolos de parada y espera

El control del flujo se establece en que el emisor debe esperar a una confirmación por parte del receptor por cada bloque de datos enviado para poder continuar la transmisión.

Tiene un bajo aprovechamiento del medio físico, sobre todo cuando los retardos en el medio son elevados.

Protocolo unilateral de parada y espera. Canal sin errores

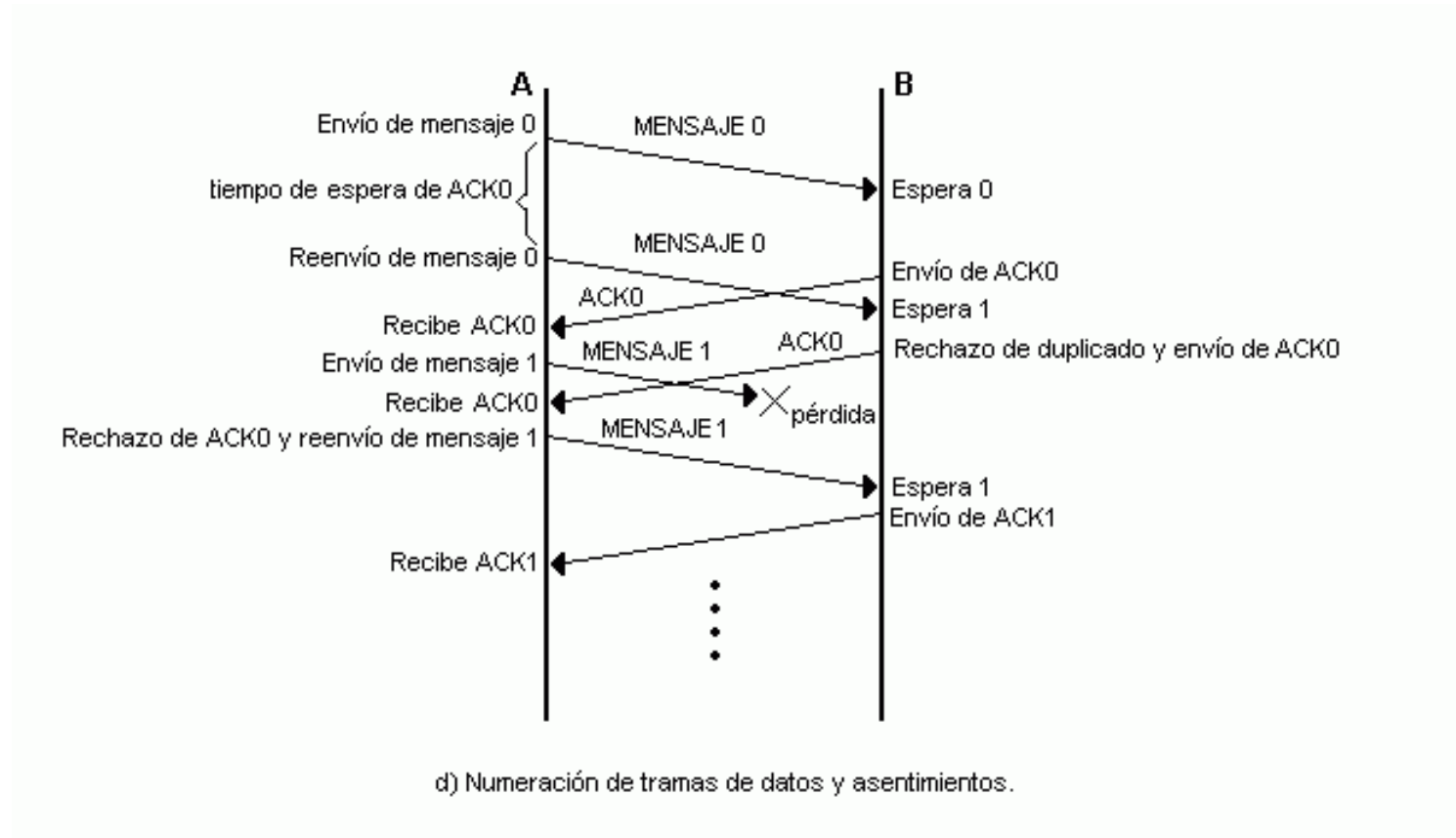


4.2 Algoritmos de control del flujo

Protocolos de parada y espera

Protocolo unilateral de parada y espera. Canal con errores

El control de la numeración de los paquetes de datos y asentimientos es suficiente para solventar los posibles errores, aunque el rendimiento de la comunicación es bajo debido a los retardos.

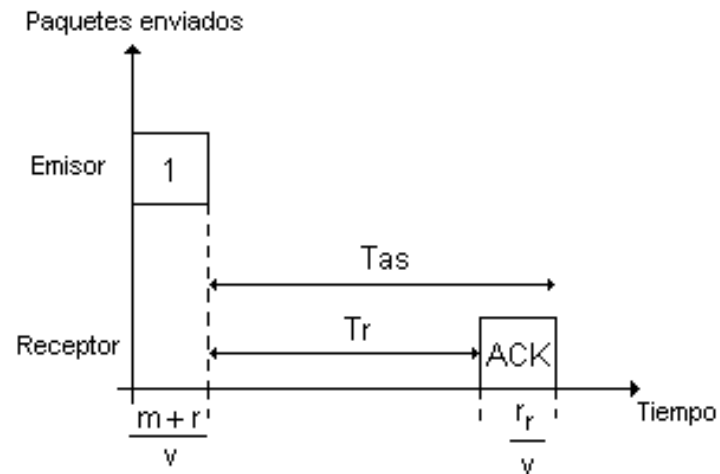


4.2 Algoritmos de control del flujo

Protocolos de ventana deslizante

Objetivo

Mejorar el aprovechamiento del canal de comunicación enviando datos aunque no se haya recibido el ACK de los datos.



Definiciones

Lista del emisor: conjunto de secuencias de numeración de los paquetes de datos.

Ejemplo: Si la numeración es con 3 bits, el número de secuencias es 8 (0-1-2-3-4-5-6-7)

Lista del receptor: conjunto de secuencias de numeración de los asentimientos de paquetes de datos.

Ejemplo: Si la numeración es con 3 bits, el número de secuencias es 8 (0-1-2-3-4-5-6-7)

4.2 Algoritmos de control del flujo

Protocolos de ventana deslizante

Definiciones

Ventana del emisor: Conjunto de secuencias de numeración de los paquetes que el emisor ha transmitido y de los que no ha recibido su ACK correspondiente.

Ventana del receptor: Conjunto de secuencias de numeración de los paquetes que el receptor espera recibir y de los que enviará ACK.

Tamaño de ventana del emisor: Número de secuencias en la ventana del emisor.

Tamaño de ventana del receptor: Número de secuencias en la ventana del receptor.

Funcionamiento del protocolo de ventana deslizante

Cada vez que el emisor envía un paquete de datos se añade su secuencia a la ventana del emisor. Existirá por tanto, un número máximo de secuencias en la ventana del emisor que se denomina ***Tamaño de la ventana del emisor (W_e)***

El receptor espera paquetes de datos cuya secuencia esté en la ventana del receptor. El número de secuencias en la ventana del receptor se denomina ***Tamaño de la ventana del receptor (W_r)***. Cuando se recibe un paquete con secuencia dentro de la ventana del receptor, se envía un ACK de la secuencia al emisor.

4.2 Algoritmos de control del flujo

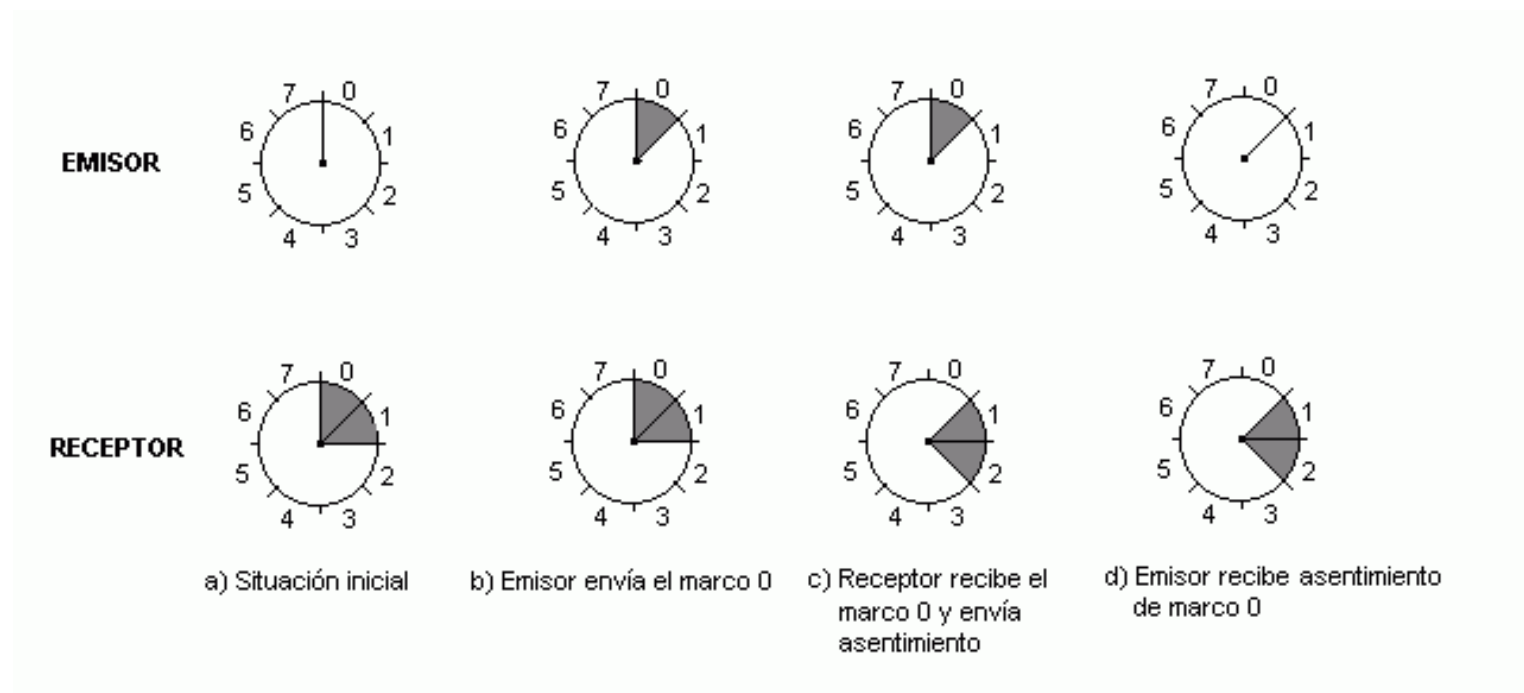
Protocolos de ventana deslizante

Ejemplo del funcionamiento del protocolo de ventana deslizante

Número de secuencias: 8 (0-7)

Tamaño de la ventana del emisor: 1

Tamaño de la ventana del receptor: 2

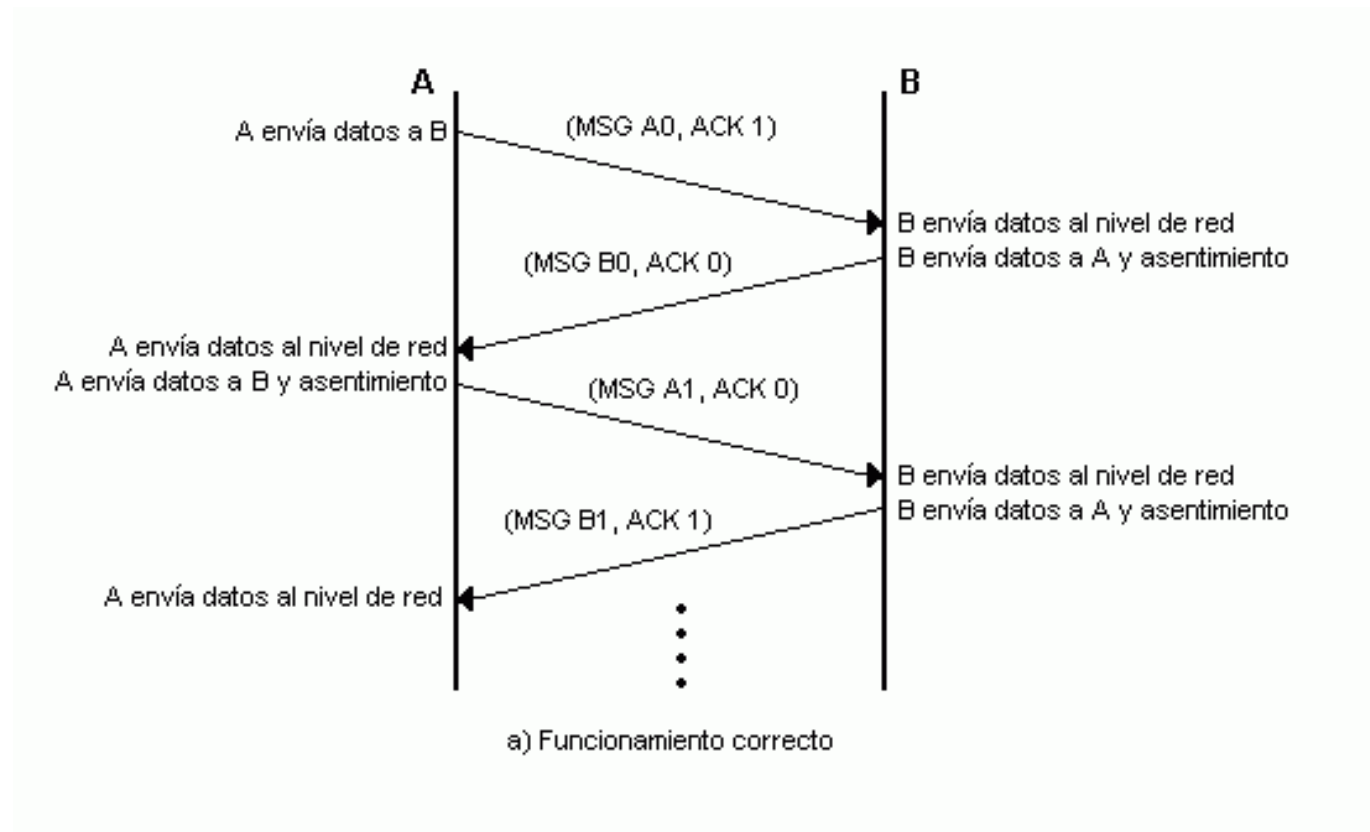


El tamaño de la ventana del emisor **VARÍA** y la del receptor es **CONSTANTE**

4.2 Algoritmos de control del flujo

Protocolos de ventana deslizante

Protocolo de ventana deslizante con numeración de 1 bit. $W_e=1$ y $W_r=1$



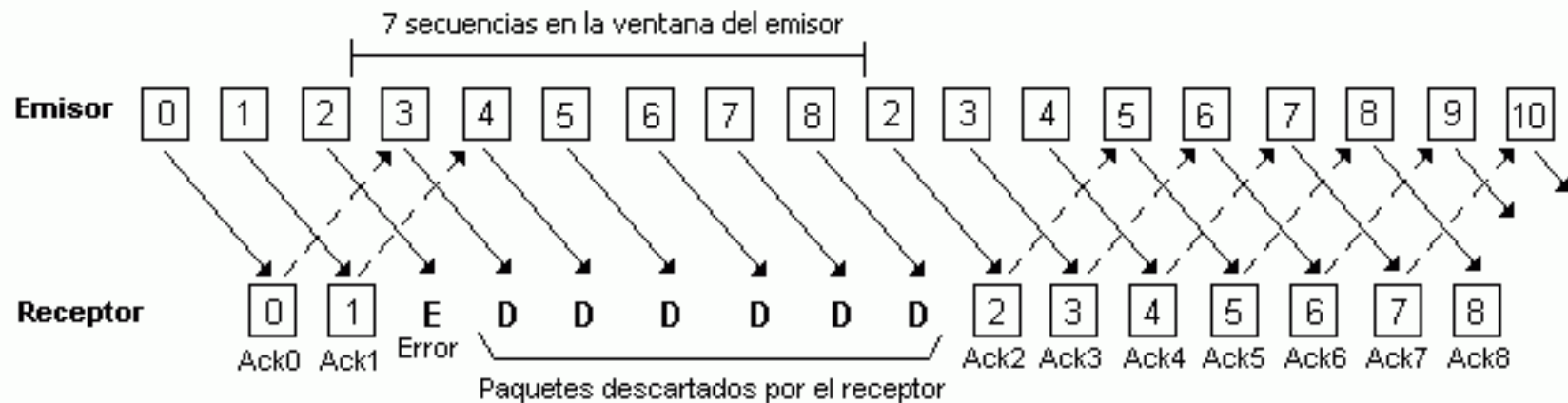
Los protocolos de ventana deslizante son bidireccionales pudiendo incorporar datos e información de confirmación en un mismo paquete.

4.2 Algoritmos de control del flujo

Protocolos de ventana deslizante

Protocolo de ventana deslizante con repetición no selectiva. $W_r=1$ SIEMPRE.

Ejemplo: $W_e=7$ y $W_r=1$. El medio físico es full-duplex.



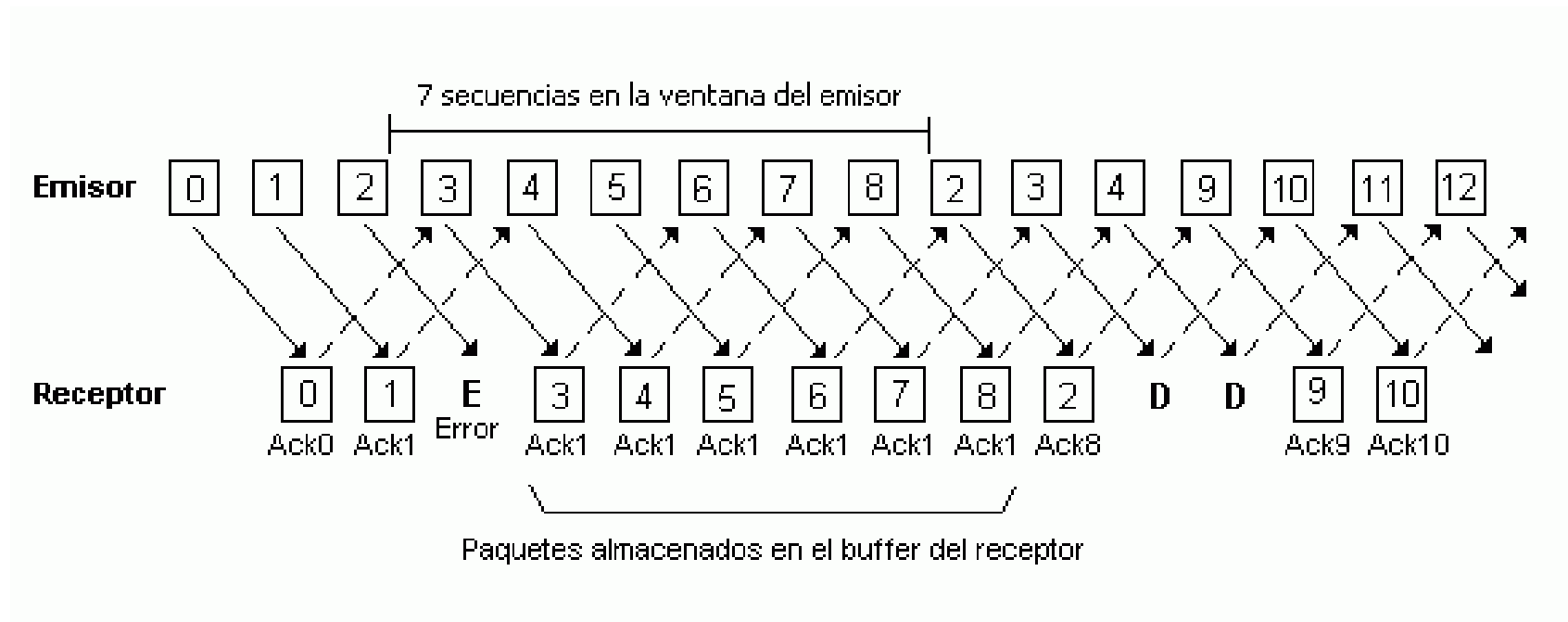
Cuanto mayor es la ventana del emisor mayor desaprovechamiento del medio físico se consigue al producirse un error.

4.2 Algoritmos de control del flujo

Protocolos de ventana deslizante

Protocolo de ventana deslizante con repetición selectiva. $W_r > 1$ SIEMPRE.

Ejemplo: $W_e = 7$ y $W_r = 7$. El medio físico es full-duplex.



En este ejemplo se aprecia un desaprovechamiento en el medio físico debido al retardo en el envío del ACK8.

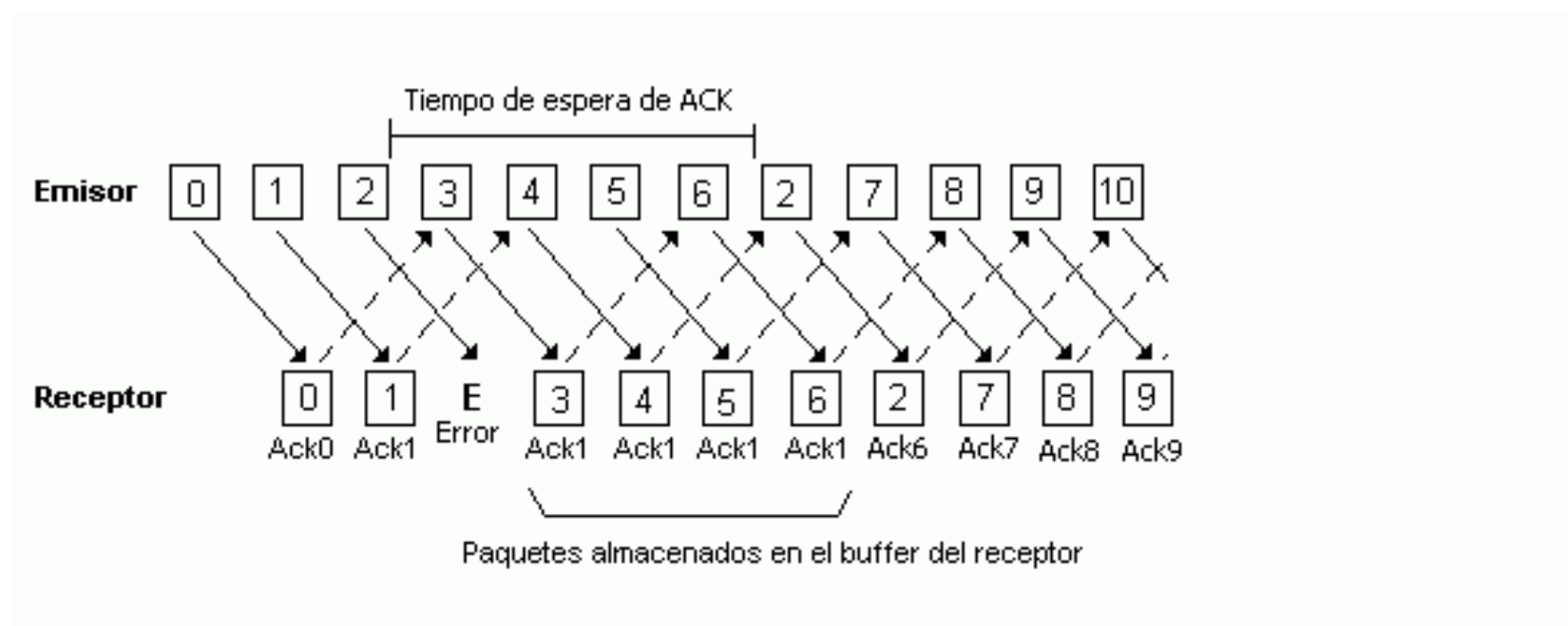
4.2 Algoritmos de control del flujo

Protocolos de ventana deslizante

Protocolo de ventana deslizante con repetición selectiva. $W_r > 1$ SIEMPRE.

Introducción de un tiempo de espera de ACK en el emisor inferior el tiempo de llenado de la ventana del emisor.

Ejemplo: $W_e = 7$ y $W_r = 7$. El medio físico es full-duplex.



Se evita el efecto del retardo en el envío de ACK's.

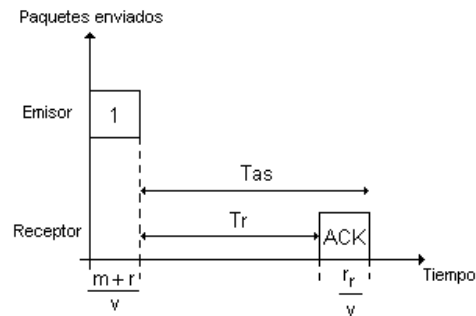
4.2 Algoritmos de control del flujo

Protocolos de ventana deslizante

Elección del tamaño de la ventana del emisor y del receptor

Ventana del emisor

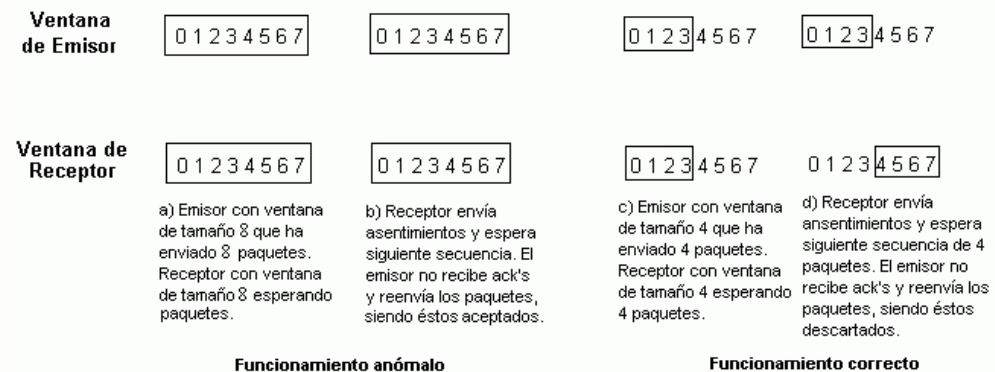
La ventana del emisor debe permitir como MÍNIMO transmitir paquetes hasta que llega el primer ACK de datos.



$$W_{emisor} = \frac{T_{total}}{T_{trama}} = \frac{\frac{m+r}{v} + T_{as}}{\frac{m+r}{v}} = \frac{m+r + v \cdot T_{as}}{m+r}$$

Ventana del receptor

La ventana del receptor no debe permitir repeticiones de secuencia en una rotación completa.



Funcionamiento anómalo

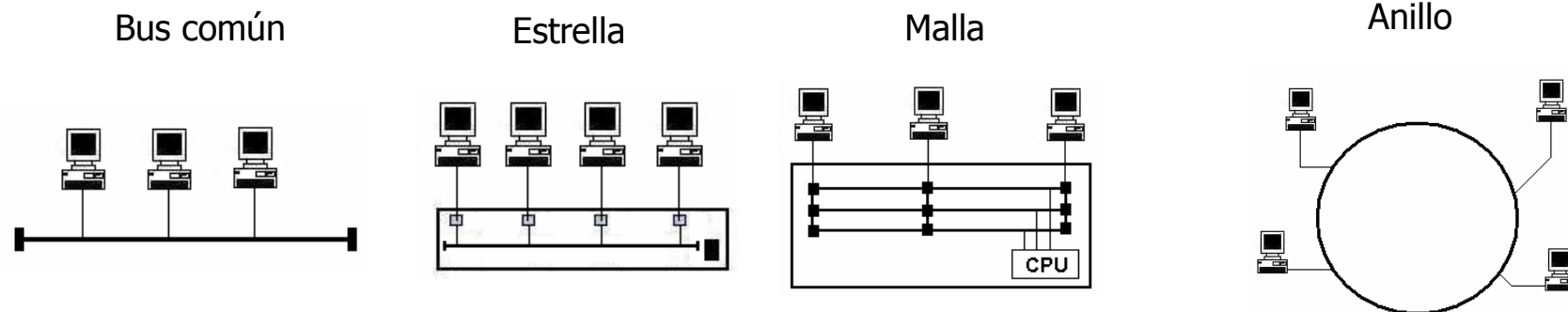
Funcionamiento correcto

4.3 Redes LAN. Normas IEEE 802.x

Definición

Una Red de Área Local (LAN – Local Area Network) se caracteriza por la interconexión de un conjunto de equipos en una extensión física reducida (metros – varios Km) y empleando un medio físico compartido.

Topologías en LAN



Necesidad de un mecanismo de reparto del medio físico

Velocidades de transmisión en LAN

10 Mbps – 10 Gbps

Medios físicos en LAN

Cables eléctricos, fibra óptica y comunicación inalámbrica (radio, infrarrojos)

4.3 Redes LAN. Normas IEEE 802.x

Arquitectura de red en LAN

Modelo TCP/IP

Aplicación
Transporte
Red
Nivel de Acceso a la Red

La arquitectura TCP/IP se desarrolla para funcionamiento en entorno WAN (nivel de red necesario para el encaminamiento)

El nivel de acceso a la red proporciona un mecanismo de intercambio de paquetes en un medio físico de transmisión (equivalente a niveles físico y de enlace en OSI)

Una red LAN puede intercambiar información empleando los niveles de enlace y físico

Modelo TCP/IP

El IEEE desarrolla una normativa para el intercambio de información en una LAN desarrollando una arquitectura de 3 niveles (LLC, MAC y físico).

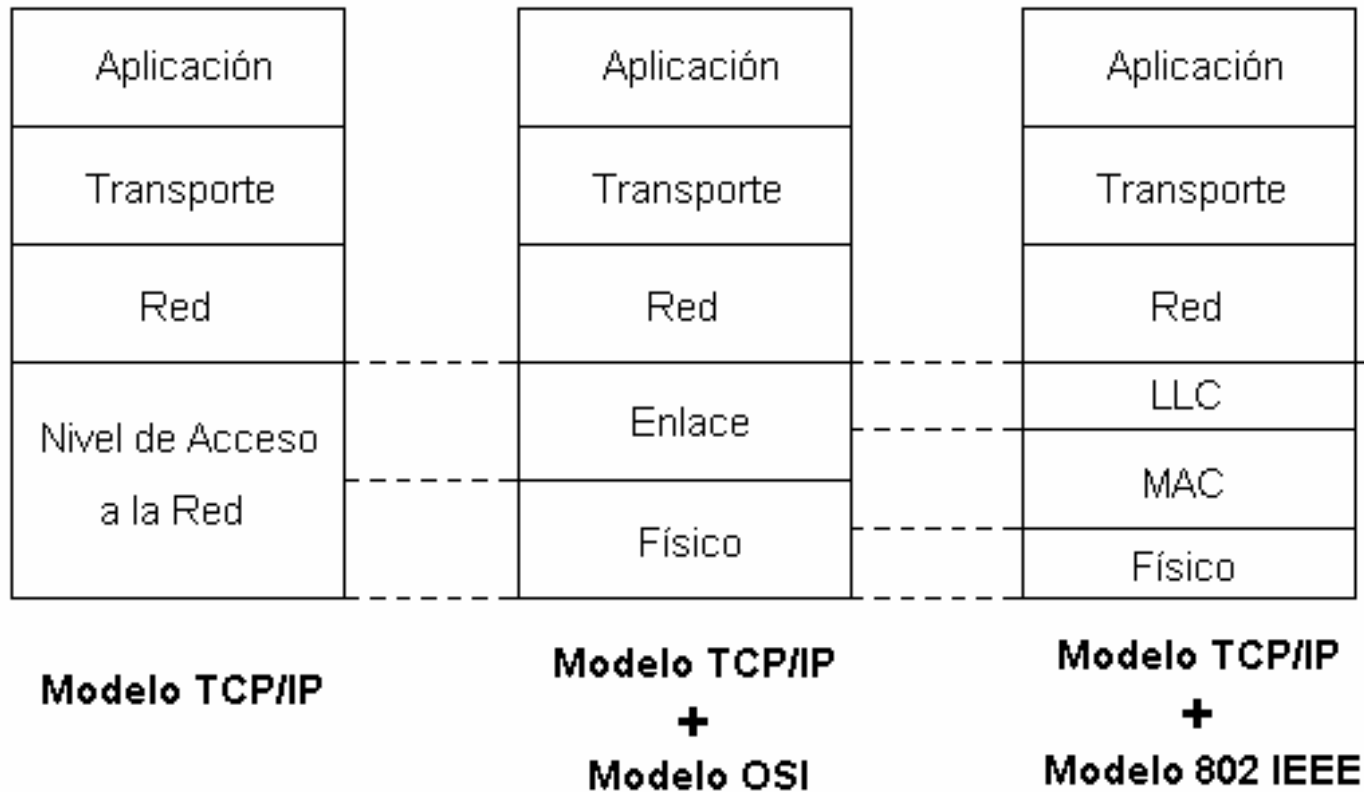
La normativa del IEEE se denomina **Modelo de Referencia IEEE 802**, que posteriormente fue adoptada por el ISO debido a su fácil integración en el modelo de arquitectura OSI.

Realmente, el modelo de referencia IEEE 802 son un conjunto de normas denominadas **normas IEEE 802.x**

4.3 Redes LAN. Normas IEEE 802.x

Arquitectura de red en LAN

Incorporación del modelo del IEEE en el modelo TCP/IP



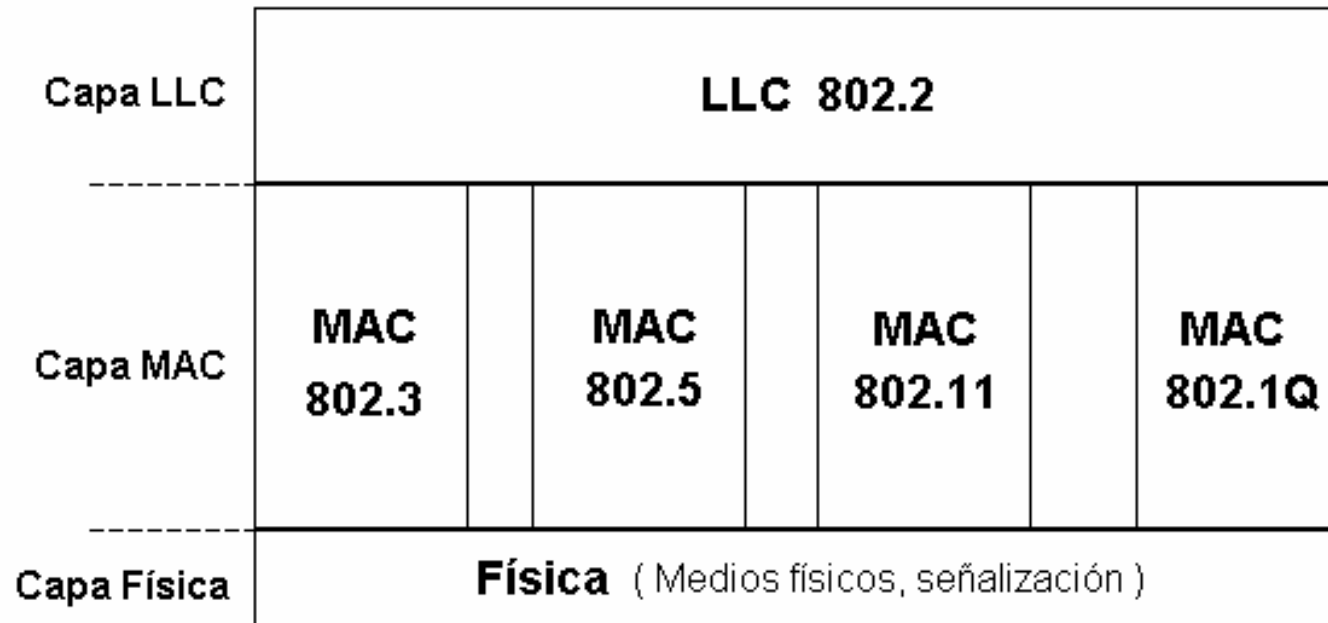
LLC: Control del Enlace Lógico. Funcionalidad de control del flujo y de errores.

MAC: Control de Acceso al Medio. Funcionalidades de reparto del medio físico, direccionamiento físico, etc.

4.3 Redes LAN. Normas IEEE 802.x

Arquitectura de red en LAN

Arquitectura IEEE 802



IEEE 802.2: Protocolo de Control del Enlace Lógico (LLC)

IEEE 802.3: Ethernet (CSMA/CD)

IEEE 802.5: Token Ring (Anillo con testigo)

IEEE 802.11x: LAN Inalámbrica

IEEE 802.1Q: LAN Virtual (VLAN)

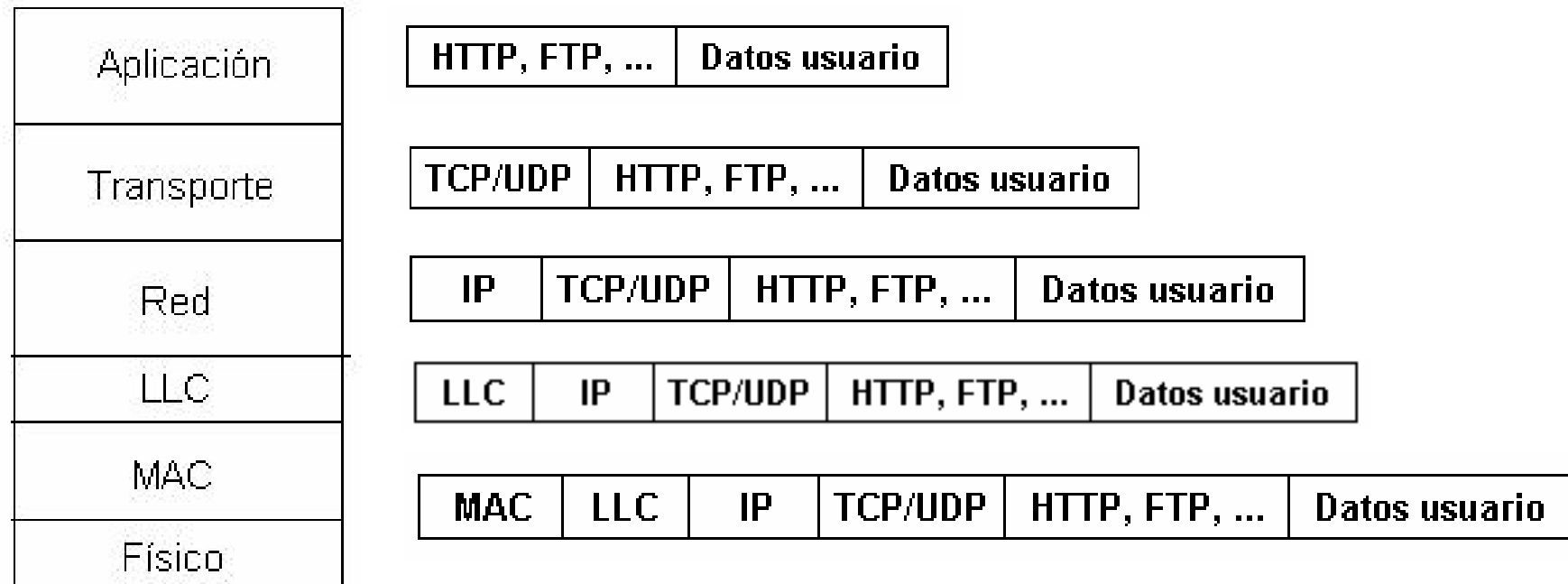
4.3 Redes LAN. Normas IEEE 802.x

Arquitectura de red en LAN

Integración TCP/IP con IEEE 802

En el documento RFC 1042 se describe cuál es el procedimiento para la transmisión de paquetes IP en redes LAN que soportan las normas del IEEE.

En **general** (excepto en el caso del IEEE 802.3 Ethernet que tiene dos formatos de paquete) la arquitectura TCP/IP emplea como capas inferiores la LLC, MAC y física del IEEE.



4.3 Redes LAN. Normas IEEE 802.x

Arquitectura de red en LAN

Protocolo IEEE 802.2 LLC

El protocolo LLC (Protocolo de Control del Enlace Lógico) se diseñó para proporcionar un conjunto de funcionalidades asociadas a la capa de Enlace del modelo OSI.

Para ello se basó en el protocolo HDLC (Protocolo de Control del Enlace de Alto Nivel) proporcionando 3 tipos de servicio al nivel superior, es decir 3 mecanismos para el envío de paquetes del nivel de red (IP):

Servicio no orientado a conexión y sin confirmación: Servicio sin control de errores ni de flujo, pero muy rápido en funcionamiento (servicio tipo 1). **Es el empleado por TCP/IP.**

Servicio orientado a conexión: Servicio con control de errores y de flujo. Funcionamiento más lento (servicio tipo 2).

Servicio no orientado a conexión con confirmación: Servicio con confirmación de paquetes (servicio tipo 3).

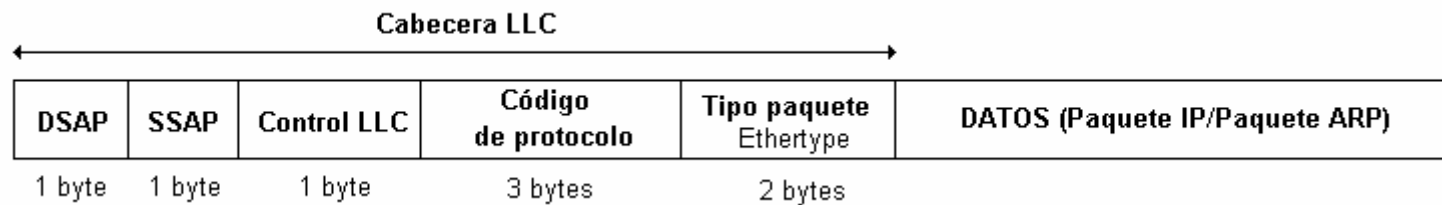
El protocolo LLC está implementado en los drivers del dispositivo de comunicación (tarjeta de red) que emplea las normativas IEEE 802.

4.3 Redes LAN. Normas IEEE 802.x

Arquitectura de red en LAN

Protocolo IEEE 802.2 LLC

Formato de paquete LLC para redes TCP/IP



DSAP: Punto de Acceso al Servicio de Destino. En el caso de arquitectura TCP/IP tiene asociado el valor 170.

SSAP: Punto de Acceso al Servicio de Origen. En el caso de arquitectura TCP/IP tiene asociado el valor 170.

Control LLC: En el caso de arquitectura TCP/IP tiene asociado el valor 3.

Código de protocolo: Indica qué tipo de información viene a continuación. En el caso de la arquitectura TCP/IP tiene asociado el valor 0.

Tipo paquete: Los paquetes de datos IP tienen asociados el valor 2048 (0x0800), y los paquetes ARP el valor 2054 (0x0806).

4.4 IEEE 802.3 Ethernet

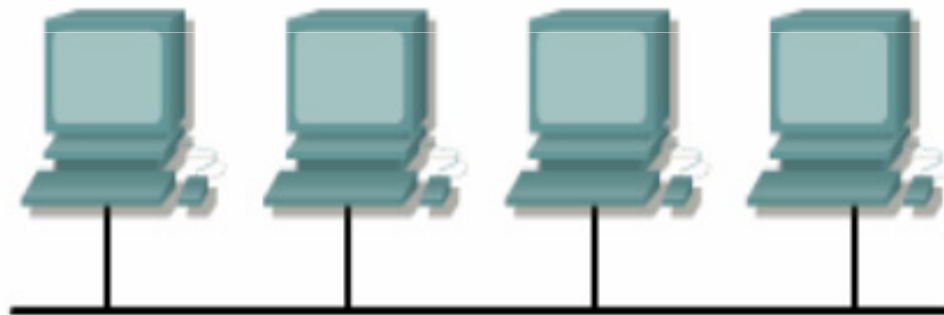
4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Orígenes

El origen de las redes Ethernet está en el desarrollo de Xerox en 1975 de la primera red local de bus común a una velocidad de 2.94 Mbps.

Posteriormente Xerox, Intel y Digital desarrollan una red Ethernet a 10 Mbps que es el fundamento del estándar IEEE 802.3.

Una red Ethernet se caracteriza por emplear un medio físico compartido entre todas las estaciones con topología de bus.



El medio físico empleado puede ser cable coaxial, cable par trenzado o fibra óptica, definiendo distintos "modelos tecnológicos" de redes Ethernet.

Debido a la necesidad de compartir el medio físico, las redes Ethernet son **semiduplex** y emplean un mecanismo denominado **CSMA/CD** para el reparto del medio físico.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Ethernet 10Base2

Las diferentes versiones tecnológicas de Ethernet se denominan empleando la nomenclatura:

Velocidad-Señalización-Medio físico

10Base2 significa: Red Ethernet a 10 Mbps, señalización en banda base (**Manchester**) y medio físico cable coaxial fino.

Velocidad: 10 (Mbps), 100 (Mbps), 1000 (Mbps), 10G (Gbps)

Señalización: Base (banda base) o Broad (banda modulada)

Medio físico: T (cable UTP), C (cable STP), F (fibra óptica), X (soporte para varios medios físicos)

10Base2 es una de las primeras versiones de Ethernet empleando cable coaxial fino. Permite una velocidad de 10 Mbps a distancias de 185 metros.

10Base5 emplea cable coaxial grueso, permitiendo una velocidad de 10 Mbps a distancias de hasta 500 metros.

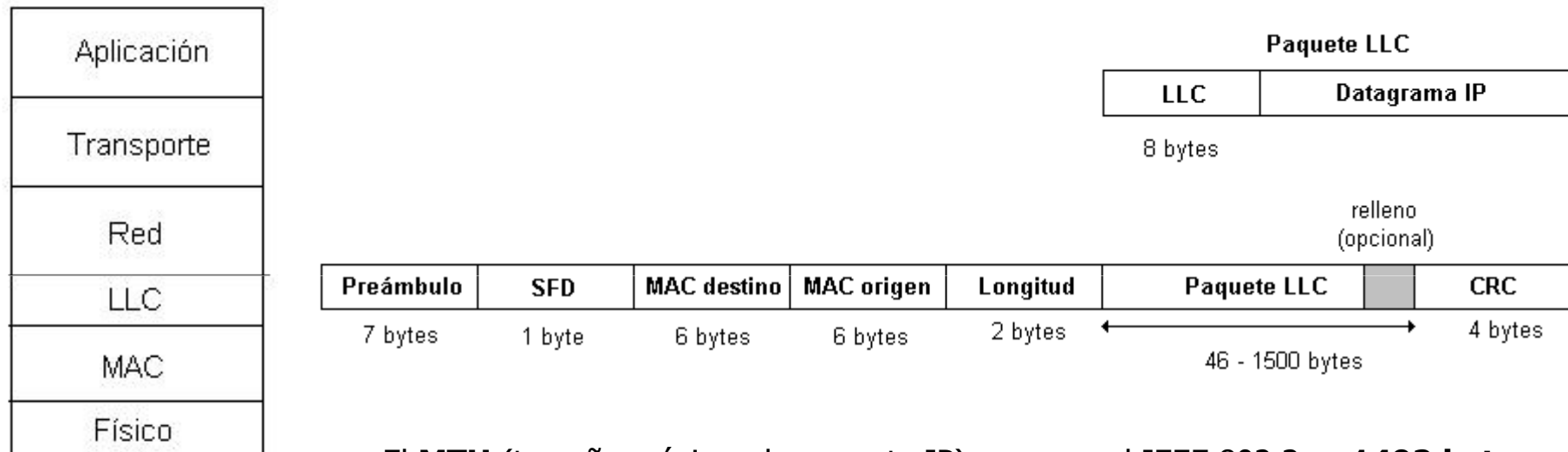
10Base2 y **10Base5** desaparecen del mercado con la introducción de los cables UTP (más tolerancia a fallos, facilidad de implantación y mejores prestaciones)

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Formato de paquete IEEE 802.3

La normativa IEEE 802.3 establece un formato de paquete donde se especifica la cabecera MAC



Modelo TCP/IP
+
Modelo 802 IEEE

El **MTU** (tamaño máximo de paquete IP) en una red IEEE 802.3 es **1492 bytes**

Preámbulo: Secuencia de 7 bytes 10101010

SFD: Delimitador de inicio de trama 10101011

MAC destino/origen: Identificador de 48 bits para cada equipo

Longitud: Tamaño del campo de datos del paquete (máximo 1500)

CRC: Código de Redundancia Cíclica de 32 bits para detección de errores

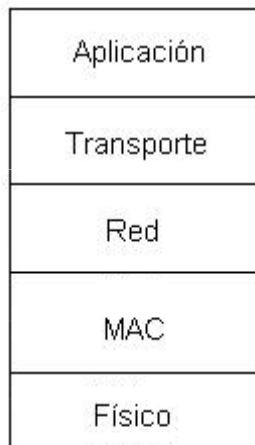
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

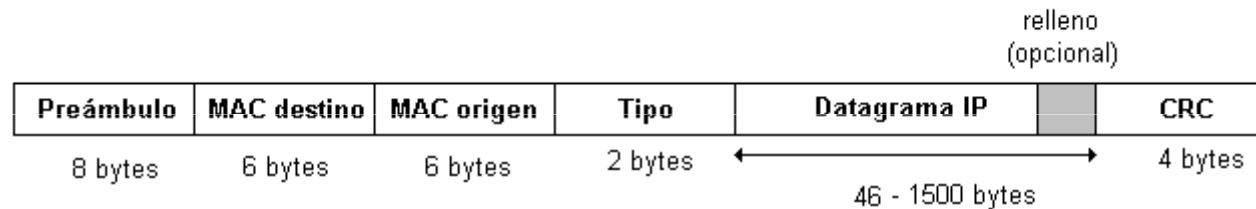
Formato de paquete Ethernet II

Las redes Ethernet de Digital/Intel/Xerox (Ethernet **DIX**) emplean un formato de paquete distinto

Este formato, denominado Ethernet II, no emplea la capa LLC y permite la introducción del datagrama IP en el paquete de nivel MAC



Modelo TCP/IP
+
Ethernet DIX



El **MTU** (tamaño máximo de paquete IP) en una red Ethernet DIX es **1500 bytes**

Este es el formato de paquete Ethernet empleado con redes TCP/IP

Preámbulo : Equivalente al campo Preámbulo + SFD del IEEE 802.3

Tipo: Código para identificar el protocolo del contenido del paquete MAC (ARP/IP)

Tipo = **0x0806** Protocolo ARP

Tipo = **0x0800** Protocolo IP

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

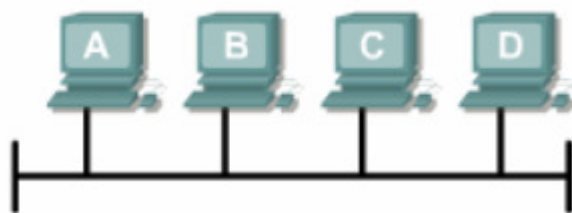
CSMA/CD – Acceso al medio con detección de portadora y de colisión

Tanto Ethernet DIX como IEEE 802.3 emplean el mismo mecanismo para compartir el bus común: CSMA/CD

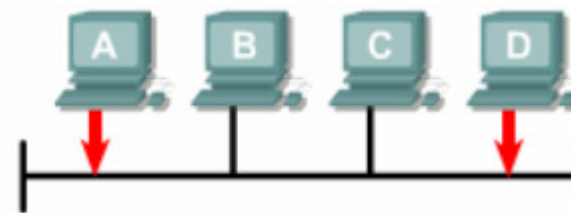
El esquema básico de funcionamiento del CSMA/CD consiste en comprobar el medio físico antes de transmitir un paquete de datos.

El esquema de funcionamiento de CSMA/CD **siempre es semiduplex**

Problema en CSMA: colisión por comprobación simultánea del bus por dos o más estaciones.



Medio físico libre

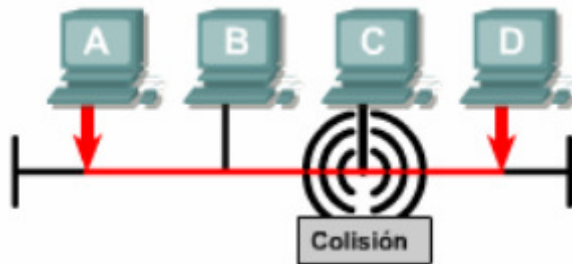


Transmisión simultánea

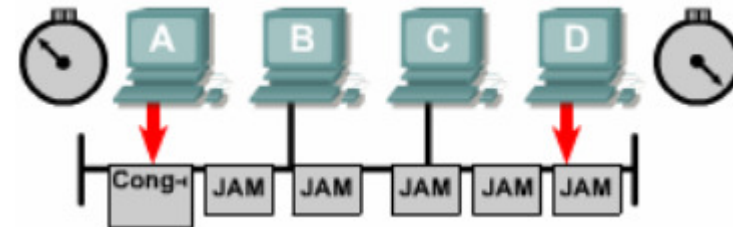
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

CSMA/CD – Acceso al medio con detección de portadora y de colisión



Detección de colisión simultánea a la transmisión



Resolución de colisiones

Para asegurar que dos estaciones que transmiten simultáneamente detectan la colisión, es necesario que la transmisión dure lo suficiente para llegar al otro extremo.

En Ethernet se define la extensión máxima de la red (con repetidores) en 2.5 Km (5 buses de 10Base5).

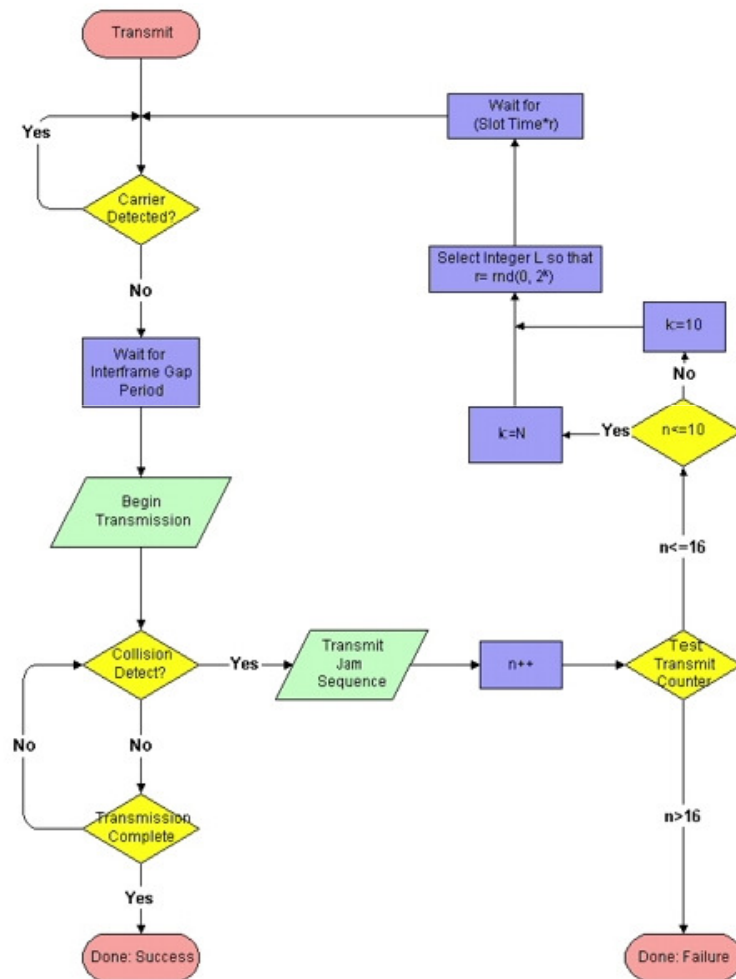
En una red a 10 Mbps y 2.5 Km de extensión, el tiempo mínimo de transmisión necesario son 512 tiempos de bit, es decir un paquete ethernet de 64 bytes (46 bytes de datos y sin tener en cuenta el preámbulo).

Al tiempo mínimo de transmisión se le denomina **ranura temporal**.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Algoritmo CSMA/CD - Transmisión



1. Escucha del medio antes de la transmisión

2. Tiempo de espera entre tramas (96 tiempos de bit)

$$T_{espera} = 96/10000000 = 9.6 \mu \text{ segundos}$$

3. Transmisión del paquete escuchando el medio

4. La **colisión** se detecta cuando la señal en el medio tiene una tensión anómala (superposición de señales)

5. Si una estación detecta una colisión la refuerza, transmitiendo una señal denominada **JAM** (señal de congestión)

6. El paquete que ha colisionado es reenviado hasta en 16 intentos

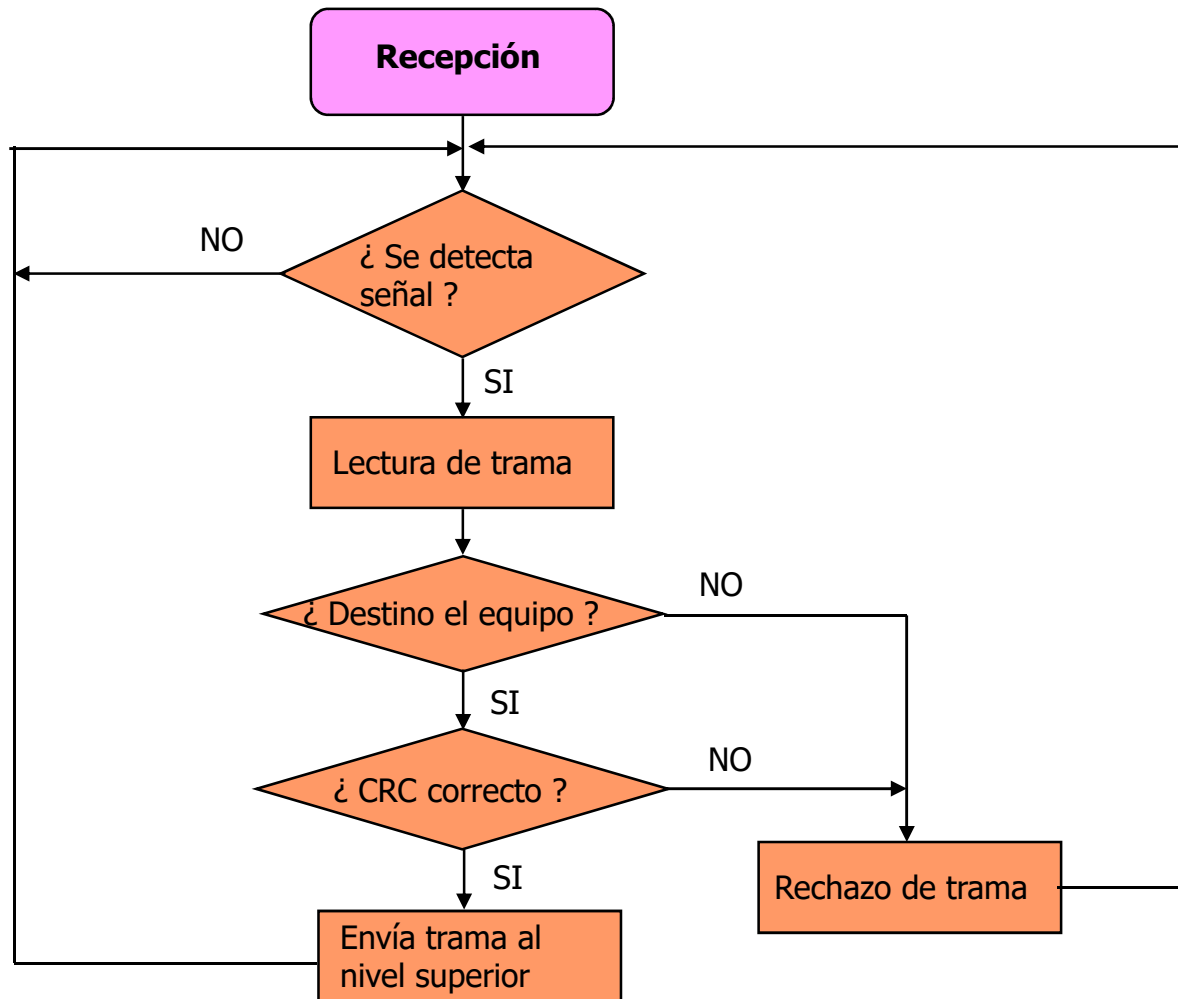
7. En cada intento se espera un número aleatorio de veces el denominado **tiempo de ranura** (regresión exponencial).

8. El tiempo de ranura se determina como el doble del tiempo mínimo que tarda un bit en propagarse en la red ethernet (51.2 μ segundos)

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Algoritmo CSMA/CD – Recepción



1. El preámbulo permite sincronizar el receptor con la trama a leer (modo asíncrono)

2. La interpretación del campo dirección destino en la trama es inmediato.

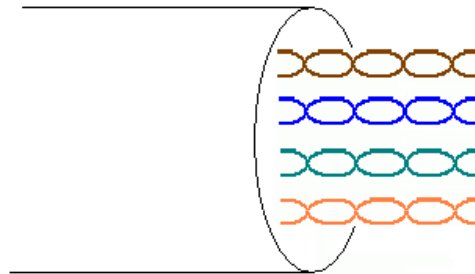
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

10BaseT – Concentrador Ethernet (Hub)

La red 10BaseT surge con la introducción de los cables pares trenzados no blindados (UTP)

Un cable UTP comercial está formado por 4 pares de hilos trenzados



La categoría del cable UTP (3,5,6) hace referencia al ancho de banda de los pares de hilos

Categoría 3: 30 MHz

Categoría 5: 100 MHz

Categoría 6: 250 MHz

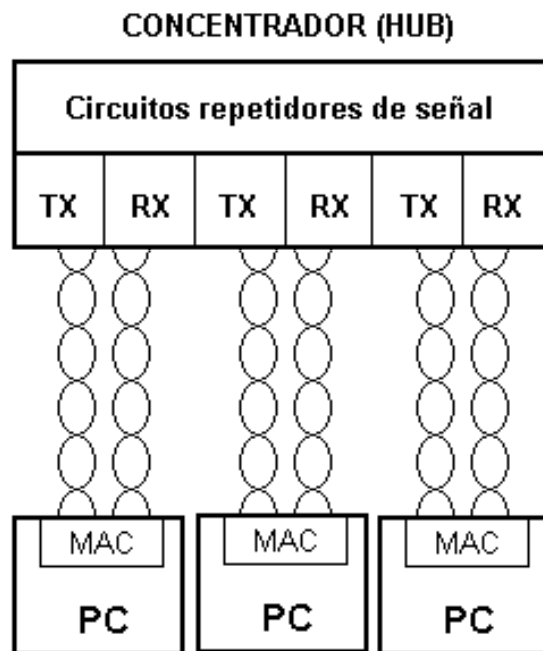
10BaseT emplea cable de categoría 3 con codificación Manchester, alcanzado sin problemas la velocidad de **10 Mbps** a distancias de **100 metros**.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

10BaseT – Concentrador Ethernet (Hub)

La red 10BaseT emplea una topología en estrella, donde el elemento central se denomina **concentrador** o **hub**.



Las colisiones se detectan cuando se recibe una señal por el par de recepción al mismo tiempo que se transmite una trama.

La detección de problemas en el cableado es más fácil que con cable coaxial.

La distancia máxima entre equipo y concentrador debe ser inferior a 100 m.

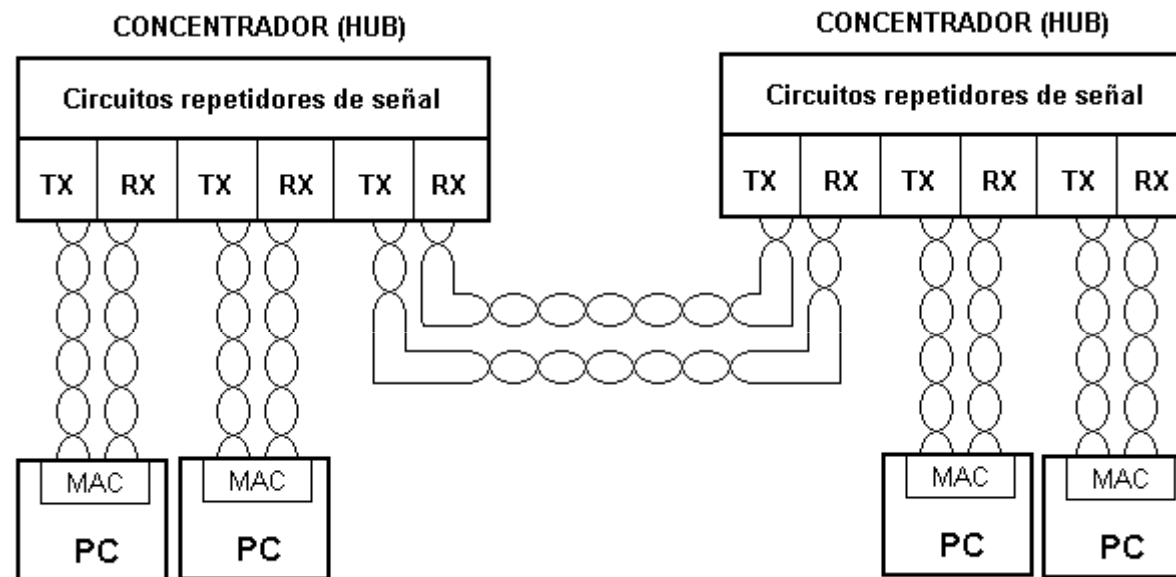
La red Ethernet puede crecer en tamaño interconectando concentradores con cables UTP cruzados (repetidores).

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Repetidores

La conexión de concentradores en cascada permite el aumento en el tamaño físico de la red Ethernet.



El número máximo de hubs que pueden colocarse en cascada (el retardo afecta al funcionamiento del CSMA/CD), está limitado por la extensión máxima de una red Ethernet que son 2.5 kilómetros (en 10Base5: 5 segmentos – 4 repetidores).

Dominio de colisión: Conjunto de dispositivos en una red que pueden colisionar al transmitir simultáneamente

Inconveniente del hub: **incrementa la probabilidad de colisiones al ser mayor el dominio de colisión**

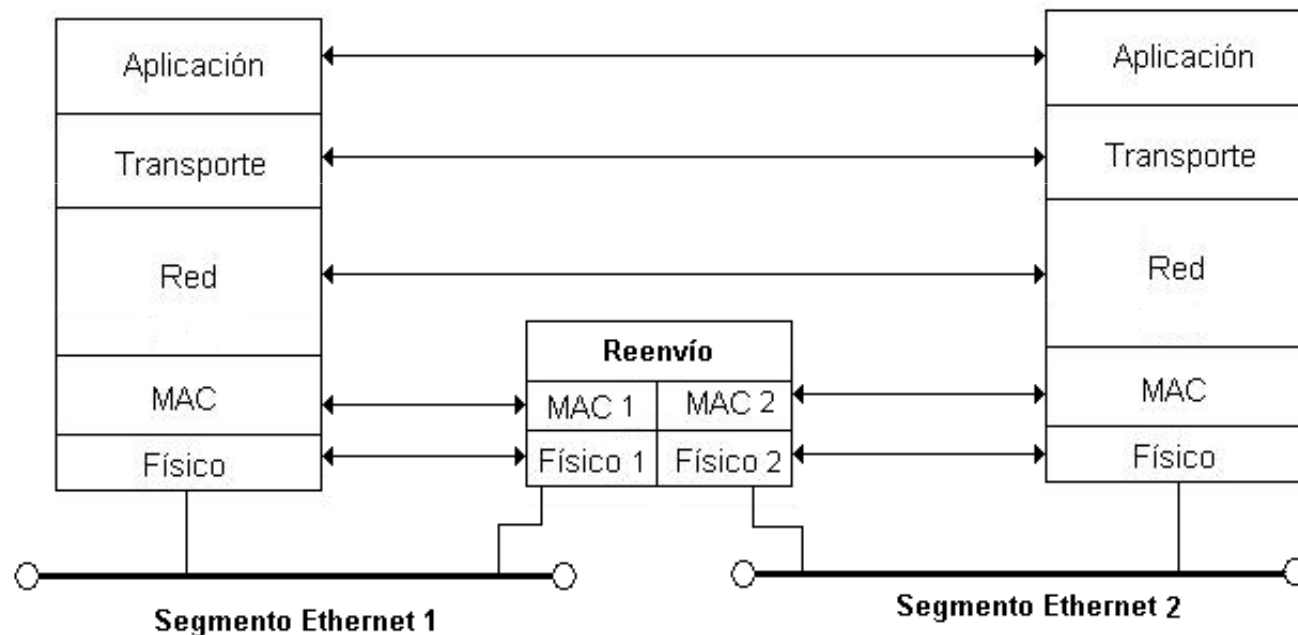
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes

La interconexión de segmentos Ethernet puede mejorarse (reducir el número de colisiones) empleando **puentes** o **bridges**.

Un puente es un dispositivo de interconexión entre dos o más segmentos Ethernet que analiza la cabecera MAC de los paquetes para determinar si hay que reenviarlos o no de un segmento a otro.



El puente divide la red en **segmentos de colisión independientes**, por lo que las LAN interconectadas con puentes no tienen limitación de extensión física al crecer.

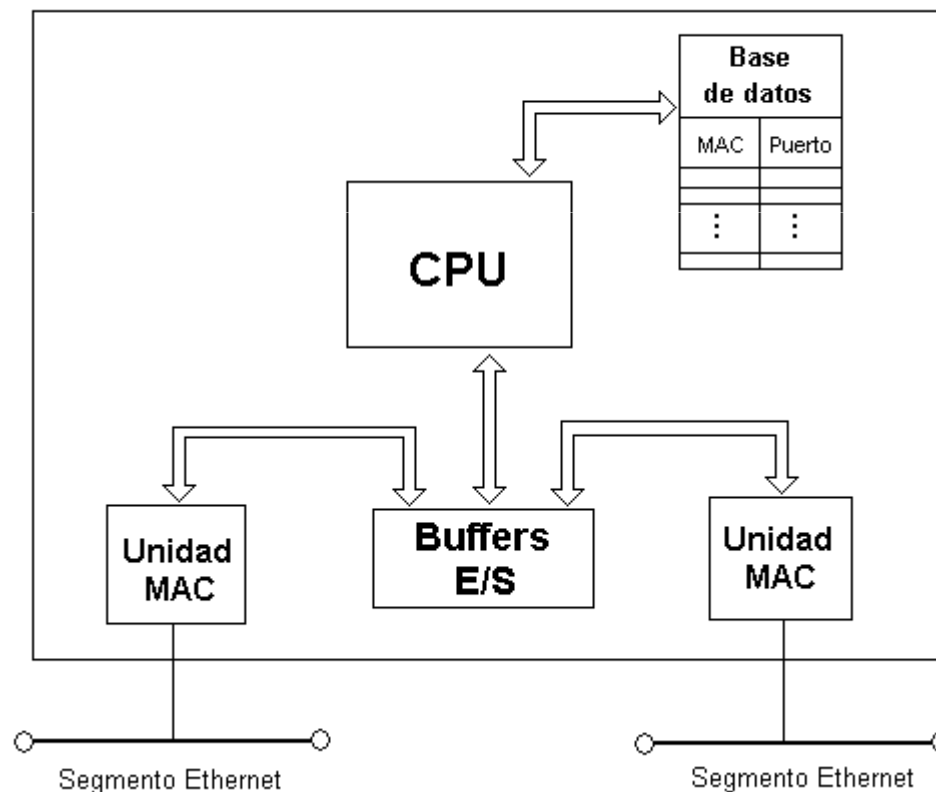
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Los puentes denominados **puentes transparentes** son aquellos en los que la decisión de cómo los paquetes se intercambian entre segmentos la toman ellos (los equipos no conocen la estructura de la red)

Estructura interna de un puente transparente



CPU: Unidad de control de funcionamiento del puente (reenvío de paquetes y aprendizaje)

Buffers E/S: Unidad de almacenamiento de tramas en proceso (lectura/envío). FIFO.

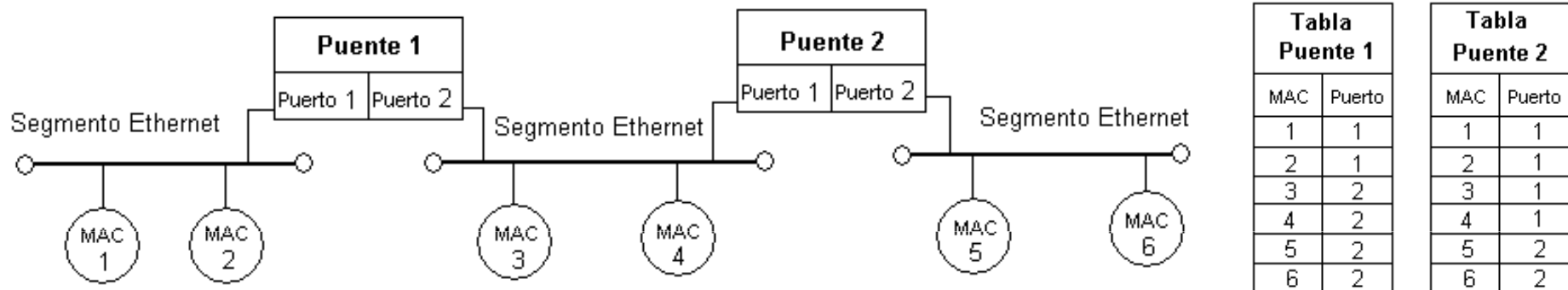
Base de datos: Tabla de asociación de direcciones MAC con números de puerto (**tabla de reenvío**).

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Ejemplo de tablas en puentes



La inicialización de la tabla requiere de un proceso de aprendizaje automático

Un puente trabaja en dos modos simultáneamente: **modo de reenvío** y **modo de aprendizaje**

Un puente lee **todos** los paquetes recibidos por un puerto (modo promiscuo) y los almacena en un buffer para procesarlos.

El algoritmo de funcionamiento de un puente transparente se especifica en la normativa IEEE 802.1D MAC Bridge.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Modo de reenvío

En el modo de reenvío se comprueba la dirección MAC de destino de cada paquete Ethernet que llega a un puerto.

Si la dirección MAC de destino se encuentra en la tabla de reenvío, el puente reenvía el paquete al puerto asociado (siempre que el puerto asociado sea distinto del puerto por donde ha llegado el paquete)

Si la dirección MAC de destino no existe en la tabla de reenvío, el paquete se reenvía a todos los puertos excepto por el que se recibió.

Los paquetes con dirección de destino la dirección de broadcast se reenvían a todos los puertos, excepto al puerto por el que se recibió el paquete de difusión.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Modo de aprendizaje

En el modo de aprendizaje se comprueba la dirección MAC de origen en cada paquete Ethernet recibido en un puerto.

Si la dirección MAC de origen no se encuentra en la tabla de reenvío, el puente crea una entrada con la dirección MAC de origen y el puerto donde se ha recibido.

Durante el proceso de aprendizaje, dado que no se conocen las direcciones MAC de los equipos, la mayor parte de los paquetes son reenviados por todos los puertos, por lo que los demás puentes aprenderán información. A este fenómeno se le conoce con el nombre de inundación.

Cada entrada en la tabla de reenvío de un puente tiene asociado un temporizador (segundos) que mide el tiempo desde que se creó la entrada en la tabla.

Si se recibe un paquete con una dirección MAC de origen por el puerto que se indica en la tabla de reenvío, el temporizador se inicializa a cero.

Si el temporizador alcanza un determinado valor máximo, la entrada de la tabla de reenvío se **elimina**. De esta forma las tablas de los puentes se ajustan a cambios en la estructura de la red.

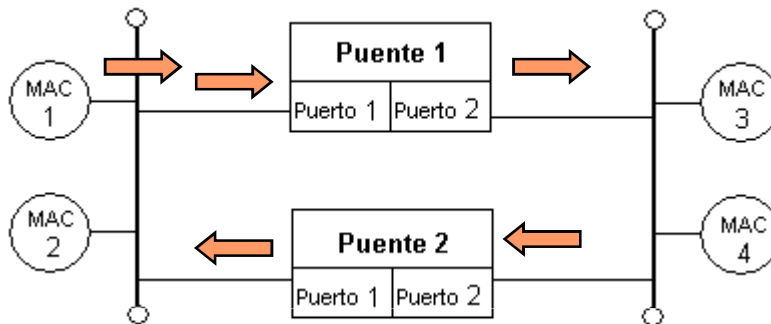
El modo de aprendizaje requiere que la LAN con puentes tenga una estructura de árbol simple (**árbol de expansión**).

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Estructura de árbol de expansión



Paquete de broadcast enviado por el equipo MAC 1

Los bucles provocan circulación indefinida de paquetes de broadcast y cambios continuos en las tablas de reenvío en el proceso de aprendizaje.

Interconexión de LAN's con bucles

Algoritmo de árbol de expansión: Algoritmo Spanning Tree

El algoritmo Spanning Tree define un protocolo de comunicación entre puentes que consigue una estructura de LAN's interconectadas por puentes sin existencia de bucles.

La definición de este algoritmo se encuentra en la norma IEEE 802.1D MAC Bridge.

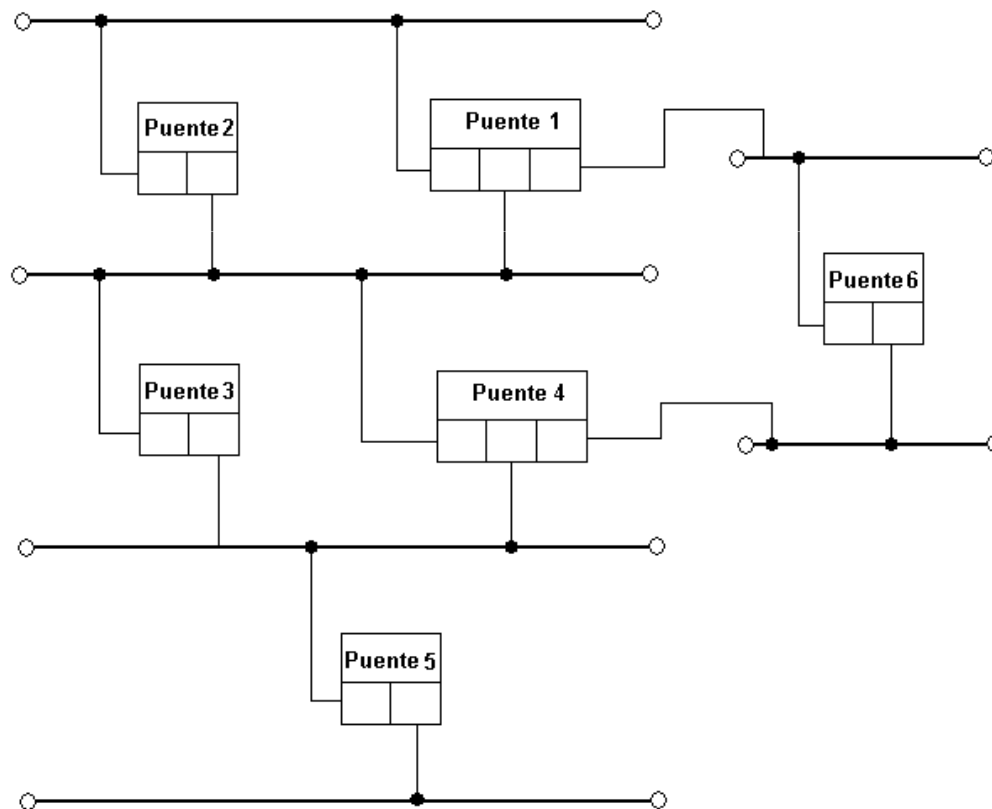
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Algoritmo de árbol de expansión: Algoritmo Spanning Tree

En numerosas ocasiones, la interconexión de LAN's se realiza con puentes en una disposición tolerante a fallos (existencia de bucles).



El algoritmo elige un puente (identificador más bajo) que será la raíz de la estructura de árbol (**puente raíz**).

En cada puente se determina un coste RPC (número de redes intermedias, velocidad de transmisión) desde cada puerto al puente raíz. Al puerto con menor coste se le denomina **puerto raíz del puente**.

En cada segmento se elige un **puerto designado**. El puerto designado de un segmento es el puerto con menor valor de RPC que esté conectado al mismo.

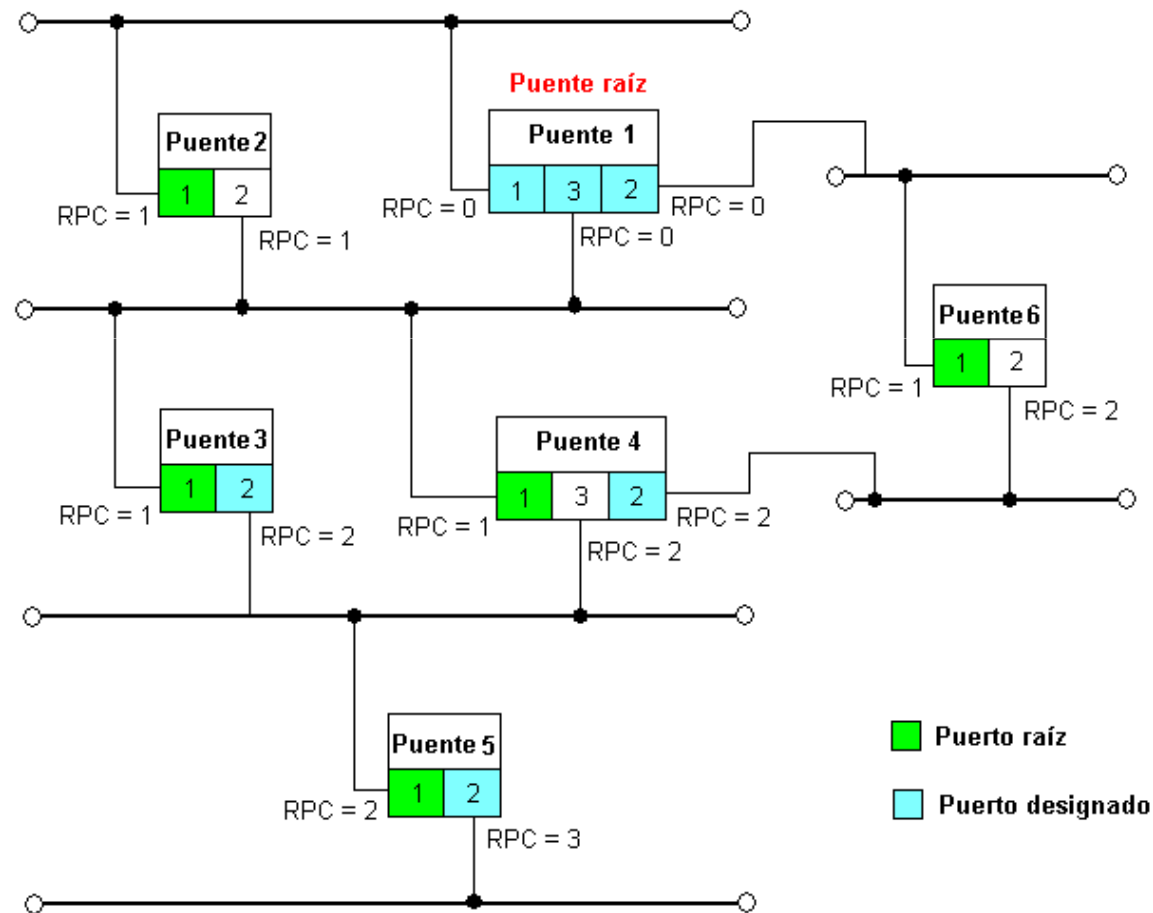
Finalmente, se activan todos los puertos raíz y designados de la red, determinando una estructura de árbol.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Algoritmo de árbol de expansión: Algoritmo Spanning Tree

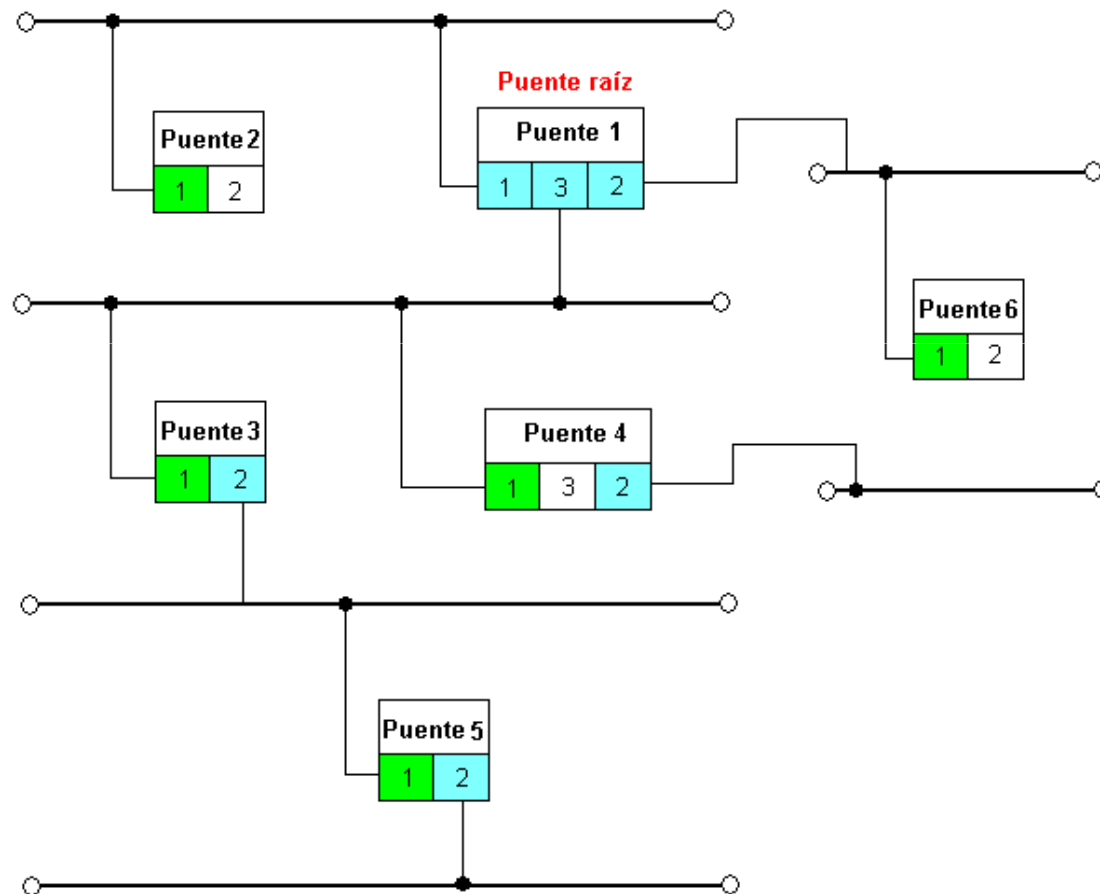


4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Puentes Transparentes

Algoritmo de árbol de expansión: Algoritmo Spanning Tree



Esta estructura se mantiene mientras que todos los puertos raíz y designados funcionen correctamente.

El puente raíz envía mensajes de control cada cierto tiempo.

Si un puente deja de recibir mensajes del puente raíz, se procederá de nuevo con el algoritmo Spanning Tree para determinar nuevos puertos raíz y designados.

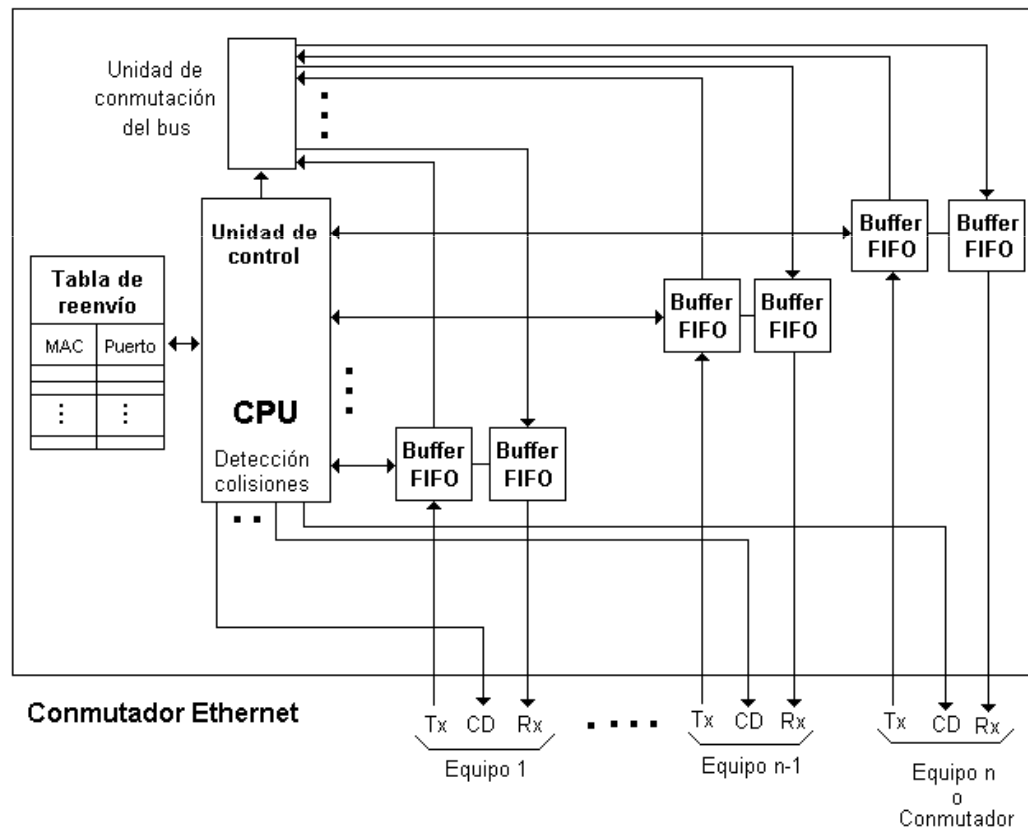
4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Ethernet Conmutada

El empleo de puentes llevó a la posibilidad de construir un puente multipuerto, donde en cada puerto se conecta un equipo en vez de un segmento de red.

Estos dispositivos se denominan **conmutadores** o **switches** definiendo las redes **Ethernet conmutadas**



Modo full-duplex: No existen colisiones (CSMA/CD no activo). Transmisión y recepción simultánea (no se emplea la línea CD).

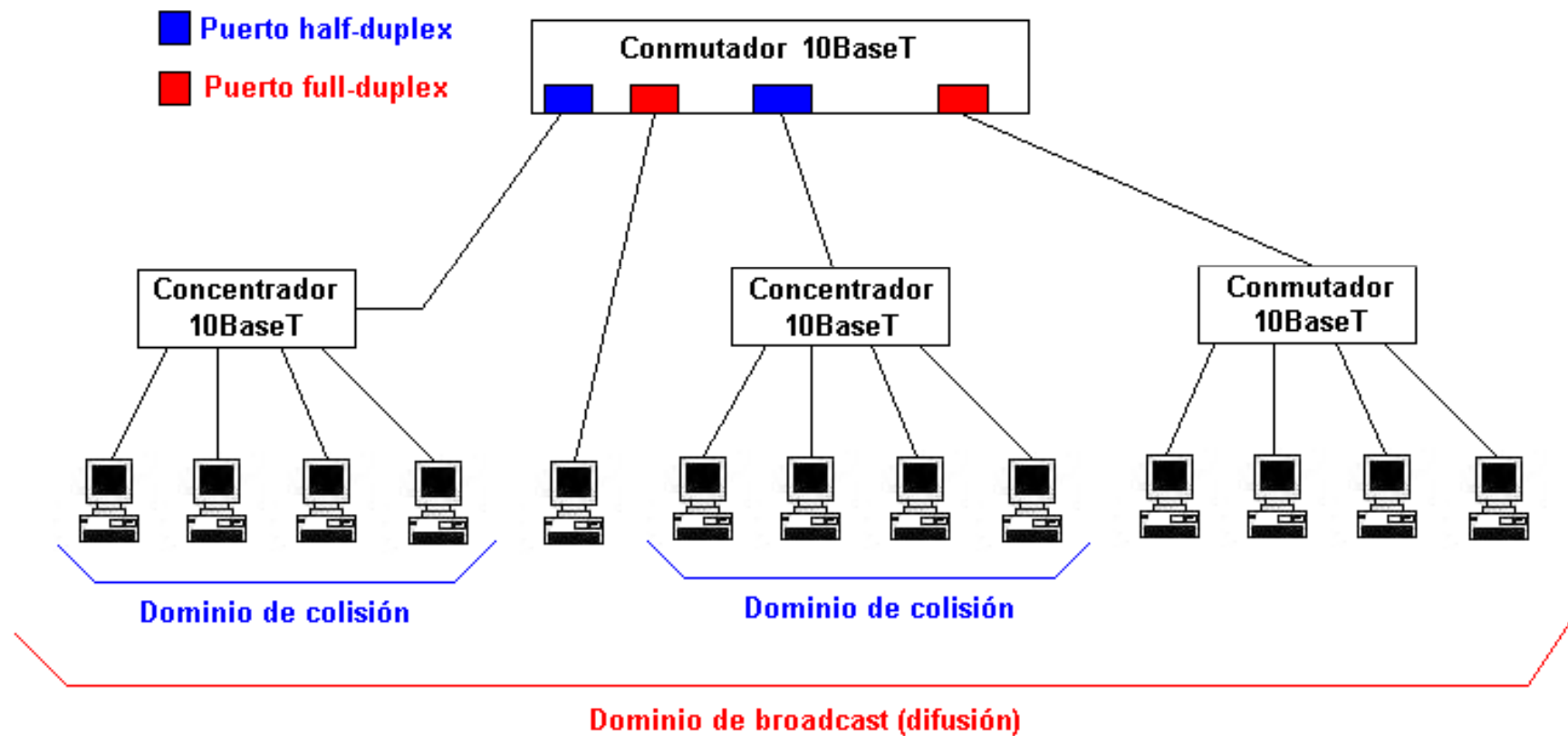
Modo half-duplex: Permite la conexión de equipos con CSMA/CD (concentrador 10BaseT). Se emplea la línea CD.

4.4 IEEE 802.3 Ethernet

4.4.1 Ethernet CSMA/CD. Conmutación y puentes

Ethernet Conmutada

LAN Ethernet mixta de concentradores/conmutadores



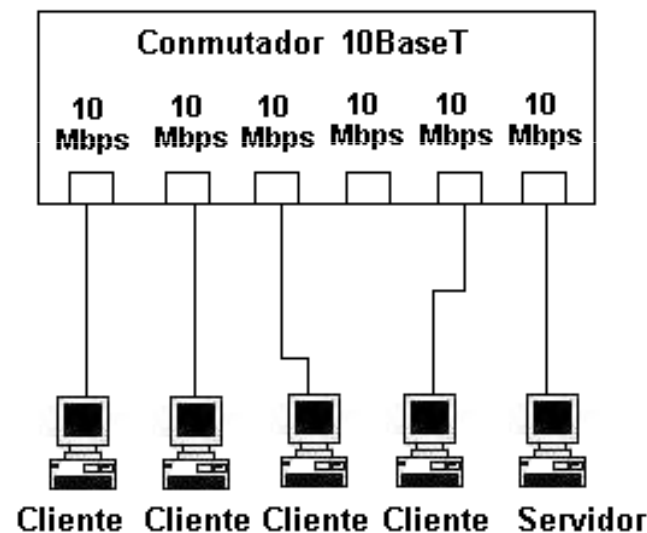
4.4 IEEE 802.3 Ethernet

4.4.2 Fast Ethernet (IEEE 802.3u)

Arquitectura cliente/servidor en Ethernet

Con el desarrollo de los conmutadores Ethernet el rendimiento que se alcanza es muy elevado si el tráfico tiene una distribución homogénea entre los equipos de la red.

En la práctica, la mayor parte de aplicaciones de red en entorno LAN (acceso a bases de datos, transferencia de archivos, web, etc.) se fundamentan en la arquitectura cliente/servidor.



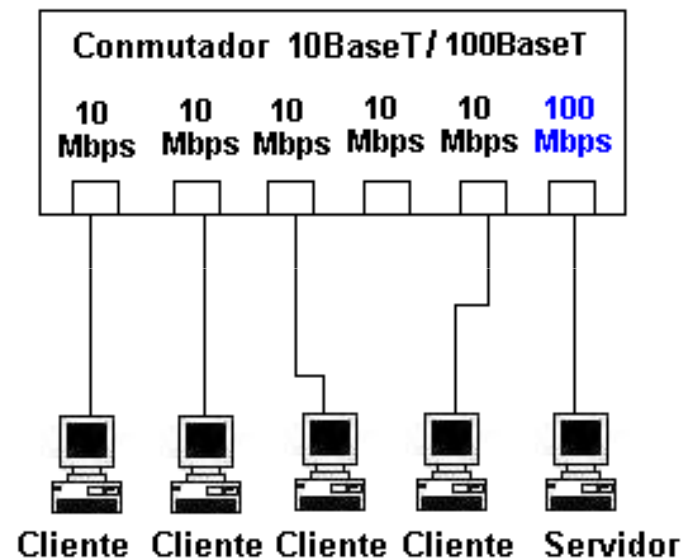
El conmutador debe emplear los buffers del puerto del servidor para repartir el tráfico de los clientes, es decir repartir el ancho de banda de 10 Mbps entre los clientes.

4.4 IEEE 802.3 Ethernet

4.4.2 Fast Ethernet (IEEE 802.3u)

Arquitectura cliente/servidor en Ethernet

Para conseguir un acceso adecuados entre clientes y servidor es necesario un puerto de mayor velocidad en el conmutador donde conectar el servidor.



Con un puerto a 100 Mbps, el servidor puede atender las peticiones y respuestas con 10 clientes a 10 Mbps de manera simultánea.

La normativa que permite la transmisión de paquetes Ethernet a 100 Mbps se denomina de forma genérica **Fast Ethernet**, existiendo diversas modalidades para la transmisión.

4.4 IEEE 802.3 Ethernet

4.4.2 Fast Ethernet (IEEE 802.3u)

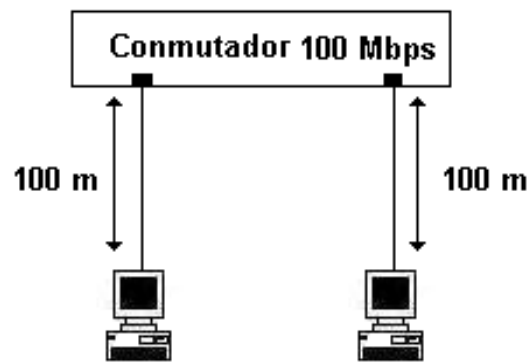
Fast Ethernet

Las redes Fast Ethernet funcionan con conmutadores, permitiendo el modo de trabajo half-duplex (CSMA/CD) y full-duplex.

Si se emplea 100 Mbps en CSMA/CD existe el problema del tamaño de paquete mínimo para la transmisión.

El tiempo mínimo de transmisión estándar en una red Ethernet con una extensión de 2.5 Km es de 51.2 μ segundos (512 bits tamaño mínimo de paquete).

En un conmutador Ethernet en modo half-duplex el dominio de colisión son 200 metros, y el tiempo mínimo de transmisión debe ser 4.1 μ segundos.



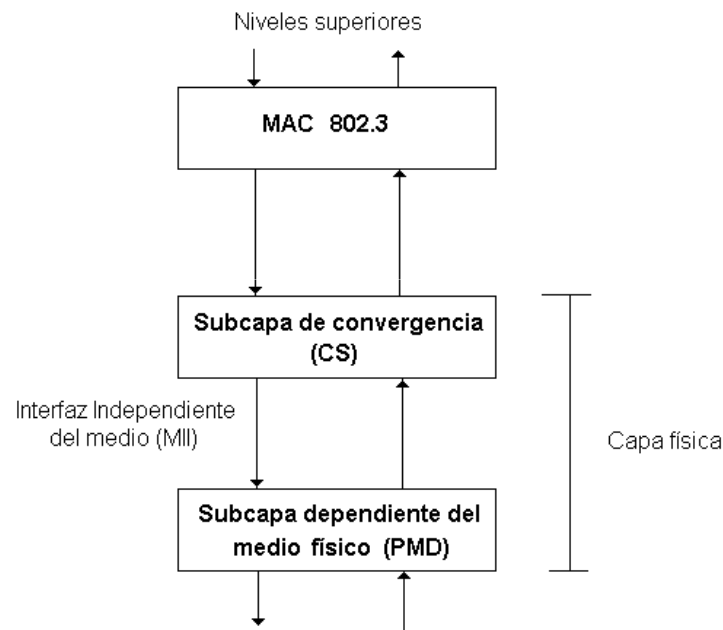
La transmisión de 512 bits a 100 Mbps supone un tiempo de 5.12 μ segundos, por lo que el tamaño mínimo de paquete es el mismo que en Ethernet 10 Mbps.

4.4 IEEE 802.3 Ethernet

4.4.2 Fast Ethernet (IEEE 802.3u)

Fast Ethernet

Para permitir la coexistencia del mismo tipo de protocolo MAC (CSMA/CD) empleando diferentes tipos de medios físicos, se introdujo una estructura de subcapas para el nivel físico.



Subcapa de convergencia: Convierte el flujo de bits de la capa MAC en grupos de 4 bits para su envío a la subcapa PMD.

Subcapa dependiente del medio físico: Transmite cada grupo de 4 bits con el mecanismo de codificación adecuado a cada tipo de medio físico.

4.4 IEEE 802.3 Ethernet

4.4.2 Fast Ethernet (IEEE 802.3u)

100BaseX

La normativa 100BaseX se desarrolló para cables UTP categoría 5, STP y fibra óptica.

El principal problema de la transmisión a alta velocidad es la sincronización emisor-receptor al transmitir la secuencia de bits.

Para introducir siempre información de sincronización en el flujo de bits, 100BaseX introduce una codificación 4B/5B.

Grupo de 4 bits	Símbolo de 5 bits
0 0 0 0	1 1 1 1 0
0 0 0 1	0 1 0 0 1
0 0 1 0	1 0 1 0 0
0 0 1 1	1 0 1 0 1
0 1 0 0	0 1 0 1 0
0 1 0 1	0 1 0 1 1
0 1 1 0	0 1 1 1 0
0 1 1 1	0 1 1 1 1

Grupo de 4 bits	Símbolo de 5 bits
1 0 0 0	1 0 0 1 0
1 0 0 1	1 0 0 1 1
1 0 1 0	1 0 1 1 0
1 0 1 1	1 0 1 1 1
1 1 0 0	1 1 0 1 0
1 1 0 1	1 1 0 1 1
1 1 1 0	1 1 1 0 0
1 1 1 1	1 1 1 0 1

Para proporcionar una velocidad de 100 Mbps para cada grupo de 4 bits de datos, es necesario que los grupos de 5 bits se transmitan a una velocidad de $5/4 \cdot 100 \text{ Mbps} = 125 \text{ Mbps}$.

La señal de reloj para los pulsos en la capa PMD será de 125 MHz, y la codificación en pulsos será distinta si el medio es fibra óptica o cable UTP.

4.4 IEEE 802.3 Ethernet

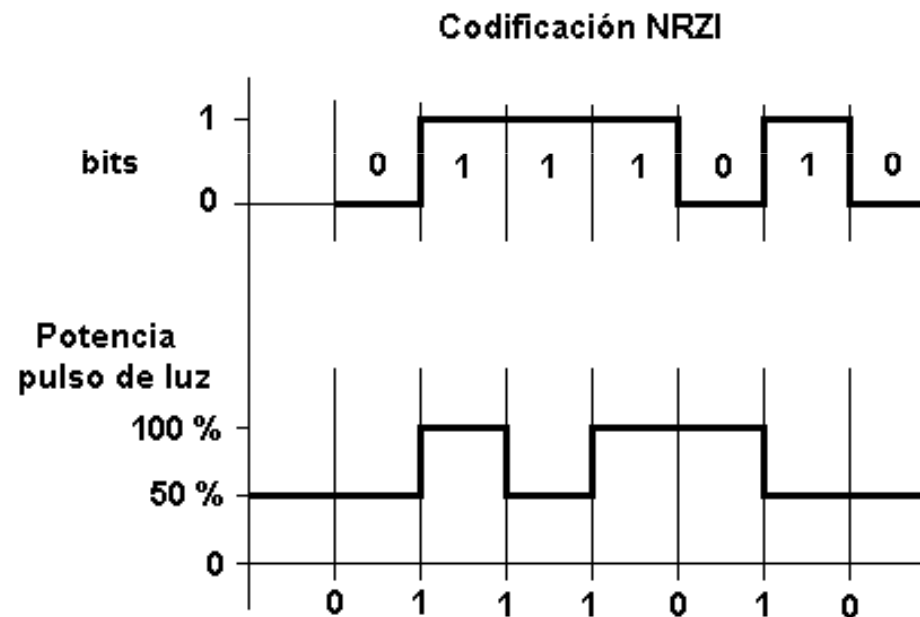
4.4.2 Fast Ethernet (IEEE 802.3u)

100BaseFX

100BaseFX emplea la normativa 100BaseX de codificación 4B/5B sobre fibra óptica.

Cada símbolo de 5 bits se convierte en pulsos luminosos empleando codificación NRZI

Se definen dos niveles de amplitud para el haz de luz que incide en la fibra (50% - 100% potencia), de forma que un cambio en la amplitud del haz indica un **1** y la inexistencia de cambio de amplitud indica un **0**.



100BaseFX emplea fibra óptica multimodo y permite alcanzar distancias de hasta 400 metros entre un equipo y el conmutador.

4.4 IEEE 802.3 Ethernet

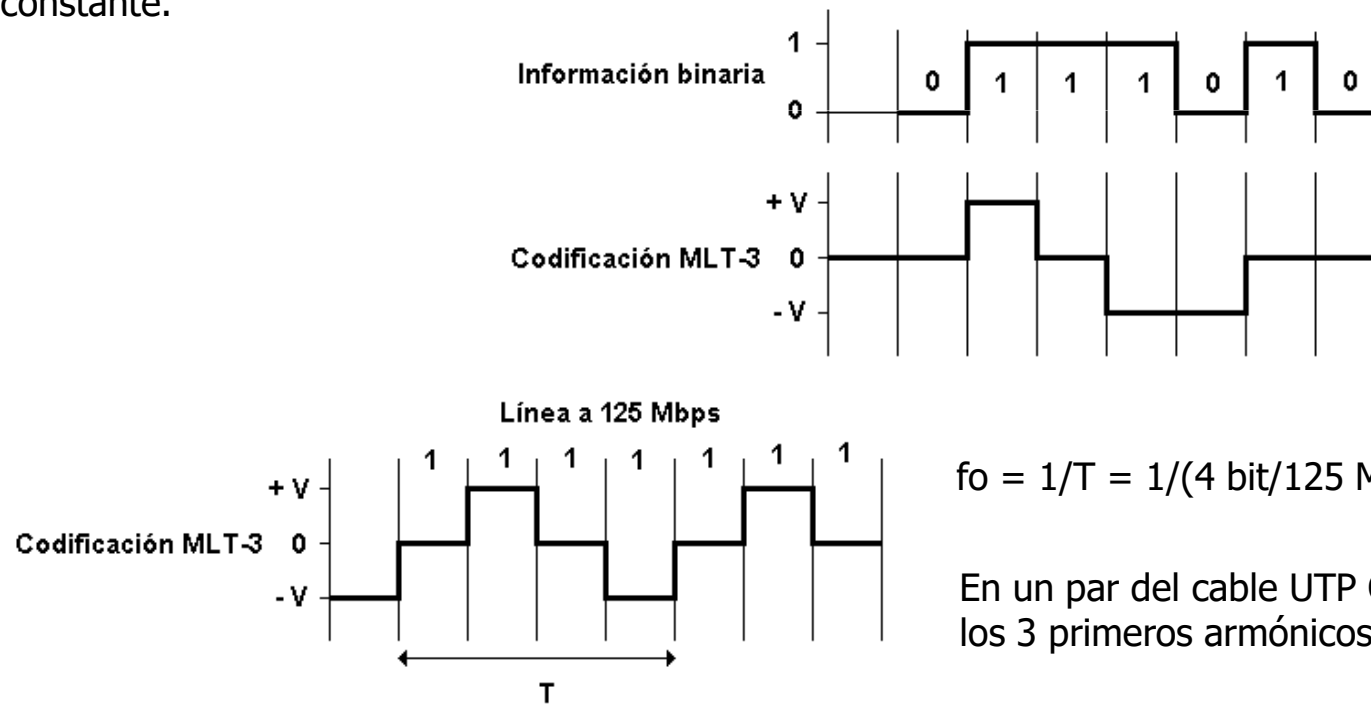
4.4.2 Fast Ethernet (IEEE 802.3u)

100BaseTX

100BaseTX emplea la normativa 100BaseX de codificación 4B/5B sobre cable UTP categoría 5 (máximo 100 metros).

Cada símbolo de 5 bits se convierte en pulsos eléctricos empleando la codificación MLT-3. (Si se empleara Manchester se necesitaría un cable de 125 Mhz de ancho de banda)

Se definen 3 niveles de amplitud de voltaje (-V, 0, +V). Si se transmite un bit a **1** la tensión varía aumentando o disminuyendo dependiendo de los valores anteriores. Si se transmite un bit a **0** la tensión se mantiene constante.



$$f_0 = 1/T = 1/(4 \text{ bit}/125 \text{ Mbps}) = 31.25 \text{ Mhz}$$

En un par del cable UTP Cat 5 pueden transmitirse los 3 primeros armónicos de la señal.

4.4 IEEE 802.3 Ethernet

4.4.3 Gigabit Ethernet (IEEE 802.3z)

Gigabit Ethernet

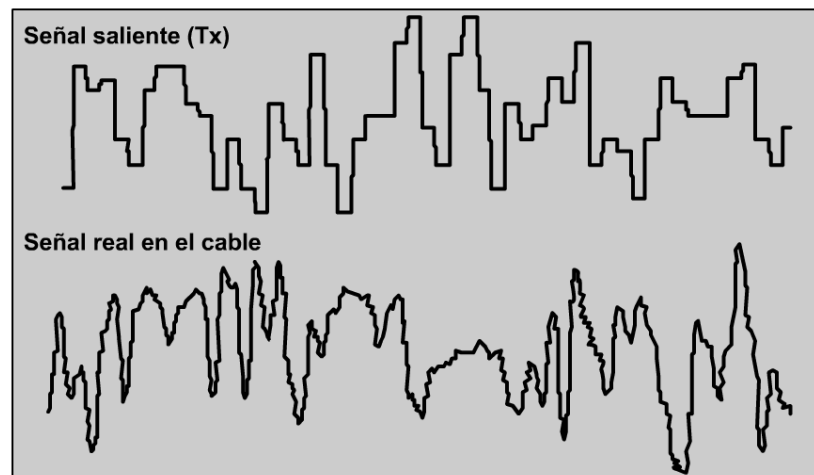
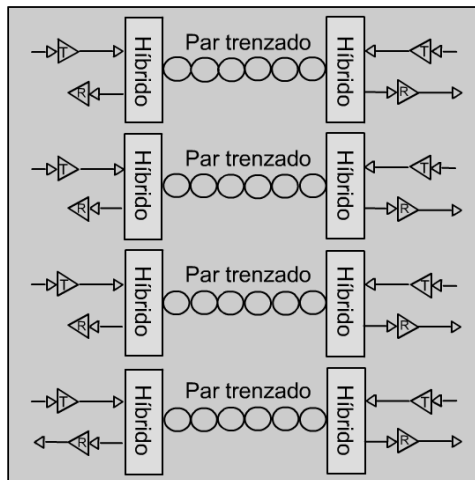
Las redes Gigabit Ethernet funcionan con conmutadores, permitiendo el modo de trabajo half-duplex (CSMA/CD) y full-duplex.

En el modo CSMA/CD, el tamaño de paquete mínimo es mayor que en Fast Ethernet, siendo de 512 bytes.

1000BaseT

Alcanzar con cable UTP categoría 5 velocidades de 1 Gbps en modo full-duplex es complejo y costoso.

1000BaseT permite alcanzar 1 Gbps a distancias de 100 metros empleando los cuatro pares de hilos para transmitir y recibir simultáneamente (cancelación de eco).



Codificación
4D-PAM5

4.4 IEEE 802.3 Ethernet

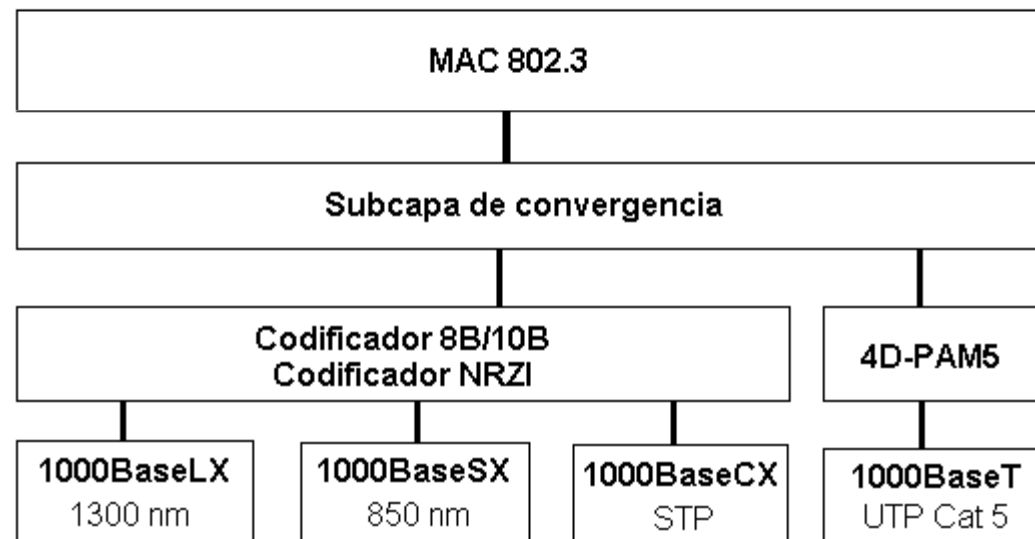
4.4.3 Gigabit Ethernet (IEEE 802.3z)

1000BaseX

La transmisión de datos a 1 Gbps por fibra óptica es menos compleja debido al enorme ancho de banda de la fibra.

Los bits del paquete Ethernet son modificados con un codificador 8B/10B, introduciendo información de sincronización para el receptor.

La señal codificada puede transmitirse por fibra óptica o mediante cable STP (distancia máxima 25 metros)



1000BaseLX y 1000BaseSX con fibra multimodo alcanza distancias de 500 metros.

1000BaseLX permite además fibra monomodo con distancias de 5 Km.

4.4 IEEE 802.3 Ethernet

4.4.3 Gigabit Ethernet (IEEE 802.3z)

10 Gigabit Ethernet (802.3ae)

Las redes 10 Gigabit Ethernet (**10GBase-XX**) funcionan con conmutadores permitiendo **solamente** el modo de trabajo full-duplex (no existe el CSMA/CD).

Emplea en general la fibra óptica como medio de transmisión, pudiendo emplear el estándar de SDH para la transmisión de los paquetes Ethernet.

Empleando fibra óptica multimodo se alcanzan distancias de hasta 300 metros, pero con monomodo se consiguen hasta 40 Km.

Puede emplearse también el cable UTP (10G-BaseT) de categoría 6 y 7, con distancias máximas de 100 metros.

Las aplicaciones de Ethernet hoy en día abarcan el campo LAN, MAN y WAN, pudiendo emplearlo para establecer enlaces punto a punto entre nodos de Internet.

2.5GBaseT – 5GBaseT (802.3bz)

En septiembre de 2016, el IEEE publica dos nuevas normativas Ethernet con tasas de velocidad de 2.5 Gbps y 5 Gbps.

Esta normativas están pensadas para ser empleadas con cable par trenzado (UTP) de categoría 5e (2.5 Gbps) y categoría 6 (5 Gbps) y distancias hasta 100 metros. Sólo se permite, al igual que en 10GBase-XX, el modo de funcionamiento full-duplex con conmutadores.

Su objetivo es permitir conexiones de puntos de acceso Wi-Fi de la norma 802.11ac (velocidades de hasta 1.3 Gbps) a troncales Ethernet.

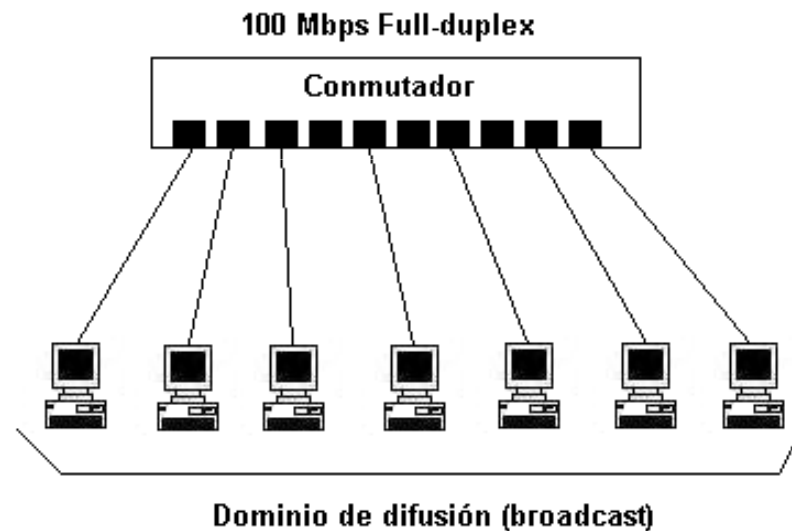
4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

Introducción

El desarrollo de redes LAN cada vez mayores empleando conmutadores introduce problemas en cuanto a la confiabilidad de la información.

La interconexión de equipos con conmutadores elimina los dominios de colisiones, pero sigue existiendo un dominio de difusión.



Problemas de seguridad

Los paquetes de difusión son "observados" por todos los equipos del conmutador.

Cualquier equipo tiene accesibilidad física al resto.

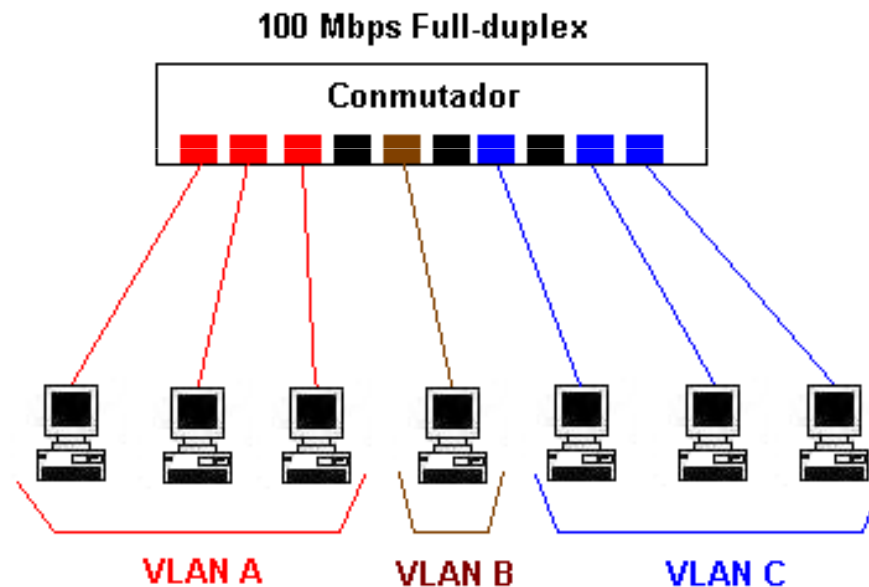
4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

Introducción

El IEEE desarrolla una normativa (IEEE 802.1Q) para poder dividir un conmutador en varios dominios de difusión distintos.

Cada dominio de difusión independiente se denomina VLAN (Virtual Local Area Network).



4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

IEEE 802.1Q. Funcionamiento

El funcionamiento de un conmutador VLAN es similar al de un puente, disponiendo de una tabla de reenvío.

Conmutador VLAN

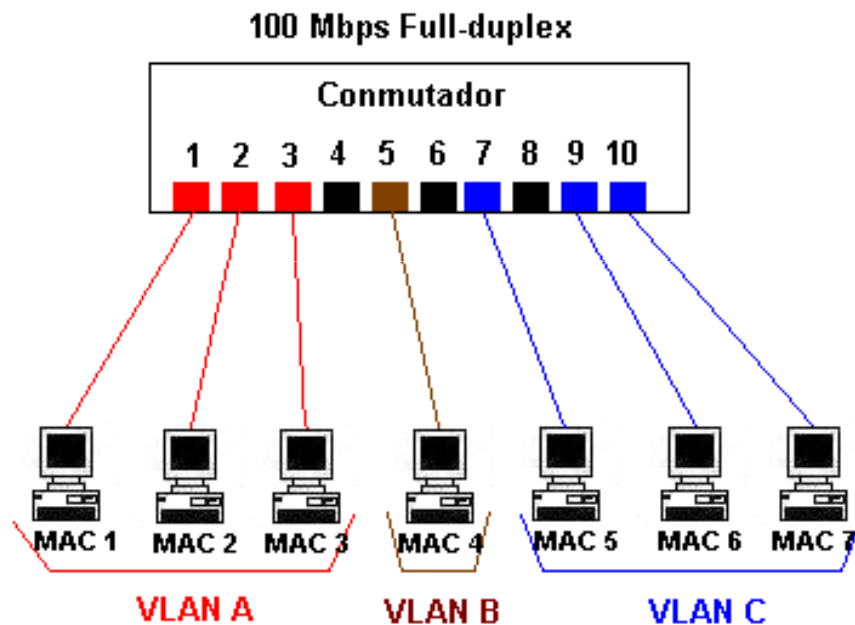


Tabla de reenvío

MAC	Id. VLAN	Puerto
1	A	1
2	A	2
3	A	3
4	B	5
5	C	7
6	C	9
7	C	10

Un conmutador VLAN reenvía las tramas de difusión de entrada en un puerto a todos los puertos etiquetados con la misma VLAN.

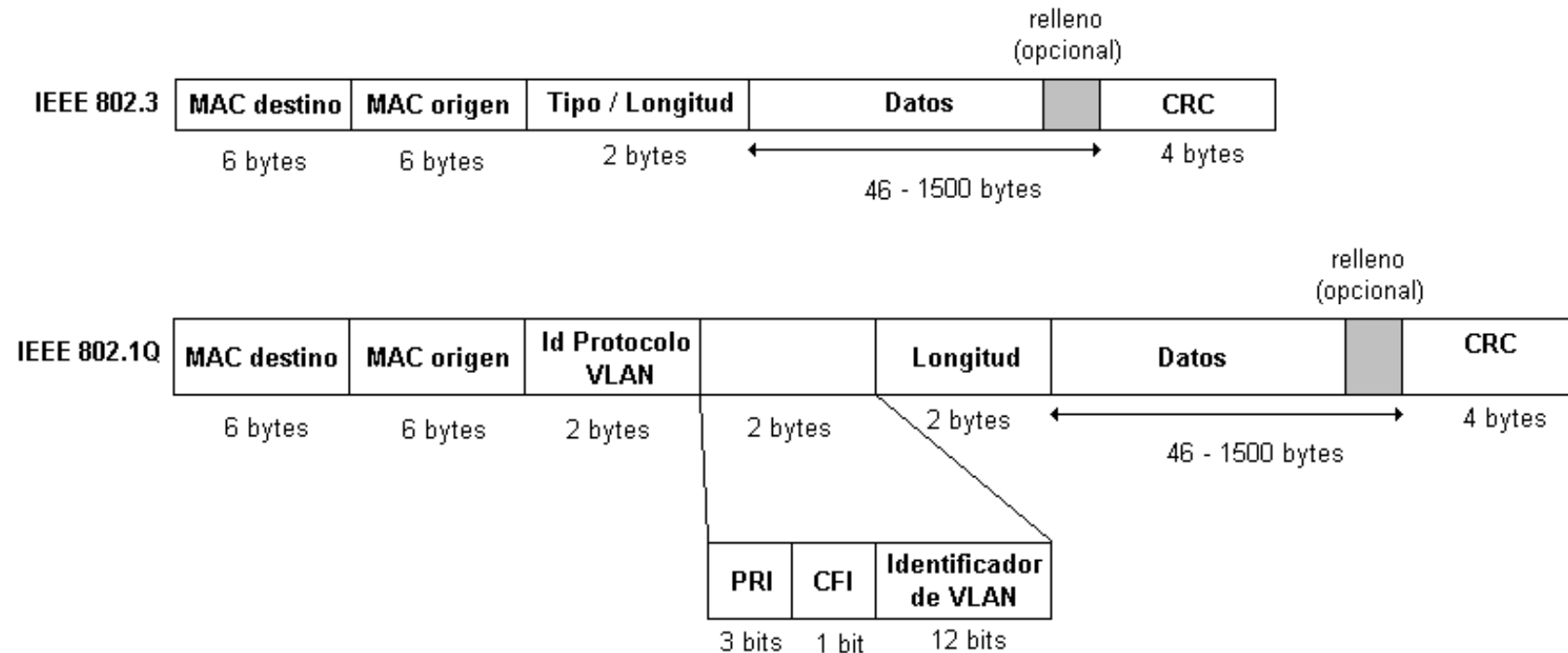
Si un equipo de una VLAN envía un paquete a una MAC que no pertenece a la misma VLAN el conmutador no lo reenvía (**Cada VLAN tiene asociada una dirección de red IP diferente para que ARP funcione**).

4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

IEEE 802.1Q. Funcionamiento

La norma IEEE 802.1Q define un nuevo formato de paquete IEEE 802.3 cuando se emplean VLANs.



Id Protocolo VLAN: Toma el valor 0x8100 para indicar que es un paquete IEEE 802.1Q.

PRI: Bits de prioridad que pueden emplearse para conmutar unos paquetes antes que otros (voz, vídeo).

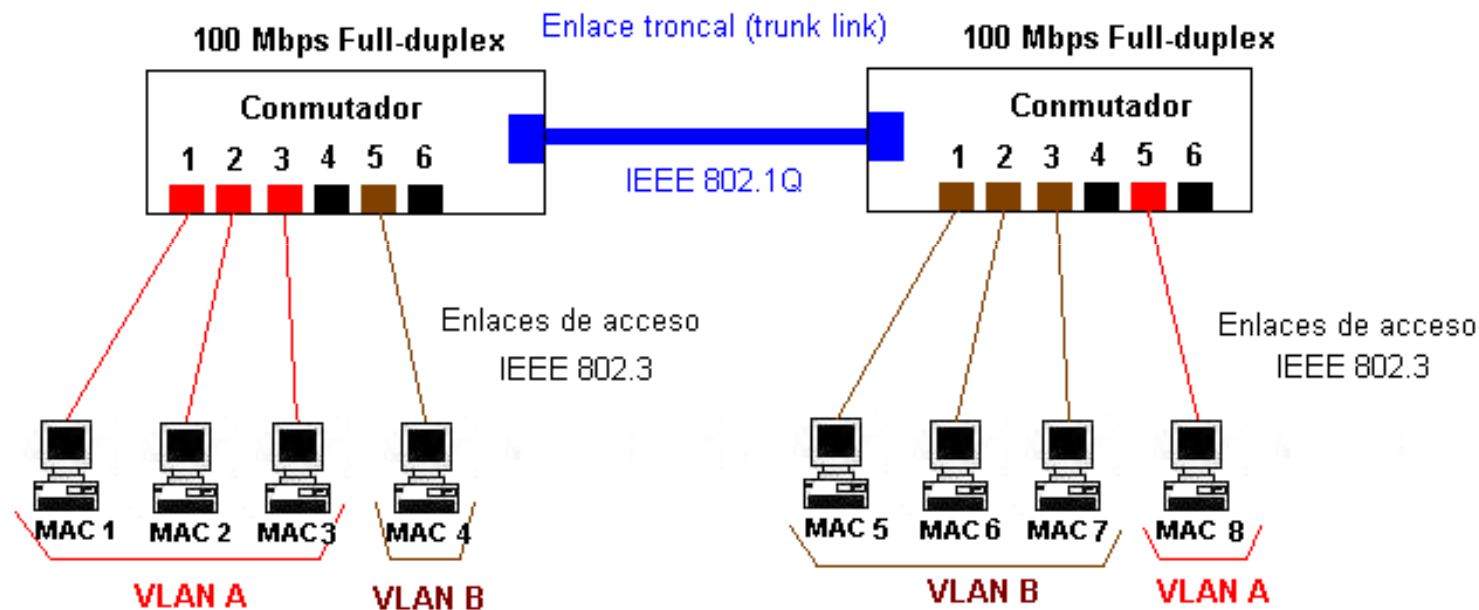
CFI: Flag para indicar que en el campo de datos hay una trama Token-Ring.

4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

IEEE 802.1Q. Funcionamiento

El formato de trama IEEE 802.1Q se emplea cuando se interconectan conmutadores VLAN entre sí, o un router a un conmutador VLAN.



Los puertos de enlaces troncales (**trunk port**) pertenecen a varias VLAN, y a través de ellos los paquetes de diferentes VLAN se intercambian entre conmutadores distintos (debido a esto es necesario el empleo del formato IEEE 802.1Q).

4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

IEEE 802.1Q. Funcionamiento

Un conmutador VLAN maneja de diferente forma los enlaces de acceso y los enlaces troncales.

Enlaces de acceso

En los enlaces de acceso los paquetes tienen el formato del IEEE 802.3. Cuando un paquete de un enlace de acceso se envía a un puerto troncal es necesario añadir el identificador VLAN asociado al enlace de acceso. Es decir, transformar al formato IEEE 802.1Q

Si el conmutador tiene que enviar un paquete de un puerto troncal a un puerto de acceso extrae del formato IEEE 802.1Q los datos para transformarlo en el formato IEEE 802.3.

Enlaces troncales

En los enlaces troncales los paquetes tienen el formato del IEEE 802.1Q.

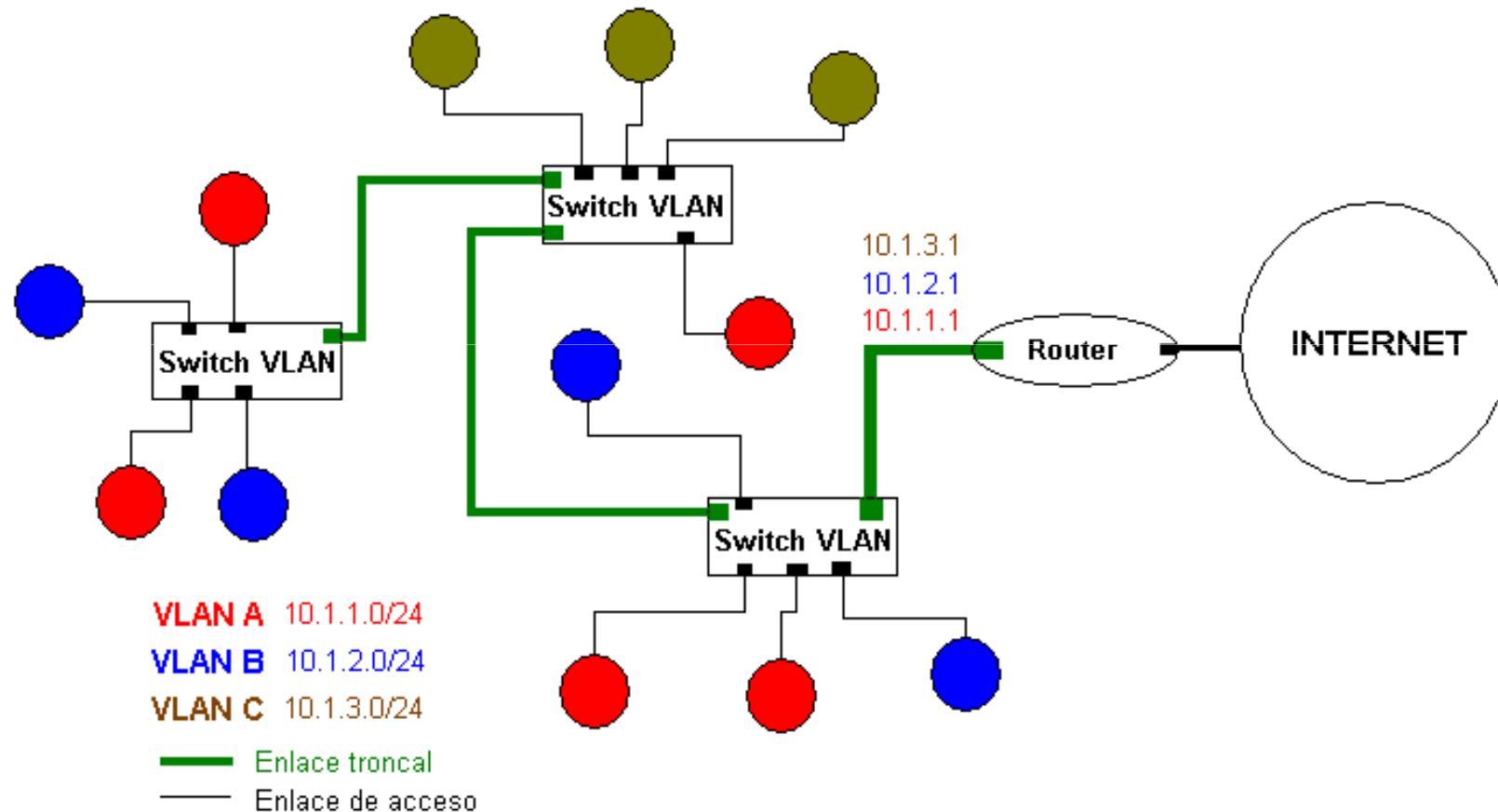
Los conmutadores VLAN emplean un protocolo denominado **GVRP (GARP VLAN Registration Protocol)** para propagar información entre los conmutadores y conocer qué VLANs hay asociadas a los puertos troncales.

Así, un conmutador, de forma automática, sabe si tiene que reenviar paquetes de una VLAN cuyo destino no está en el conmutador a otros conmutadores conectados a través de puertos troncales.

4.4 IEEE 802.3 Ethernet

4.4.4 IEEE 802.1Q. Redes de Área Local Virtuales (VLAN)

IEEE 802.1Q. Arquitectura



4.5 IEEE 802.11x. LAN Inalámbrica

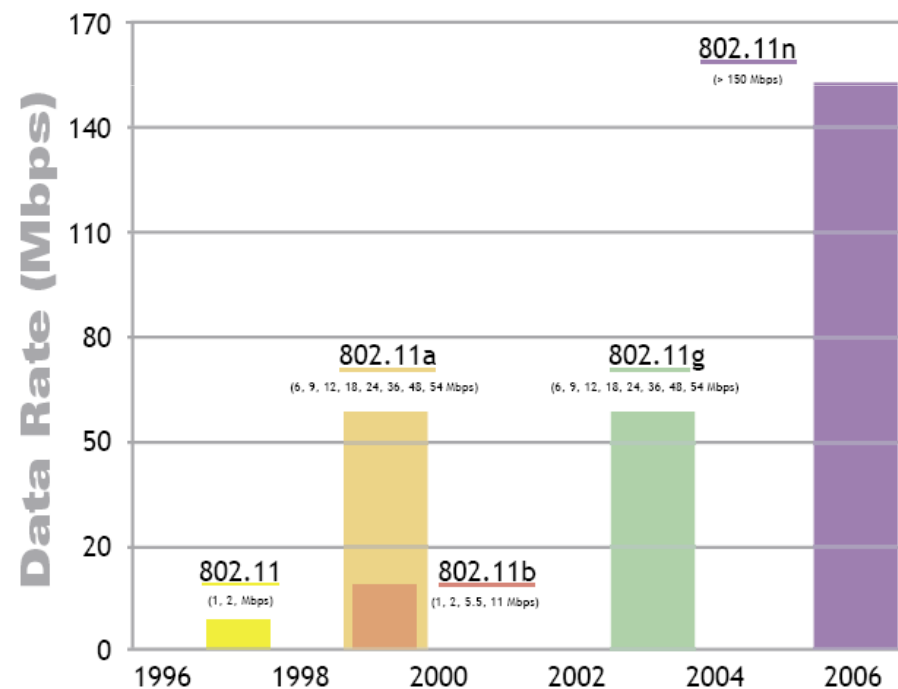
4.5.1 Introducción

Historia

Una red LAN inalámbrica es una red de área local que emplea ondas electromagnéticas como soporte físico para la comunicación de datos.

Las tecnologías de comunicación inalámbrica son más complejas y por tanto de mayor coste económico que las redes de cable.

Con el desarrollo en los años 90 de la telefonía móvil y los ordenadores portátiles se consigue una tecnología de comunicación inalámbrica con unas prestaciones competitivas a un coste razonable.



4.5 IEEE 802.11x. LAN Inalámbrica

4.5.1 Introducción

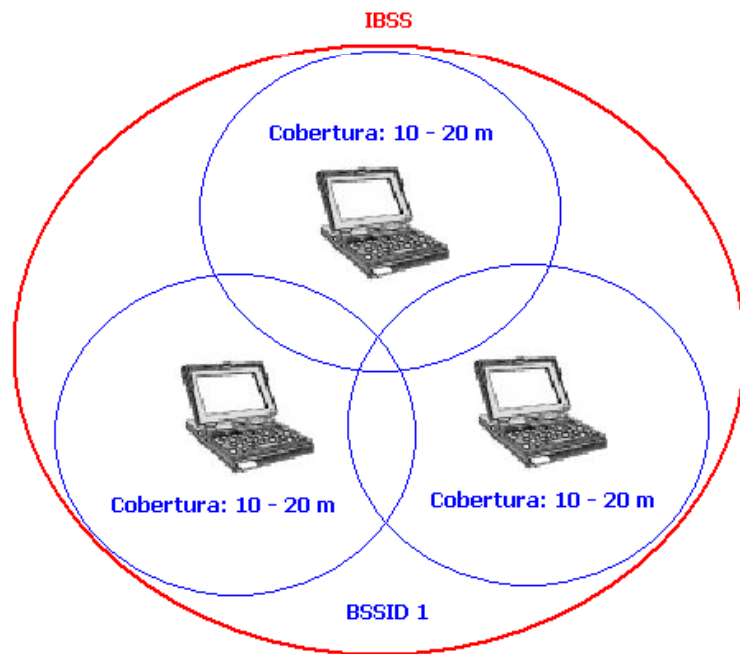
Nomenclatura

BSS (Basic Service Set): Conjunto de servicio básico. Grupo de estaciones que se comunican entre ellas.

Infraestructure BSS (**BSS**): Red inalámbrica con puntos de acceso (red de infraestructura).

Independent BSS (**IBSS**): Red inalámbrica ad-hoc.

Red Inalámbrica ad-hoc



SSID (Service Set Identifier): Identificador de un BSS. Cadena de 32 caracteres máximo.

Identifica a un BSS y se emplea en los mecanismos de gestión (por ejemplo asociación a AP).

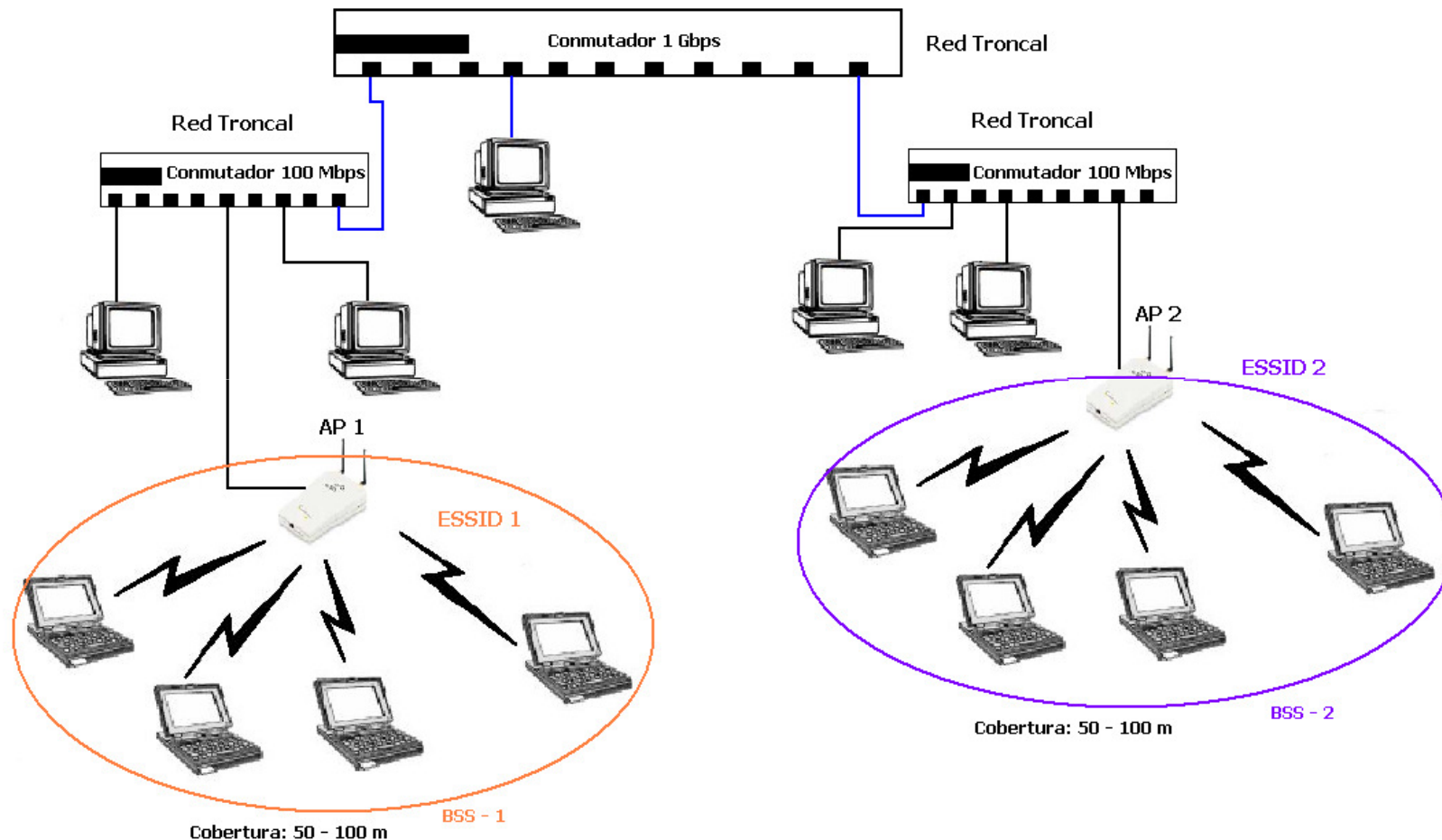
BSSID (Basic Service Set Identifier): SSID en redes ad-hoc.

ESSID (Extended Service Set Identifier): SSID en redes de infraestructura.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.1 Introducción

Red Inalámbrica de Infraestructura



AP (Access Point): Punto de Acceso. Actúa como puente entre la LAN de cable y un BSS.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.1 Introducción

Normativas de comunicación inalámbrica

El IEEE es el organismo que ha propuesto los estándares de redes LAN inalámbricas, existiendo diversas tecnologías donde destacan:

IEEE 802.11b: Comunicación inalámbrica empleando una señal portadora de 2.4 Ghz. Esta frecuencia está declarada para su uso libre, por lo que pueden existir interferencias con otros dispositivos del mercado.

Realmente no se emplea una única portadora, si no que existen 13 portadoras entre los 2.4 y 2.5 GHz. Cada una de estas portadoras define un canal, de forma que todos los equipos que pertenecen a un BSS deben emplear la misma portadora.

El AP debe configurarse para emplear una canal que no tenga interferencias en la zona. Así, es necesaria una política de gestión de canales cuando se utilizan varios AP.

La norma IEEE 802.11b emplea modulación de múltiples niveles (amplitud y fase) en cada canal, permitiendo alcanzar velocidades de 1, 2, 5.5 y 11 Mbps.

IEEE 802.11g: Comunicación inalámbrica empleando una señal portadora de 2.4 Ghz. Con esta normativa se consigue alcanzar velocidades de hasta 54 Mbps.

IEEE 802.11n (Wi-Fi 4): Permite emplear la portadora de 2.4 GHz y la de 5 GHz (19 canales) consiguiendo velocidades de hasta 600 Mbps.

IEEE 802.11ac (Wi-Fi 5): Emplea solamente la portadora de 5 GHz (19 canales) y varias antenas, consiguiendo velocidades de hasta 1.3 Gbps.

La velocidad de transmisión con wireless no es fija, le afecta el ruido del entorno de trabajo.

4.5 IEEE 802.11x. LAN Inalámbrica

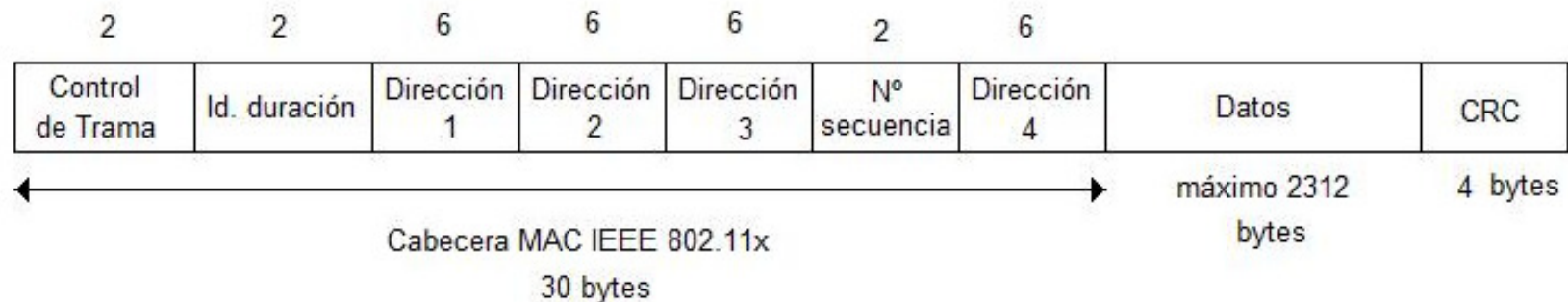
4.5.2 Acceso al medio

Características

Las redes LAN 802.11 se caracterizan por presentar una elevada tasa de error en el medio físico. Este problema condiciona cuál es el mecanismo de reparto del uso del medio físico.

La elevada tasa de error en el medio introduce dos necesidades:

1. Tamaño de paquete pequeño. Es necesario un tamaño de paquete pequeño, pues los errores provocarán reenvíos de datos. Los paquetes del nivel superior (LLC) serán fragmentados por el protocolo MAC del 802.11. La norma 802.11 especifica un tamaño máximo de datos de 2312 bytes. En la actualidad, con la existencia de redes Ethernet con MTU de 1500 bytes, los Sistemas Operativos emplean un MTU de 1500 bytes en los interfaces Wi-Fi.



2. Protocolo MAC 802.11 confirmado. Debido a la elevada tasa de error, es necesario que el protocolo de control de acceso al medio sea capaz de confirmar los paquetes transmitidos en el medio inalámbrico. Así, los reenvíos necesarios se realizarán rápidamente.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

El protocolo MAC del 802.11 distingue entre dos modos de funcionamiento para el uso del medio físico:

1. DCF (Función de coordinación distribuida)

Empleadas en wireless de infraestructura y ad-hoc.

2. PCF (Función de coordinación centralizada)

Empleadas en wireless de infraestructura, donde el AP controla el acceso al medio compartido.

DCF – Función de coordinación distribuida

En el modo DCF cada estación compite por el uso del medio físico. El mecanismo de reparto empleado es el **CSMA/CA** (Acceso al medio con detección de portadora y evitación de colisiones).

Las estaciones comprueban si el medio físico está libre detectando una señal denominada **CCA** (Estimación de desocupación del canal). Esta señal la transmiten los dispositivos en escucha en la red.

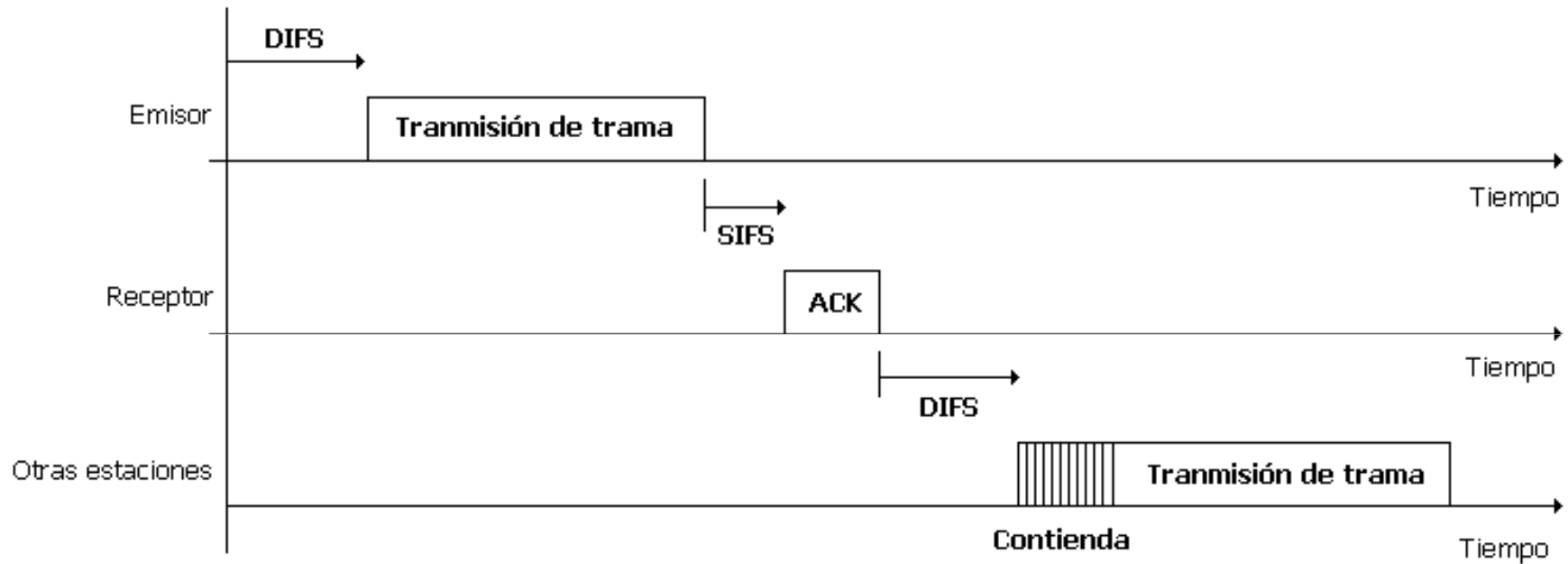
Si una estación encuentra el medio libre durante un tiempo denominado DIFS (espacio de tiempo entre la transmisión de tramas en DCF), entonces transmitirá el paquete de datos. Si recibe una confirmación del envío se considerará que la transmisión ha sido correcta.

Si la estación detecta que el medio físico está ocupado, espera a que se detecte de nuevo el medio físico libre durante un tiempo DIFS. Al expirar este tiempo, el equipo entra en una situación de contienda esperando un tiempo aleatorio. Al finalizar el tiempo aleatorio, si el medio físico está libre transmitirá, y si no esperará un nuevo periodo de contienda.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

DCF – Función de coordinación distribuida



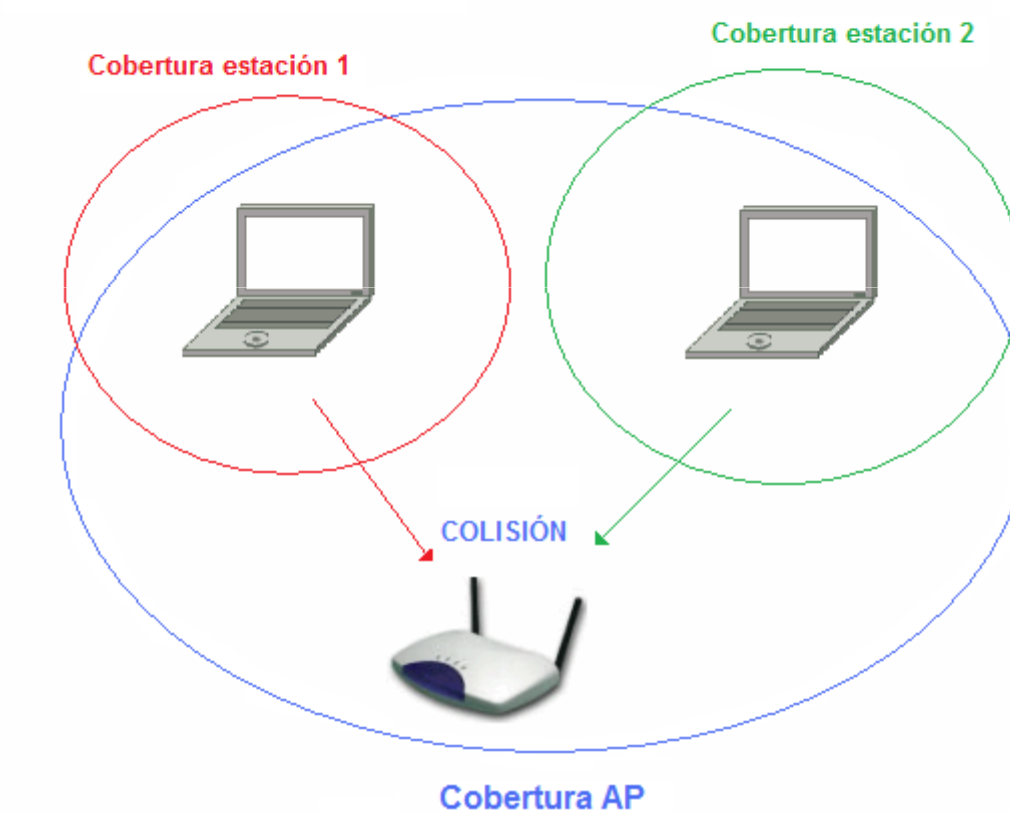
CSMA/CA

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

DCF – Función de coordinación distribuida

El problema de la estación oculta



4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

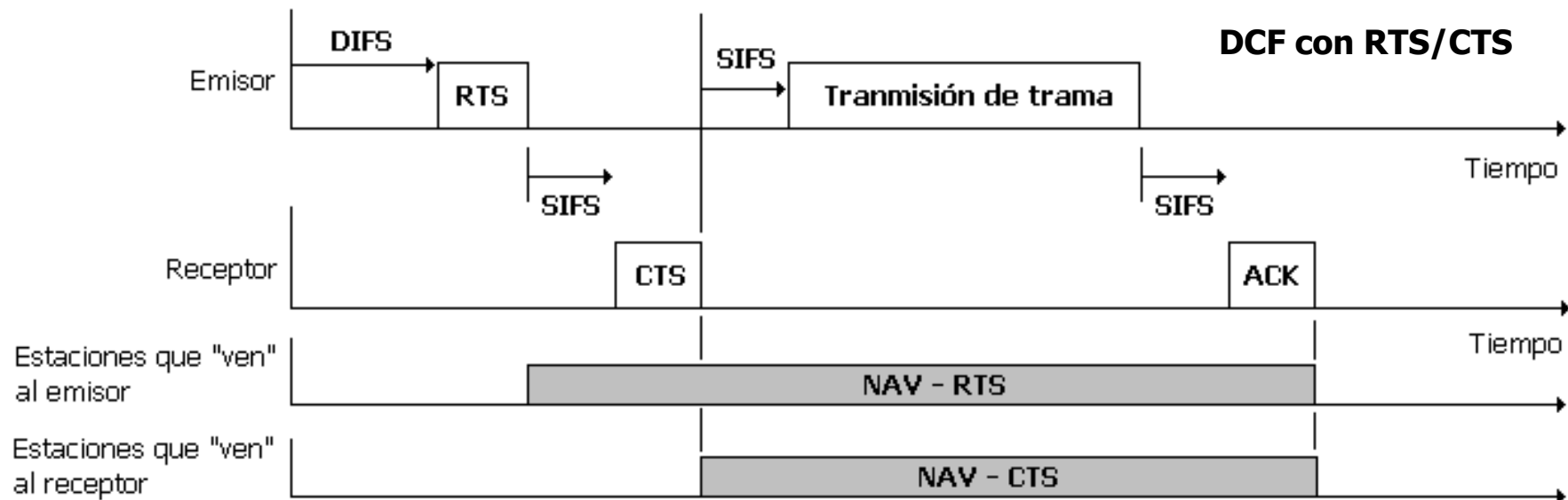
DCF – Función de coordinación distribuida

Variante DCF con RTS/CTS

Para evitar el problema de la estación oculta (un AP detecta dos estaciones, pero las estaciones no se detectan entre ellas) se introduce un mecanismo de reserva de la red.

La estación que transmite envía un paquete de tipo **RTS** que indica a las demás estaciones "visibles" el tiempo durante el que no pueden transmitir (**NAV – Vector de reserva de red**).

El receptor confirma el paquete RTS con un paquete de tipo **CTS** que indica a las demás estaciones "visibles" el tiempo durante el que no pueden transmitir.



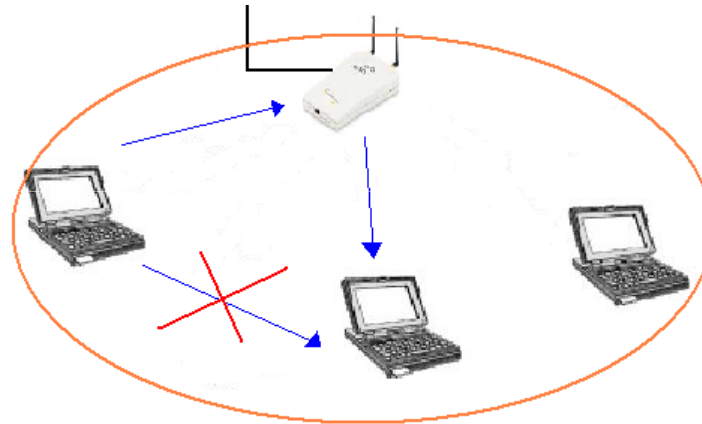
4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

PCF – Función de coordinación centralizada

Este modo de funcionamiento está definido sólo para las redes de infraestructura, pues precisa de la existencia de un punto de acceso **AP**.

Cuando existe un AP todas las comunicaciones se realizan a través de él. Es decir, si una estación quiere transmitir un paquete a otra estación, se enviará la información al AP y éste lo reenviará a la estación destino.



El AP divide el tiempo de transmisión en la red en celdas de tiempo denominadas **supertramas**.

Cada supertrama se divide en dos periodos de tiempo:

Un periodo en el que no hay colisiones y el AP controla el uso del medio (selección de equipos a transmitir)

Un periodo de contienda donde se emplea CSMA/CA o CSMA/CA con RTS/CTS.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.2 Acceso al medio

PCF – Función de coordinación centralizada

Periodo de no colisión

En el periodo de no colisión, el AP envía a una estación un paquete solicitando que le envíe un bloque de datos.

Cuando el bloque de datos es recibido por el AP, envía otra solicitud a otra estación.

Este proceso finaliza cuando el AP envía un paquete de finalización del periodo libre de colisiones. El resto de tiempo de la supertrama emplea la contienda para transmitir información entre el AP y las estaciones.

Durante el periodo de no colisión se realizan también las funciones de gestión de la red wireless, que básicamente son **añadir/eliminar un equipo de la red wireless**.

Para añadir un equipo en la red (registrar un equipo en el AP) el AP envía cada cierto tiempo un paquete denominada **trama de baliza o señalización** (beacon frame).

Cuando una estación recibe una trama de invitación a registrarse contesta, pudiendo el AP aceptarla o no (filtrado por MAC).

Si una estación es registrada puede aplicarse un proceso adicional de autenticación (opcional pero muy recomendable) antes de que sea permitido el envío de paquetes de datos.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

Wi-Fi Alliance

Wi-Fi Alliance es una asociación de fabricantes de tecnología de red inalámbrica basada en la norma IEEE 802.11x (Cisco, Microsoft, Nokia, Intel, Dell, etc). <http://www.wi-fi.org/>

Esta asociación ha desarrollado la marca Wi-Fi™ para identificar sistemas de comunicación LAN inalámbricos que son compatibles, pues emplean las normas del IEEE 802.11x.

Uno de los campos de normalización de la Wi-Fi Alliance es la seguridad en redes Wi-Fi.

Principios de seguridad

La seguridad en una red Wi-Fi se fundamenta en dos principios:

Autenticación: Una estación (cliente) debe identificarse como un usuario autorizado de la red Wi-Fi.

Existen diferentes mecanismos de autenticación, cada uno de ellos con un nivel inherente de seguridad.

Integridad de la información: La información debe transmitirse cifrada para evitar espías (sniffers).

Existen diferentes mecanismos de cifrado en redes Wi-Fi, desarrollados en base a vulnerabilidades de seguridad que se han ido detectando.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

Autenticación

Cuando una estación desea conectarse a una red Wi-Fi inicia un proceso de registro en el AP de la red.

Para realizar el registro, la estación debe conocer el SSID de la red. Aquí es posible introducir un mecanismo de seguridad.

Los AP transmiten cada cierto tiempo un paquete de señalización indicando cuál es su SSID e invitando a equipos a añadirse. Esta acción puede deshabilitarse en el AP, de forma que los equipos no “ven” la red y sólo pueden conectarse si conocen el SSID.

Si la estación conoce el SSID puede registrarse en el AP. Un nivel de seguridad adicional consiste en permitir solamente el registro de estaciones con una dirección MAC almacenada en una lista del AP.

Finalizado el proceso de registro, es posible llevar a cabo un proceso de autenticación (opcional).

En general, los AP no suelen realizar este control de acceso en el registro de la estación, pues la flexibilidad de los sistemas Wi-Fi radica en que cualquier estación pueda registrarse. El proceso de control de acceso suele llevarse a cabo en la autenticación.

Sólo en sistemas muy controlados (redes LAN personales o de hogar, redes LAN corporativas con pocos equipos) el sistema de control de acceso por dirección MAC es empleado.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

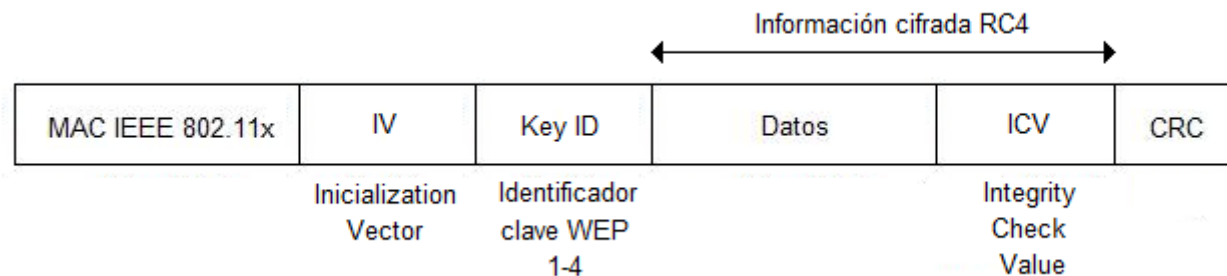
Autenticación y cifrado WEP

WEP (Wired Equivalente Privacy) fue el primer protocolo de encriptación empleado en el estándar IEEE 802.11x hacia 1999 y que se basa en el algoritmo de cifrado RC4.

El funcionamiento de WEP está basado en el conocimiento de una misma clave secreta por parte de la estación y el AP (PSK – Pre-Shared Key)

El mecanismo de autenticación consiste en que la estación proporcione una información cifrada al AP con la clave secreta. Si la información es cifrada correctamente el AP permite la conexión de la estación a la red Wi-Fi.

El objetivo de WEP no es tanto la autenticación como el cifrado de todos los paquetes intercambiados entre la estación y el AP.



La seguridad de WEP se fundamenta en una clave secreta de 64 o 128 bits, pero que no es suficiente. Actualmente, WEP está obsoleto pues es posible descubrir cualquier clave en unos pocos minutos con el software apropiado.

4.5 IEEE 802.11x. LAN Inalámbrica

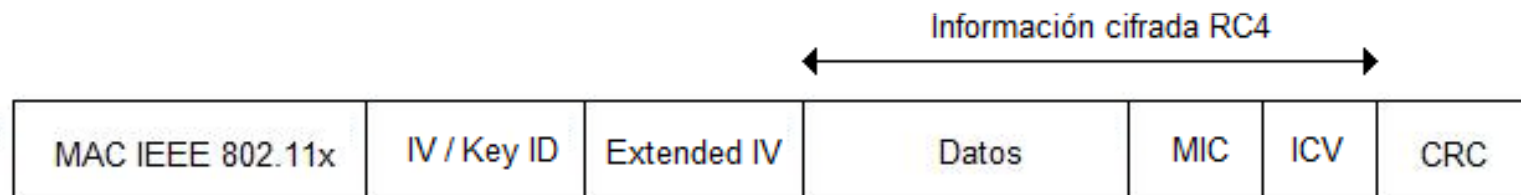
4.5.3 Seguridad en redes Wi-Fi™

Autenticación y cifrado WPA

WPA (Wi-Fi Protected Access) fue desarrollado por la Wi-Fi Alliance en 2003 para sustituir a WEP.

La principal vulnerabilidad de WEP es la capacidad de obtener la clave de cifrado. Así, WPA mantiene el mismo algoritmo de cifrado de WEP (RC4), pero introduce el mecanismo TKIP (*Temporal Key Integrity Protocol*).

TKIP modifica la clave de cifrado entre el cliente y el AP cada cierto tiempo, además de introducir un mecanismo de verificación de la integridad de los paquetes cifrados (MIC – *Message Integrity Code*).



Al aumentar el tamaño del campo IV, proporciona una mayor entropía (aleatoriedad) en el proceso de cifrado, y unido a la variación de la clave de cifrado, una mayor seguridad.

En la actualidad, el cifrado WPA basado en TKIP se ha roto. Por tanto, no se seguro emplearlo aunque dado que se requiere unos 15 minutos para descubrir una clave, puede configurarse TKIP para cambiar claves cada 2 minutos o menos (esto puede afectar al rendimiento). En septiembre 2009, investigadores de la Universidad de Hiroshima han conseguido romper un cifrado WPA en 1 minuto.

Otra solución es emplear WPA2.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

Autenticación y cifrado WPA

En el procedimiento de autenticación, WPA admite dos mecanismos:

WPA–Personal o WPA-PSK: En este mecanismo, cliente y AP disponen de una clave de acceso prefijada para permitir el acceso a la red inalámbrica (mismo mecanismo de WEP). La clave PSK inicial es modificada posteriormente en el cifrado al emplear TKIP.

Al emplear este mecanismo de autenticación, la vulnerabilidad principal es la fortaleza de la clave prefijada ante ataque por fuerza bruta.

Debido a la vulnerabilidad de WPA indicada anteriormente, este mecanismo de autenticación sólo es asumible en entornos no críticos (redes personales o de hogar) .

WPA–Enterprise: En este mecanismo, cada cliente autentica su acceso al AP empleando un servidor de autenticación (RADIUS). La gestión de la autenticación se realiza empleando el estándar IEEE 802.1x.

La base del funcionamiento del 802.1x es el protocolo de autenticación EAP (*Extensible Authentication Protocol*).

EAP se emplea en otros entornos, como las redes VPN, y permite realizar la autenticación de un cliente contra un servidor de autenticación (en general suele emplearse Radius).

El potencial de EAP es que permite múltiples mecanismos de autenticación (CHAP, Kerberos, certificados de seguridad, autenticación con clave pública, etc.)

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

Autenticación y cifrado WPA

WPA–Enterprise

Los mecanismos de autenticación empleados más frecuentemente en WPA son tres:

EAP/TLS: Autenticación basada en un certificado de servidor y cliente (requiere una infraestructura de clave públicas por parte de la entidad gestora del AP).

EAP/TTLS o PEAP: Autenticación basada en un certificado de servidor. El cliente se valida con un nombre de usuario y contraseña en un servidor RADIUS. (Ejemplo: acceso Wi-Fi en la Universidad de Alicante).

LEAP (*Lightweight* EAP): Autenticación propietaria de Cisco Systems y que no emplea certificados de seguridad. La autenticación de un cliente se realiza empleando alguno de los mecanismos de autenticación que soporte un servidor RADIUS donde se almacenan los usuarios autorizados. Uno de los mecanismos que soporta RADIUS es CHAP, que permite el intercambio de la contraseña del usuario cifrada.

El objetivo de estos tres mecanismos es proporcionar a un usuario autorizado la denominada MK – *Master Key*, clave primaria con la que se inicia el mecanismo de cifrado TKIP.

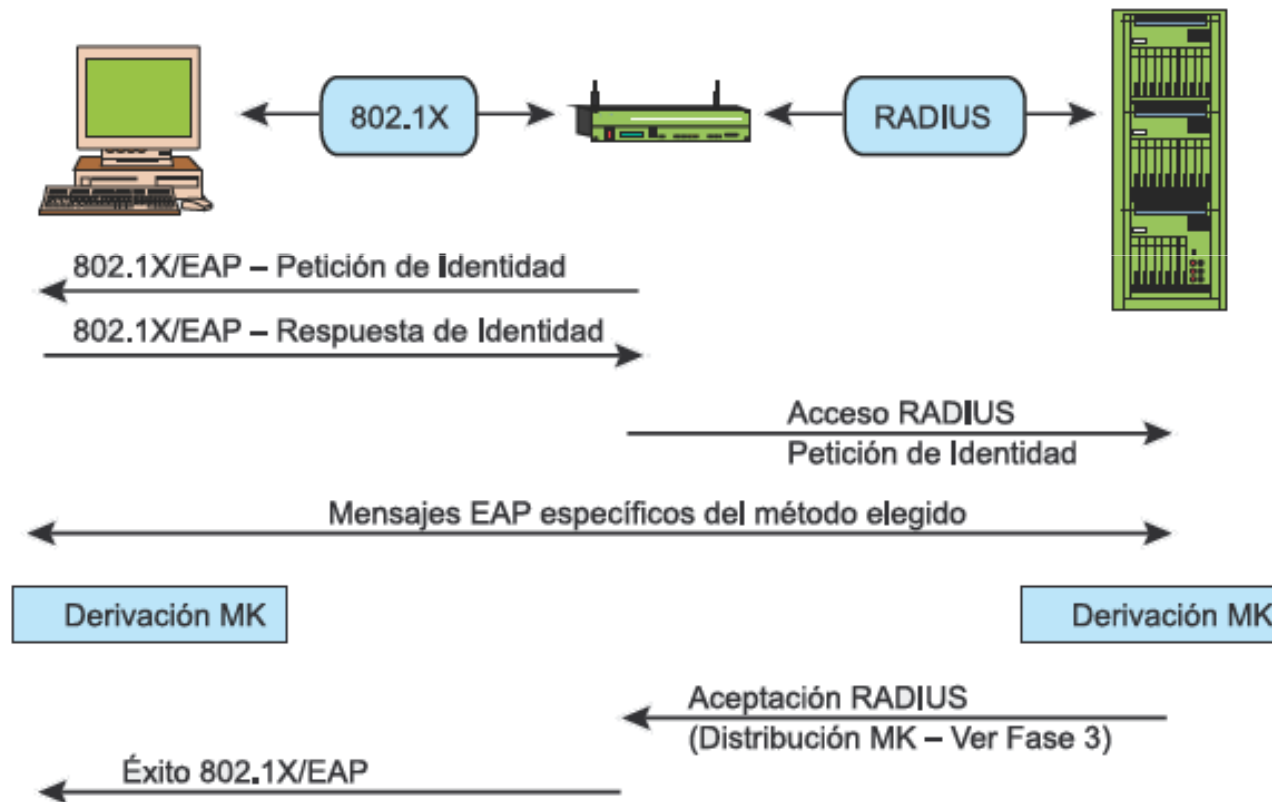
4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

Autenticación y cifrado WPA

WPA–Enterprise

Esquema del mecanismo de autenticación 802.1x



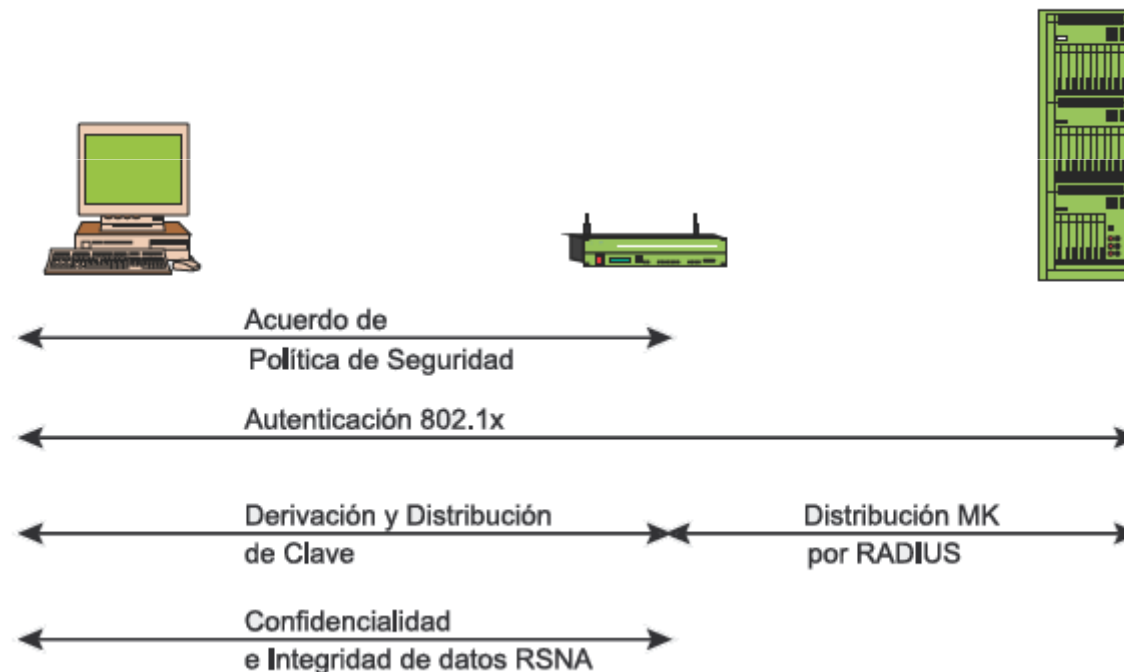
4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

IEEE 802.11i – WPA2™

Durante la implantación de WPA para superar los críticos problemas de seguridad de WEP, la Wi-Fi Alliance estaba desarrollando un sistema de seguridad Wi-Fi que completa en 2004 en la normativa IEEE 802.11i o WPA2 como marca comercial.

WPA2 introduce un paradigma de seguridad Wi-Fi, basado en toda la tecnología desarrollada para WPA.



RSNA – Robust Security Network Association. Proporciona un sistema con integridad y confidencialidad.

4.5 IEEE 802.11x. LAN Inalámbrica

4.5.3 Seguridad en redes Wi-Fi™

IEEE 802.11i – WPA2™

WPA2 no introduce variaciones en los mecanismos de autenticación empleados en WPA (se denominan WPA2-Personal y WPA2-Enterprise), pero sí permite mejorar la seguridad del cifrado.

WPA2 permite emplear, además de TKIP, otro mecanismo de cifrado denominado **AES** (Advanced Encryption Standard).

AES es un estándar de cifrado del NIST (Instituto Nacional de Estándares de EEUU) adoptado como mecanismo estándar de cifrado por el gobierno de EEUU.

AES emplea claves de cifrado de 128 bits cuando se emplea en WPA2. En la actualidad, este esquema de cifrado no se ha roto y por tanto es el más recomendable para accesos Wi-Fi. Sin embargo, existen vulnerabilidades (ataque de fuerza bruta en WPA2-PSK, denegación de servicio empleando desautenticación) que han llevado a introducir WPA3 en junio de 2018.

Wi-Fi CERTIFIED WPA3™

WPA3 establece mejoras en varias líneas:

- a) Aumento de la seguridad del cifrado WPA2-PSK. WPA3-PSK desarrolla un nuevo protocolo para establecer claves de cifrado seguras a partir de las claves PSK débiles que suelen emplear los usuarios.
- b) Aumento de la seguridad del cifrado en WPA3-Enterprise empleando AES con una clave de 192 bits.
- c) Mecanismos de cifrado individuales en las redes Wi-Fi abiertas con el procedimiento Wi-Fi CERTIFIED Enhanced Open™.

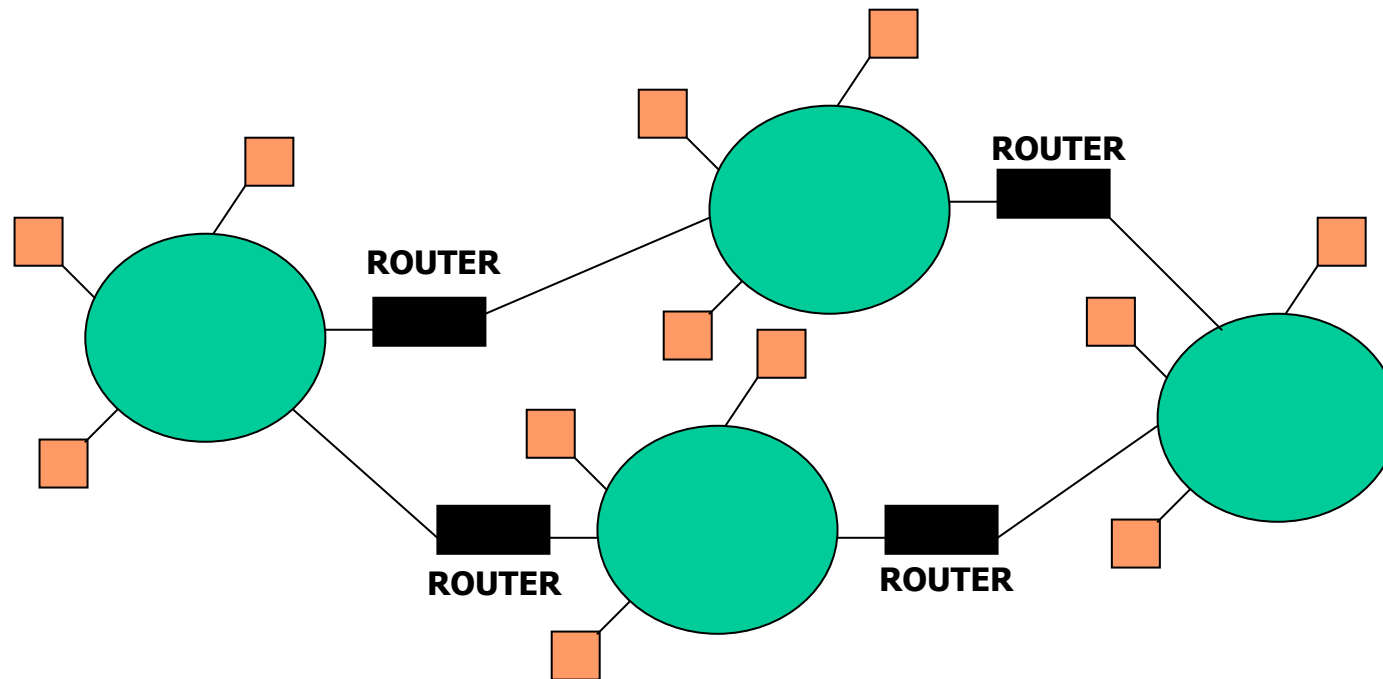
TEMA 5

NIVEL DE RED

5.1 Funcionalidades

Objetivos de la capa de red

Encaminamiento: Procedimiento por el que un paquete de información puede ser intercambiado entre cualquier par de equipos en una red de comunicaciones.



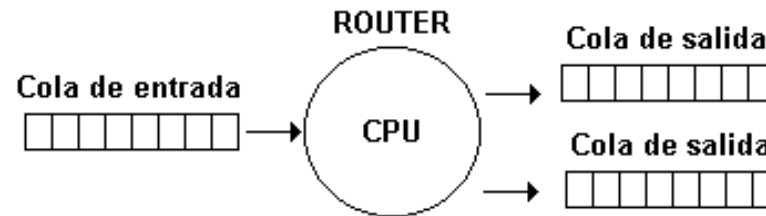
La arquitectura TCP/IP define un funcionamiento de red de datagramas en su capa de red:

Cada paquete de información incorpora dirección origen y dirección destino

En cada router se decide cuál es el siguiente salto que ha de realizar cada paquete.

5.1 Funcionalidades

Arquitectura de un router en una red TCP/IP



Funcionalidades básicas:

- Encaminamiento

- Gestión del flujo de información:

Vt=64 Kbps

{ Web 32 Kbps
Correo 16 Kbps
Otros 16 Kbps

- Seguridad:

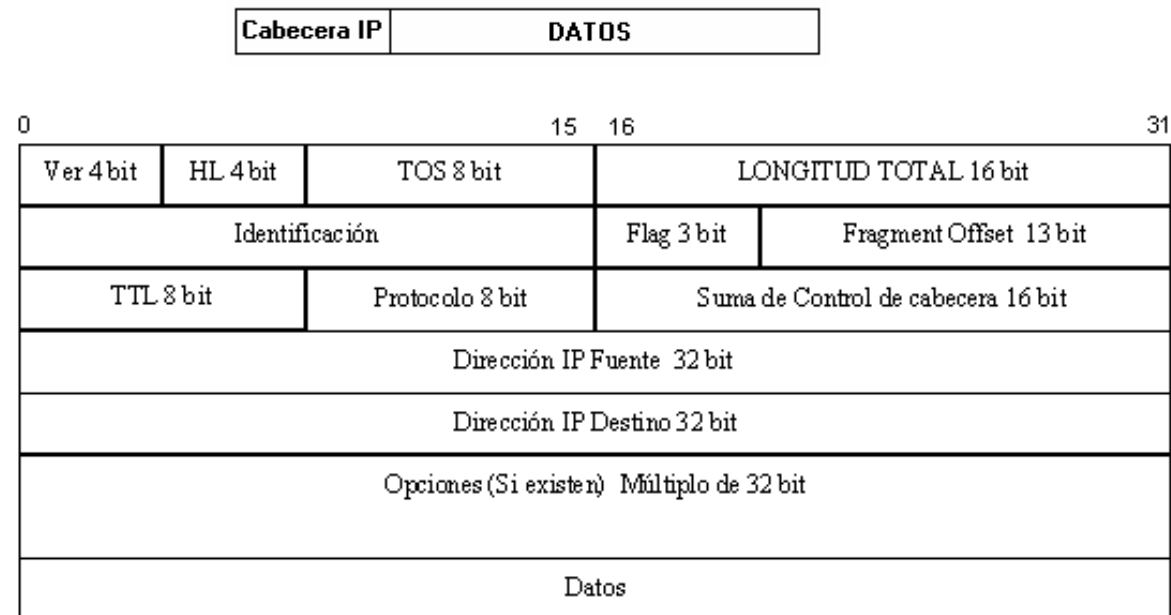
{ Firewall (cortafuegos): acceso limitado

{ Encriptación de datos: Protocolo IPSEC

5.1 Funcionalidades

5.1.1 Protocolo IP. RFC 791

- Define un sistema de numeración para identificar máquinas en una red formada por la interconexión de diferentes segmentos físicos.
- Define un formato de paquete de nivel de red (interred) para el control del encaminamiento (cabecera IP)



- Define el mecanismo de encaminamiento de los paquetes en los routers.

5.1 Funcionalidades

5.1.1 Protocolo IP. RFC 791

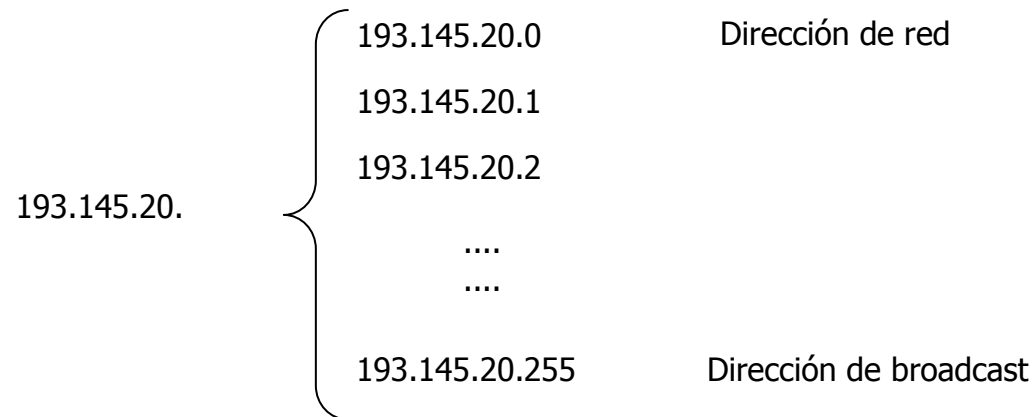
Direccionamiento IP

Dirección IP 193.145.20.23

¿ Identificador de red ?  Máscara de red de una red IP

Valor de 32 bits (X.X.X.X)  11111111..1000000000000000

Máscara de red = 255.255.255.0  193.145.20.23 pertenece a la red 193.145.20.



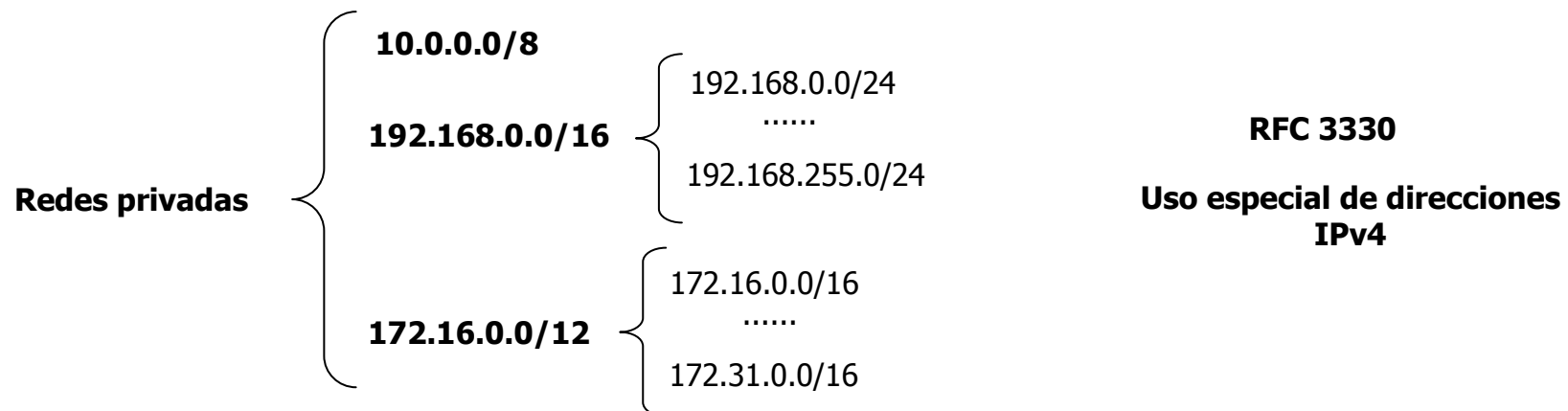
5.1 Funcionalidades

5.1.1 Protocolo IP. RFC 791

Direccionamiento IP

Clase	7bit	24bit	
A	0	Red	Máquina
			0.0.0.0 127.255.255.255
B	1 0	14bit Red	16bit Máquina
			128.0.0.0 191.255.255.255
C	1 1 0	21bit Red	8bit Máquina
			192.0.0.0 223.255.255.255
D	1 1 1 0	28bit Multicast	
			224.0.0.0 239.255.255.255
E	1 1 1 1 0	27bit Futuras Ampliaciones	
			240.0.0.0 247.255.255.255

Clases de direcciones IP



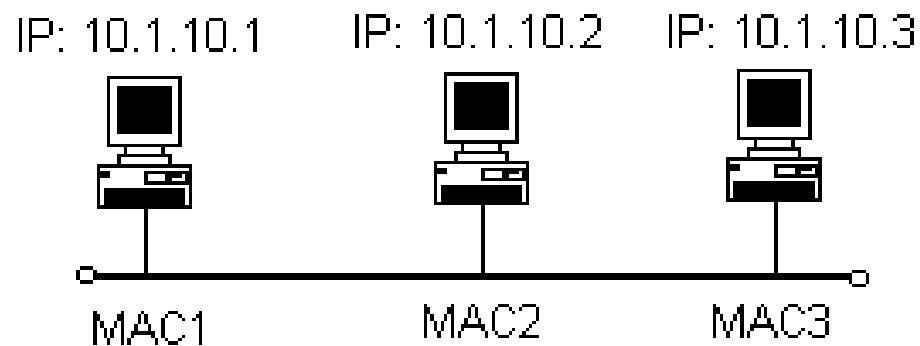
5.1 Funcionalidades

5.1.2 Direccionamiento de redes con el protocolo IP

Redes de difusión

Todas las estaciones que comparten un mismo medio físico en una red de difusión tienen que tener asignada la misma dirección de red IP.

La elección de la clase se determina dependiendo del número de máquinas en el segmento, siendo en general suficiente con redes de la clase C (hasta 254 máquinas).



Red 10.1.10.0/24

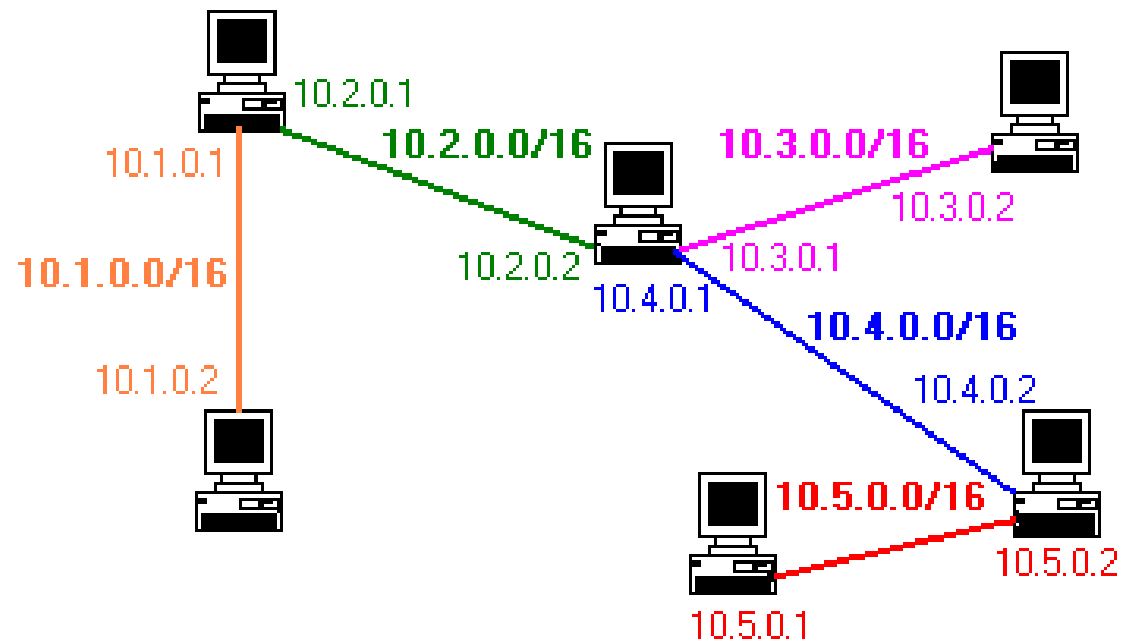
5.1 Funcionalidades

5.1.2 Direccionamiento de redes con el protocolo IP

Redes punto a punto

Las estaciones en los extremos de una red punto a punto tienen que tener asignada la misma dirección de red IP.

Por cada enlace punto a punto se especifica una dirección de red IP.



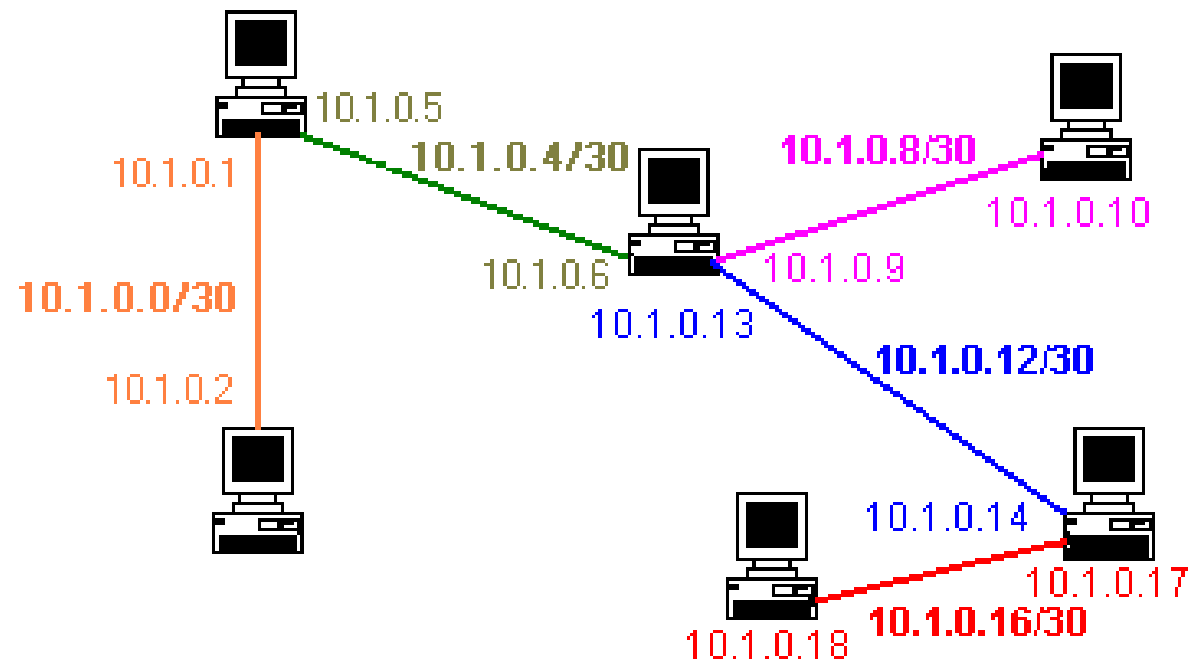
ii DESAPROVECHAMIENTO DE LAS DIRECCIONES IP !!

5.1 Funcionalidades

5.1.2 Direccionamiento de redes con el protocolo IP

Redes punto a punto

Para evitar la reserva innecesaria de direcciones IP, la máscara de red en una línea punto a punto se escoge para reservar el número de direcciones IP necesarias: 2 direcciones para máquinas, 1 para red y 1 para difusión.



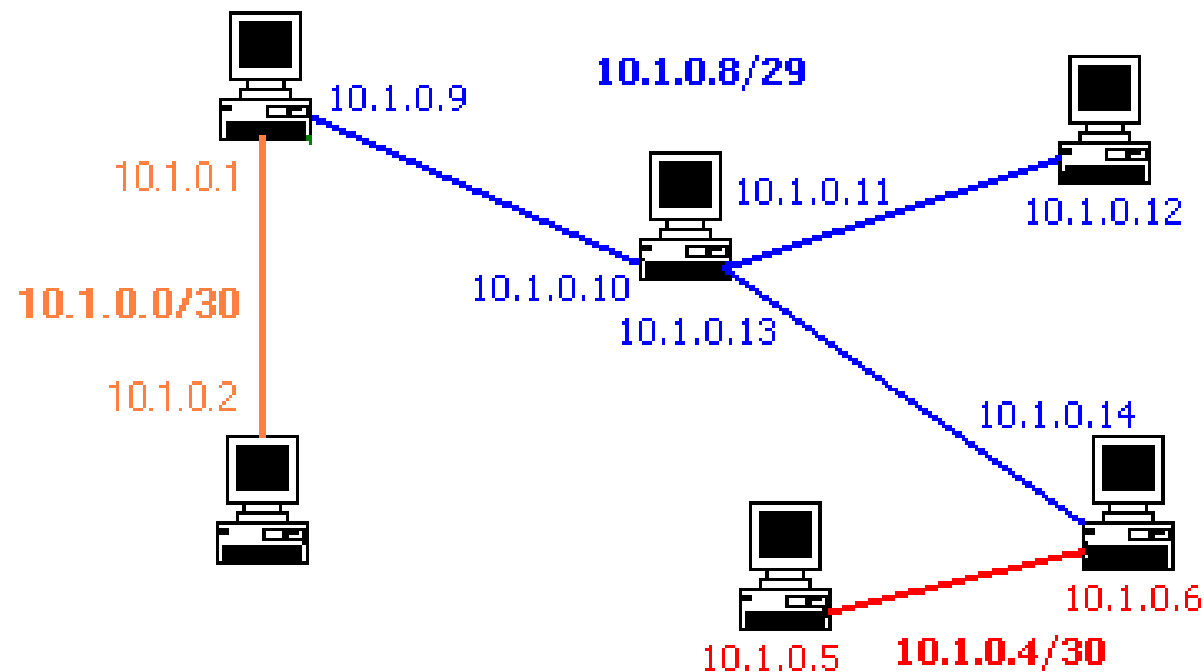
5.1 Funcionalidades

5.1.2 Direccionamiento de redes con el protocolo IP

Redes punto a punto

En el caso de enlaces multipunto a punto, es posible reducir la reserva de direcciones IP debido a las direcciones de red y difusión de cada enlace punto a punto.

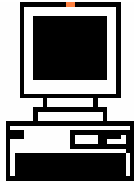
Para ello se agruparán en una sola red IP todos los enlaces punto a punto que parten de un mismo router, consiguiendo un ahorro adicional en el número de direcciones IP reservadas.



5.1 Funcionalidades

5.1.3 Tablas de encaminamiento

Dispositivos que precisan tablas de encaminamiento



Estación, PC, host de la red

Precisa de una tabla de encaminamiento sencilla: una entrada para la red a la que pertenece y otra para la puerta de enlace



Router, encaminador de la red

Precisa de una tabla de encaminamiento compleja: necesita entradas en la tabla de encaminamiento para cada red que conoce y una para la puerta de enlace

Formato de una tabla de rutas o tabla de encaminamiento

Una tabla de encaminamiento consta de una fila (entrada) por cada red IP que conoce el router.

Se distinguen 3 tipos de entrada:

Entradas asociadas a redes conectadas directamente (la puerta de enlace es una dirección IP del router).

Entradas asociadas a redes alcanzables (la puerta de enlace es la dirección IP de un router).

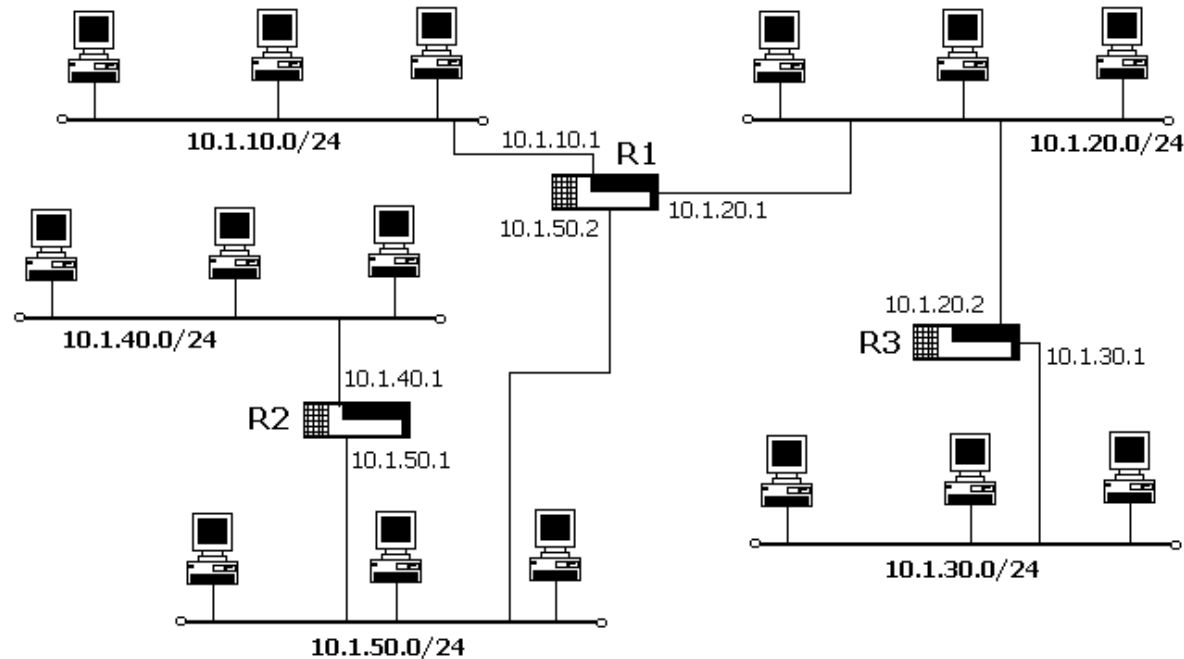
Entrada de la puerta de enlace por defecto (la puerta de enlace es la dirección IP de un router).

Destino	Máscara de red	Puerta de enlace
10.1.10.0	255.255.255.0	10.1.10.1
10.2.10.0	255.255.255.0	10.1.10.3
0.0.0.0	0.0.0.0	10.1.10.4

5.1 Funcionalidades

5.1.3 Tablas de encaminamiento

Tablas de encaminamiento en redes de difusión



R1

Destino	Máscara	p. de enlace
10.1.10.0	255.255.255.0	10.1.10.1
10.1.20.0	255.255.255.0	10.1.20.1
10.1.50.0	255.255.255.0	10.1.50.2
10.1.30.0	255.255.255.0	10.1.20.2
10.1.40.0	255.255.255.0	10.1.50.1

R2

Destino	Máscara	p. de enlace
10.1.40.0	255.255.255.0	10.1.40.1
10.1.50.0	255.255.255.0	10.1.50.1
10.1.10.0	255.255.255.0	10.1.50.2
10.1.20.0	255.255.255.0	10.1.50.2
10.1.30.0	255.255.255.0	10.1.50.2

R3

Destino	Máscara	p. de enlace
10.1.20.0	255.255.255.0	10.1.20.2
10.1.30.0	255.255.255.0	10.1.30.1
10.1.10.0	255.255.255.0	10.1.20.1
10.1.40.0	255.255.255.0	10.1.20.1
10.1.50.0	255.255.255.0	10.1.20.1

5.1 Funcionalidades

5.1.3 Tablas de encaminamiento

Tablas de encaminamiento en redes de difusión

Reducción del tamaño de las tablas de rutas

R1

Destino	Máscara	p. de enlace
10.1.10.0	255.255.255.0	10.1.10.1
10.1.20.0	255.255.255.0	10.1.20.1
10.1.50.0	255.255.255.0	10.1.50.2
10.1.30.0	255.255.255.0	10.1.20.2
10.1.40.0	255.255.255.0	10.1.50.1

R2

Destino	Máscara	p. de enlace
10.1.40.0	255.255.255.0	10.1.40.1
10.1.50.0	255.255.255.0	10.1.50.1
10.1.10.0	255.255.255.0	10.1.50.2
10.1.20.0	255.255.255.0	10.1.50.2
10.1.30.0	255.255.255.0	10.1.50.2

R3

Destino	Máscara	p. de enlace
10.1.20.0	255.255.255.0	10.1.20.2
10.1.30.0	255.255.255.0	10.1.30.1
10.1.10.0	255.255.255.0	10.1.20.1
10.1.40.0	255.255.255.0	10.1.20.1
10.1.50.0	255.255.255.0	10.1.20.1

R1

Destino	Máscara	p. de enlace
10.1.10.0	255.255.255.0	10.1.10.1
10.1.20.0	255.255.255.0	10.1.20.1
10.1.50.0	255.255.255.0	10.1.50.2
10.1.30.0	255.255.255.0	10.1.20.2
10.1.40.0	255.255.255.0	10.1.50.1

R2

Destino	Máscara	p. de enlace
10.1.40.0	255.255.255.0	10.1.40.1
10.1.50.0	255.255.255.0	10.1.50.1
0.0.0.0	0.0.0.0	10.1.50.2

R3

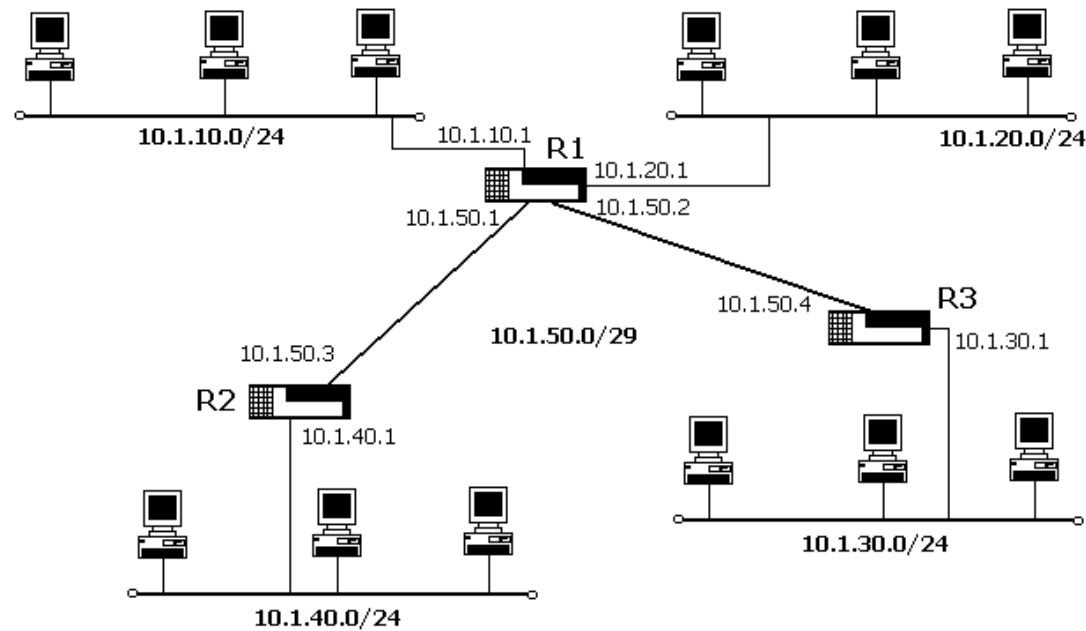
Destino	Máscara	p. de enlace
10.1.20.0	255.255.255.0	10.1.20.2
10.1.30.0	255.255.255.0	10.1.30.1
0.0.0.0	0.0.0.0	10.1.20.1

La reducción del número de entradas en la tabla de rutas permite un encaminamiento más rápido

5.1 Funcionalidades

5.1.3 Tablas de encaminamiento

Tablas de encaminamiento en redes punto a punto



R1

Destino	Máscara	p. de enlace
10.1.10.0	255.255.255.0	10.1.10.1
10.1.20.0	255.255.255.0	10.1.20.1
10.1.50.3	255.255.255.255	10.1.50.1
10.1.50.4	255.255.255.255	10.1.50.2
10.1.40.0	255.255.255.0	10.1.50.3
10.1.30.0	255.255.255.0	10.1.50.4

R2

Destino	Máscara	p. de enlace
10.1.40.0	255.255.255.0	10.1.40.1
10.1.50.0	255.255.255.248	10.1.50.3
10.1.10.0	255.255.255.0	10.1.50.1
10.1.20.0	255.255.255.0	10.1.50.1
10.1.30.0	255.255.255.0	10.1.50.1

R3

Destino	Máscara	p. de enlace
10.1.30.0	255.255.255.0	10.1.30.1
10.1.50.0	255.255.255.248	10.1.50.4
10.1.10.0	255.255.255.0	10.1.50.2
10.1.20.0	255.255.255.0	10.1.50.2
10.1.40.0	255.255.255.0	10.1.50.2

5.1 Funcionalidades

5.1.3 Tablas de encaminamiento

Tablas de encaminamiento en redes punto a punto

R1

Destino	Máscara	p. de enlace
10.1.10.0	255.255.255.0	10.1.10.1
10.1.20.0	255.255.255.0	10.1.20.1
10.1.50.3	255.255.255.255	10.1.50.1
10.1.50.4	255.255.255.255	10.1.50.2
10.1.40.0	255.255.255.0	10.1.50.3
10.1.30.0	255.255.255.0	10.1.50.4

R2

Destino	Máscara	p. de enlace
10.1.40.0	255.255.255.0	10.1.40.1
10.1.50.0	255.255.255.248	10.1.50.3
10.1.10.0	255.255.255.0	10.1.50.1
10.1.20.0	255.255.255.0	10.1.50.1
10.1.30.0	255.255.255.0	10.1.50.1

R3

Destino	Máscara	p. de enlace
10.1.30.0	255.255.255.0	10.1.30.1
10.1.50.0	255.255.255.248	10.1.50.4
10.1.10.0	255.255.255.0	10.1.50.2
10.1.20.0	255.255.255.0	10.1.50.2
10.1.40.0	255.255.255.0	10.1.50.2

R1

Destino	Máscara	p. de enlace
10.1.10.0	255.255.255.0	10.1.10.1
10.1.20.0	255.255.255.0	10.1.20.1
10.1.50.3	255.255.255.255	10.1.50.1
10.1.50.4	255.255.255.255	10.1.50.2
10.1.40.0	255.255.255.0	10.1.50.3
10.1.30.0	255.255.255.0	10.1.50.4

R2

Destino	Máscara	p. de enlace
10.1.40.0	255.255.255.0	10.1.40.1
10.1.50.1	255.255.255.255	10.1.50.3
10.1.10.0	255.255.255.0	10.1.50.1
10.1.20.0	255.255.255.0	10.1.50.1
10.1.30.0	255.255.255.0	10.1.50.1

R3

Destino	Máscara	p. de enlace
10.1.30.0	255.255.255.0	10.1.30.1
10.1.50.2	255.255.255.255	10.1.50.4
10.1.10.0	255.255.255.0	10.1.50.2
10.1.20.0	255.255.255.0	10.1.50.2
10.1.40.0	255.255.255.0	10.1.50.2

R2

Destino	Máscara	p. de enlace
10.1.40.0	255.255.255.0	10.1.40.1
10.1.50.1	255.255.255.255	10.1.50.3
0.0.0.0	0.0.0.0	10.1.50.1

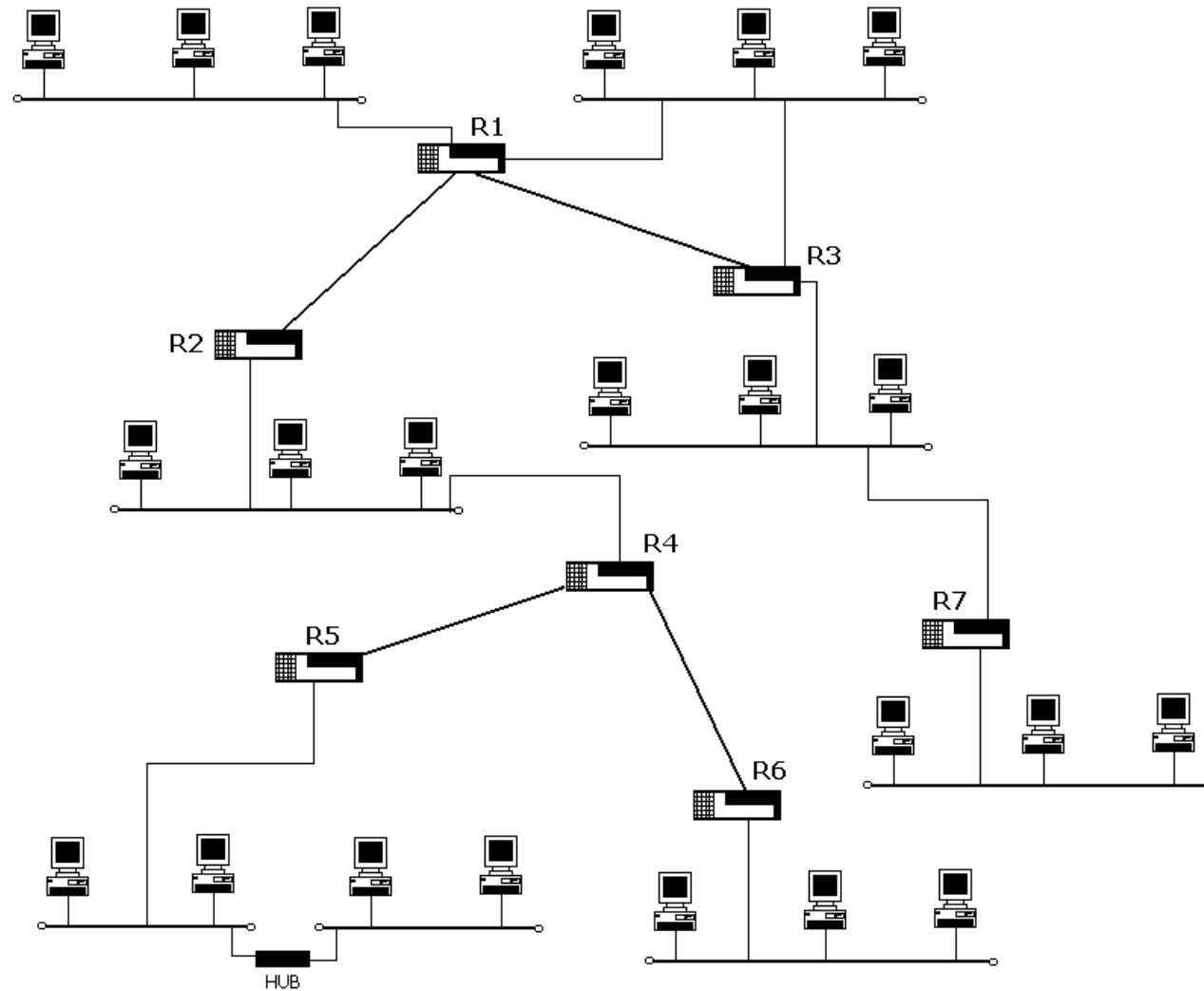
R3

Destino	Máscara	p. de enlace
10.1.30.0	255.255.255.0	10.1.30.1
10.1.50.2	255.255.255.255	10.1.50.4
0.0.0.0	0.0.0.0	10.1.50.2

5.1 Funcionalidades

5.1.3 Tablas de encaminamiento

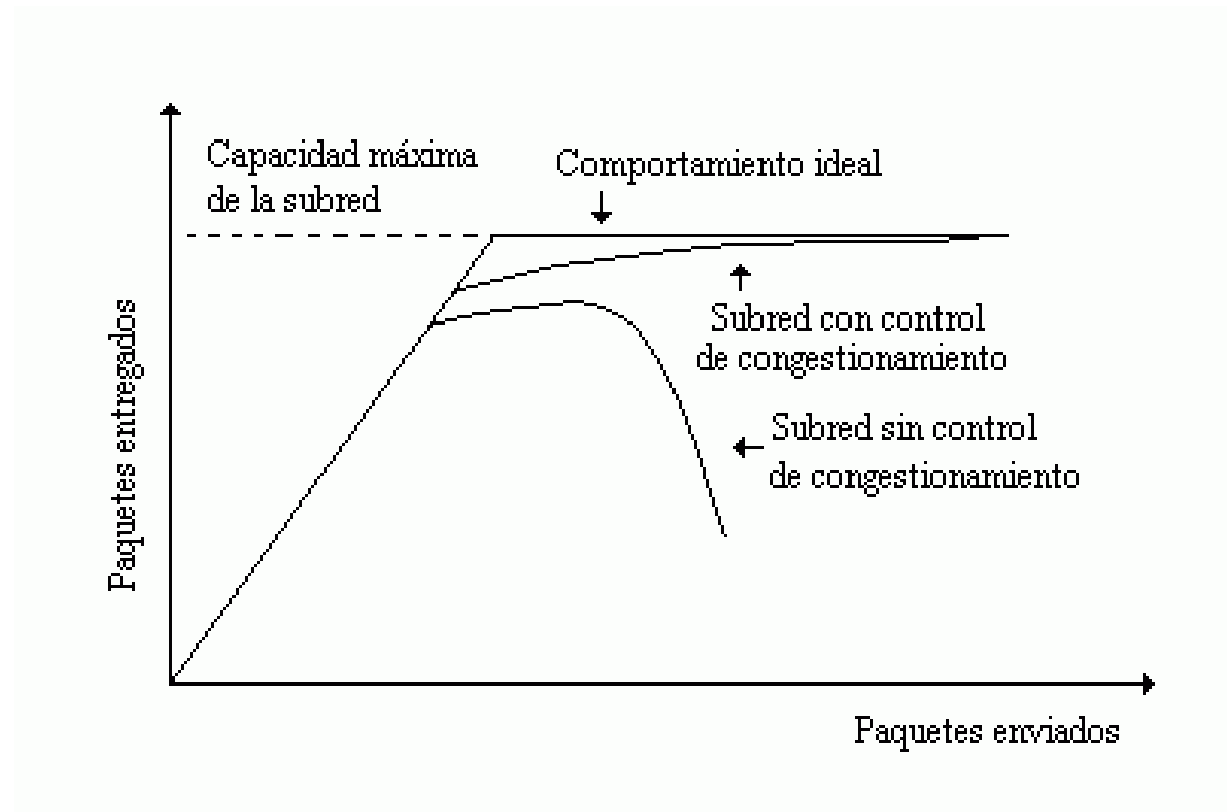
Ejercicio propuesto



5.1 Funcionalidades

5.1.4 Congestionamiento en redes IP

Una red de conmutación de paquetes presenta **congestión** si al aumentar el flujo de paquetes de entrada a la red (número de paquetes por segundo que entran en la red), disminuye el flujo de paquetes de salida (número de paquetes por segundo que salen de la red).



5.1 Funcionalidades

5.1.4 Congestionamiento en redes IP

La congestión se produce debido a que los routers de la red son incapaces de realizar el encaminamiento de los paquetes que reciben en un tiempo adecuado, debido a que les llegan demasiado rápido. Esto provoca un aumento en las colas de entrada de paquetes en los routers, lo que a su vez implica una mayor ralentización en el proceso de encaminamiento.

Si el congestionamiento no se detecta a tiempo en la red y no se toman medidas de corrección, la red se bloqueará quedando inutilizada para el intercambio de información.

Causas del congestionamiento

Routers con insuficiente capacidad de proceso. Será necesario aumentar la capacidad de los encaminadores de la red si va a aumentar el flujo de paquetes que circulará en la red.

Fragmentación de la información con el protocolo IP. Si la información a intercambiar es fragmentada por el protocolo IP en gran medida (MTU pequeño en la red), los routers precisan más tiempo para encaminar la misma información que con un MTU más grande, ya que tienen que analizar más cabeceras IP.

Detección del congestionamiento

Routers con insuficiente capacidad de proceso. Es necesario monitorizar cuál es el porcentaje de uso de la CPU de los routers. Si el valor de utilización es superior al 60-70%, se hace necesario emplear un router con mayores prestaciones (procesador de gama más alta).

Fragmentación de la información con el protocolo IP. Es necesario verificar que los MTU de la red están elegidos adecuadamente y que la fragmentación se evita con mecanismos como la norma RFC 1191. Detectando la presencia de mensajes ICMP Source Quench o Fragment Reassembly Time Exceeded se conoce si la fragmentación está provocando un efecto nocivo en la red.

5.1 Funcionalidades

5.1.4 Congestionamiento en redes IP

Corrección del congestionamiento

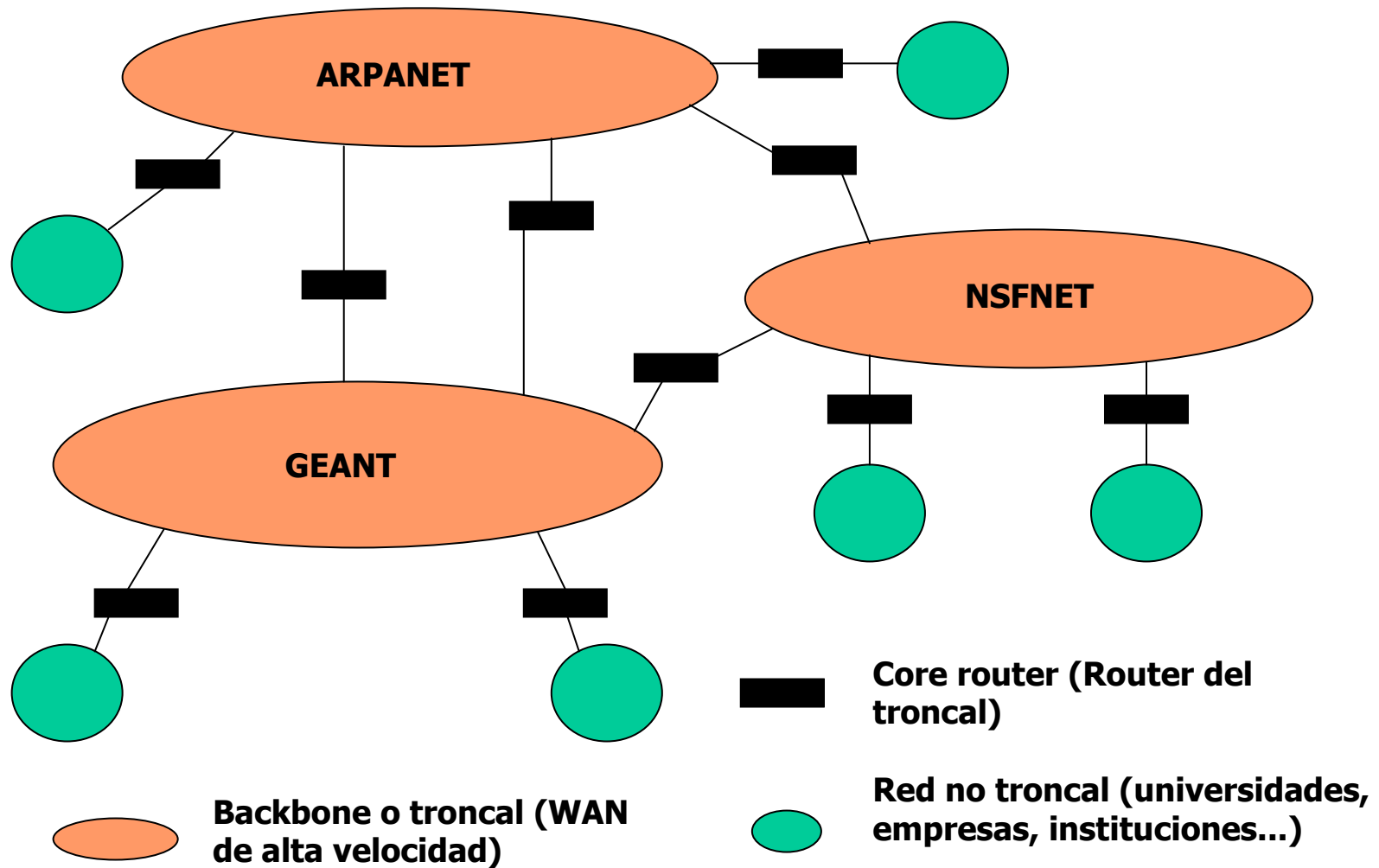
Si en una red se detecta una situación de congestionamiento, hay una única solución para que la red no quede bloqueada: **reducir el flujo de entrada de paquetes a la red.**

Esta estrategia es empleada por el protocolo TCP, que permite el envío de un número máximo de paquetes sin esperar a recibir la confirmación de que han llegado correctamente al destinatario. En el caso de que los ACKs no lleguen (retardo elevado en la red por congestión), el protocolo TCP es capaz de reducir su flujo de transmisión.

En la redes IP existen muchos flujos de datos que no emplean TCP y consumen grandes recursos en la red: comunicaciones VPN (*Virtual Private Network*), flujos UDP tiempo real, etc. Esto supone que el control de la congestión es una tarea que deben realizar los routers de Internet (como así hacen) realizando un encaminamiento lo más adecuado posible (ralentizar flujos no sensibles al retardo, priorizar flujos sensibles al retardo).

5.1 Funcionalidades

5.1.5 Estructura de Internet en Backbones o Troncales



5.1 Funcionalidades

5.1.5 Estructura de Internet en Backbones o Troncales

Características de los core routers (routers del troncal)

Conocimiento de todos los destinos de Internet

Tablas de encaminamiento grandes y complejas.

Alteraciones en la topología provocan cambios en todas las tablas de los core routers (añadir una nueva red).

Simplificación de las tablas de rutas

Conocimiento parcial de la red con rutas por defecto. Provocan inconsistencias (destinos inexistentes) y rutas no óptimas.

Conocimiento parcial de la red con un "super core router" con todo el conocimiento de la estructura de Internet. Irrealizable: no existe una máquina que pueda encaminar todos los paquetes de Internet y un fallo en ese nodo provocaría falta de conectividad.

Gestión de las tablas de encaminamiento

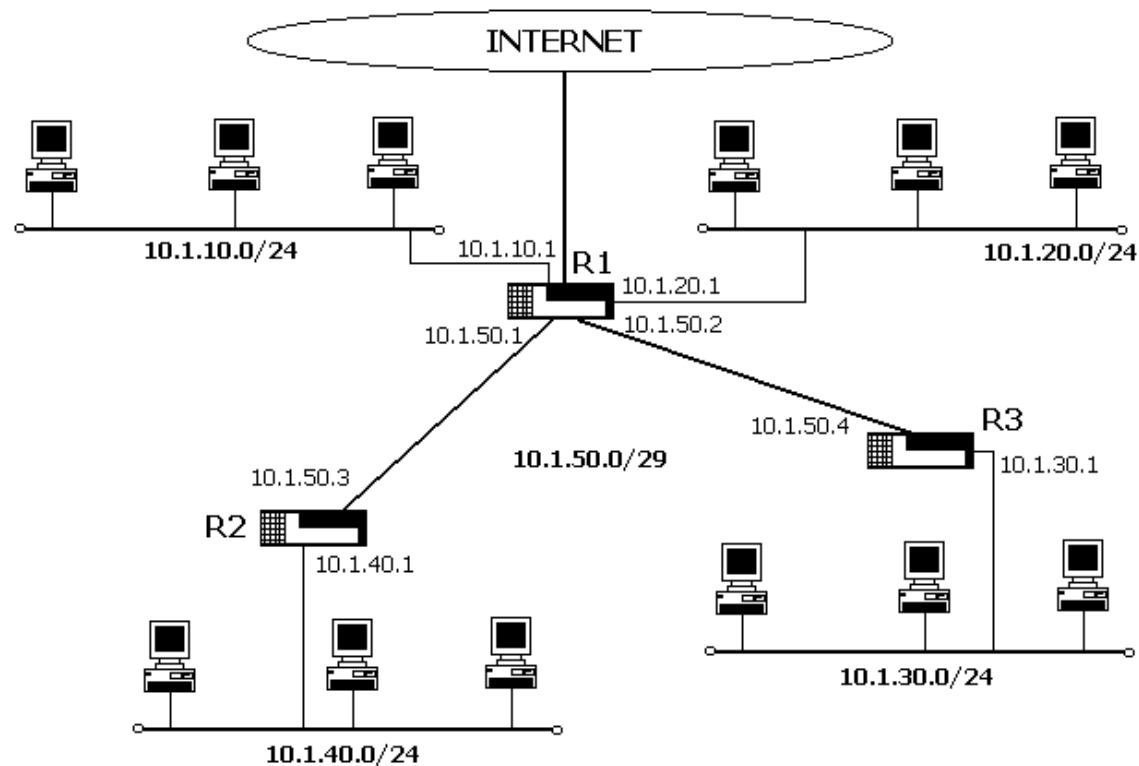
Sistema manual: los operadores actualizan las tablas ante fallos y cambios en la topología. Sólo apto en redes pequeñas y poco dinámicas.

Sistema automático: algoritmos de intercambio de información de encaminamiento entre los routers para actualizar y optimizar las tablas de encaminamiento. Empleado en Internet y redes LAN/WAN grandes.

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.1 Definición de Sistemas Autónomos (SA)

Red corporativa con conexión a Internet



Sistema autónomo: Conjunto de redes y routers controlados por una única autoridad administrativa (un único gestor de políticas de encaminamiento).

Política de encaminamiento: Conjunto de estrategias o directrices para decidir cuáles son los caminos óptimos a seguir en una red de comunicaciones.

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.1 Definición de Sistemas Autónomos (SA)

Encaminamiento en sistemas autónomos

Los sistemas autónomos disponen de un conjunto de redes con direccionamiento público y conectividad con cualquier máquina de Internet. Ej: Proveedores de acceso (ISPs), organismos públicos (Universidades, administración pública, etc).

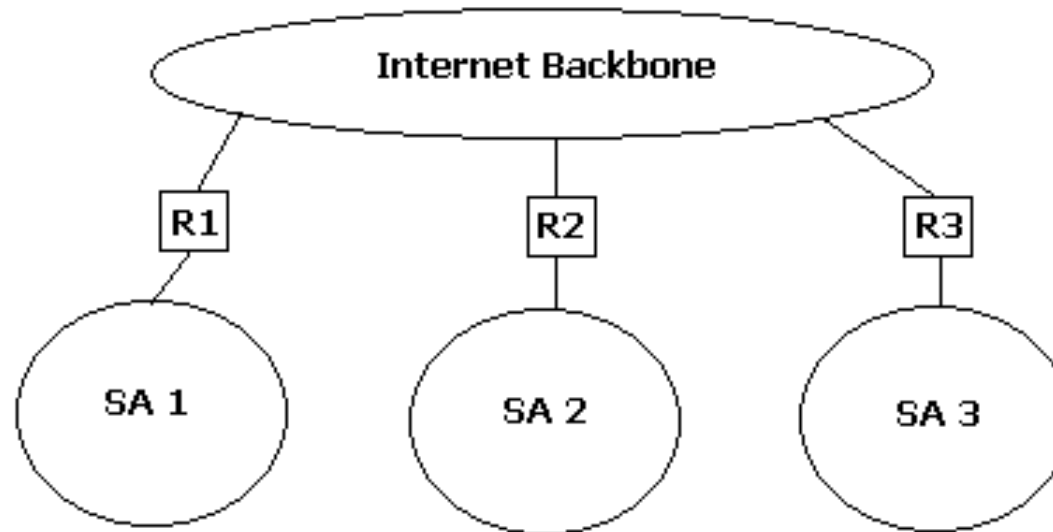
El encaminamiento óptimo en Internet requiere del intercambio de información de encaminamiento entre todos los routers de internet: IMPRACTICABLE.

Solución: intercambio de información de encaminamiento a dos niveles

- Intercambio de información de **encaminamiento entre sistemas autónomos** (BGP - Border Gateway Protocol)
- Intercambio de información de **encaminamiento dentro de sistemas autónomos** (RIP - Routing Information Protocol, OSPF - Open Shortest Path First)

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.2 Encaminamiento entre los SA de Internet



El encaminamiento óptimo en Internet requiere del intercambio de información de encaminamiento de todas la redes, lo que provoca:

Tiempo de convergencia de la red elevado: no tolera cambios rápidos en la estructura de la red como fallos en enlaces.

Consumo excesivo de ancho de banda para el intercambio de toda la información de encaminamiento

5.2 Algoritmos de gestión de tablas de encaminamiento

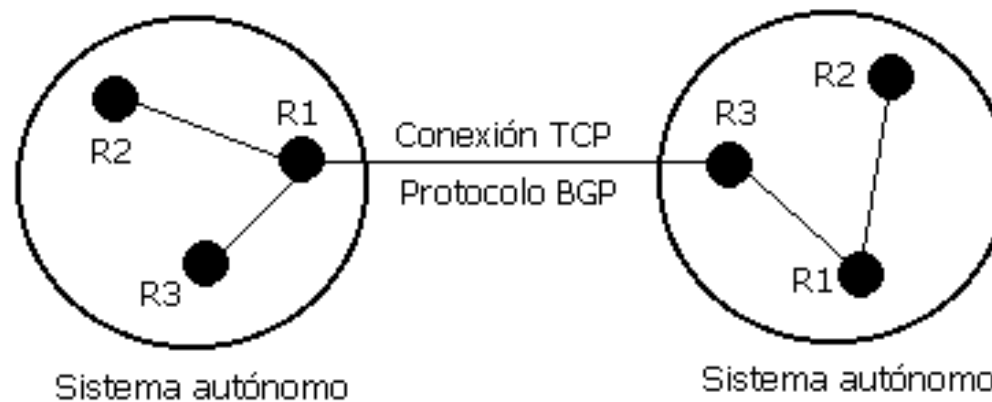
5.2.2 Encaminamiento entre los SA de Internet

Protocolo de encaminamiento BGP (Border Gateway Protocol)

Protocolo para el intercambio de información de encaminamiento entre sistemas autónomos.

Características:

En cada sistema autónomo se especifica un router de frontera (o más, en general uno) que dialoga con los routers de frontera de otros sistemas autónomos.



La información de encaminamiento se intercambia empleando conexiones TCP (puerto servidor 179) entre routers de frontera.

BGP informa acerca de alcanzabilidad y conectividad entre sistemas autónomos (qué redes pertenecen a qué sistemas autónomos)

BGP reduce la información intercambiada comunicando una sola vez todas las redes accesibles a través de un sistema autónomo, y después actualiza la información que se modifica. Además agrupa destinos en una sola denominación.

BGP soporta autenticación para preservar la validez de la información de encaminamiento intercambiada.

5.2 Algoritmos de gestión de tablas de encaminamiento

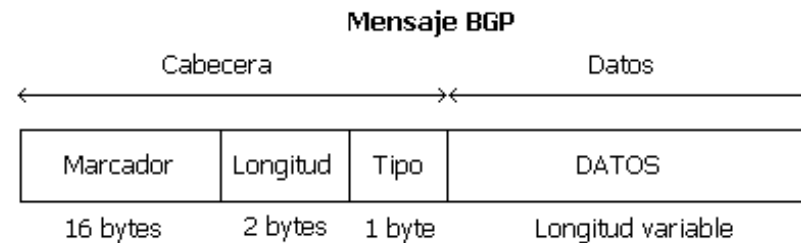
5.2.2 Encaminamiento entre los SA de Internet

Protocolo de encaminamiento BGP (Border Gateway Protocol)

Funcionamiento del protocolo BGP

El protocolo BGP se fundamenta en el establecimiento de una conexión TCP para el intercambio de diferentes mensajes BGP.

Cada mensaje BGP consta de un paquete con cabecera y datos. La cantidad de datos y su formato depende del tipo de mensaje BGP.



Mensaje BGP Open: Es el primer mensaje que se intercambia entre dos routers frontera que establecen la conexión TCP. Se intercambian parámetros como el identificador de sistema autónomo, intervalos de tiempo en el envío de mensajes BGP, etc.

Mensaje BGP Update: Este mensaje informa acerca de destinos existentes en el sistema autónomo y destinos que se han eliminado en el sistema autónomo.

Mensaje BGP Keepalive: Este mensaje informa de que un extremo de la comunicación sigue activo. TCP no controla que los dos extremos estén activos cuando no intercambian datos, por lo que BGP define un mensaje para este propósito.

Mensaje BGP Notification: Este mensaje informa acerca de errores en la comunicación BGP (mensajes BGP con errores: rutas incorrectas o incongruentes) y permite el control en la comunicación (finalización de la conexión, expiración de tiempo de espera de paquetes Keepalive, etc)

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.2 Encaminamiento entre los SA de Internet

Protocolo de encaminamiento BGP (Border Gateway Protocol)

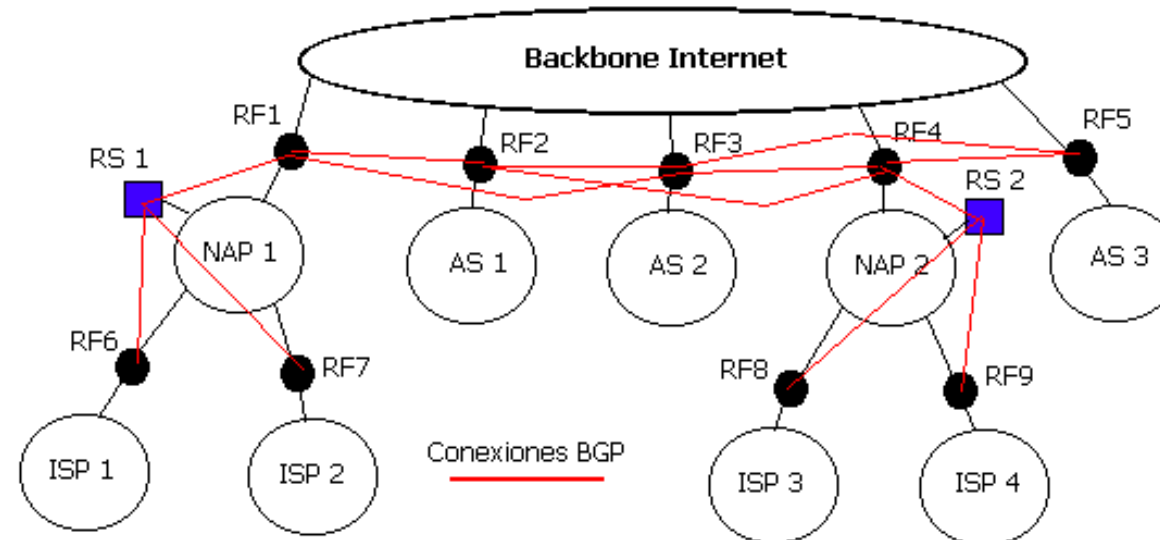
Empleo de BGP en los proveedores de acceso a Internet (ISPs)

Para conseguir conectividad en Internet todos los sistemas autónomos tienen que estar conectados al backbone de Internet para intercambiar mensajes BGP.

No existe disponibilidad para que cualquier ISP esté conectado al backbone de Internet (ARPANET - NSFNET en USA), y existen los denominados Network Access Point (NAPs).

En cada NAP acceden los sistemas autónomos de varios ISPs que intercambian información de encaminamiento con BGP entre el backbone de Internet y los ISPs.

Para evitar inconsistencias en el encaminamiento entre los ISPs, en cada NAP hay un router servidor (RS) con el que dialogan cada uno de los routers frontera de los ISPs para el intercambio de mensajes BGP.



5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.2 Encaminamiento entre los SA de Internet

Protocolo de encaminamiento BGP (Border Gateway Protocol)

Conclusiones

BGP sólo informa de accesibilidad, no de rutas a seguir o rutas de menor coste (no entiende métricas).

BGP establece conexiones entre pares de routers frontera, por lo que tiene que existir conectividad entre todos los routers frontera de Internet.

BGP informa sobre destinos existentes y no existentes, evitando así la presencia de mensajes ICMP destino no alcanzable entre diferentes ISPs.

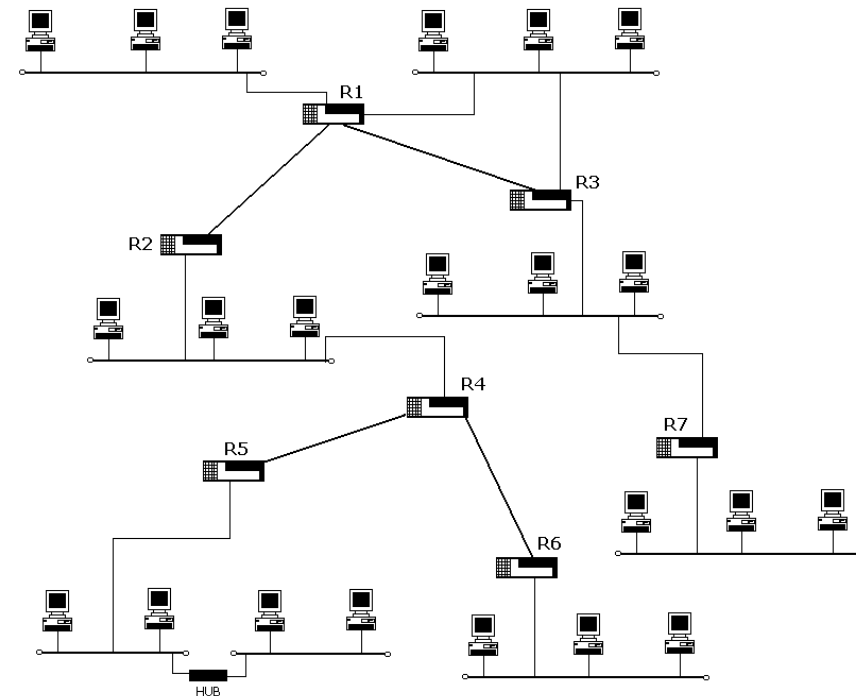
5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los SA de Internet

Tablas de encaminamiento en un sistema autónomo

El encaminamiento estático (tablas de rutas fijas) no es adecuado:

- Cambios en la red implican actualización de tablas en todos los routers (ejemplo: añadir una nueva red)
- Tiempo de respuesta ante fallos elevado (ejemplo: fallo de un enlace, la actualización de tablas es manual)



Es necesario un mecanismo de configuración y actualización de tablas de encaminamiento automático

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los SA de Internet

Protocolo de Información de Encaminamiento (RIP)

El origen de RIP (Routing information protocol – RFC 1058) está en un software desarrollado por la Universidad de Berkeley para proporcionar consistencia y fiabilidad en la interconexión de redes locales con sistema operativo BSD UNIX.

Se fundamenta en un algoritmo de vector de distancia (Algoritmo de Bellman-Ford)

Cada router dispone de una tabla con información de destinos y una métrica (número de saltos) para alcanzar el destino.

Cada router propaga la información de sus rutas conocidas a través de mensajes en la red, y los routers que la reciben actualizan sus tablas si encuentran rutas más cortas a un mismo destino.

Tabla Router K

Destino	Distancia	P. Enlace
Red 1	1	Directa
Red 2	1	Directa
Red 4	8	Router L
Red 17	5	Router M
Red 24	6	Router J
Red 30	2	Router Q
Red 42	2	Router J

Mensaje RIP Router J

Destino	Distancia
Red 1	2
Red 4	3
Red 17	6
Red 21	4
Red 24	5
Red 30	10
Red 42	3

Tabla Router K actualizada

Destino	Distancia	P. Enlace
Red 1	1	Directa
Red 2	1	Directa
Red 4	4	Router J
Red 17	5	Router M
Red 24	6	Router J
Red 30	2	Router Q
Red 42	2	Router J
Red 21	5	Router J

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los SA de Internet

Protocolo de Información de Encaminamiento (RIP)

Al informar el router J que la Red 42 tiene un aumento de coste, indica que ha habido un fallo en algún enlace, por lo que la ruta a la Red 42 en el router K debe ser modificada.

Para solventar este problema, RIP introduce una serie de reglas adicionales:

Para cada entrada en la tabla de rutas (distancia, métrica) existe un temporizador (180 segundos). Si la ruta no es informada (distancia, métrica) de nuevo en ese tiempo, es eliminada. Ej: En el caso anterior, al cabo de 180 segundos la ruta (Red 42, 2) es eliminada, y se sustituirá por (Red 42, 4).

Existe un número máximo de saltos para la métrica de RIP que es 16. Esto evita problemas de convergencia del algoritmo, es decir, llegar a una solución estable.

Propagación de la información con RIP (versión 1 – RFC 1058)

Los mensajes RIP con información de las rutas de un router se envían dentro de paquetes UDP.

Existen mensajes RIP de petición y respuesta, de forma que los paquetes RIP de petición son enviados al puerto UDP 520 del router, y los paquetes RIP de respuesta proceden del puerto UDP 520.

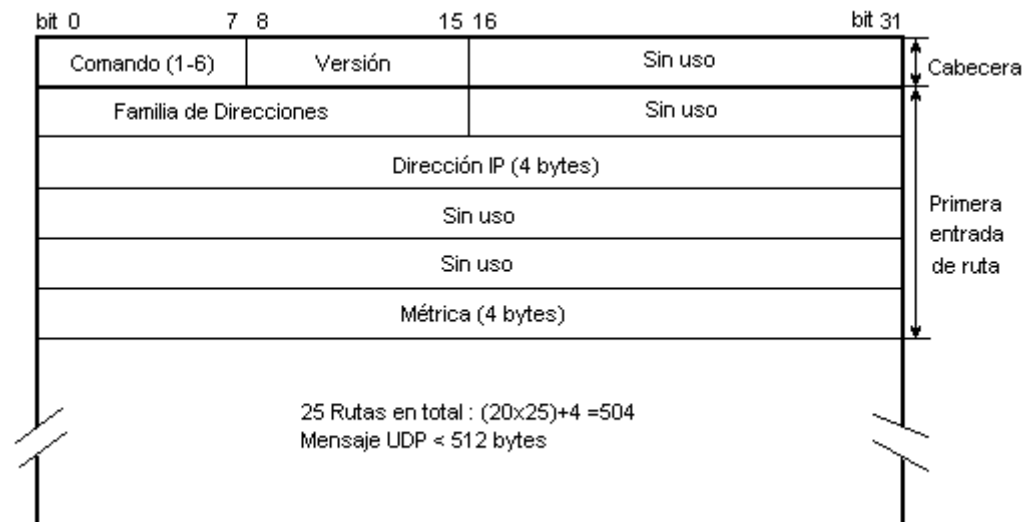
Para que los mensajes RIP lleguen a todas las estaciones del segmento físico (difusión de la información), los paquetes UDP son enviados a la dirección de broadcast de la red IP donde se difunden.

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los SA de Internet

Protocolo de Información de Encaminamiento (RIP)

Formato del mensaje RIP versión 1



No es posible especificar la máscara de red del destino ni el router a través del cual se alcanza el destino.

El envío de mensajes RIP a la dirección de broadcast hace que las máquinas que no soportan RIP procesen paquetes hasta la capa de transporte (UDP).

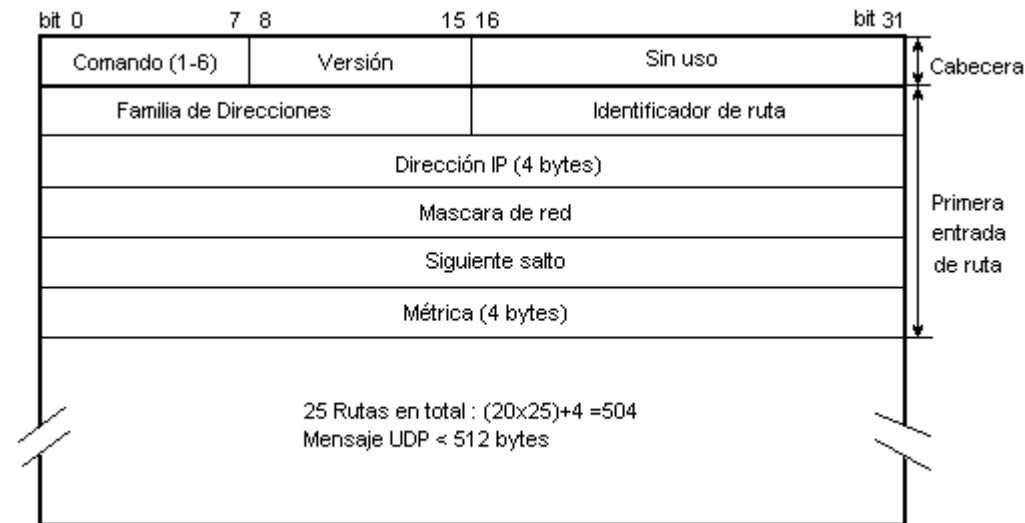
Para solventar estos problemas se introduce la versión 2 de RIP.

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los SA de Internet

Protocolo de Información de Encaminamiento (RIP)

Propagación de la información con RIP (versión 2 – RFC 2453)



Formato del mensaje RIP versión 2

Los mensajes RIP son enviados a la dirección IP 224.0.0.9 (dirección IP de multicast), de forma que sólo las estaciones que tienen habilitado contestar a esa dirección procesan el paquete.

CONCLUSIONES

RIP permite el encaminamiento dinámico en redes de tamaño pequeño (hasta 16 saltos) con una estructura sencilla (inexistencia de muchos bucles).

RIP presenta problemas de convergencia lenta ante cambios en la red y posibilidad de que se introduzcan bucles infinitos. Para evitar esto emplea estrategias como temporizadores y un número máximo de saltos.

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los SA de Internet

Protocolo Abierto del Camino más Corto Primero (OSPF – RFC 1583)

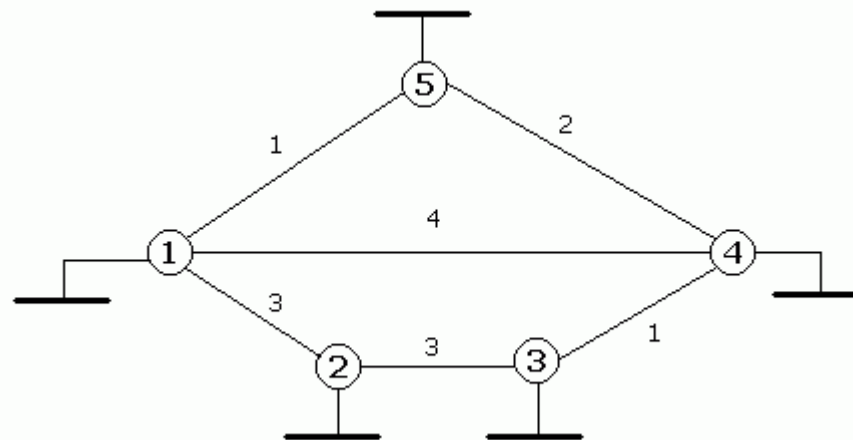
OSPF (Open Shortest Path First) es una alternativa al protocolo RIP a la hora de establecer las métricas de la rutas.

RIP sólo tiene en cuenta el número de saltos, pero no la velocidad de transferencia, por lo que las rutas con menos saltos no tienen porque ser las más rápidas.

OSPF se fundamenta en el denominado estado del enlace, asignando un coste dependiendo de las características del enlace (alta velocidad, baja velocidad, activado, desactivado, etc.).

El conjunto de routers de una red que emplean OSPF conforman un grafo, donde se determinan las rutas más cortas entre cualquier par de nodos (router, o en definitiva redes) del grafo (red).

OSPF emplea el algoritmo de Dijkstra para determinar las rutas de menor coste en la red.



5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los SA de Internet

Protocolo Abierto del Camino más Corto Primero (OSPF – RFC 1583)

Para determinar las rutas de menor coste es necesario intercambiar información entre los routers que emplean OSPF. Esta información se intercambia en forma de mensajes de diferentes tipos.

Los mensajes OSPF se encapsulan dentro de paquetes IP dirigidos a la dirección de multicast 224.0.0.5 (todos los routers OSPF) y 224.0.0.6 (routers OSPF designados).

Mensajes OSPF

OSPF Hello: Permite determinar qué vecinos tiene accesible un router.

OSPF Database description: Informa de la topología de la red de comunicaciones.

OSPF Link status request: Permite solicitar a los routers vecinos información acerca de los enlaces activos.

OSPF Link status update: Un router informa a sus vecinos del estado de sus enlaces.

5.3 Multicasting

El término multicasting hace referencia a la multidifusión, que es aplicable al direccionamiento IP.

Clase	7bit	24bit	
A	0	Red	Máquina
			0.0.0.0 127.255.255.255
B	1 0	14bit Red	16bit Máquina
			128.0.0.0 191.255.255.255
C	1 1 0	21bit Red	8bit Máquina
			192.0.0.0 223.255.255.255
D	1 1 1 0	28bit Multicast	
			224.0.0.0 239.255.255.255
E	1 1 1 1 0	27bit Futuras Ampliaciones	
			240.0.0.0 247.255.255.255

Para este propósito está definida la clase D del direccionamiento IP, pudiendo establecer 2^{28} direcciones de multidifusión, o lo que es lo mismo 2^{28} direcciones de grupos de máquinas.

Cada máquina en Internet procesa los paquetes IP dirigidos a su dirección IP y a la dirección IP del broadcast de su red. Adicionalmente, una máquina de Internet puede ser configurada para que pertenezca a cualquier grupo de multidifusión, por lo que también procesaría los paquetes dirigidos al grupo al que pertenezca.

5.3 Multicasting

Cada dirección de multidifusión tiene asociada una función específica, de forma que cada dirección de multicast identifica grupos de máquinas en Internet que llevan a cabo una función común.

Dirección Multicast	Denominación del grupo
224.0.0.0	Reservada
224.0.0.1	Todos los equipos de la subred
224.0.0.2	Todos los routers en la subred
224.0.0.5	Routers OSPF
224.0.0.6	Routers OSPF designados
224.0.0.9	Routers RIP2

Una máquina que pertenece a un grupo de multicast puede estar en cualquier lugar de Internet, por lo que los routers de interconexión entre redes tienen que propagar los paquetes IP dirigidos a direcciones de multicast (hay que habilitar el router para ello).

Existe una restricción, y es que los paquetes dirigidos a grupos de gestión de encaminamiento (desde la dirección 224.0.0.1 a la 224.0.0.255) no son propagados nunca (para evitar congestión).

5.3 Multicasting

Cuando un paquete IP se envía a una dirección multicast ¿ qué dirección de nivel de enlace se emplea ?

Si el nivel de enlace soporta multicasting (Ej: Ethernet) cada dirección IP de multicast tiene asociada una dirección de enlace de multicast.

Si el nivel de enlace no soporta multicasting cada dirección IP de multicast tendrá asociada la dirección de broadcast del nivel de enlace, o el caso de redes punto a punto el otro extremo del enlace.

IGMP – Protocolo de Gestión de Grupo en Internet

Este protocolo, que al igual que ICMP funciona sobre IP estableciendo diferentes tipos de mensajes IGMP, permite la gestión del encaminamiento con multicasting.

Básicamente, el protocolo define dos funcionalidades básicas:

Cuando una estación se añade a un grupo multicast, envía un mensaje IGMP al grupo indicando que se ha añadido, de forma que los routers del grupo actualizan rutas para enviar paquetes multicast al nuevo host.

Cada cierto tiempo, los routers de un grupo multicast sondean a los miembros del grupo de su red local para saber si están activos. Si no hay ningún miembro activo, el router informa a los demás que en esa red no hay miembros y no hay que reenviar paquetes multicast.

Aplicaciones

Mecanismo de propagación de información en algoritmos de encaminamiento para evitar carga computacional en dispositivos que no son routers y que no emplean el algoritmo.

Reducción de consumo de ancho de banda en la transmisión de streaming de audio y vídeo en Internet (en desarrollo).

5.4 IPv6 (RFC 2460)

5.4.1 Limitaciones de IPv4

La principal limitación que ha conducido a la introducción de una nueva versión de protocolo IP es la limitación en el direccionamiento IPv4 a 32 bits.

IPv6 introduce direcciones IP de 128 bits, lo que supone disponer de aproximadamente 6×10^{23} direcciones por metro cuadrado de la superficie terrestre.

La fragmentación provoca un efecto nocivo en el rendimiento de la red, por lo que IPv6 no permite la fragmentación de un paquete IP en un router intermedio.

La fragmentación se realiza en el origen, determinando éste el valor de MTU mínimo en el camino de origen a destino, o bien tomando el valor mínimo de MTU que tiene que soportar una red IPv6, 1280 bytes.

IPv6 mejora el campo de opciones de IPv4, permitiendo un uso más eficiente en el encaminamiento.

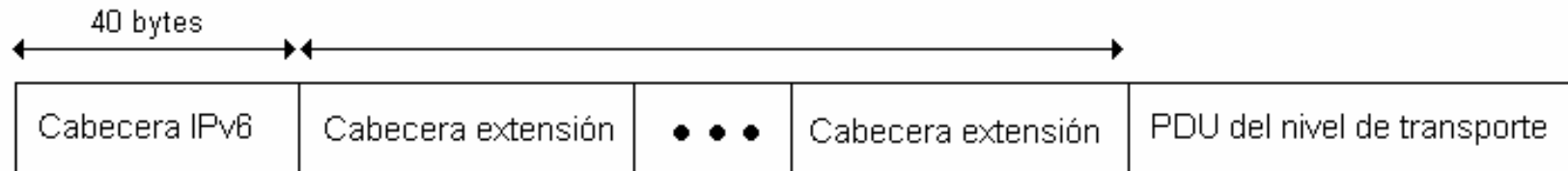
IPv6 mejora la gestión de QoS en IP. Para ello, además de identificar clases de tráfico (prioridades) con un campo equivalente al TOS de la cabecera IPv4, IPv6 identifica flujos de tráfico.

En IPv6 se pueden identificar flujos de tráfico de la misma prioridad, lo que es muy interesante para gestionar en los routers varios flujos de audio y vídeo procedentes de un mismo equipo.

5.4 IPv6 (RFC 2460)

5.4.2 Cabecera IPv6

Una PDU de IPv6 consta de una cabecera fija y común a todos los paquetes (cabecera IPv6), un conjunto de cabeceras de extensión y la PDU del nivel superior (transporte).



Se han definido las siguientes cabeceras de extensión:

Cabecera de opciones salto a salto: Define acciones a tomar en cada router que atraviesa el paquete (generar mensajes ICMP, descartar paquetes, priorizar el paquete, etc.)

Cabecera de encaminamiento: Proporciona un encaminamiento adicional, similar al encaminamiento en el origen de IPv4.

Cabecera de fragmentación: La fragmentación en IPv6 se realiza en el origen, y es el destinatario el encargado del reensamblado del paquete. Emplea un mecanismo similar a IPv4.

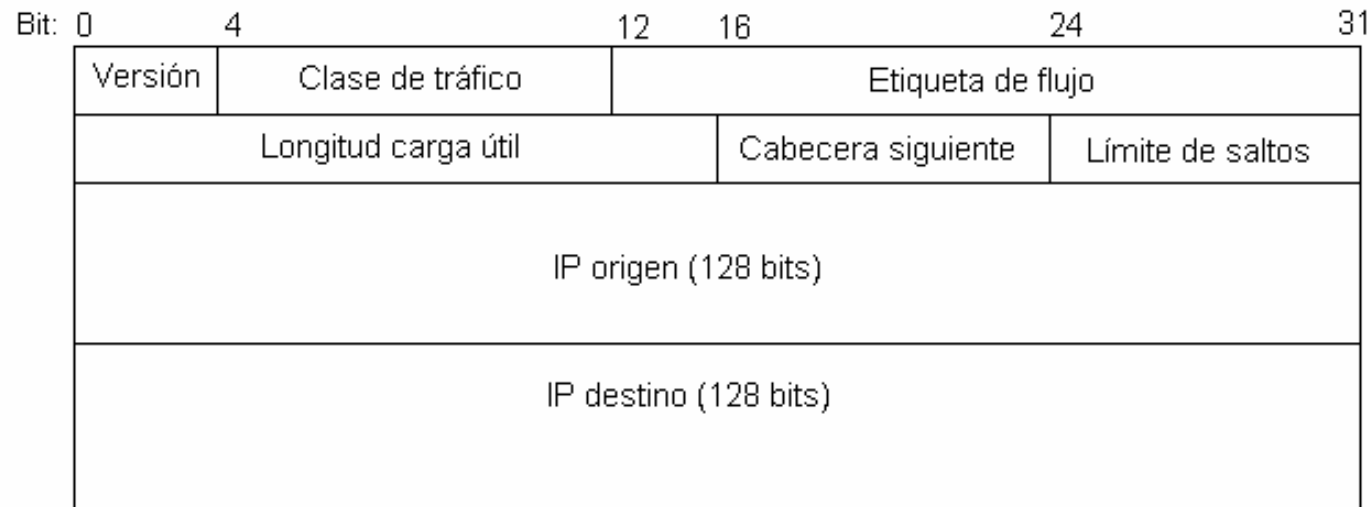
Cabecera de opciones para el destino: Contiene información opcional para ser examinada en el nodo destino.

Cabecera de autenticación y encapsulado de seguridad: Cabeceras AH y ESP de IPSEC .

5.4 IPv6 (RFC 2460)

5.4.2 Cabecera IPv6

Formato de la cabecera IPv6



Clase de tráfico: Equivalente al campo TOS de IPv4. Permite establecer clases distintas de tráfico.

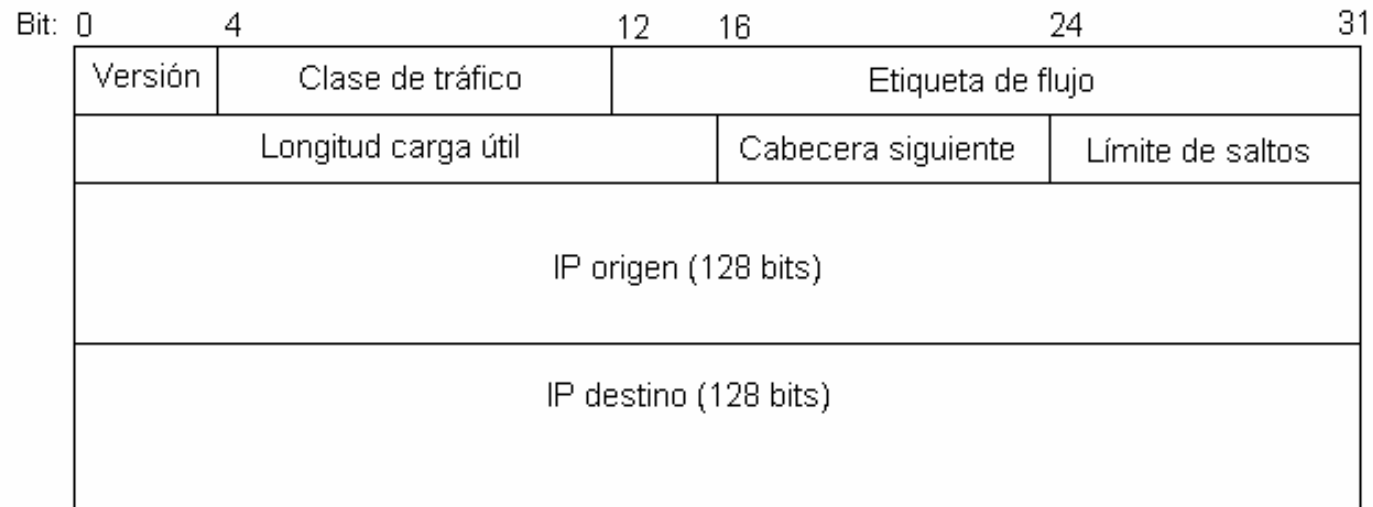
Etiqueta de flujo: Permite identificar flujos de paquetes entre dos aplicaciones origen y destino. Un flujo puede estar compuesto de varias conexiones TCP (intercambio de ficheros con varias conexiones simultáneas). Una aplicación puede generar varios flujos (un aplicación de videoconferencia genera un flujo de audio y otro de vídeo que los routers deben encaminar de manera diferente).

Longitud carga útil: Tamaño en bytes de las cabeceras de extensión y la PDU de nivel superior.

5.4 IPv6 (RFC 2460)

5.4.2 Cabecera IPv6

Formato de la cabecera IPv6



Cabecera siguiente: Especifica qué cabecera sigue a la IPv6. Puede ser una cabecera de extensión o un protocolo de nivel superior (TCP, UDP).

Límite de saltos: Establece el número máximo de saltos de un paquete IP, al igual que en IPv4.

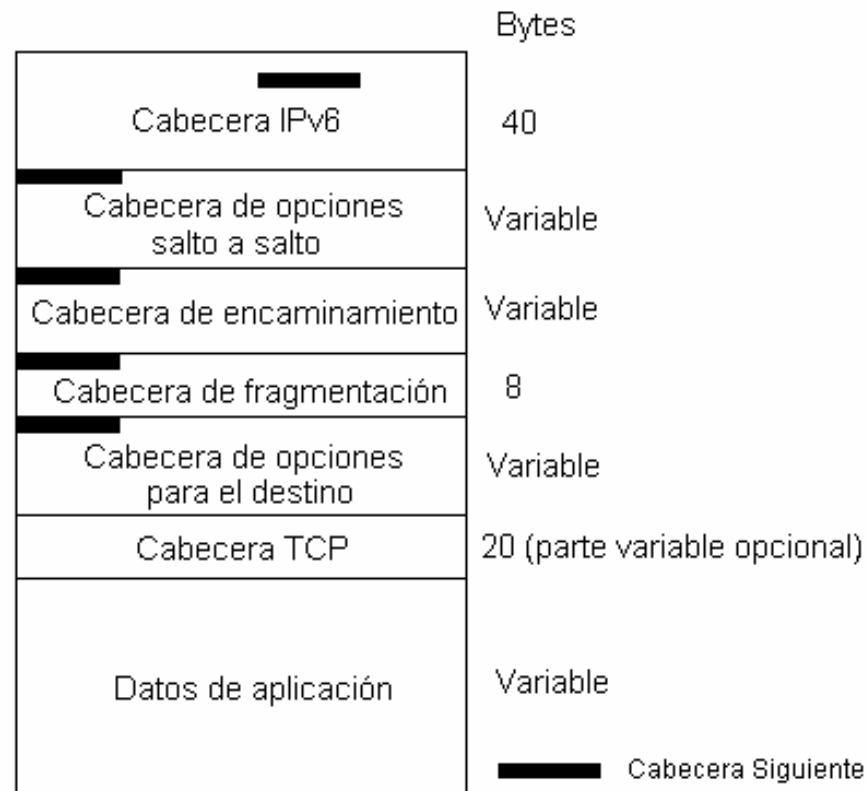
Dirección IP origen y destino: Especifica entre qué interfaces se intercambian los datos.

5.4 IPv6 (RFC 2460)

5.4.2 Cabecera IPv6

Anidamiento de cabeceras extendidas en IPv6

Cuando un dispositivo analiza un paquete IPv6 recorre todas las cabeceras existentes (IPv6 y extendidas) empleando el campo 'cabecera siguiente', hasta que encuentra la cabecera de nivel superior y envía los datos a la capa superior.



5.4 IPv6 (RFC 2460)

5.4.3 Direcciones IPv6 (RFC 2373)

IPv6 introduce un nuevo sistema de direccionamiento conceptualmente distinto al de IPv4.

Al establecer direcciones IP de 128 bits desaparece el problema de la falta de direcciones IP, y el concepto de dirección IPv6 se asigna a un interfaz de comunicación, no a un equipo.

Así, un dispositivo IPv6 está identificado por cualquiera de las direcciones IP de sus interfaces.

Una característica fundamental de las direcciones IPv6 es que son dinámicas y únicas. La dirección IPv6 asignada a un interfaz es un valor de 128 bits combinación de la MAC del interfaz y del proveedor de acceso que emplea.

Así, el proceso de encaminamiento es mucho más rápido en los routers, pues permite establecer jerarquías de direccionamiento más realistas como por operador, proximidad geográfica, etc.

Además, IPv6 permite tres tipos distintos de direcciones IP:

- a) Direcciones de unidifusión (*unicast*): Identifican a un interfaz individual.
- b) Direcciones de multidifusión (*multicast*): Identifica a un conjunto de interfaces que pertenecen a un grupo definido.
- c) Direcciones de monodifusión (*anycast*): Identifica a un conjunto de interfaces que pertenecen a un grupo, pero el paquete sólo se entrega a la interfaz más cercana (según la métrica de distancia de los protocolos de encaminamiento).

5.4 IPv6 (RFC 2460)

5.4.3 Direcciones IPv6 (RFC 2373)

La notación de una dirección IPv6 se establece en 8 grupos de 4 dígitos hexadecimales separados por el símbolo `:`.

2001:BA98:7654:3210:FEDC:BA98:7654:3210

Es posible reducir la notación de una dirección IPv6 omitiendo los grupos que contengan ceros y empleando doble `:`.

2001:BA98:0000:3210:0000:BA98:0000:3210 ⇔ 2001:BA98::3210::BA98::3210

Formato de una dirección unicast IPv6



TLA: *Top-Level Aggregation*. Identificador asociado a una zona geográfica del planeta (África, Europa, Norteamérica, etc.).

Res: Uso reservado, para ampliar el TLA o NLA.

NLA: *Next-Level Aggregation*. Identificador asociado a grandes proveedores de Internet y empresas globales a nivel nacional o regional.

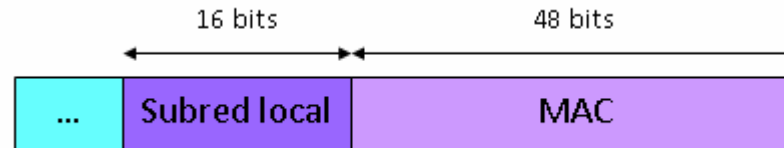
SLA: *Site-Level Aggregation*. Identificador asociado a un Proveedor de Servicios de Internet (ISP) nacional, local o regional (Ejemplo: Telefónica, Vodafone, BT, etc.).

Interface: Identificador asociado a un dispositivo, combinación de la dirección MAC y la subred donde se encuentra.

5.4 IPv6 (RFC 2460)

5.4.3 Direcciones IPv6 (RFC 2373)

Formato del campo Interface en una dirección IPv6



El valor de **subred local** es asignado por el administrador de la red donde se encuentra el dispositivo.

Con este esquema, cualquier dispositivo conectado a una red IPv6 tiene un valor dinámico (cambia según la red física en la que se conecte) pero **único y reservado para él** (debido a la MAC única).

Esta característica facilita la movilidad (conocimiento de la ubicación) y titularidad (identificación) de los dispositivos de comunicación IPv6.

5.4.4 Transición IPv4 – IPv6

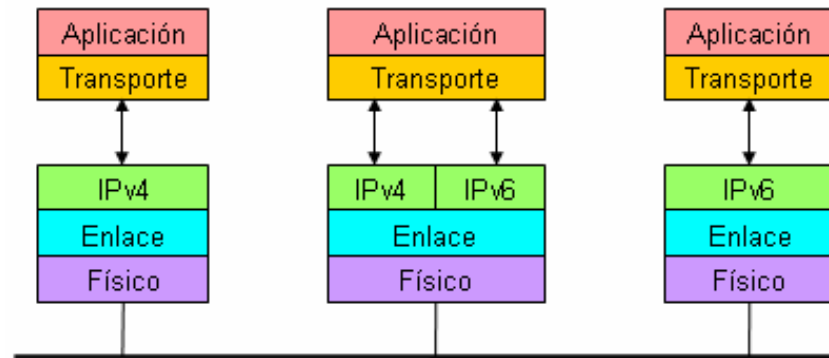
Debido a la incompatibilidad entre el protocolo IPv6 e IPv4 (formato de paquete y direccionamiento diferentes) es necesario una estrategia para el cambio de las redes IPv4 a IPv6.

Esta transición, actualmente, está compuesta por troncales de red que operan mayoritariamente en IPv6, dispositivos de usuario final que operan en IPv4 y dispositivos finales que operan en IPv6 (en fase de despliegue).

5.4 IPv6 (RFC 2460)

5.4.4 Transición IPv4 – IPv6

Un dispositivo IPv4 sólo puede tener conectividad con dispositivos con IPv4, por tanto, si es necesaria conectividad IPv4-IPv6 entre dispositivos es necesario disponer de dos pilas de protocolo IP en paralelo.



Cuando la conectividad es entre equipos con la misma versión de protocolo (IPv4 o IPv6) y deben atravesar una red intermedia con una versión de IP distinta, se recurre al procedimiento del túnel.

Este procedimiento encapsula un paquete IPv4 (IPv6) como dato dentro de un paquete IPv6 (IPv4) para su transporte en esa red intermedia.

Más información <http://www.ipv6.es>

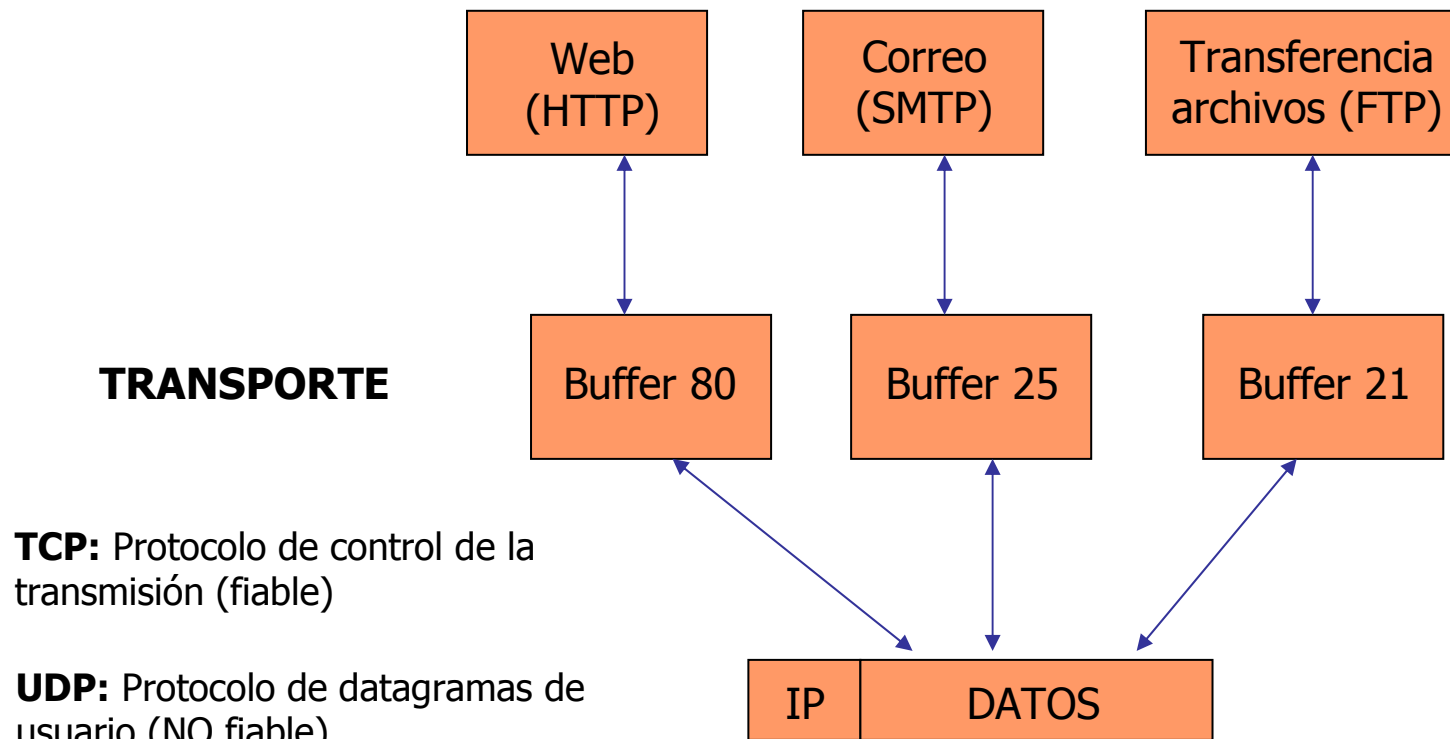
TEMA 6

NIVEL DE TRANSPORTE

6.1 Funcionalidades del nivel de transporte

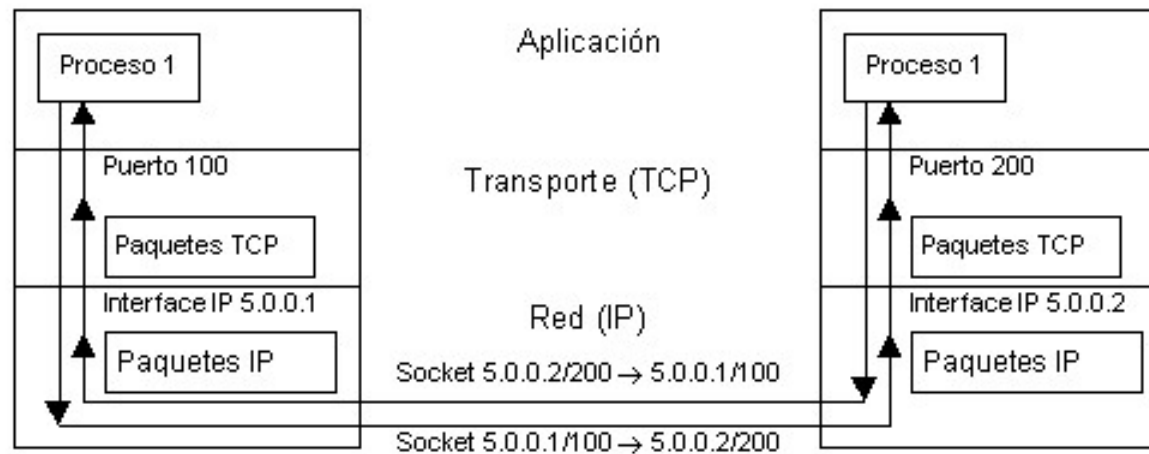
6.1.1 Interfaz capa de aplicación-capas de red

Interfaz entre la capa de aplicación y red para la gestión de comunicaciones extremo a extremo (conexiones) entre equipos de Internet.



6.1 Funcionalidades del nivel de transporte

6.1.2 Multiplexión de conexiones



Un socket está identificado por el conjunto:

IP_origen:puerto_origen -> IP_destino:puerto_destino

IP

TCP

5.0.0.1 -> 5.0.0.2	100 -> 200	DATOS
--------------------	------------	-------

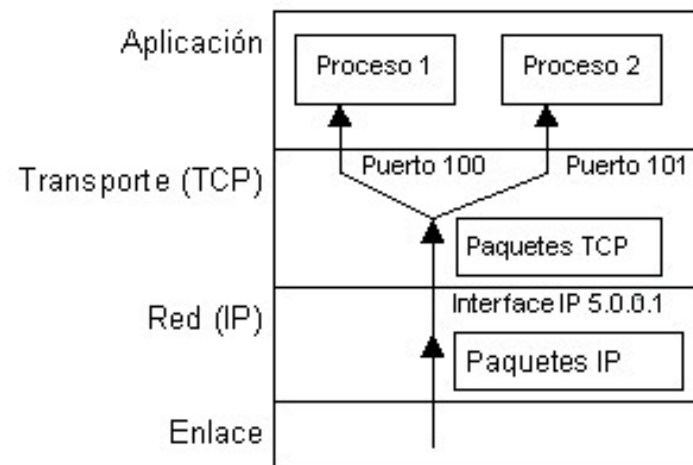
IP

TCP

5.0.0.2 -> 5.0.0.1	200 -> 100	DATOS
--------------------	------------	-------

6.1 Funcionalidades del nivel de transporte

6.1.2 Multiplexión de conexiones



La capa de transporte soporta múltiples conexiones entre un par de equipos empleando el número de puerto para separar los paquetes IP de cada conexión.

6.2 Protocolo de Datagramas de Usuario (UDP)

6.2.1 Funcionalidades

El protocolo UDP (User Datagram Protocol) está definido en RFC 768

Las características principales de este protocolo son:

Sin conexión. No emplea ninguna sincronización origen – destino.

Trabaja con paquetes o datagramas enteros, no con bytes individuales como TCP. Una aplicación que emplea el protocolo UDP intercambia información en forma de bloques de bytes, de forma que por cada bloque de bytes enviado de la capa de aplicación a la capa de transporte, se envía un paquete UDP.

No es fiable. No emplea control del flujo ni ordena los paquetes.

Su gran ventaja es que provoca **poca carga adicional en la red**, ya que es sencillo y emplea cabeceras muy simples.

Un paquete **UDP puede ser fragmentando por el protocolo IP** para ser enviado fragmentado en varios paquetes IP si resulta necesario.

Un paquete UDP admite utilizar como dirección IP de destino la **dirección de broadcast** de la red IP ya que no emplea conexiones

6.2 Protocolo de Datagramas de Usuario (UDP)

6.2.1 Funcionalidades

Formato del paquete UDP



Puerto fuente y puerto destino. Valores de 16 bits correspondientes a los puertos de nivel de transporte.

Longitud. Número total de bytes en el paquete UDP original (incluye cabecera y datos), antes de ser fragmentado en paquetes IP.

SVT. Suma de verificación, aplicada a la cabecera y datos UDP, además de a algún campo de la cabecera IP.

6.2.2 Aplicaciones

Transmisión de datos en LAN's fiables. Por ejemplo con TFTP.

Operaciones de sondeo. Protocolos DNS, SNMP y NTP, servicios echo y daytime.

6.3 Protocolo de Control de la Transmisión (TCP)

6.3.1 Funcionalidades

El protocolo TCP (Transmission Control Protocol) está definido en RFC 793

Las características principales de este protocolo son:

Trabaja con un flujo de bytes. El nivel de aplicación entrega o recibe desde el de transporte bytes individuales. TCP agrupa esos bytes en paquetes de tamaño adecuado para mejorar el rendimiento y evitar a la vez la fragmentación a nivel IP.

Transmisión orientada a conexión. Se requiere una secuencia de conexión previa al envío - recepción de datos entre cliente y servidor, y una desconexión final.

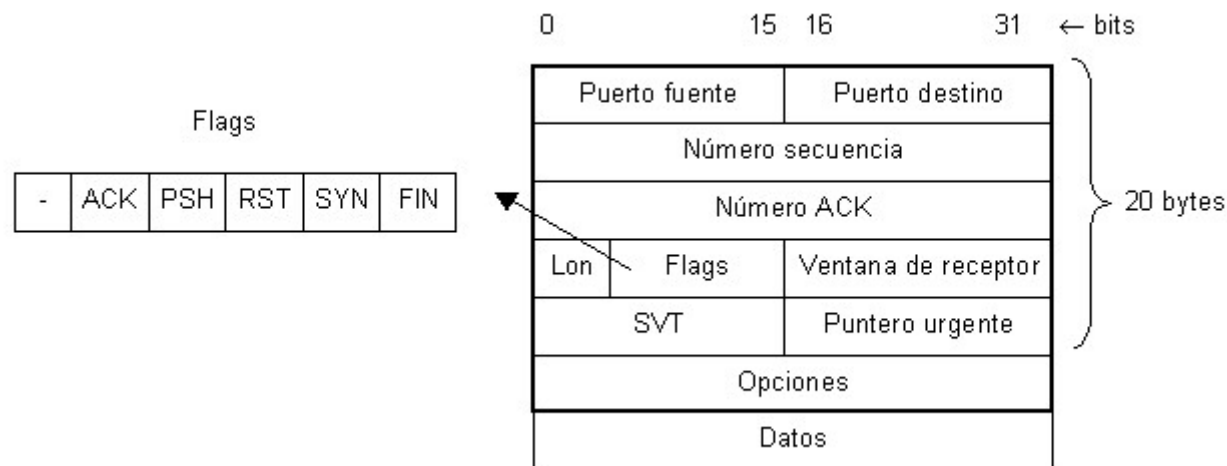
Fiable. Emplea control de flujo mediante ventana deslizante de envío continuo y asentimientos positivos o ACKs para confirmar las tramas válidas recibidas. La ventana deslizante se aplica a los bytes: se numeran y confirman bytes y no paquetes.

Flujo de bytes ordenado. Aunque IP trabaja con datagramas, un receptor TCP ordena los paquetes que recibe para entregar los bytes al nivel superior en orden.

6.3 Protocolo de Control de la Transmisión (TCP)

6.3.1 Funcionalidades

Formato del paquete TCP



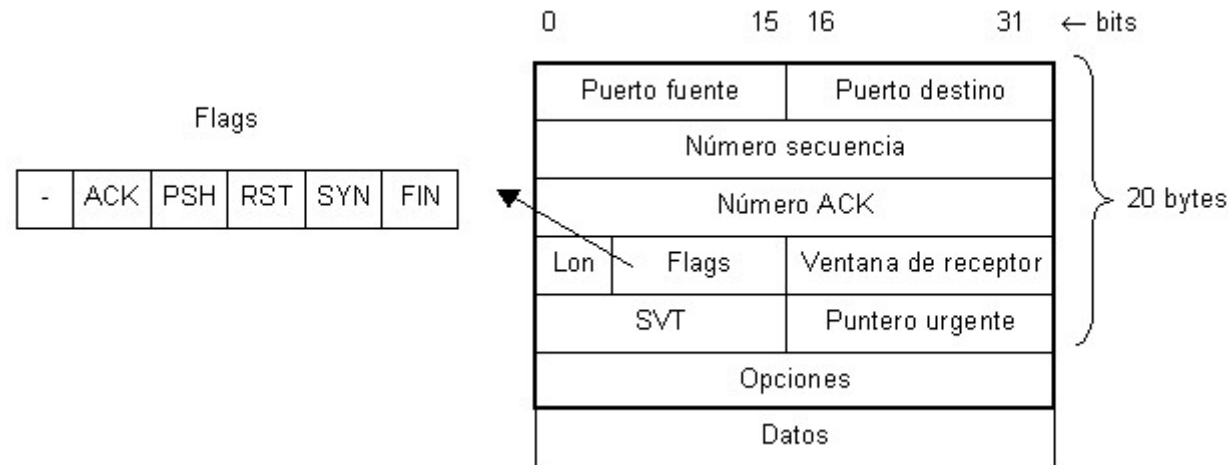
Puerto fuente y puerto destino. Valores de 16 bits correspondientes a los identificadores de los puertos de nivel de transporte.

Número de secuencia. Número de secuencia de numeración del primer byte del campo de datos del paquete.

Número de ACK. Número de la siguiente secuencia de numeración de los bytes del campo de datos que se espera recibir en un próximo paquete.

6.3 Protocolo de Control de la Transmisión (TCP)

6.3.1 Funcionalidades



Flags. Campo con bits con significado propio, del cual se usan sólo 5.

ACK. Cuando toma el valor 1 indica que el número de ACK es válido y debe interpretarse, es decir, el paquete tiene información de asentimiento.

PSH (push). Cuando toma el valor 1 indica que la capa de transporte debe pasar los datos a la capa de aplicación sin esperar a recibir más datos.

RST (reset). Indica un rechazo de la conexión. Se usa cuando ha habido un problema en la secuencia de bytes, cuando falla un intento de iniciar conexión o para rechazar paquetes no válidos.

SYN (synchronice). Se utiliza para solicitar establecimiento de una conexión.

FIN. Se utiliza para solicitar la liberación de una conexión.

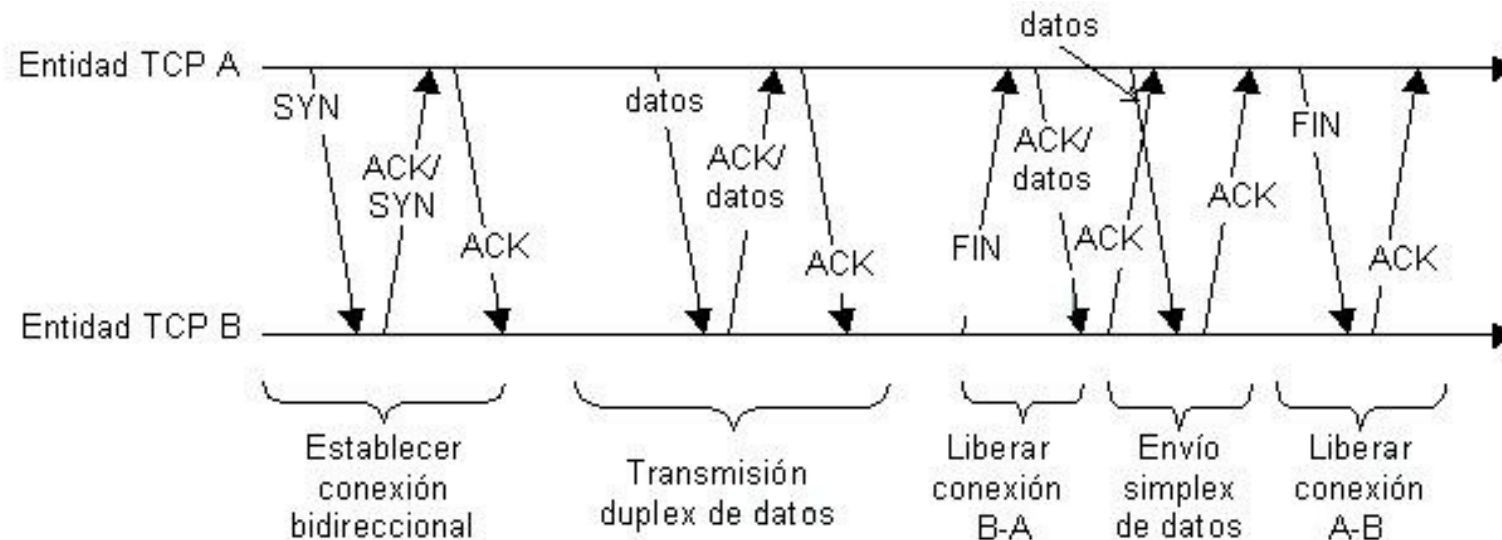
Ventana. Sirve para informar sobre el número de bytes que el emisor del paquete es capaz de recibir en su buffer de recepción. Si vale 0 indica que no puede recibir datos (aunque sí puede interpretar los paquetes con flags ACK, RST, FIN...).

6.3 Protocolo de Control de la Transmisión (TCP)

6.3.2 Gestión de la conexión

Secuencia de funcionamiento de TCP

- Establecimiento bidireccional de la conexión.
- Intercambio de datos.
- Liberación bidireccional de la conexión.

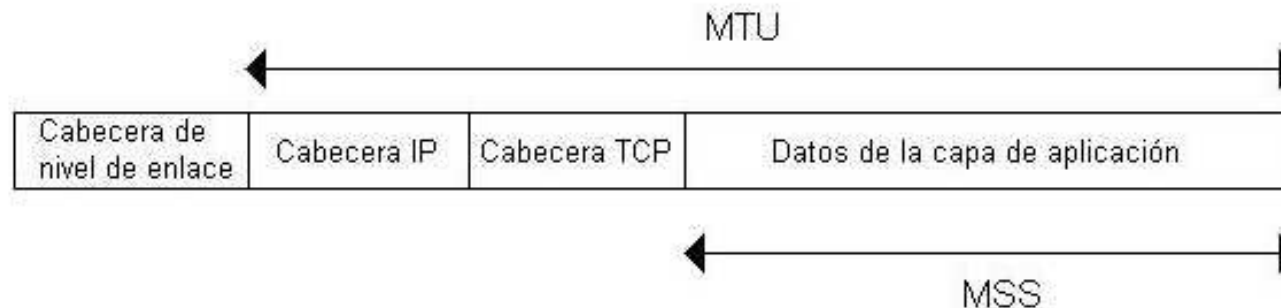


6.3 Protocolo de Control de la Transmisión (TCP)

6.3.2 Gestión de la conexión

MSS y norma RFC 1191

Se define el MSS (*Maximum Segment Size*) como la cantidad máxima de datos que puede incorporar un paquete (segmento) TCP. Este valor depende del MTU de la red donde se transmite el paquete TCP.



Para evitar la fragmentación IP, en el establecimiento de la conexión se negocia el valor del MSS. Este valor se intercambia en el campo de opciones de los paquetes SYN de establecimiento de conexión. Como MSS se establece el menor de los intercambiados por los extremos.

Si en una red intermedia entre origen y destino existe un MSS menor que el negociado, la norma RFC 1191 permite reducir el MSS. Para ello se activa el bit don't fragment en la cabecera IP de los paquetes TCP y se emplean los mensajes ICMP *Destination Unreachable* para configurar MSS menores en una conexión determinada.

6.3 Protocolo de Control de la Transmisión (TCP)

6.3.3 Control del flujo de datos

Si la red no proporciona ningún mecanismo para controlar la congestión, éste ha de llevarse a cabo con los protocolos de la arquitectura de red.

El protocolo de la capa de transporte TCP es un protocolo que presenta las características de:

- a) Protocolo fiable con confirmación de paquetes.
- b) Transmisión orientada a conexión.
- c) Control del flujo de bytes.

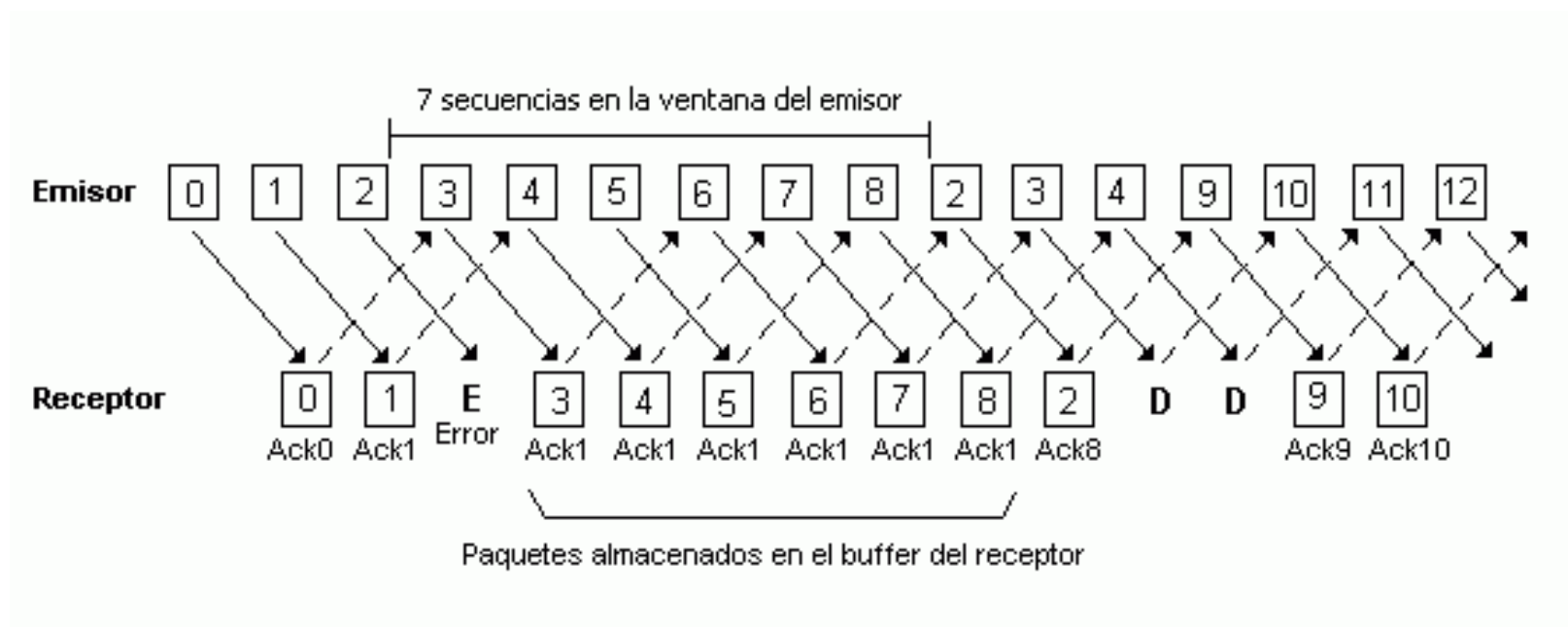
El control del flujo de bytes permite un control de la congestión, adaptándose TCP al retardo en el envío de la información en la red.

TCP emplea un algoritmo de ventana deslizante para el control del flujo.

6.3 Protocolo de Control de la Transmisión (TCP)

6.3.3 Control del flujo de datos

Funcionamiento de un protocolo de ventana deslizante. Caso $W_e=7$ y $W_r=7$



6.3 Protocolo de Control de la Transmisión (TCP)

6.3.3 Control del flujo de datos

TCP emplea números de secuencia de bytes y tamaños de ventana en bytes

El control del flujo se realiza variando el tamaño de la ventana del receptor (campo window en la cabecera TCP):

- a) Si la ventana del receptor aumenta, el emisor puede enviar más información sin esperar a recibir ACK (aumenta ventana del emisor).
- b) Si la ventana del receptor disminuye, el emisor envía menos información sin esperar a recibir ACK (disminuye ventana del emisor). Caso límite: window=0.

Pérdida de segmentos. Reenvío de la información.

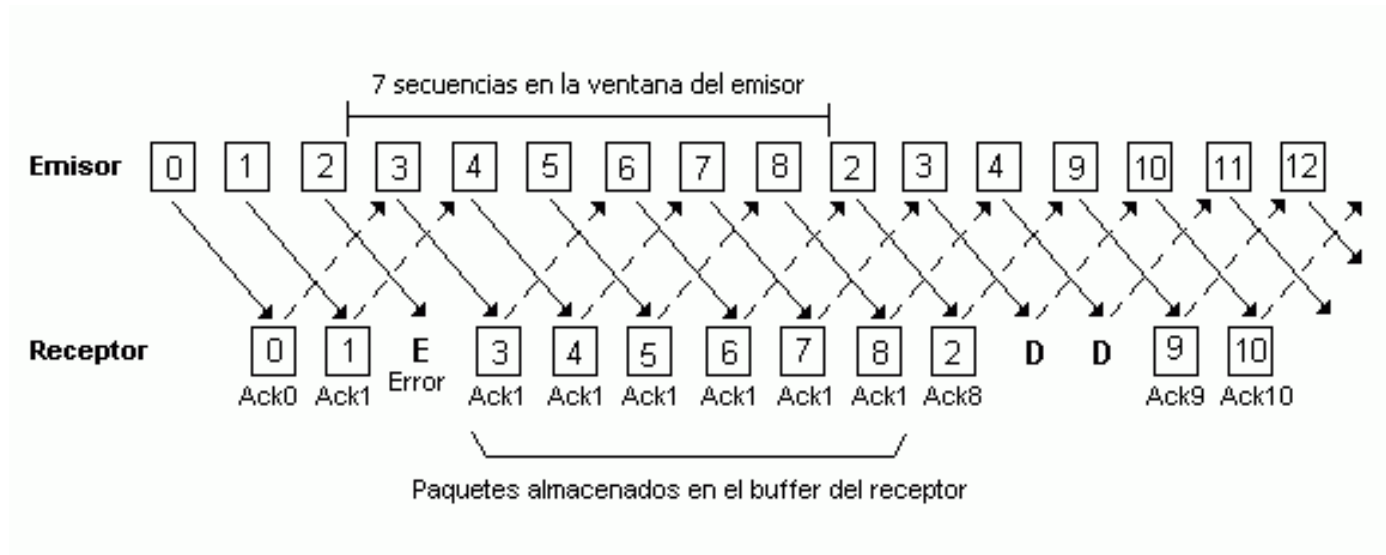
Segmento: paquete TCP con datos.

Cada vez que TCP recibe un ACK, la ventana del emisor permite enviar un nuevo fragmento.

Si un segmento no llega al receptor o llega con errores, el receptor no enviará ACK. Los siguientes segmentos que envíe el emisor (hasta su tamaño de ventana máximo) se almacenarán en el buffer del receptor pero éste enviará ACK de la secuencia previa al paquete erróneo.

6.3 Protocolo de Control de la Transmisión (TCP)

6.3.3 Control del flujo de datos



El emisor tiene especificado un tiempo de espera de ACK para cada segmento. Si el ACK no llega se procede con el reenvío del primer segmento sin ACK en la ventana del emisor.

Para evitar reenvíos inútiles se espera al ACK del reenvío, así se comprobará que hay que continuar con otro segmento distinto del siguiente en espera.

6.3 Protocolo de Control de la Transmisión (TCP)

6.3.3 Control del flujo de datos

Cálculo del tiempo de espera de ACK. Algoritmo de Karn.

El tiempo de espera de un ACK (Timeout) debe ser calculado de forma que:

- Sea lo suficientemente grande para evitar que los retardos en la red no provoquen reenvíos innecesarios por retardos en el envío del ACK.
- Sea lo suficientemente pequeño para que no haya periodos de inactividad en el envío de datos en la red.

El valor del timeout se calcula de forma dinámica durante el funcionamiento de TCP a partir del RTT (Round Trip Time) o tiempo de ida y vuelta. Este RTT se calcula como el tiempo transcurrido desde el envío de un segmento y la llegada de su ACK.

El timeout se calcula como $\text{Timeout} = \beta * \text{RTT}$. El RTT se actualiza en cada envío de segmento, por lo que el timeout se adapta a los retardos en la red. El factor β se establece entre 1 y 2, de forma que se consiga un reenvío adecuado. (La especificación original recomienda el valor de 2).

Este mecanismo presenta un problema: ¿que ocurre si un ACK llega demasiado tarde ?

Al reenviar el paquete y llegar el ACK del primero enviado, el RTT se actualiza al nuevo valor. Este será demasiado pequeño, y se producirán reenvíos inútiles, afectando a la fluidez de la comunicación.

6.3 Protocolo de Control de la Transmisión (TCP)

6.3.3 Control del flujo de datos

La situación anterior se resuelve con el algoritmo de Karn.

Cuando se produce un reenvío, el valor del timeout se incrementa en función del último timeout calculado: $\text{nuevo_Timeout} = \gamma * \text{Timeout}$. γ toma el valor de 2 para evitar inestabilidades.

El timeout se volverá a calcular en función del RTT cuando se envíe un nuevo segmento que no haya sido reenviado.

Control de la congestión en TCP. RFC 2581

La congestión en una red es una situación de retardo elevado en el envío de información, debido a la sobrecarga de encaminamiento en los routers de una red.

Cuando en una red TCP/IP se produce una situación de congestión, TCP reacciona reenviando datos debido a la expiración de los timeouts. El reenvío genera más tráfico y por tanto más congestión, alcanzando la red un estado de bloqueo denominado colapso de congestión.

Para reducir la congestión, TCP debe reducir la tasa de envío de datos, es decir reducir su ventana de emisor.

TCP dispone de una serie de mecanismos para reducir su tasa de envío de datos cuando los retardos son elevados, descritos en el documento RFC 2581.

6.3 Protocolo de Control de la Transmisión (TCP)

6.3.3 Control del flujo de datos

Prevención de la congestión por decremento multiplicativo

Esta técnica se fundamenta en la definición en el emisor de una nueva ventana denominada ventana de congestión, un valor en bytes al igual que la ventana del emisor.

En todo momento, la ventana del emisor se calcula como el valor mínimo de dos valores: la ventana de congestión y la ventana que informa el receptor.

TCP supone que la expiración del timeout de un segmento es debido a la congestión, y actualiza los siguientes valores: Con cada expiración de timeout para un segmento, reduce el tamaño de la ventana de congestión a la mitad, y multiplica por dos el timeout de los paquetes en la ventana del emisor. Esto provoca que conforme expiran temporizadores, el emisor envía cada vez menos datos.

Recuperación de una situación de congestión. Algoritmo de inicio lento.

Una vez que se evita la congestión y comienzan a llegar ACK's, el timeout vuelve a decrementarse y la ventana de congestión debería aumentar.

Sin embargo, si la recuperación es a la misma velocidad que la reducción del envío de datos, se puede producir un efecto "ola" de congestión periódica, la red queda oscilando entre congestión – no congestión.

Para evitar esto, la recuperación se realiza más lentamente. Para ello, el valor de la ventana de congestión se incrementa en un tamaño de MSS bytes, cada vez que el emisor recibe un ACK.

6.3 Protocolo de Control de la Transmisión (TCP)

6.3.3 Control del flujo de datos

El problema de los paquetes pequeños. Algoritmo de Nagle. RFC 896.

Si una aplicación envía a la capa TCP información en bloques de pocos bytes (Telnet envía un carácter (byte) al equipo remoto y espera un eco del carácter para enviar el siguiente), puede producirse una situación de desaprovechamiento del medio físico.

El emisor enviará bloques de un byte al receptor y éste hará ACK's de un byte. De esta forma el envío de información se ralentiza, sobre todo si el RTT es alto en la red.

Para evitar que el intercambio de datos sea byte a byte, el algoritmo de Nagle hace que TCP agrupe los bytes enviados por la aplicación en un segmento TCP. El primer byte será enviado y TCP almacena los bytes que lleguen del nivel superior hasta la llegada del ACK. A continuación enviará todos los bytes acumulados en otro segmento, y acumulará los siguientes hasta la llegada del ACK. Si se alcanza el tamaño del MSS en el buffer, TCP envía el segmento sin esperar al ACK.