



# Tema 3. Capa de enlace a datos

Introducción a las Redes de Computadores

Isidro Calvo

Dpto. Ingeniería de Sistemas y Automática

Octubre 2012



# Índice

- Funciones de la capa de enlace de datos
  - Servicios proporcionados a la capa de red
  - Enramado
  - Control de errores
  - Control de flujo
- Detección y control de errores
  - Códigos de detección de errores
  - Códigos de corrección de errores
- Verificación de protocolos
- Ejemplos de protocolos de enlace de datos
- Subcapa de control de acceso al medio
- Protocolos de acceso múltiple
  - ALOHA
  - CSMA
  - Protocolos libres de colisiones
  - Protocolos de contención limitada
  - Protocolos de acceso múltiple por división de longitud de onda
  - Protocolos para LANs inalámbricas
- Redes de ejemplo: Ethernet y Wifi



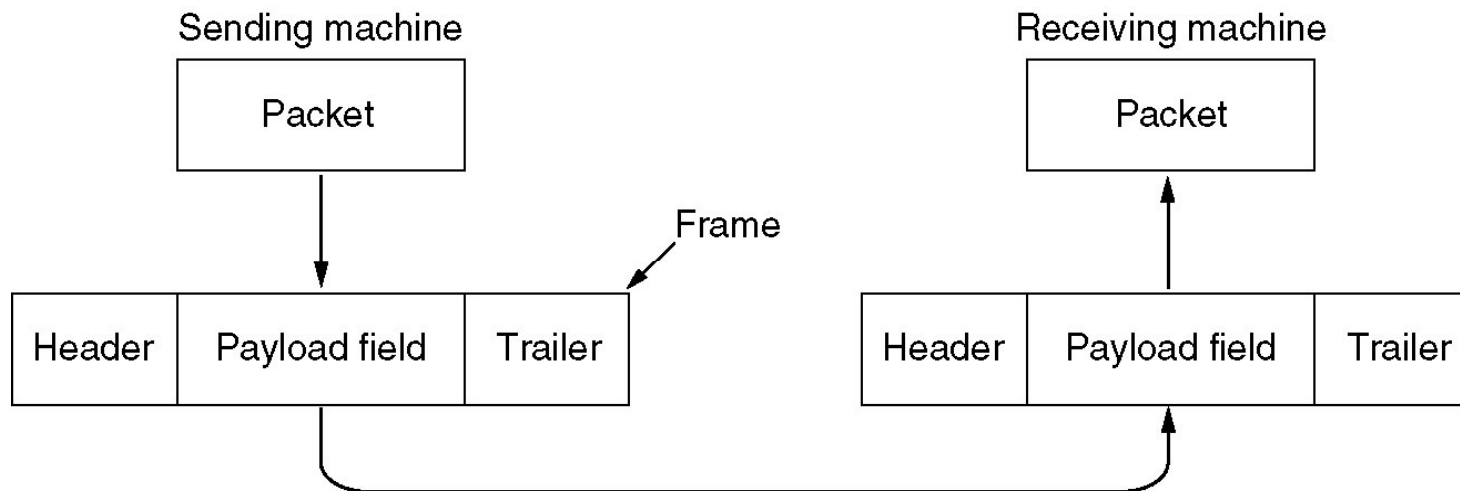
# Funciones de la capa de enlace a datos

## Objetivo y consideraciones

- Sean varias máquinas conectadas a través de un canal de comunicaciones que actúa como medio físico:
  - P.e. Cable coaxial, línea telefónica, canal inalámbrico, etc.
- **Objetivo:**
  - Lograr una comunicación confiable y eficiente entre dos máquinas
- Consideraciones a tener en cuenta:
  - Los circuitos de comunicación producen errores ocasionales
  - Tasa de envío de datos finita
  - Retardo de propagación diferente de cero (entre el momento en que se envía un bit y el momento en que se recibe)
- Los protocolos usados para comunicaciones deben considerar estos factores

# Cuestiones de diseño de la capa de enlace

- Proporcionar una interfaz de servicio bien definida con la capa de red
- Enramado
- Manejar los errores de transmisión
- Regular el flujo de datos para que los receptores lentos no sean saturados por los emisores rápidos

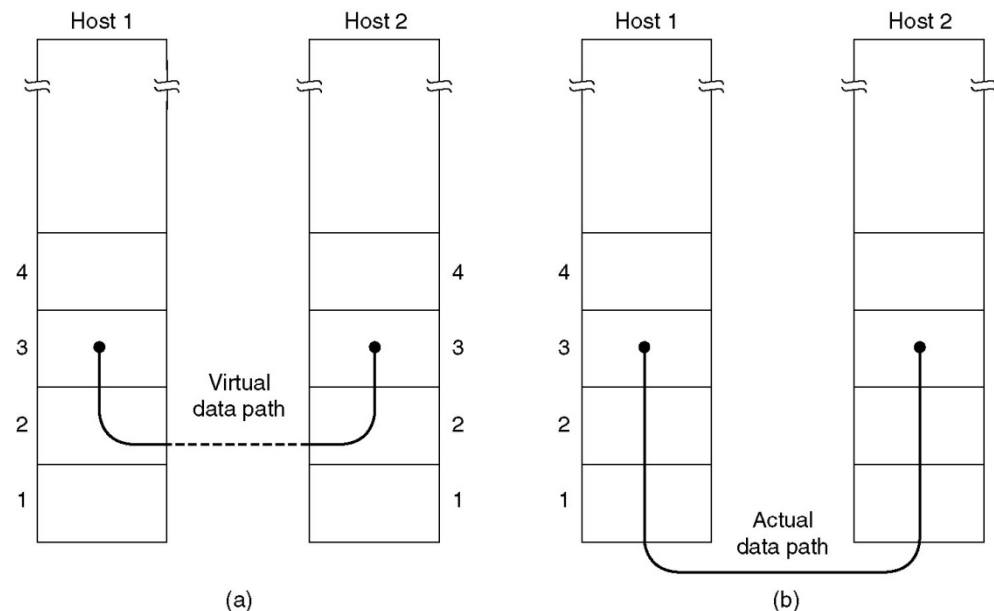


**NOTA: Algunos de los protocolos analizados para la capa de enlace de datos, como el control de errores y de flujo, también se implementan en otras capas, p.e. la capa de transporte**

# Cuestiones de diseño de la capa de enlace

## Servicios proporcionados a la capa de red

- En la capa de red hay una entidad (proceso) que entrega bits a la capa de enlace de datos para enviarlos a destino
- La capa de enlace de datos es responsable de transmitir los bits a la máquina de destino
- La trayectoria real sigue el camino de la derecha (b) pero resulta más cómodo asumir que los dos procesos se comunican usando un protocolo de enlace de datos (a)





# Cuestiones de diseño de la capa de enlace

## Tipos de servicios ofrecidos a la capa 3

- La capa de enlace a datos puede diseñarse para ofrecer diferentes tipos de servicios a la capa de red:
  - ☐ Servicios NO orientados a conexión SIN confirmación de recepción
  - ☐ Servicios NO orientados a conexión CON confirmación de recepción
  - ☐ Servicios ORIENTADOS a conexión CON confirmación de recepción
- Los tipos de servicios ofrecidos a la capa de red pueden variar de sistema a sistema
- Los **paquetes** (*capa de red*) pueden no tener un tamaño máximo, mientras que las **tramas** (*capa de enlace*) normalmente tienen un tamaño máximo impuesto por el hardware



# Cuestiones de diseño de la capa de enlace

## Tipos de servicios ofrecidos a la capa 3

- **Servicios NO ORIENTADOS a conexión SIN confirmación de recepción**
  - No se mantienen conexiones lógicas
  - El emisor envía tramas independientes sin pedir confirmación en recepción
  - Si se pierde una trama no se realiza ningún intento por detectar la pérdida ni recuperar el error (La recuperación se realiza en las capas superiores)
  - Son servicios apropiados cuando:
    - La tasa de errores de la red es muy baja. Canales muy fiables (p.e. fibra óptica)
    - Se transmite tráfico de ***tiempo real*** (p.e. multimedia)
  - La mayoría de las LANs usan estos servicios en la capa de enlace



# Cuestiones de diseño de la capa de enlace

## Tipos de servicios ofrecidos a la capa 3

### ■ Servicios NO ORIENTADOS a conexión CON confirmación de recepción

- ☐ No se mantienen conexiones lógicas
- ☐ Se confirma de forma individual la recepción de cada trama enviada
- ☐ Si no se recibe confirmación en un tiempo especificado se reenvía la trama
- ☐ Normalmente se utiliza un temporizador en origen
- ☐ Útiles en canales inestables (p.e. en tecnologías inalámbricas)
- ☐ Utiliza protocolos que introducen mayor sobrecarga
- ☐ Evaluar la relación *Sobrecarga del protocolo vs. Robustez de la tecnología*
  - Ej: Red inalámbrica vs. Fibra óptica





# Cuestiones de diseño de la capa de enlace

## Tipos de servicios ofrecidos a la capa 3

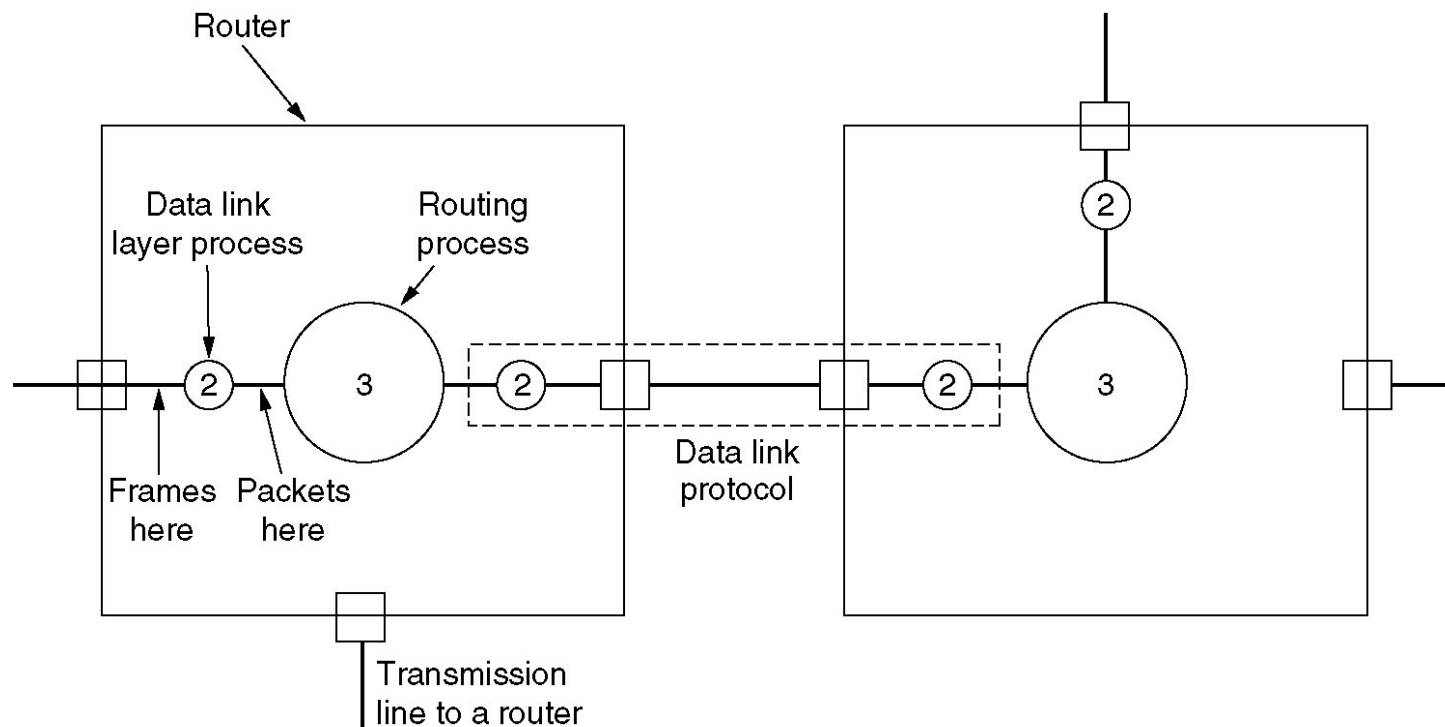
- **Servicios ORIENTADOS a conexión CON confirmación de recepción**
  - Las máquinas origen y destino establecen una conexión lógica antes de transferir datos
  - La conexión se mantiene durante el transcurso de la comunicación
  - Cada trama está numerada
  - La capa de enlace garantiza que todas las tramas llegan en orden a destino
  - Las tramas pueden recibirse más de una vez debido a solicitudes de retransmisión por parte del receptor
  - Proporciona a los procesos de la capa de red el equivalente a un flujo de bits confiable
  - Se definen tres fases:
    1. Se establece la conexión. En ambos lados se inicializan las variables y contadores necesarios
    2. Se transmiten una o más tramas
    3. La conexión se cierra. Se liberan las variables, búferes y otros recursos

# Mecanismos de detección y corrección de errores

## Interfaz capa de Enlace

- Se puede usar directamente la capa de enlace desde los programas
- Típicamente, se usará una librería con un conjunto de funciones o clases que proporcionará la funcionalidad a los programas
- Ej:

InterfazCapaEnlace
<i>Attributes</i>
<i>Operations</i>
public void wait_for_event( eventType event )
public void from_network_layer( packet p )
public void to_network_layer( packet p )
public void from_physical_layer( frame r )
public void to_physical_layer( frame s )
public void start_timer( seq_nr k )
public void stop_timer( seq_nr k )
public InterfazCapaEnlace( )

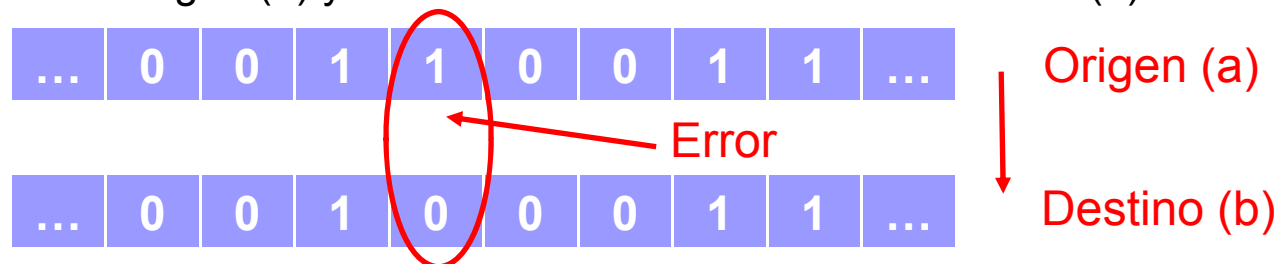


# Cuestiones de diseño de la capa de enlace

## Entramado

- La capa física permite enviar un flujo de bits puros, pero no asegura que se entregue libre de errores

□ Ej: Trama en origen (a) y trama recibida en destino con un error (b)



- La cantidad de bits transmitidos puede ser menor, igual o mayor que la cantidad de bits recibidos
- Es responsabilidad de la capa de enlace detectar y corregir los errores
- División del flujo de datos en tramas
- Se utilizan mecanismos que permiten calcular **sumas de verificación** por trama
  - Si las sumas de verificación calculadas en origen y destino son diferentes, el receptor sabe que se ha producido al menos un error y se toman medidas.



# Cuestiones de diseño de la capa de enlace

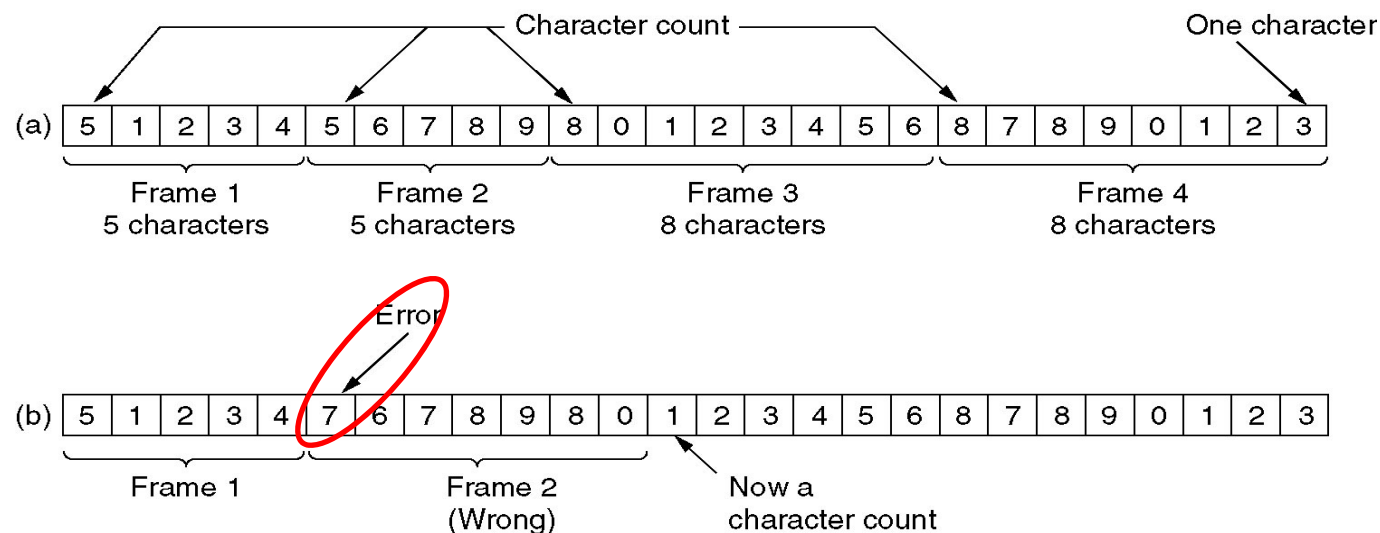
## Mecanismos de entramado

- Existen diferentes mecanismos para dividir el flujo de bits en tramas
  - Introducir intervalos de tiempo entre las tramas
    - Ej: Espacios entre palabras en texto común
    - Requiere una temporización muy exacta
  - Conteo de caracteres
  - Banderas con relleno de caracteres para que todas las tramas empiecen y acaben de igual forma
  - Banderas de inicio y fin, con relleno de bits
  - Violaciones de codificación de la capa física

# Mecanismos de entramado

## Conteo de caracteres

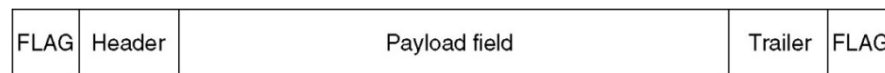
- Conteo de caracteres:
  - A partir del número de caracteres se determina el origen y fin de la trama
  - Si la cuenta se altera por un error de transmisión se produce un error de sincronía del que es difícil recuperarse



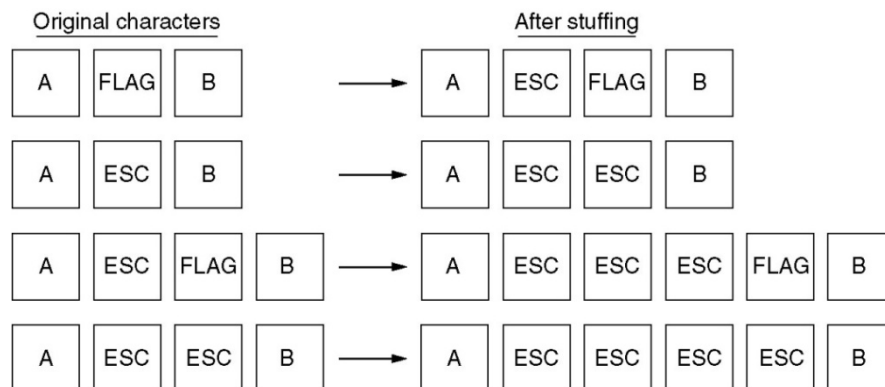
# Mecanismos de entramado

## Banderas con relleno de caracteres

- Las banderas (FLAGS) se usan para que todas las tramas empiecen y acaben de igual forma
  - Cada trama empieza y acaba con una secuencia de bits especiales (P.e. un carácter especial)
  - Si el receptor pierde la sincronía sólo tiene que buscar la secuencia de inicio de nueva trama
  - Aparecen problemas al enviar datos binarios (p.e. programas objeto o números de punto flotante) ya que pueden reproducir los bits del FLAG
  - **Relleno de caracteres:** Se añade un carácter especial (p.e. ESC) justo antes de cada bandera “accidental”



(a)



(b)



## Mecanismos de entramado

# Banderas con relleno de caracteres

- Es el método usado en el protocolo PPP (*Point to Point Protocol*) que es el protocolo que la mayoría de ordenadores usa para comunicarse con los proveedores de servicios de Internet
- **Inconvenientes:**
  - Está fuertemente orientado a caracteres de 8 bits (p.e. UNICODE usa caracteres de 16 bits)
- **Conclusión:**
  - Fue necesario desarrollar técnicas que permitan enviar caracteres de tamaño arbitrario



# Mecanismos de entramado

## Banderas con relleno de bits

- Permite que las tramas de datos contengan un número arbitrario de bits
- Admite códigos de caracteres con un número arbitrario de bits por carácter
- Funcionamiento:
  - Cada trama empieza y termina con un patrón especial de bits (en realidad es una bandera): 01111110
  - Cada vez que la capa de enlace de datos del emisor encuentra 5 bits a uno consecutivos en los datos, automáticamente inserta un bit 0 en el flujo de bits saliente
  - Este relleno es equivalente a la inserción del carácter ESC en el método anterior
  - Cuando el receptor detecta 5 bits a uno consecutivos en los datos, automáticamente extrae (borra) el bit 0 de relleno
  - Así, la secuencia de 6 bits a uno SIEMPRE indica la bandera de PRINCIPIO o FIN de trama

(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0

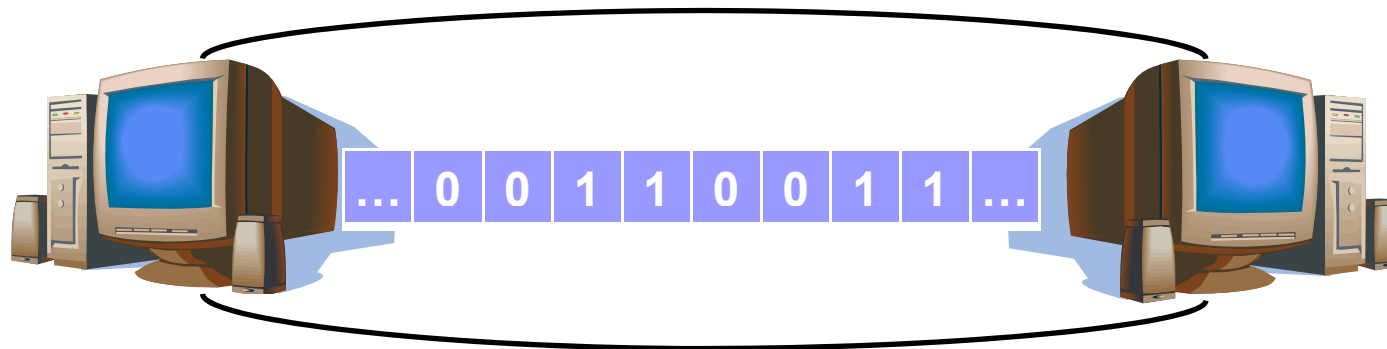
Stuffed bits

(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

# Mecanismos de entramado

## Violación de codificación de capa física

- Se aplica a redes en las que la codificación en el medio físico contiene cierta redundancia
- P.e. algunas LAN codifican un bit de datos usando dos bits físicos:
  - Un bit 1 es un par alto-bajo y un 0 es un par-bajo alto
  - Las combinaciones alto-alto y bajo-bajo no se usan para datos, pero algunos protocolos las usan para delimitar tramas





# Cuestiones de diseño de la capa de enlace

## Ejemplo: Trama Ethernet

Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype or length	Payload	Frame check sequence (32-bit CRC)	Interframe gap						
7 octets of 10101010	1 octet of 10101011	6 octets	6 octets	(4 octets)	2 octets	46–1500 octets	4 octets	12 octets						
		64–1522 octets												
72–1530 octets														
84–1542 octets														

**(Untitled) - Ethereal**

File Edit View Go Capture Analyze Statistics Help

Filter:  Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
59	6.389297	158.227.233.191	158.227.233.255	BROWSE	Host Announcement A005009, workstation, Server, NI workstation
60	6.621151	158.227.232.9	255.255.255.255	UDP	Source port: 17500 Destination port: 17500
61	6.621715	158.227.232.9	158.227.233.255	UDP	Source port: 17500 Destination port: 17500
62	7.118140	158.227.233.21	10.30.13.6	DNS	Standard query A s7.addthis.com
63	7.142484	10.30.13.6	158.227.233.21	DNS	Standard query response CNAME wilddcard.addthis.com.edgekey.net CNAME e2943.c.akamaiedge.r
64	7.143104	158.227.233.21	2.20.236.20	TCP	1961 > http [SYN] Seq=0 Ack=0 win=65535 Len=0 MSS=1460
65	7.180464	2.20.236.20	158.227.233.21	TCP	http > 1961 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1380
66	7.180503	158.227.233.21	2.20.236.20	TCP	1961 > http [ACK] Seq=1 Ack=1 win=65535 Len=0

☒ Frame 64 (62 bytes on wire, 62 bytes captured)  
 Arrival Time: Oct 18, 2011 15:57:30.852880000  
 [Time delta from previous packet: 0.000620000 seconds]  
 [Time since reference or first frame: 7.143104000 seconds]  
 Frame Number: 64  
 Packet Length: 62 bytes  
 Capture Length: 62 bytes  
 [Protocols in frame: eth:ip:tcp]

☒ Ethernet II, Src: 00:1a:4b:7b:7a:fe (00:1a:4b:7b:7a:fe), Dst: 88:43:e1:ce:35:40 (88:43:e1:ce:35:40)  
 Destination: 88:43:e1:ce:35:40 (88:43:e1:ce:35:40)  
 Source: 00:1a:4b:7b:7a:fe (00:1a:4b:7b:7a:fe)  
 Type: IP (0x0800)

☒ Internet Protocol, Src: 158.227.233.21 (158.227.233.21), Dst: 2.20.236.20 (2.20.236.20)  
 Version: 4  
 Header length: 20 bytes  
☒ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)  
 Total Length: 48  
 Identification: 0x4d31 (19761)  
☒ Flags: 0x04 (Don't Fragment)  
 Fragment offset: 0  
 Time to live: 128  
 Protocol: TCP (0x06)  
☒ Header checksum: 0x3775 [correct]  
 Source: 158.227.233.21 (158.227.233.21)  
 Destination: 2.20.236.20 (2.20.236.20)

☒ Transmission Control Protocol, Src Port: 1961 (1961), Dst Port: http (80), Seq: 0, Ack: 0, Len: 0  
 Source port: 1961 (1961)  
 Destination port: http (80)  
 Sequence number: 0 (relative sequence number)  
 Header length: 28 bytes  
☒ Flags: 0x0002 (SYN)  
 Window size: 65535  
 Checksum: 0x9155 [correct]  
☒ Options: (8 bytes)

```

0000  88 43 e1 ce 35 40 00 1a 4b 7b 7a fe 08 00 45 00  .C..5@.. K{z...E.
0010  00 30 4d 31 40 00 80 06 37 75 9e e3 e9 15 02 14  .0M1@... 7u.....
0020  ec 14 07 a9 00 50 bb 1e b8 90 00 00 00 00 70 02  ....P.. ....p.
0030  ff ff 91 55 00 00 02 04 05 b4 01 01 04 02      ...U....
  
```

Ethernet (eth), 14 bytes

P: 775 D: 775 M: 0 Drops: 0



# Cuestiones de diseño de la capa de enlace

## Control de errores

- Se cuenta que Carlos I revisaba cada día las resoluciones de la Justicia y daba el visto bueno a las mismas.
- Para ello utilizaba una sola frase: **“Perdón, imposible ejecutar condena”** – ello, por la mañana-; por la tarde las revisaba nuevamente y, si lo creía conveniente, cambiaba de sitio la coma: **“Perdón imposible, ejecutar condena”**.
- ¡Imaginad el efecto de un error de comunicaciones en una coma en la transmisión del mensaje como éste!



# Cuestiones de diseño de la capa de enlace

## Control de errores

- Para asegurar que todas las tramas llegan a destino y se entregan en orden apropiado a la capa de red normalmente se proporciona realimentación
  - P.e. enviando mensajes de confirmación desde destino al origen
  - El protocolo define el formato de estas tramas que pueden ser positivas (el mensaje fue enviado con éxito) o negativas (algo falló)
- También se puede perder una trama completa
  - Frecuentemente se utilizan temporizadores (***time outs***) en el emisor que disparan alguna acción si no se recibe el correspondiente mensaje desde el receptor
  - Se puede reenviar la misma trama un número de veces antes de notificar el error a las capas superiores
  - Estos parámetros: ***tiempo del time out*** y ***número de reintentos*** son parámetros típicos de configuración del protocolo de comunicaciones
- Una misma trama puede ser enviada más de una vez
  - Se requiere que las tramas incorporen un número de secuencia



# Cuestiones de diseño de la capa de enlace

## Control de flujo

- **¿Qué hacer con un emisor que quiere transmitir tramas sistemáticamente a mayor velocidad que la que puede procesarlas el receptor?**
  - P.e. si el emisor se ejecuta en una computadora más potente (o con menor carga) que el receptor
- **Soluciones posibles:**
  - ***Control de flujo basado en realimentación:*** El receptor devuelve información al emisor autorizando a enviar más datos o indicando su estado
  - ***Control de flujo basado en tasa:*** El protocolo tiene un mecanismo integrado que limita la tasa a la que el emisor puede transmitir los datos. Se negocia la tasa de transmisión.



# Mecanismos de detección y corrección de errores

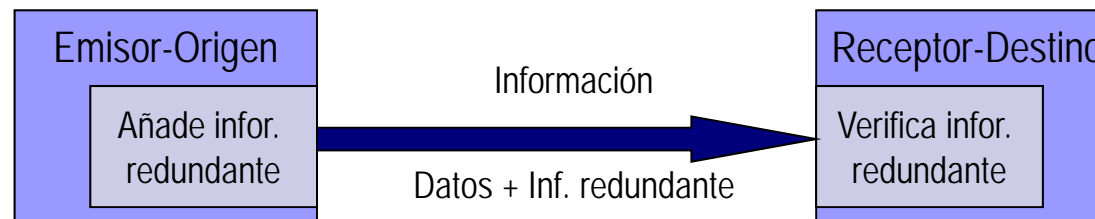
- Los datos pueden transmitirse a través de diferentes medios de transmisión con diferentes tasas de error
  - Ejemplos:
    - Sistema telefónico (Parte digital – ↑ Fiable vs. Parte analógica – ↓ Fiable)
    - Comunicación inalámbrica – ↓ ↓ ↓ Fiable
- Consideraciones:
  - Los errores tienden a aparecer en ráfagas
  - Los datos siempre se envían en bloques de bits
  - Ejemplo:
    - Tamaño de bloque de 1000 bits y tasa de errores de 0.001 por bit ⇒ Todos los bloques tendrían un error (imposibilitando la comunicación efectiva)
    - Como los errores aparecen en ráfagas (p.e. de 100), en promedio sólo un bloque de cada 100 se vería afectado
- Introducción de **información redundante** para el control de errores
- Principales mecanismos de control de errores
  - Códigos de **detección** de errores (canales ↑ fiables)
  - Códigos de **corrección** de errores (canales ↓ fiables)



# Mecanismos de detección y corrección de errores

## ¿Qué es un error?

- Una trama consiste en  $m$  bits de datos de mensaje y  $r$  bits redundantes o de verificación
- La trama a enviar por el canal de comunicación consta de  $n$  bits. Donde  $n = m + r$



- La unidad básica que contiene bits de datos y de verificación recibe el nombre de **palabra codificada**
- **De las  $2^n$  combinaciones de bits a enviar por el canal sólo  $2^m$  son válidas!!!**
- Si el receptor ve una combinación no válida sabe que se ha producido un error en la transmisión
- **Los errores no distinguen entre los bits de datos y los redundantes**

# Mecanismos de detección y corrección de errores

## Distancia de Hamming

- Sean dos palabras codificadas cualesquiera, se puede determinar la cantidad de bits diferentes sin más que aplicar el operador XOR

A:	10001001
B:	10110001
A XOR B:	00111000

- La cantidad de posiciones de bits en la que difieren dos palabras codificadas se llama **distancia de Hamming** (Ej:  $d=3$ )
- Las propiedades de detección y corrección de errores de un código dependen de su distancia de Hamming.
- Se puede demostrar que:
  - Para **detectar**  $d$  errores se necesita un código con distancia  $d+1$
  - Para **corregir**  $d$  errores se necesita un código con distancia  $2d+1$



# Mecanismos de detección y corrección de errores

## Códigos de *detección* de errores

- Permiten detectar en el receptor si la información recibida es correcta, pero no permiten identificar la posición del bit o bits erróneos cuando los hay
- Normalmente requieren introducir menos información redundante que los códigos de corrección de errores
- El procedimiento más común en caso de detección de un error es que el receptor solicite la retransmisión de la trama errónea
- Otra alternativa es descartar la trama
- Las propiedades de detección y corrección de errores de un código dependen de su distancia de Hamming
  - Se necesita un código con una distancia  $d+1$  para detectar  $d$  errores
- Ejemplos:
  - Bit de paridad (Permite detectar un error)
  - Checksum
  - Códigos de redundancia cíclica (CRC)

# Mecanismos de detección y corrección de errores


## Códigos de *detección* de errores

### ■ Bit de paridad

- Paridad **par**: Se añade un bit con el objetivo de que el número total de 1's en la palabra sea par
- Paridad **impar**: Se añade un bit con el objetivo de que el número total de 1's en la palabra sea impar

- La paridad impar es más utilizada al permitir detectar fallos en la conexión física, ya que las palabras con todos sus bits a 0 ó a 1 (00000000 y 11111111) no son válidas
- Sólo permite detectar un bit erróneo por palabra (Distancia de Hamming d=2)
- Ejemplo (*Paridad Impar*):

Carácter ASCII	Bit Paridad	Resto bits
'1'	0	0110001
'2'	0	0110010
'3'	1	0110011
'A'	1	1000001



# Mecanismos de detección y corrección de errores

## Códigos de *detección* de errores

### ■ Código de redundancia cíclica (CRC)

- Los códigos CRC están diseñados para que pequeños cambios en la palabra de datos produzcan una gran diferencia entre un CRC y otro; por ese motivo es posible detectar el error
- Se basa en el tratamiento de cadenas de bits como representaciones de polinomios con coeficientes 0 y 1 (Ej: 110001 corresponde a  $x^5 + x^4 + x^0$ ) y el uso de aritmética polinomial
- El emisor y el receptor deben acordar un polinomio generador :  $G(x)$
- El algoritmo para calcular la suma de verificación del polinomio  $M(x)$  es el siguiente (*ver Wikipedia: Comprobación de redundancia cíclica*):
  - Sea  $r$  el grado de  $G(x)$ . Añadir  $r$  bits cero al final de la trama para que contenga  $m+r$  bits
  - Dividir la cadena de bits correspondiente al nuevo polinomio  $x^r M(x)$  entre  $G(x)$
  - Poner los bits obtenidos en el residuo en los  $r$  bits cero de  $x^r M(x)$
- **Aunque el cálculo del CRC puede parecer complicado, en el año 1961 se diseñó un circuito sencillo con un registro de desplazamiento para calcular y comprobar las sumas de verificación por hardware. En la práctica casi siempre se usa este hardware.**

# Mecanismos de detección y corrección de errores

## Códigos de *detección* de errores

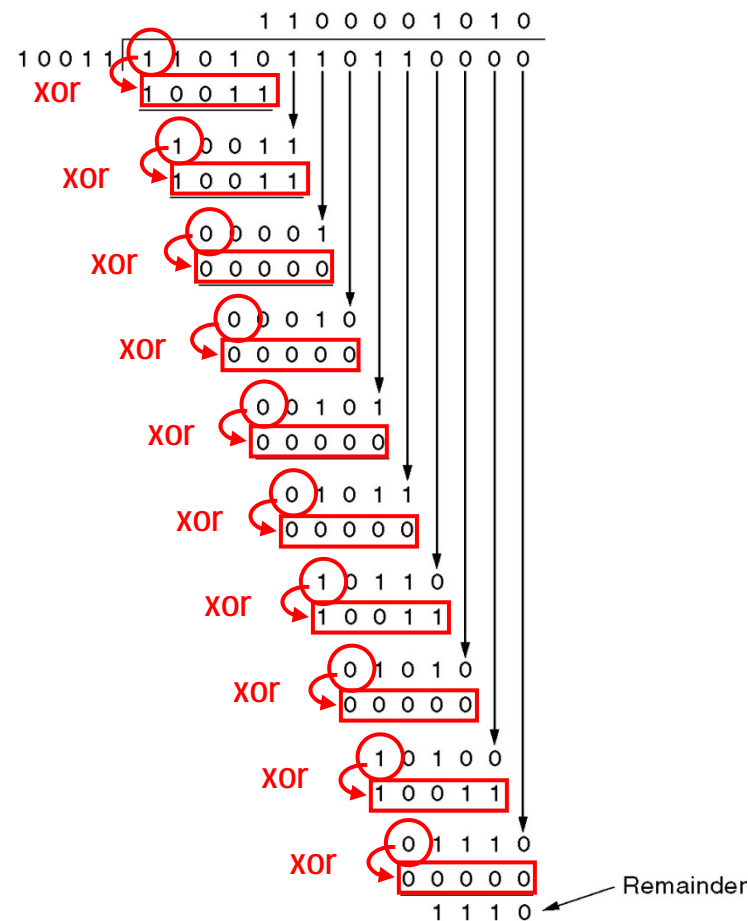
### ■ Cálculo del CRC

- Si 0, se pone 00000
- Si 1, se pone  $G(x) = 10011$

Frame : 1 1 0 1 0 1 1 0 1 1

Generator: 1 0 0 1 1

Message after 4 zero bits are appended: 1 1 0 1 0 1 1 0 1 1 0 0 0 0



Transmitted frame: 1 1 0 1 0 1 1 0 1 1 1 1 1 0



# Mecanismos de detección y corrección de errores

## Códigos de *corrección* de errores

- Permiten detectar los errores así como corregir algunos errores
- Normalmente requieren introducir más información redundante que los códigos de corrección de errores
- El protocolo puede recuperar un conjunto de errores en la trama
- Las propiedades de detección y corrección de errores de un código dependen de su distancia de Hamming
  - Se necesita un código con una distancia  **$2d+1$**  para corregir  $d$  errores
- Ejemplos:
  - Códigos de Hamming

# Mecanismos de detección y corrección de errores

## Códigos de *corrección* de errores

- Supongamos un código de 8 símbolos de distancia Hamming 3 (todas las palabras están separadas como mínimo por una distancia Hamming de 3)
- Si se recibe 010100 (código no válido) y lo comparamos con los códigos legales:

Símbolo	Código	Distancia Hamming de 010100
'A'	000000	2
'B'	001111	4
'C'	010011	3
'D'	011100	1
'E'	100110	3
'F'	101001	5
'G'	110101	2
'H'	111010	4

- 'D' está a una distancia Hamming 1 del código recibido. **Se puede suponer** que el código realmente enviado era el 011100 (habiéndose cambiado el bit  $b_4$  de 1 a 0)
- Podría haber sucedido que el código enviado fuese G (110101) habiéndose producido dos errores (en  $b_5$  y  $b_0$ ). Sin embargo, la probabilidad de que esto suceda es mucho menor





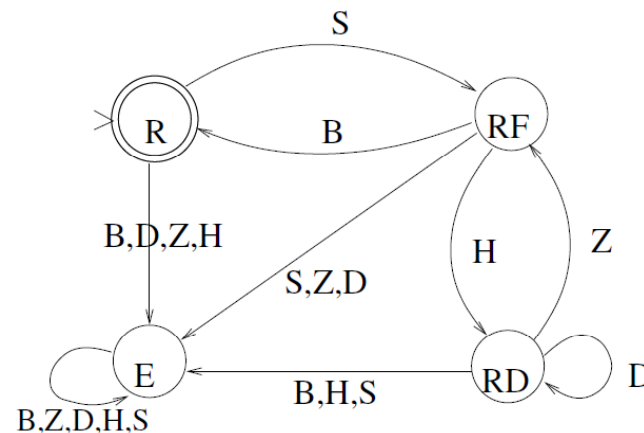
# Verificación de protocolos

- Los protocolos usados en comunicaciones son complejos
- Es necesario utilizar técnicas matemáticas formales que permitan especificar y verificar los protocolos
- Ejemplos:
  - **Modelo de máquina de estados finitos:** Permiten representar el comportamiento de sistemas con entradas y salidas, en donde las salidas dependen no sólo de las señales de entradas actuales sino también de las anteriores. Requieren definir un conjunto de estados (uno de ellos es el estado inicial) y transiciones (causadas por la recepción de un mensaje o combinación de bits)
  - **Modelos de redes de Petri:** Son representaciones matemáticas para modelar sistemas distribuidos discretos. Las redes de Petri están formada por lugares, transiciones y arcos dirigidos, así como por fichas (*tokens*) que ocupan posiciones.

# Verificación de protocolos

## Máquinas de estados finitos

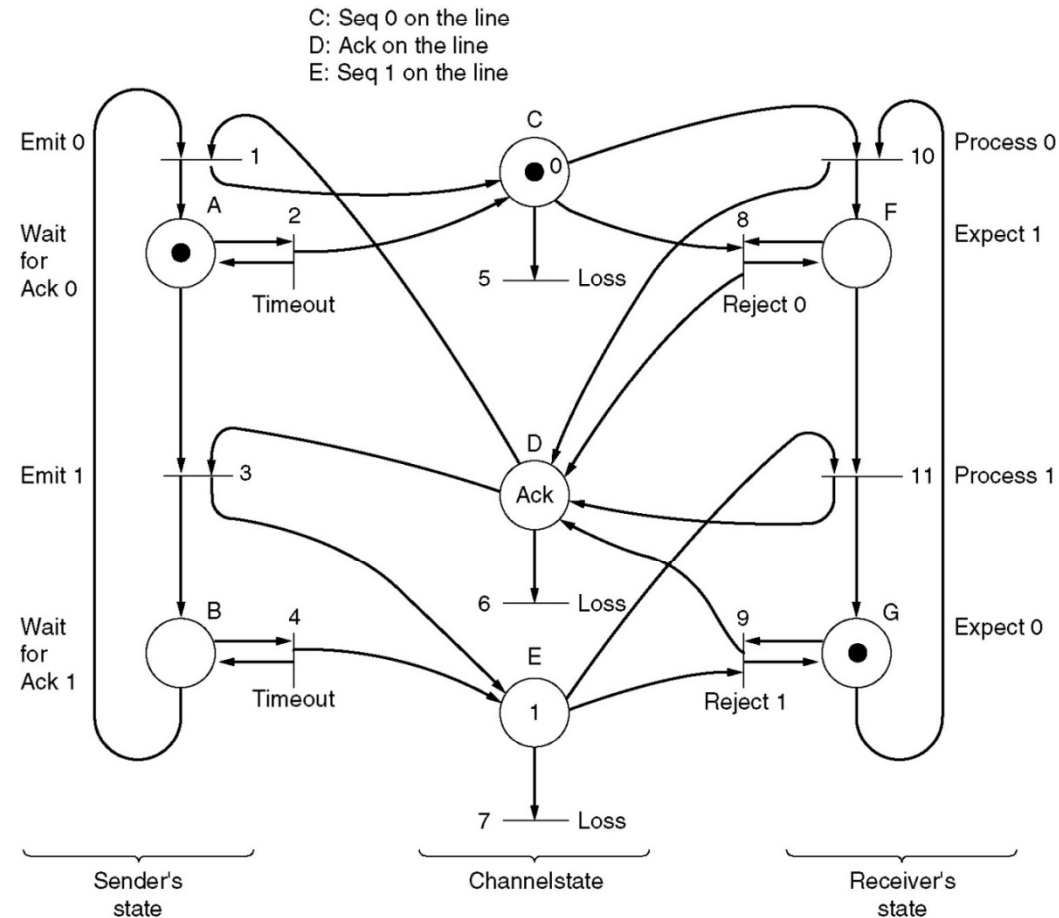
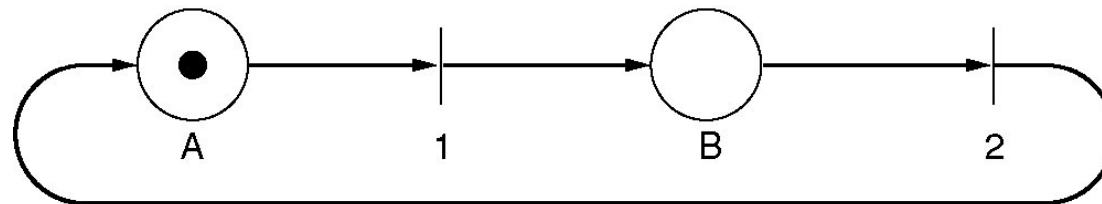
- El protocolo KERMIT es un protocolo antiguo (diseñado en 1981) para permitir la comunicación a través de líneas telefónicas.
- Puede usarse para transferir archivos o para emulación de terminal.
- **Ejemplo:** Autómata de estados finitos para la recepción de ficheros con **KERMIT**



- **Estados:** {R: Estado de espera; RF: Esperando cabecera de fichero; RD: Procesando datos de fichero; E: Estado de error}
- **Símbolos recibidos:** {S: Cabecera de transmisión; H: Cabecera de fichero; D: Símbolos contenidos en el fichero; Z: Fin de fichero; B: Fin de transmisión}

# Verificación de protocolos

## Redes de Petri





# Protocolos de enlace de datos

- **Misión:** Protocolos orientados a comunicar dos máquinas de manera confiable sobre líneas inestables
- Estos protocolos proporcionan:
  - ☐ Control de errores (mediante confirmaciones en recepción)
  - ☐ Control de flujo (usando ventanas corredizas)



# Protocolos de enlace de datos

- Algunos protocolos de enlace de datos comunes:

- **HLDC** (*High-Level Data Control*): Estandarizado por el ISO. Es un protocolo de comunicaciones de propósito general punto a punto y multipunto. Proporciona recuperación de errores en caso de pérdida de paquetes de datos, fallos de secuencia y otros, por lo que ofrece una comunicación confiable entre el transmisor y el receptor.
- **PPP** (*Point-to-Point Protocol*): es un protocolo asociado a la pila TCP/IP (RFC 1661). Permite establecer una comunicación a nivel de enlace entre dos computadoras. Diseñado para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un modem telefónico (RTC).

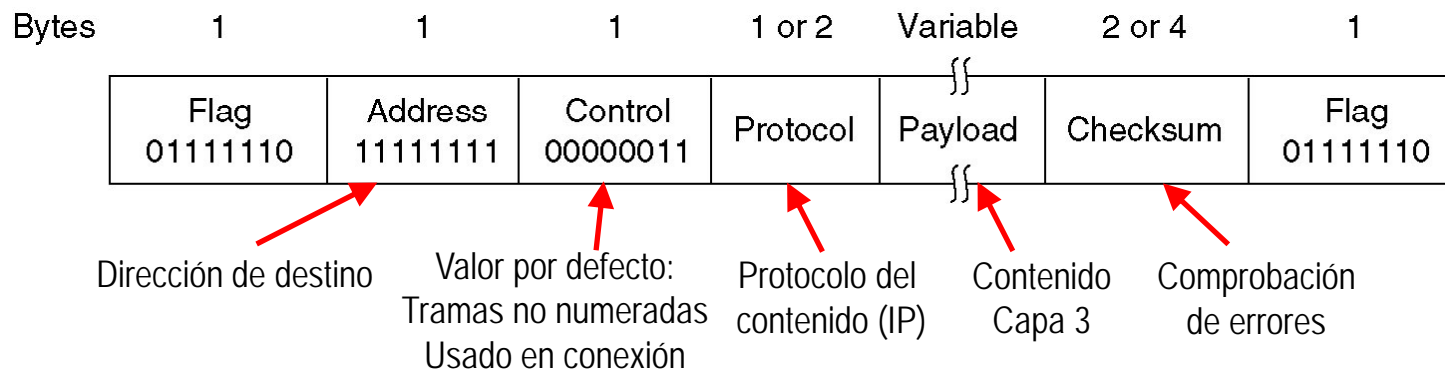
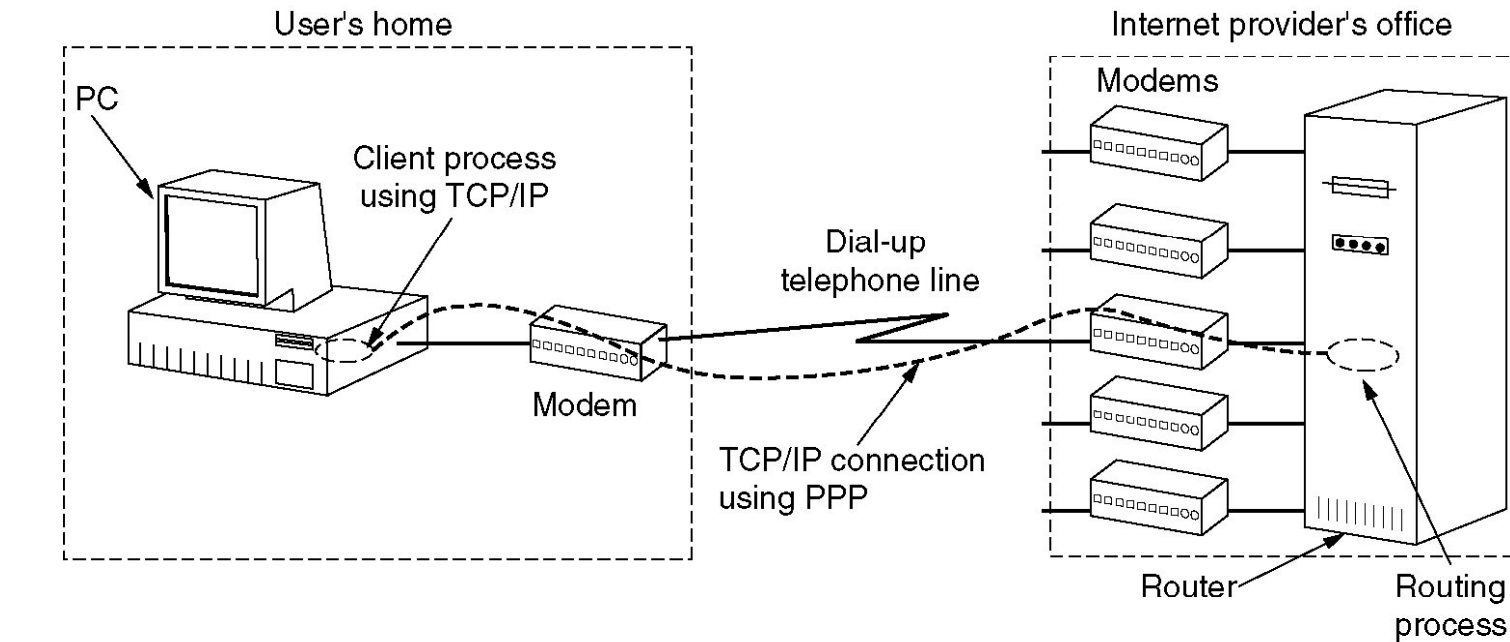
Proporciona las siguientes funcionalidades:

- Transporte de datos
- Autenticación
- Asignación dinámica de la dirección IP

**NOTA:** Algunas versiones más modernas (PPPoE, PPPoA) se utilizan sobre líneas de banda ancha tales como Ethernet, cablemodem o ADSL.

# Protocolos de enlace de datos

## Point-to-Point Protocol





# Subcapa de control de acceso al medio

- Existen dos tipos básicos de redes:
  - Las que utilizan **conexiones punto a punto**
    - No hay problema de acceso al medio
  - Las que utilizan un **canal de difusión compartido** (Ej: cable compartido o espectro electromagnético)
    - ¿Cómo se establece el acceso al medio? ¿Quién puede usar el canal cuando hay competencia por él?
    - Los protocolos usados para determinar el turno en un canal de difusión compartido pertenecen a una subcapa de la capa de enlace de datos => subcapa **MAC** (Control de acceso al medio)
    - Este problema tiene especial importancia en redes LAN
- **Objetivo subcapa MAC: Asignar un único canal de difusión entre computadoras competidoras**



# Subcapa de control de acceso al medio

## Asignación estática vs. dinámica

- Asignación estática
  - Técnicas de asignación de canal estáticas:
    - Multiplexión por división en frecuencia (FDM)
    - Multiplexión por división en tiempo (TDM)
  - Se desperdicia mucho ancho de banda si:
    - Número de emisores varía continuamente
    - Tráfico a ráfagas
  - **CONCLUSIÓN:** Pobre rendimiento para redes de computadoras
- Asignación dinámica
  - Se decide dinámicamente quién puede enviar información por el canal
  - Supuestos previos:
    - Computadoras independientes
    - Canal único (No hay formas externas de comunicación)
    - Posibilidad de colisiones (Si dos estaciones transmiten simultáneamente)
    - Tiempo continuo vs. tiempo en intervalos discretos (ranuras)
    - Detección de portadora (↑ frecuente) vs. sin detección de portadora





# Subcapa de control de acceso al medio

## Protocolos de acceso múltiple

- ALOHA
  - ☐ ALOHA puro
  - ☐ ALOHA ranurado
  
- Protocolos de acceso múltiple con detección de portadora (*Carrier Sense Multiple Access, CSMA*)
  - ☐ *Collision Detection* (CSMA/CD)
  - ☐ *Collision Avoidance* (CSMA/CA)
  - ☐ *Non-Persistent* (CSMA-NP)
  - ☐ *Persistent* (CSMA-P, CSMA-pP, CSMA-1P)
  - ☐ *Bus Arbitration* (CSMA/BA)



# Subcapa de control de acceso al medio

## ALOHA

- Desarrollado por la Universidad de Hawai en 1970
- **Objetivo:** Permitir la comunicación entre ordenadores situados en diferentes islas a través de ondas de radio.
- La idea básica es aplicable a cualquier sistema en el que usuarios no coordinados compitan por el uso de un único canal compartido
- **Interés:** Fue mejorado en varias fases y proporciona las bases de Ethernet (IEEE802.3) y WiFi (IEEE802.11)
- Dos versiones:
  - **ALOHA puro:** Versión original
  - **ALOHA ranurado:** Versión más avanzada que mejora el rendimiento



## Subcapa de control de acceso al medio

# ALOHA puro - Funcionamiento

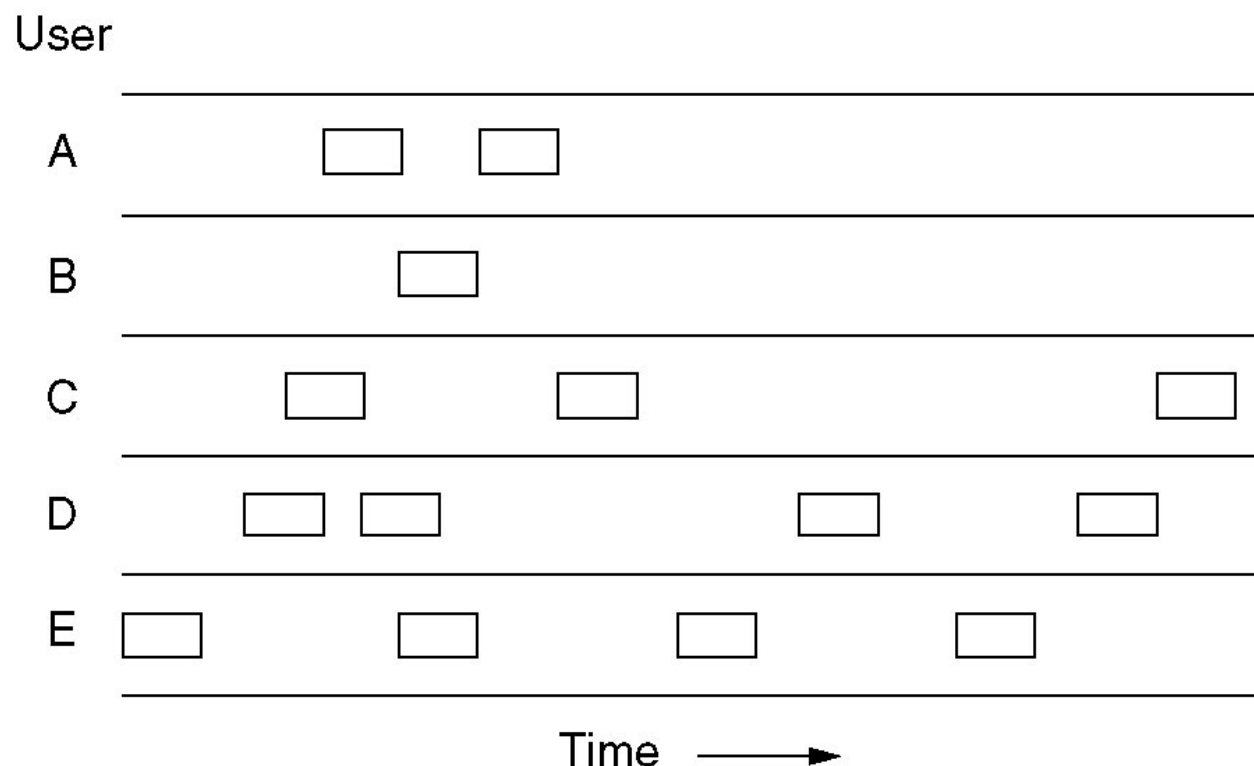
- La primera versión del protocolo era básica:
  - Si tienes datos que enviar, envíalos.
  - Si el mensaje colisiona con otra transmisión, intenta reenviarlos más tarde.
- Consecuencias:
  - Se permite que los usuarios transmitan datos en cualquier momento
  - Las estaciones no saben de antemano si otra estación intenta transmitir
  - Pueden aparecer colisiones que dañarán las tramas
- Implantación:
  - Un emisor puede saber si la trama fue destruida escuchando al canal
  - Si se destruye la trama el emisor lo detecta y espera un tiempo aleatorio para reenviar la trama




## Subcapa de control de acceso al medio ALOHA puro - Rendimiento

- El tráfico enviado incluye:
  - Tramas enviadas por primera vez
  - Tramas reenviadas debido a colisiones
- ¿Cuál es la eficiencia de una red ALOHA?
  - Si el tráfico es pequeño => Hay pocas colisiones
  - Si aumenta el tráfico => Aumentan las colisiones => Se penaliza el rendimiento
- El rendimiento máximo es de un 18.4%
  - Esto significa que el 81,6% del total disponible de ancho de banda se está desperdiciando básicamente debido a estaciones tratando de emitir al mismo tiempo

## Subcapa de control de acceso al medio ALOHA puro - Ejemplo



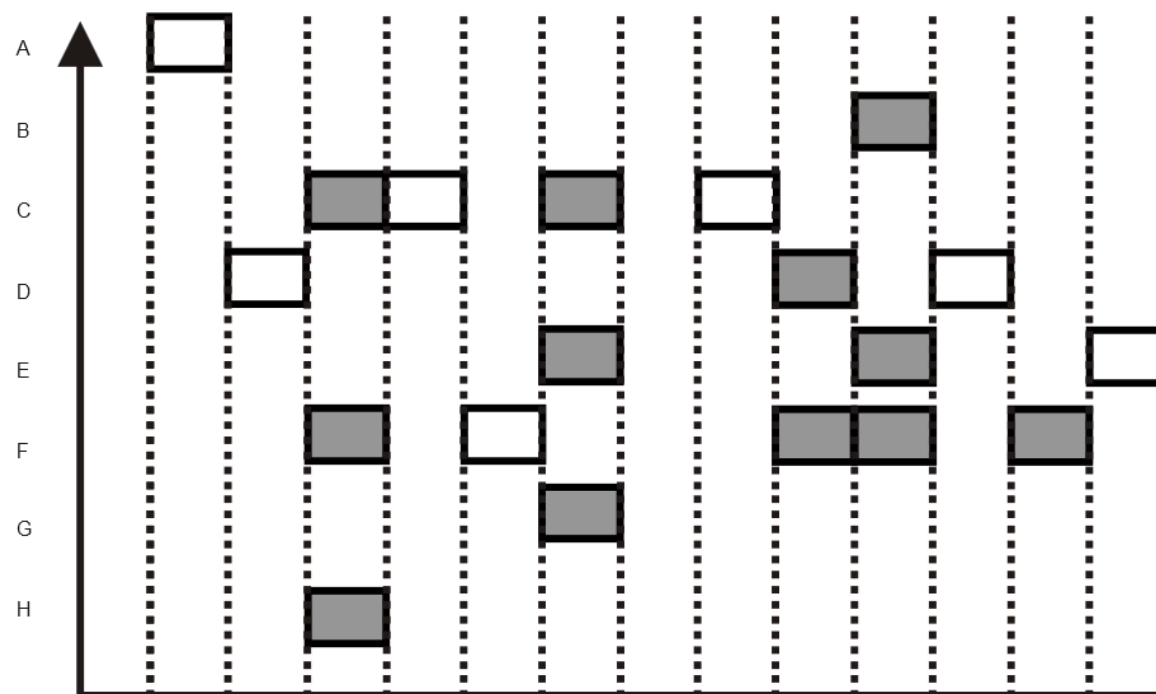
**¿Cuántas tramas se entregan bien?**



## Subcapa de control de acceso al medio ALOHA ranurado / Slotted ALOHA

- Es una versión mejorada de ALOHA para incrementar el rendimiento
- Introduce ranuras de tiempo
- Funcionamiento:
  - Similar a ALOHA
  - Una estación no puede emitir en cualquier momento, sino justo al comienzo de una ranura, y así las colisiones se reducen.
  - Requiere sincronización global de tiempo (Todas las estaciones conectadas a la red tienen el mismo reloj)
- El rendimiento máximo es de un 36.8%

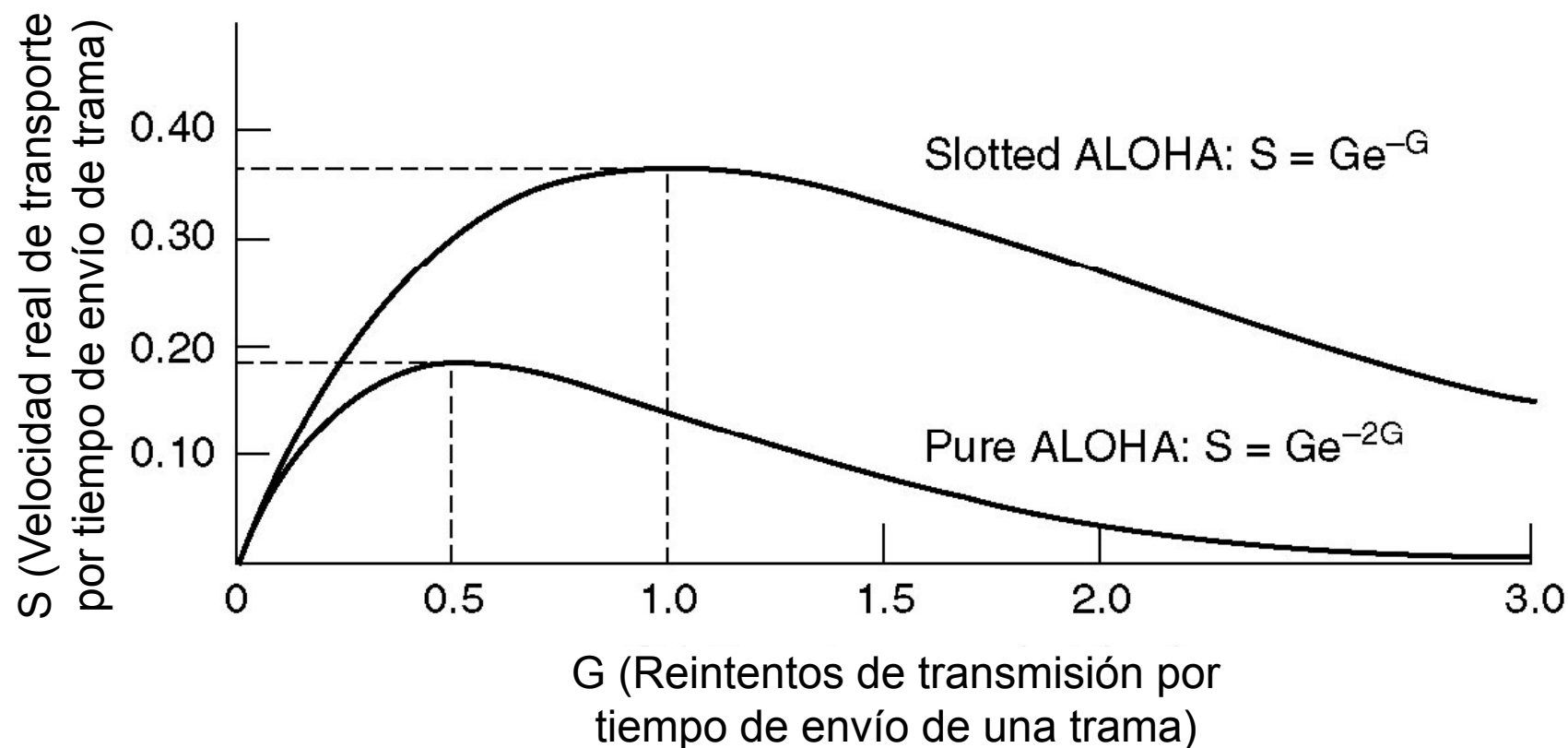
## Subcapa de control de acceso al medio ALOHA ranurado - Ejemplo



Las tramas en gris colisionan con otras tramas  
Las tramas en blanco se entregan correctamente

## Subcapa de control de acceso al medio

# ALOHA rendimiento







## Subcapa de control de acceso al medio

# Conclusiones ALOHA

- Es un protocolo antiguo e interesante por ser el primer intento serio de gestionar un canal compartido entre varias estaciones
- En ALOHA las estaciones no tienen en cuenta que hacen el resto de estaciones
- Se obtiene un pobre aprovechamiento del medio (18.4% en ALOHA puro y 36.8% en ALOHA ranurado)



## Subcapa de control de acceso al medio

# Protocolos con detección de portadora (CSMA)

- Protocolos de acceso múltiple con detección de portadora (*Carrier Sense Multiple Access*, CSMA)
- Son algoritmos en los que las estaciones **escuchan antes de enviar**
- Existen diferentes tipos de algoritmos
  - *Non-Persistent* (CSMA-NP)
  - *Persistent* (CSMA-P, CSMA-pP, CSMA-1P)
  - *Collision Detection* (CSMA/CD)
  - *Collision Avoidance* (CSMA/CA)
  - *Bitwise Arbitration* (CSMA/BA)



## Subcapa de control de acceso al medio

# Protocolos con detección de portadora (CSMA)

- Persistencia vs. No persistencia
- CSMA persistente-1 (*Greedy Approach*)
  - ☐ Cuando una estación tiene datos que enviar primero escucha el canal para saber si otra está transmitiendo en este momento
  - ☐ Si el canal está ocupado la estación se queda escuchando hasta que se desocupe
  - ☐ Cuando la estación detecta que el canal está inactivo transmite una trama
  - ☐ Si ocurre una colisión la estación espera un tiempo aleatorio y comienza de nuevo
  - ☐ Deben evitarse tiempos de propagación grandes dado que se impide que las demás estaciones se enteren a tiempo.
  - ☐ El protocolo se denomina CSMA persistente 1 porque hay una probabilidad del 100% de que la trama se transmita cuando el canal esté libre

**Ejercicio: Calcular el tiempo que tarda en enviarse un bit en una red a través de un cable de 1 Km. ¿Y un paquete de 1000KB? Delay de una conversación a través de 800 Km si se envían 64KBps en cada dirección**



## Subcapa de control de acceso al medio

# Protocolos con detección de portadora (CSMA)

- Persistencia vs. No persistencia
- CSMA no-persistente
  - Se intenta ser menos egoista que en el protocolo CSMA persistente-1
  - Antes de enviar se escucha el canal, si está libre se intenta enviar
  - Si está ocupado, no se escucha el canal de forma continua para transmitir la trama sino que se espera un periodo aleatorio y repite el algoritmo



## Subcapa de control de acceso al medio

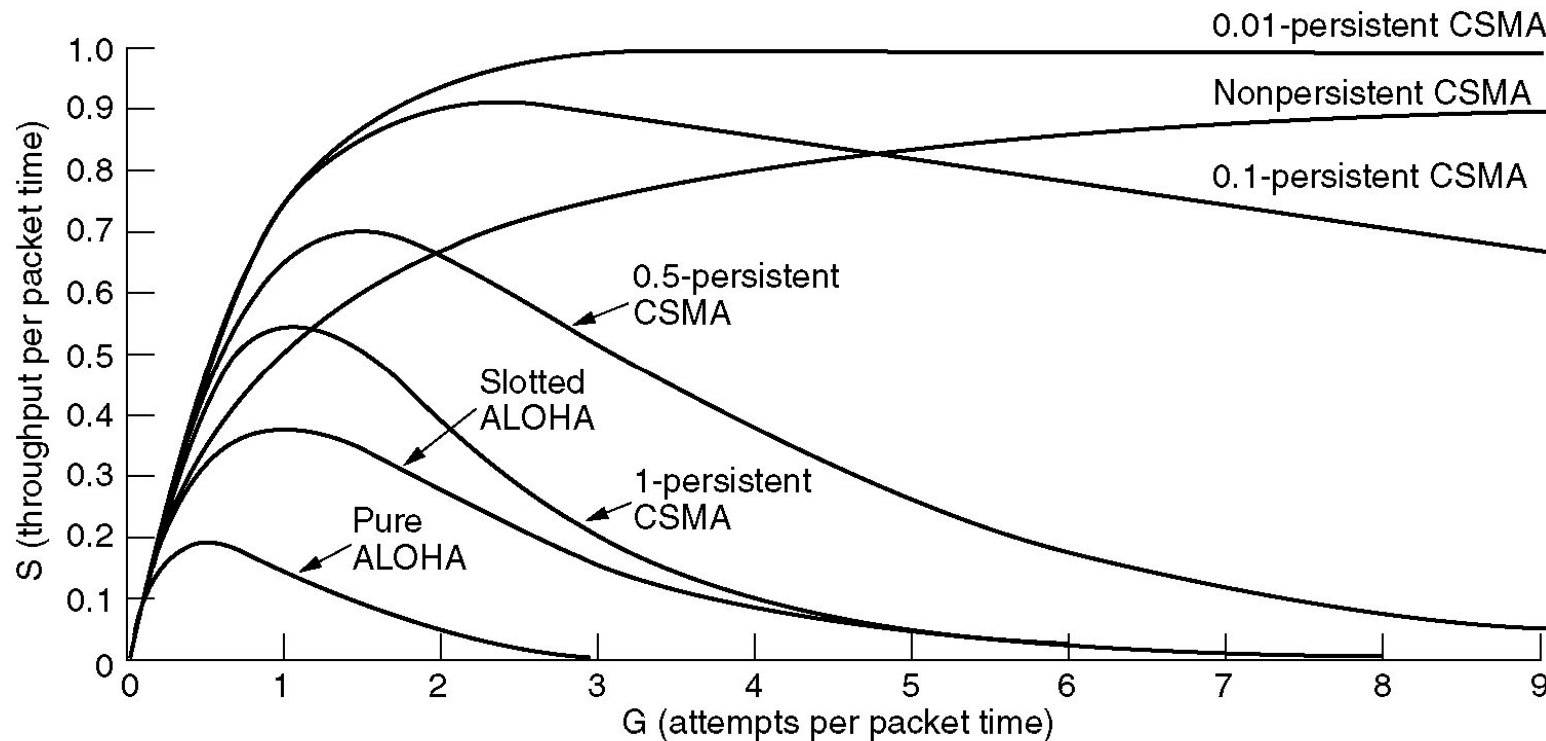
# Protocolos con detección de portadora (CSMA)

- Persistencia vs. No persistencia
- CSMA persistente-p
  - Se aplica en canales ranurados
  - Si una estación quiere enviar información escucha el canal
  - Si está inactivo la estación transmite con una probabilidad  $p$

## Subcapa de control de acceso al medio

# Protocolos con detección de portadora (CSMA)

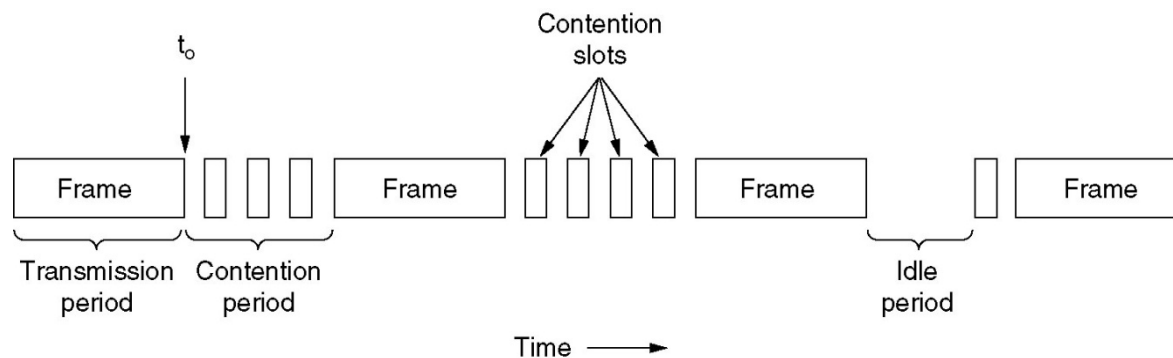
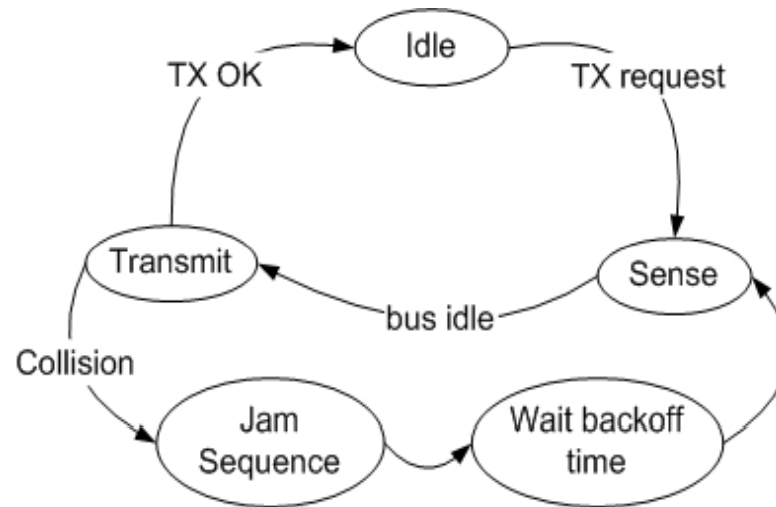
- Protocolos de acceso múltiple con detección de portadora (*Carrier Sense Multiple Access, CSMA*)



## Subcapa de control de acceso al medio

# Protocolos con detección de portadora (CSMA)

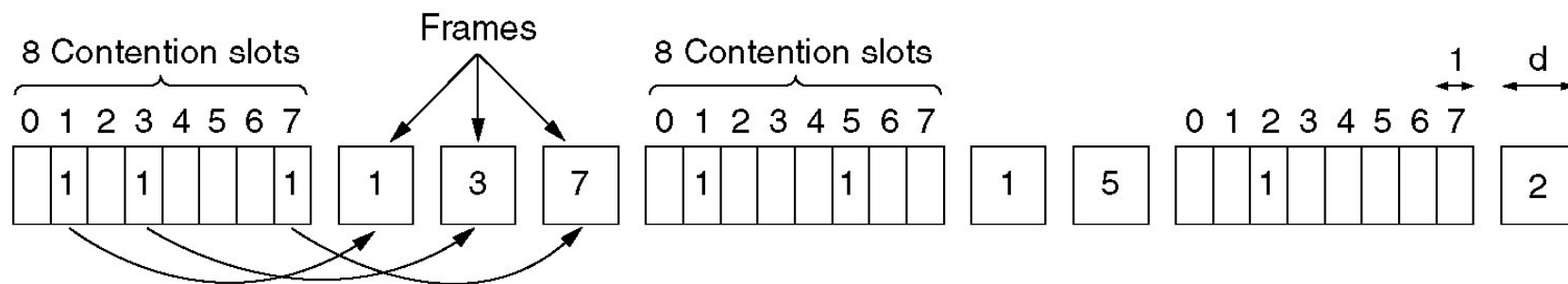
- Carrier Sense Multiple Access / Collision Detection (CSMA/CD)



## Subcapa de control de acceso al medio

# Protocolos con detección de portadora (CSMA)

- Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)
- Protocolos de mapa de bits:
  - Se asigna una dirección a cada una de las estaciones
  - Se usa una trama (**Contention Frame**) en la que están representadas todas las estaciones existentes en la red (**Contention Slots**). P.e. 8 estaciones en la figura
  - Aquellas estaciones que quieren enviar una trama lo indican en la trama de contención poniendo un 1
  - Así todas las estaciones saben quiénes van a enviar tramas y en qué orden

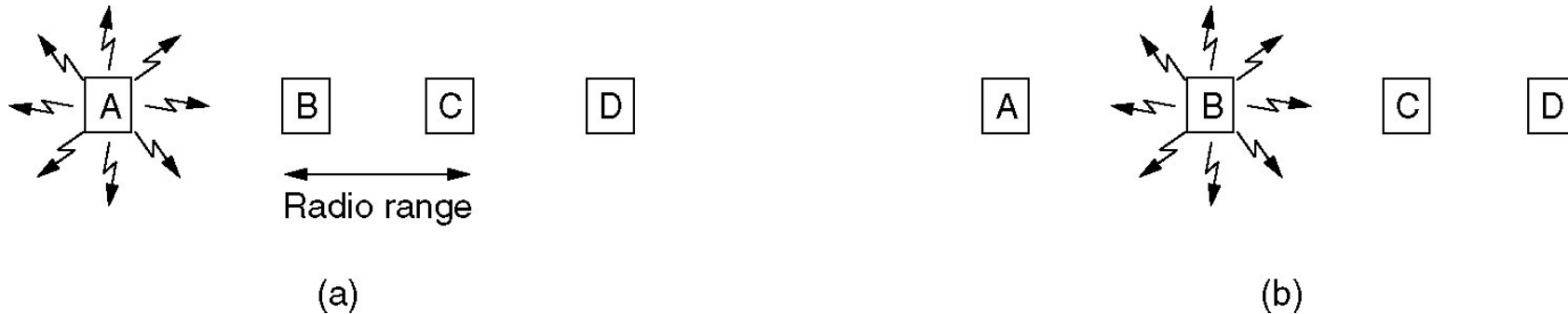




## Subcapa de control de acceso al medio

# Protocolos con detección de portadora (CSMA)

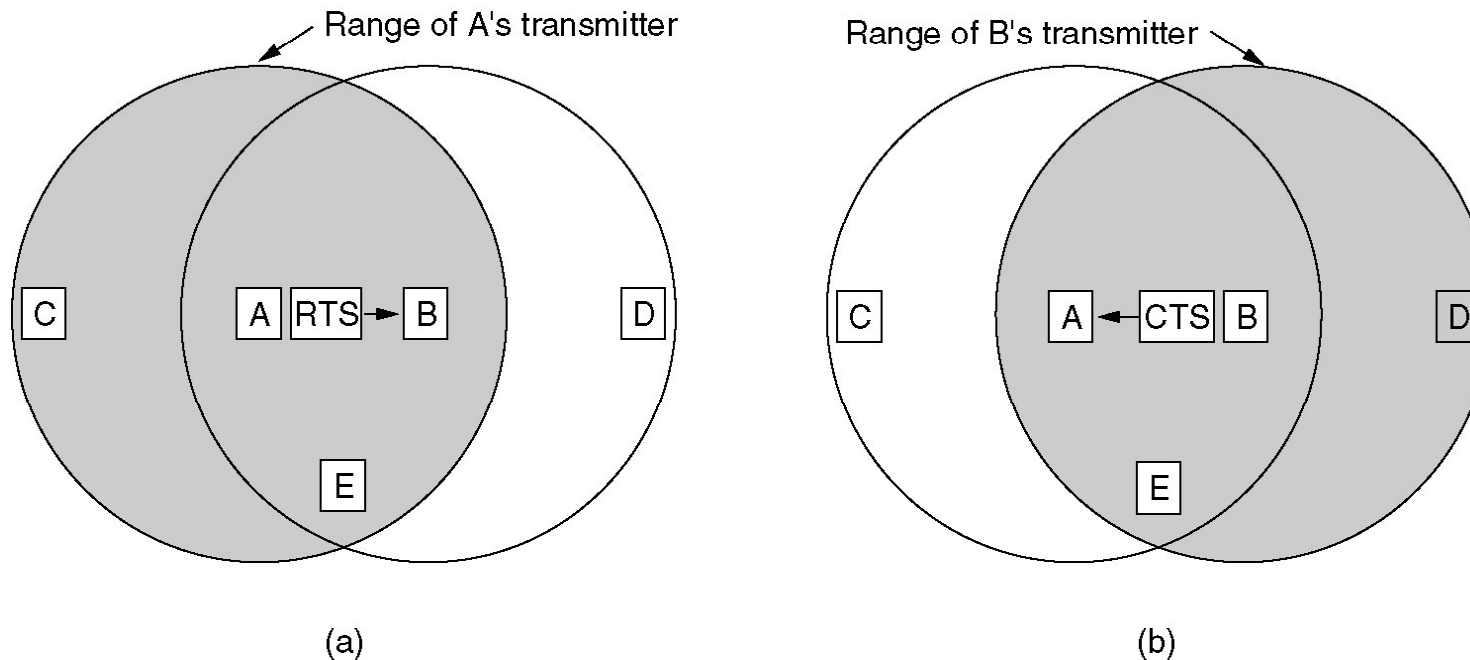
- Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)
- Protocolos de redes inalámbricas:



## Subcapa de control de acceso al medio

# Protocolos con detección de portadora (CSMA)

- Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)
  - Protocolo MACA (*Multiple Access with Collision Avoidance*)
  - Usado en IEEE802.11
  - RTS: *Request to Send* / CTS: *Confirmation to Send*

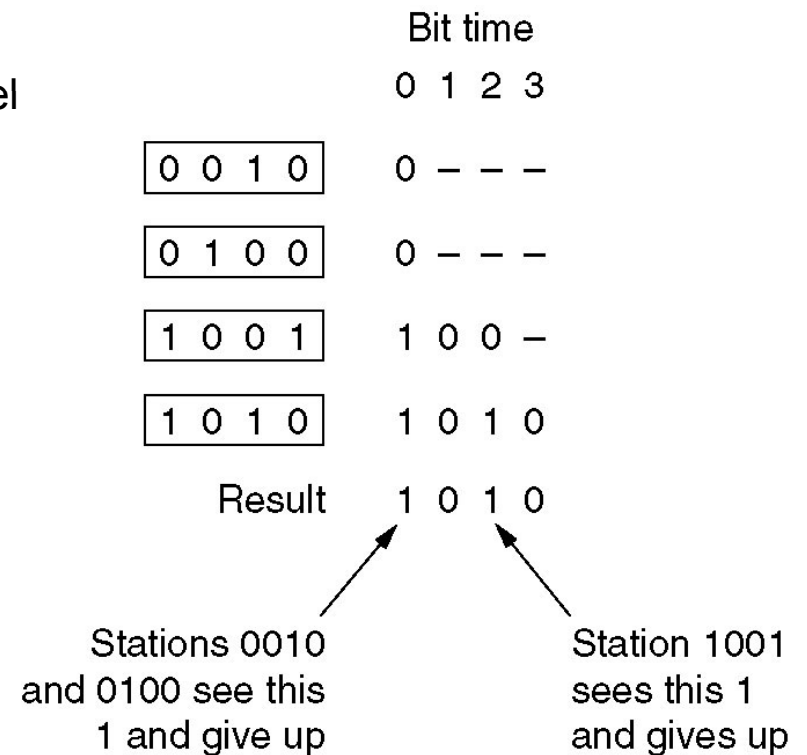


# Subcapa de control de acceso al medio

## Protocolos con detección de portadora (CSMA)

### ■ Carrier Sense Multiple Access / Bitwise Arbitration (CSMA/BA)

- Arbitración del bus en base a la cabecera del mensaje (dirección o tipo de mensaje)
- Se decide qué mensaje tiene prevalencia





# Subcapa de control de acceso al medio Ethernet

- Cableado Ethernet
- Codificación Manchester
- Subcapa MAC
- El algoritmo de retroceso exponencial binario
- Rendimiento de Ethernet
- Switched Ethernet
- Fast Ethernet
- Gigabit Ethernet
- IEEE 802.2: Logical Link Control



# Ethernet

## Origen y estado actual

- **Creada a mediados de los 70s** (!) por Robert Metcalfe del Xerox Palo Alto Research Center.
- Inicialmente orientada a **compartir periféricos de alto coste** en entornos ofimáticos (en concreto, fue desarrollada para conectar impresoras a computadoras)
- **Muy popular** en la actualidad, siendo usada en muchos dominios más allá de su uso original. Particularmente en **sistemas industriales**, es el más sólido candidato para la unificación de los protocolos de comunicación, desde el nivel de planta hasta el de gestión.
- Estandarizada a mediados de los 80s como **IEEE 802.3**



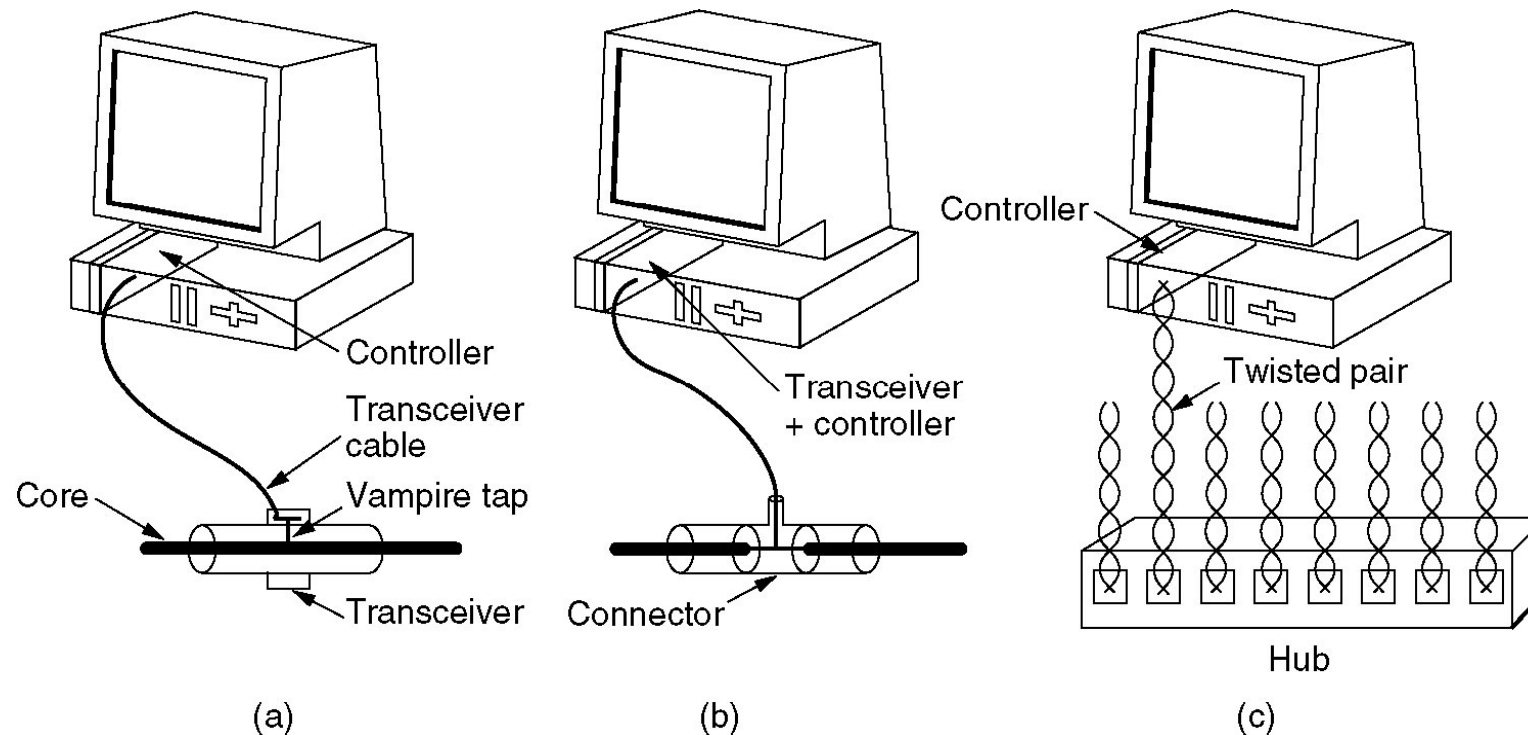
# Ethernet

## Principales características

- **Bus** serie **Multi-master, broadcast**, (inicialmente) o **Estrella** (en la actualidad)
  - **Bus**: ☺ cableado más sencillo / ☹ los fallos en cualquier punto imposibilitan la comunicación por completo; Búsqueda difícil de fallos
  - **Estrella**: ☹ Cableado más caro y complejo / ☺ mejor tolerancia a fallos, Búsqueda de fallos más fácil y rápida
- Transmisión sincrónica con codificación de bits Manchester
- Velocidad de transmisión de **10, 100Mbit/s, 1 y 10Gbit/s**
- Número de nodos máximo de **1024** (normalmente está limitado por el número de puertos del equipamiento)
- Máximo de 2 hubs entre 2 nodos (100Mbit/s)
- 2 arquitecturas: **shared** (hubs), **segmented** (switches)
- Clases de **direccionamiento**: unicast, multicast and broadcast

# Ethernet

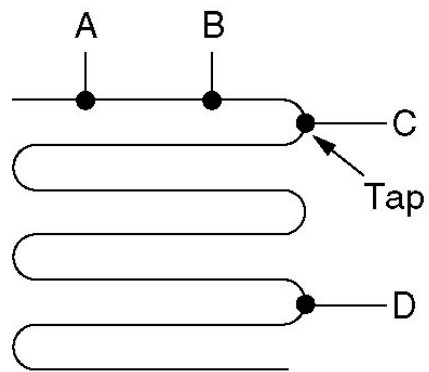
## Cableado (Ethernet original 10Mbps)



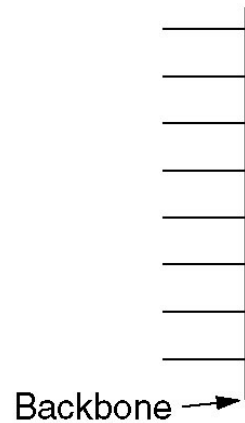
Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

# Ethernet

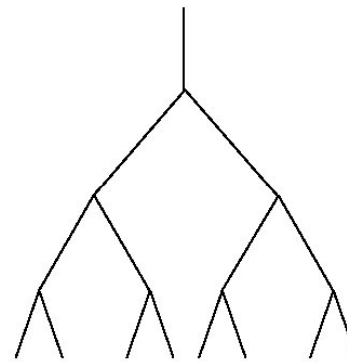
## Cableado - Topologías



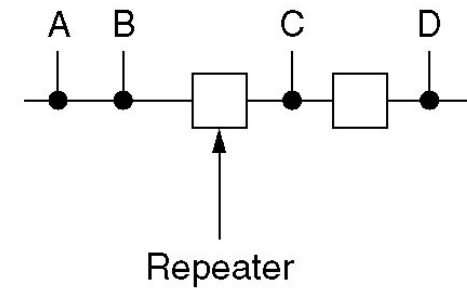
(a)



(b)



(c)

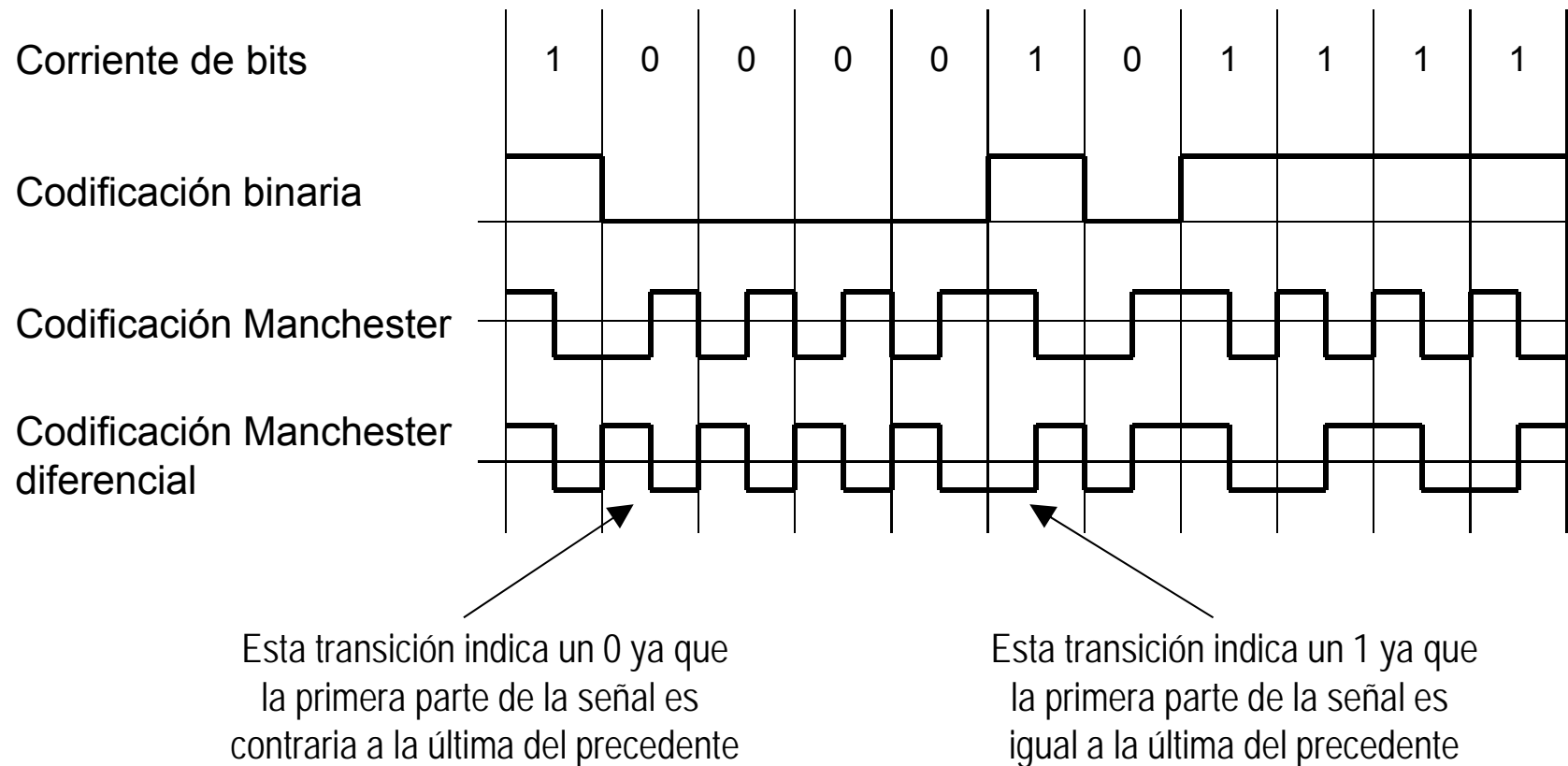


(d)

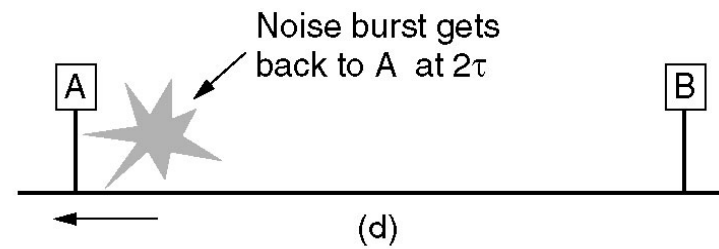
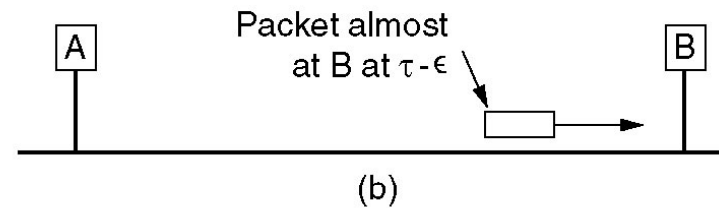
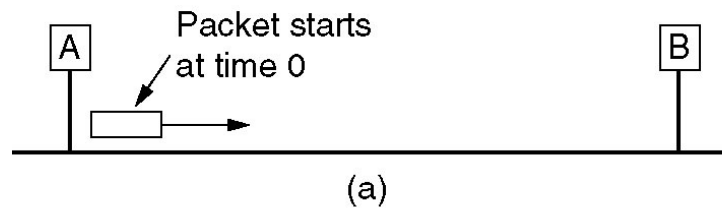


# Ethernet

## Codificación Manchester



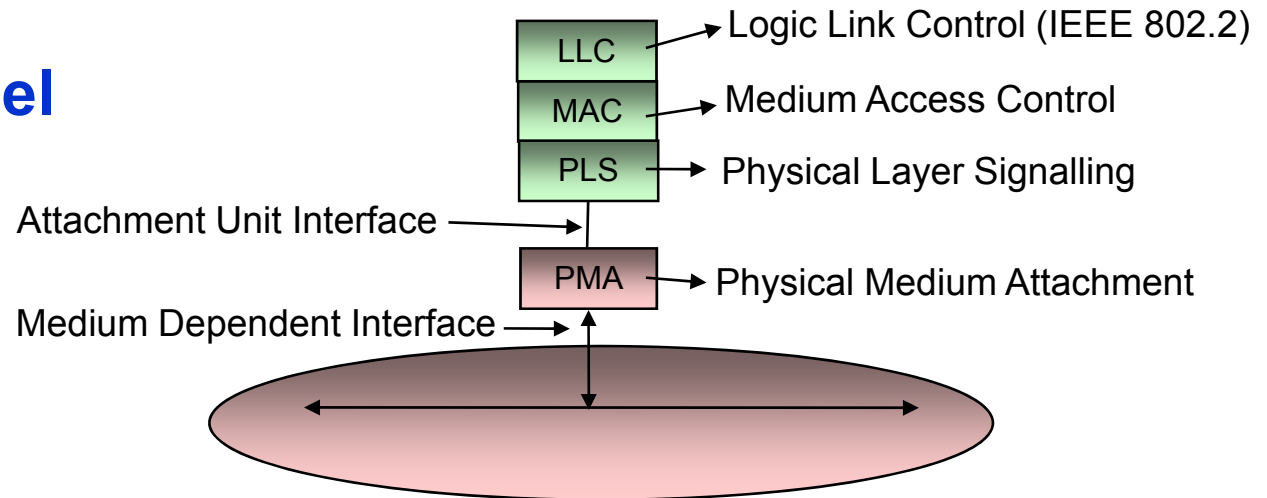
# Ethernet Colisiones



# Ethernet

## Interfaces de red y tramas

- Arquitectura del interfaz de red



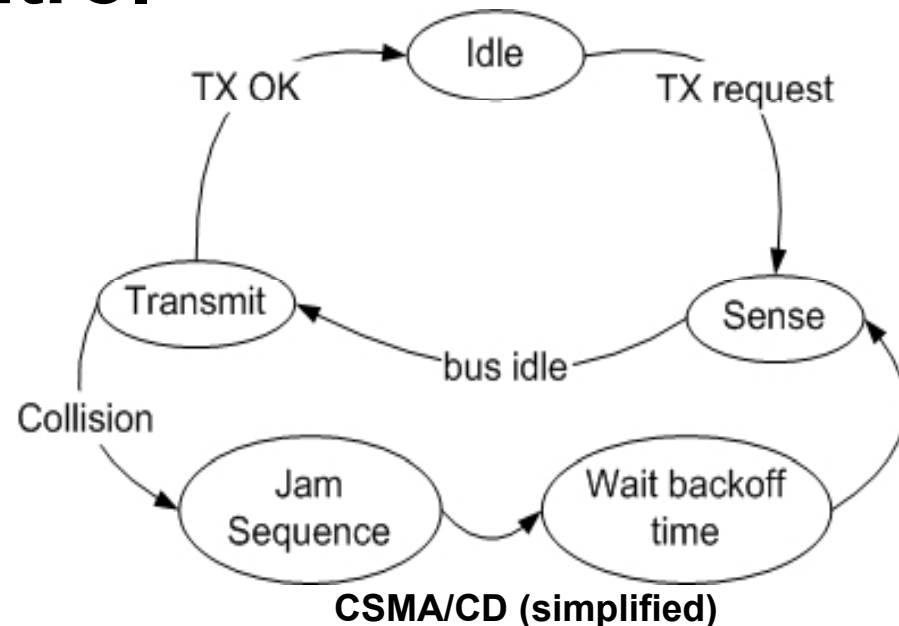
- Estructura de la trama

Dst. Addr	Src. Addr	Type/Len	LLC	SNAP	Data	CRC
6	6	2	3	5	38-1492 46-1500	4

# Ethernet

## Medium Access Control

- **CSMA/CD** no determinista (usado sólo en Ethernet)
- Se transmite con 100% de probabilidad cuando se considera que el medio está libre
- Pueden ocurrir **colisiones**
- Cuando se detecta una **colisiones** se envía una señal de **jamming** (de 32 bits)
- Las tramas varían entre 64 (min) y 1518 (max) bytes  
físicamente se añaden 7+1 octetos como preámbulo & SOF (Start of frame) y 96 bit times como IFS

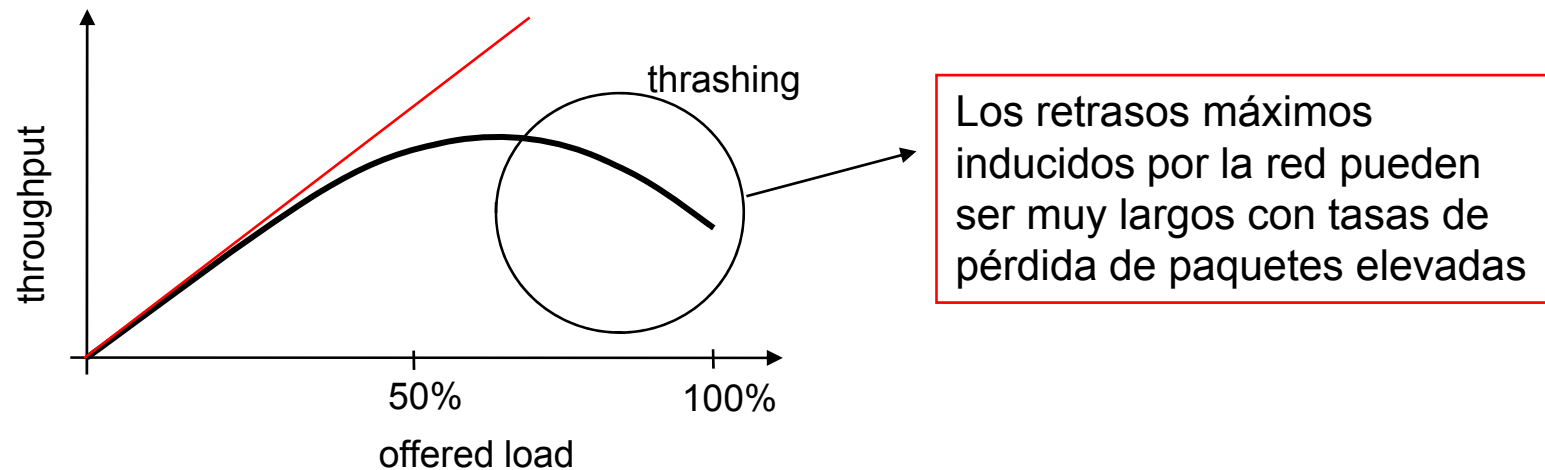


# Ethernet

## Comportamiento en sobrecarga

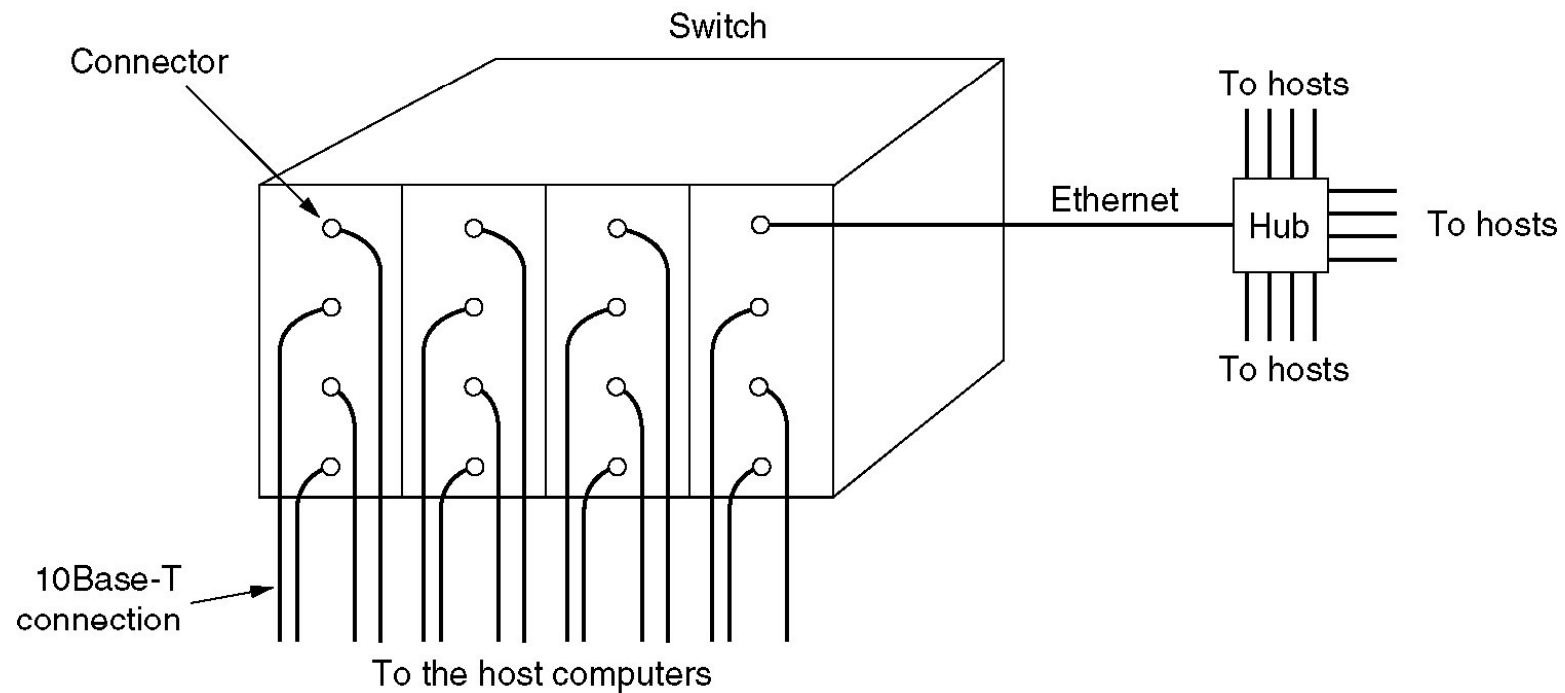
### ✓ Thrashing effect

A medida que aumenta la carga la carga distribuida por la red (rendimiento) disminuye



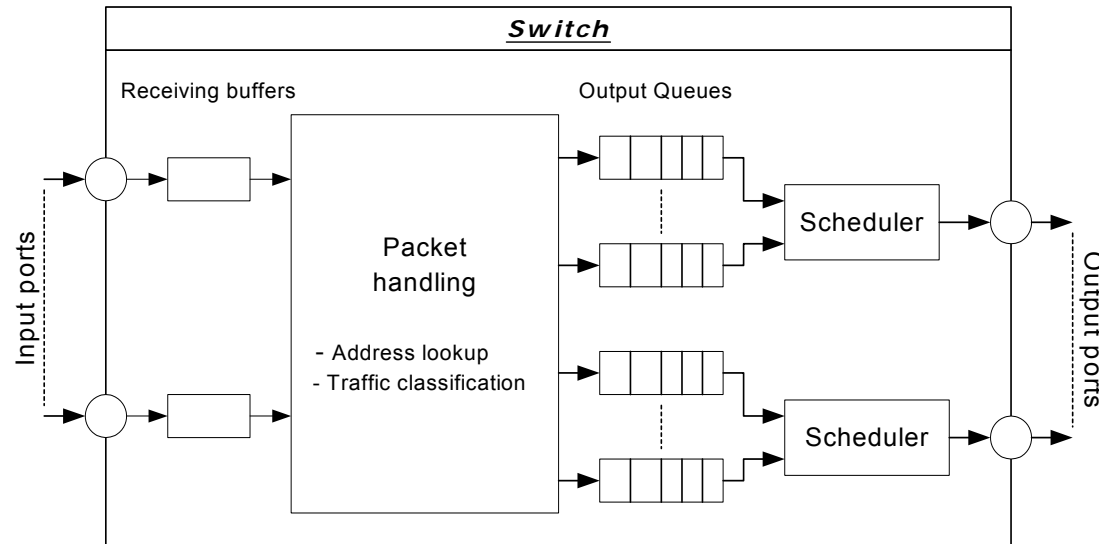
# Ethernet

## Ethernet Switches



# Ethernet

## Ethernet Switches



- Hoy en día se ha convertido en la solución más común (incluso en redes de propósito general)
- **No hay colisiones**; los nodos ven un dominio privado (arquitectura micro-segmentada)
- Los mensajes dirigidos a un puerto de salida ocupado se almacenan temporalmente en la memoria del switch
- Se definen hasta 8 niveles de prioridad para los mensajes



# Ethernet

## Ethernet Conmutada / Switched Ethernet

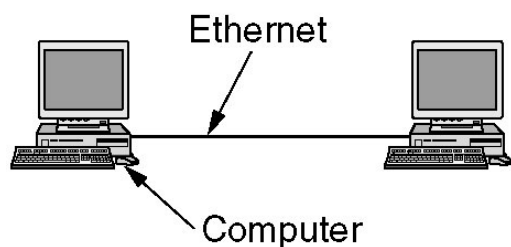
- Se ha convertido en la solución más común
  - Los switches actuales son no bloqueantes
  - 802.1D – Permiten varias colas con prioridad (802.1p)
  - 802.1Q – Permiten LANs virtuales
- **No es perfecta!**
  - Se producen inversiones de prioridad en las colas (normalmente FIFO)
  - Se produce interferencia mutua a través de la memoria compartida y la CPU
  - Se añade un retraso en el envío adicional (con jitter causado por la búsqueda en la tabla de direcciones, aprendizaje de direcciones, etc.)
  - Los retrasos varían en función de la tecnología del switch y la gestión de los algoritmos de gestión del tráfico



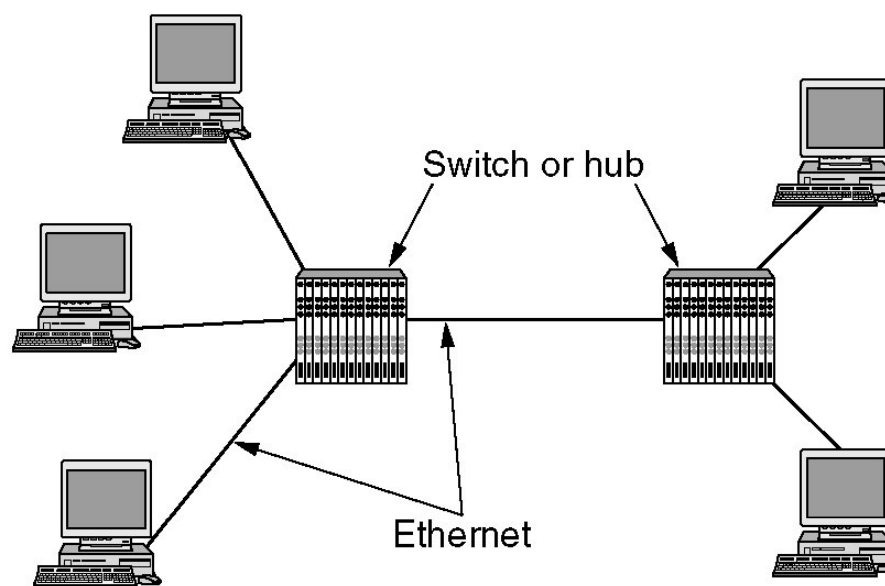
# Ethernet

## Ethernet Conmutada / Switched Ethernet

- Conexiones típicas con cable cruzado y topologías con switches o hubs



(a)



(b)



# Ethernet

## Cableado Ethernet

- Cableado Ethernet 100Mbps (Fast Ethernet)

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

- Cableado Gigabit Ethernet 1 Gpbs

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 $\mu$ ) or multimode (50, 62.5 $\mu$ )
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP



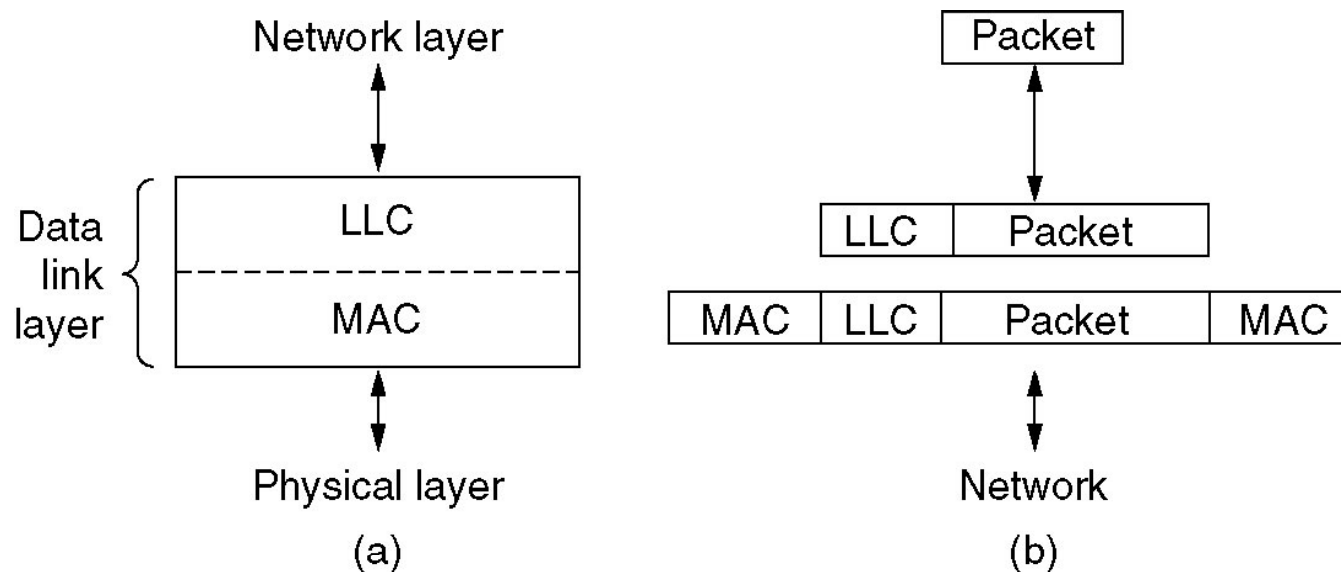
# Subcapa de control lógico de enlace

- **Recordando:** Protocolos de enlace de datos (PPP y HDLC)
  - Protocolos orientados a comunicar dos máquinas de manera confiable sobre líneas inestables
  - Proporcionan control de flujo
  - Proporciona control de errores
- La subcapa MAC de IEEE802 (p.e. Ethernet ó Wifi) no proporcionan mecanismos de comunicación confiables
- Lo que ofrecen los protocolos IEEE802 es un servicio de envío de tramas lo mejor posible (*best effort*)
- Estas redes son adecuadas para enviar información IP, dado que los paquetes IP no esperan garantías de distribución en la capa de red (sí pueden esperarlo en la capa de transporte)
- **Algunos sistemas requieren un protocolo de enlace de datos con control de errores y de control de flujo**

# Subcapa de control lógico de enlace

## Protocolo IEEE802.2

- IEEE802.2 Logical Link Control (LLC) es un protocolo similar a HDLC que proporciona control de errores y de control de flujo sobre una red no confiable
  - Agrega números de secuencia, confirmación de recepción, etc
- IEEE802.2 (LLC) puede operar sobre todos los protocolos 802 (Ethernet, Wifi, etc.)





## Subcapa de control lógico de enlace Protocolo IEEE802.2

- El protocolo IEEE802.2 permite tres tipos de servicio:
  - Servicio no confiable de datagramas
  - Servicio de datagramas sin confirmación de recepción
  - Servicio confiable orientado a la conexión



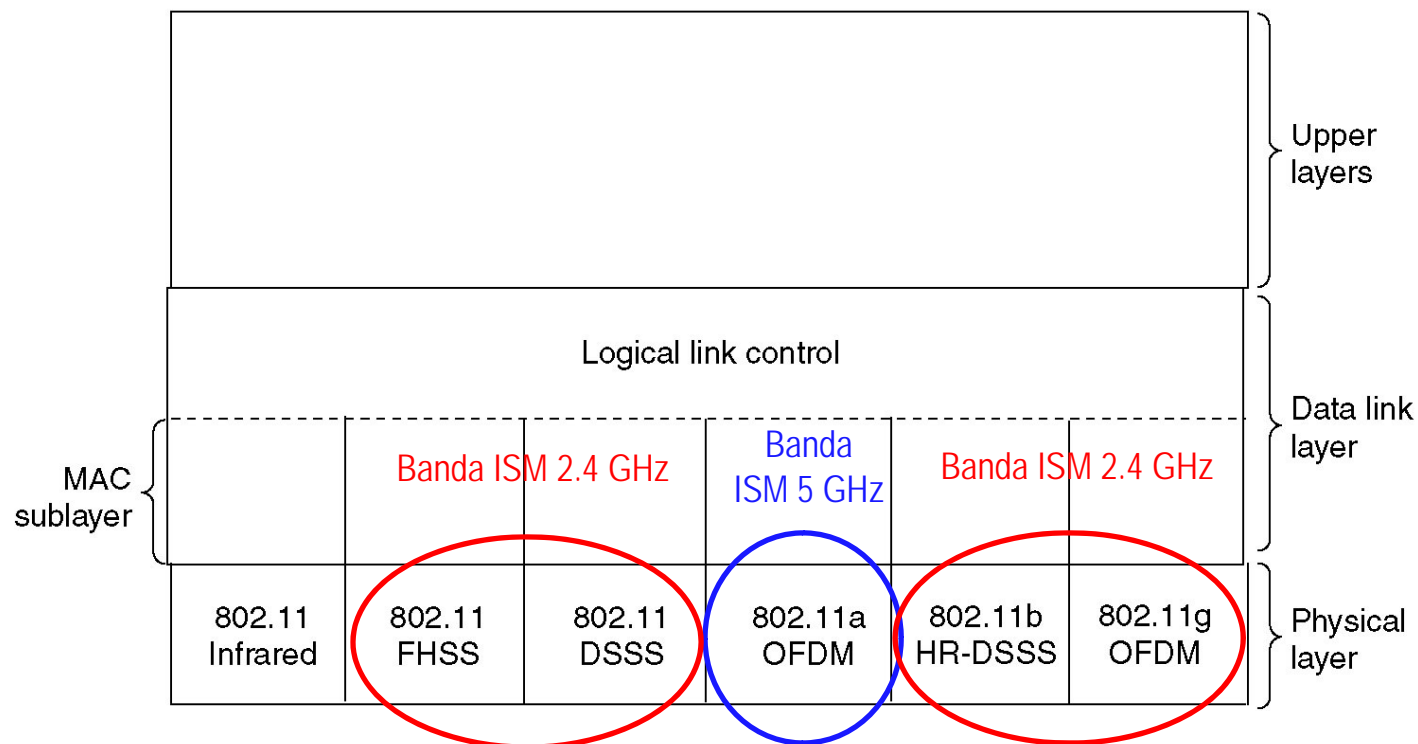
# Redes de área local inalámbricas

- Definidas en el estándar IEEE802.11
  - ☐ Pila de protocolos de 802.11
  - ☐ Capa física en 802.11
  - ☐ Topologías de red
  - ☐ Capa de acceso al medio (MAC) en 802.11
  - ☐ Estructura de las tramas
  - ☐ Seguridad

# IEEE802.11

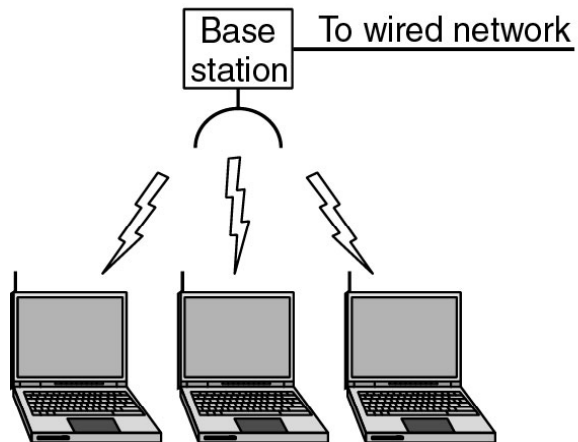
## Pila de protocolos

- Diferentes medios de transmisión:
  - Infrarrojo (Posibles interferencias con mandos de infrarrojos: garaje...)
  - Radio de corto alcance: Bandas no reguladas ISM 2.4 y 5 GHz (Posibles interferencias con hornos microondas)

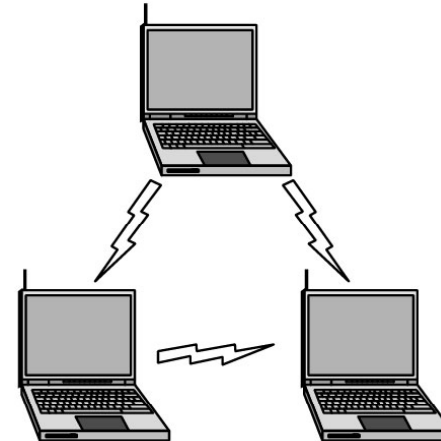


# IEEE802.11

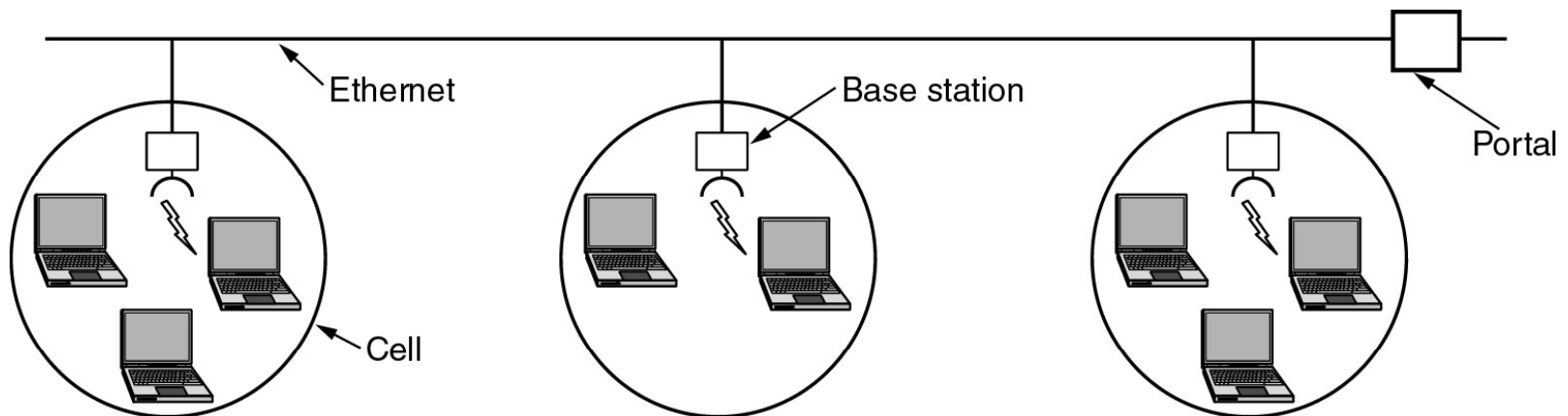
## Topologías de red



Red inalámbrica con una estación base (Access Point)



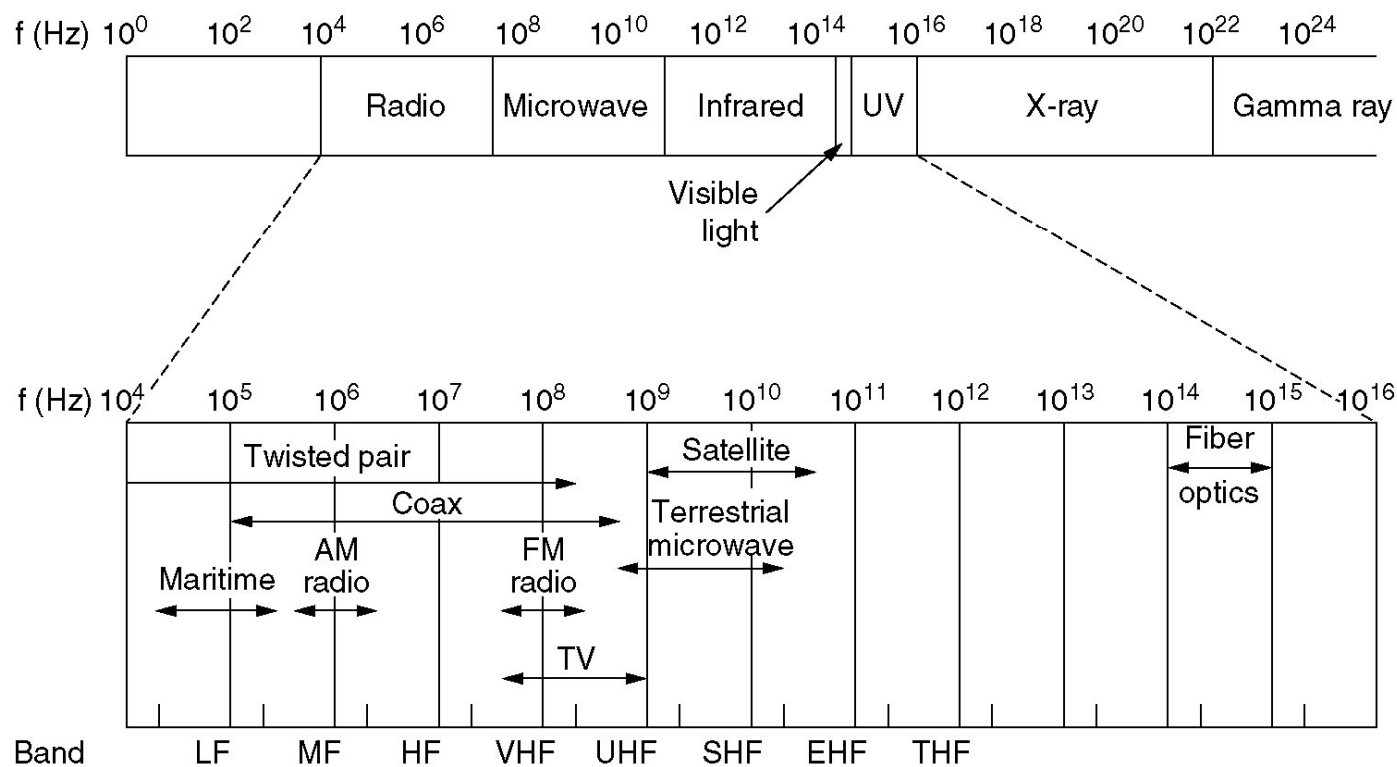
Comunicación *ad hoc*





# Transmisión sin hilos

## Espectro electromagnético



$$f = \frac{v}{\lambda}$$

■ Donde:

- $\lambda$  es la longitud de la onda
- $f$  es la frecuencia
- $v$  es la velocidad ( $3 \cdot 10^8$  m/s en el vacío)



## IEEE802.11

# Características de las ondas electromagnéticas

- El comportamiento de las ondas electromagnéticas (OE) influye en el diseño de las redes inalámbricas
  - Interferencias: Otras redes WLAN, otros dispositivos (p.e. Hornos microondas)
  - La potencia de transmisión de un AP está regulada (para reducir interferencias)
  - Atenuación con la distancia y el medio (p.e. en edificios el acero y hormigón)
  - Reflexiones y dispersión de la señal



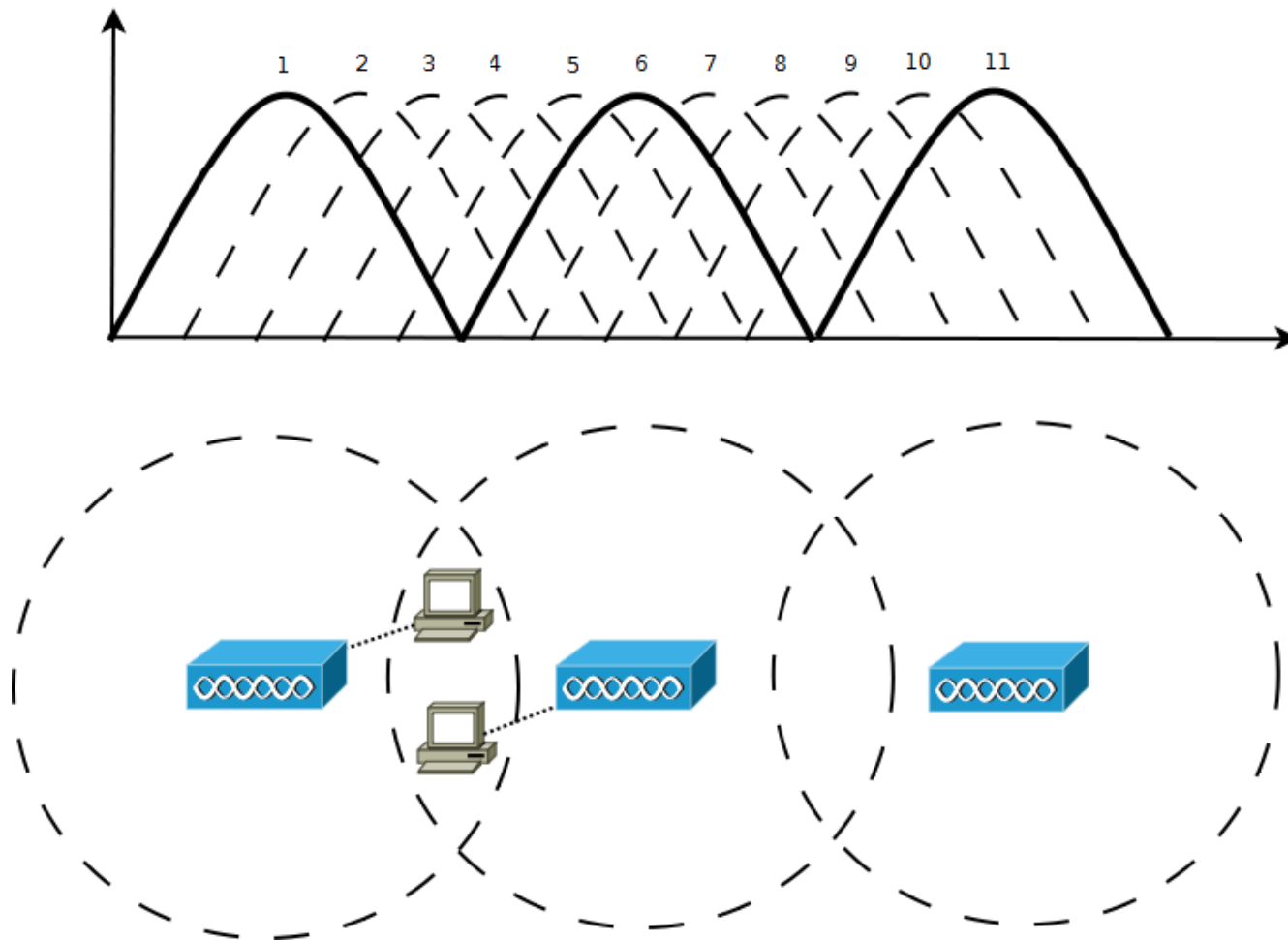
# IEEE802.11

## Codificación inalámbrica

- Los dispositivos WLAN (NIC o AP) tienen que modular (cambiar) la frecuencia, amplitud o fase de las señales de radio para enviar los datos
- Tres tipos de codificación:
  - **Espectro disperso por salto de frecuencia** (FHSS, *Frequency Hopping Spread Spectrum*) utiliza todas las frecuencias de la banda, saltando a otras diferentes. Así consigue evitar las interferencias causadas por otros dispositivos, logrando enviar datos con éxito en algunas frecuencias. Se usa en las versiones más antiguas del estándar, 802.11
  - **Espectro disperso de secuencia directa** (DSSS, *Direct Sequence Spread Spectrum*) Se usa en la banda 2.4GHz y puede haber 11 canales superpuestos. Aunque muchos canales están superpuestos, 3 canales (los situados en los extremos inferior, superior y el canal central) no se superponen evitándose las interferencias. Se usa en 802.11b
  - **Multiplexión por división de la frecuencia ortogonal** (OFDM, *Orthogonal Frequency Division Multiplexing*) Al igual que DSSS usa varios canales no superpuestos. Se usa en 802.11a y 802.11g

# IEEE802.11

## Canales DSSS superpuestos en 2.4 GHz





# IEEE802.11

## Estándares IEEE802.11

Característica	802.11a	802.11b	802.11g
Año de ratificación	1999	1999	2003
Velocidad <b>máxima</b> usando DSSS	---	11 Mbps	11 Mbps
Velocidad <b>máxima</b> usando OFDM	54 Mbps	---	54 Mbps
Banda de frecuencia	5 GHz	2,4 GHz	2,4 GHz
Canales (no superpuestos)	23 (12)	11 (3)	11 (3)
Velocidades requeridas por el estándar (Mbps)	6;12;24	1;2;5.5;11	6;12;24



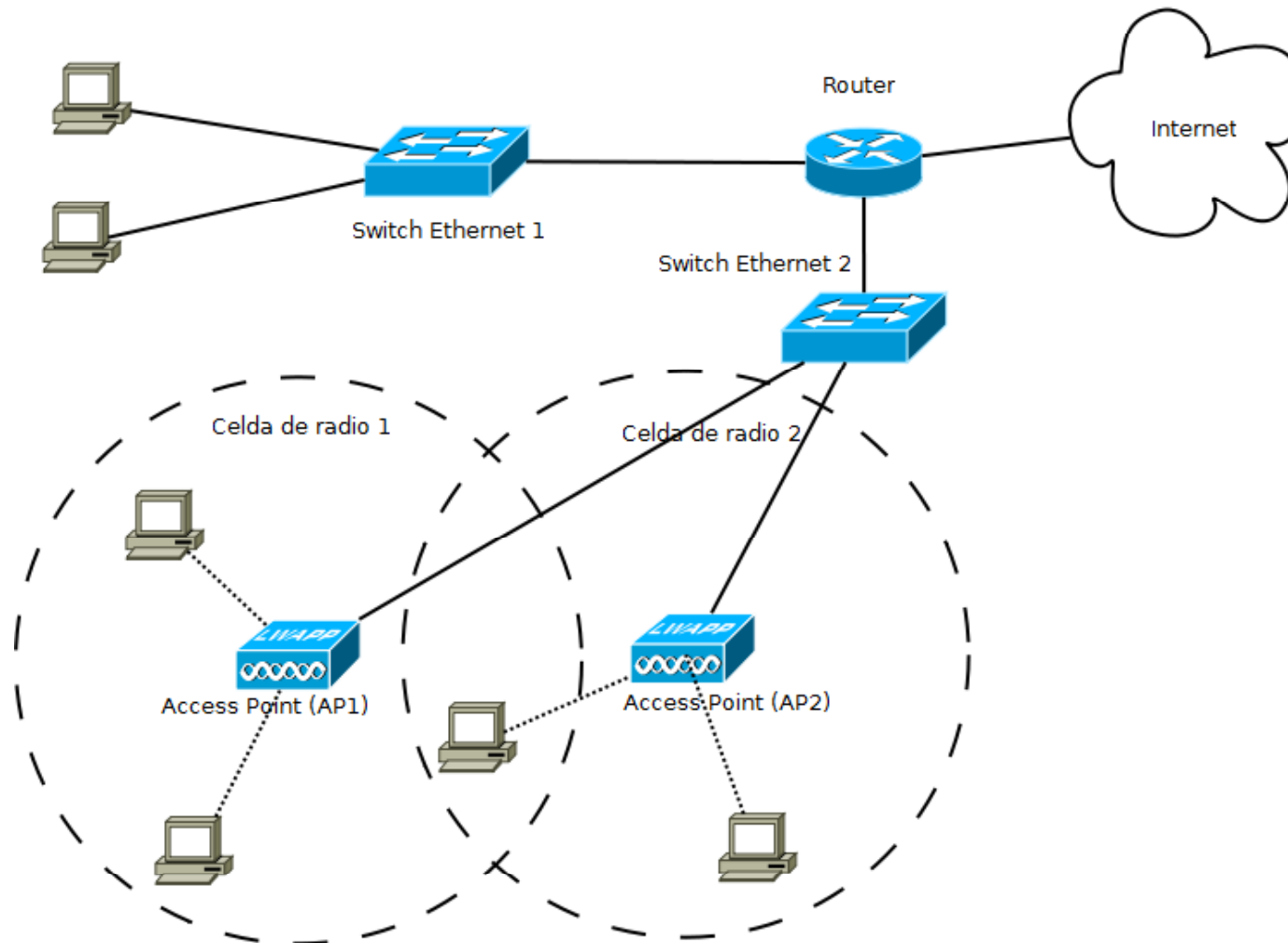
## IEEE802.11

# Modos de funcionamiento de una WLAN

Modo	Nombre de conjunto del servicio	Descripción
Ad hoc	Conjunto de servicios básico e independiente (IBSS, <i>Independent Basic Service Set</i> )	Permite que dos dispositivos se comuniquen directamente. No se necesita AP.
Infraestructura (Un AP)	Conjunto de servicios básico (BSS, <i>Basic Service Set</i> )	Una sola WLAN creada con un AP y todos los dispositivos conectados a ese AP
Infraestructura (Más de un AP)	Conjunto de servicios extendido (ESS, <i>Extended Service Set</i> )	Varios Aps crean una WLAN, permitiendo el tránsito y un área de cobertura más grande

# IEEE802.11

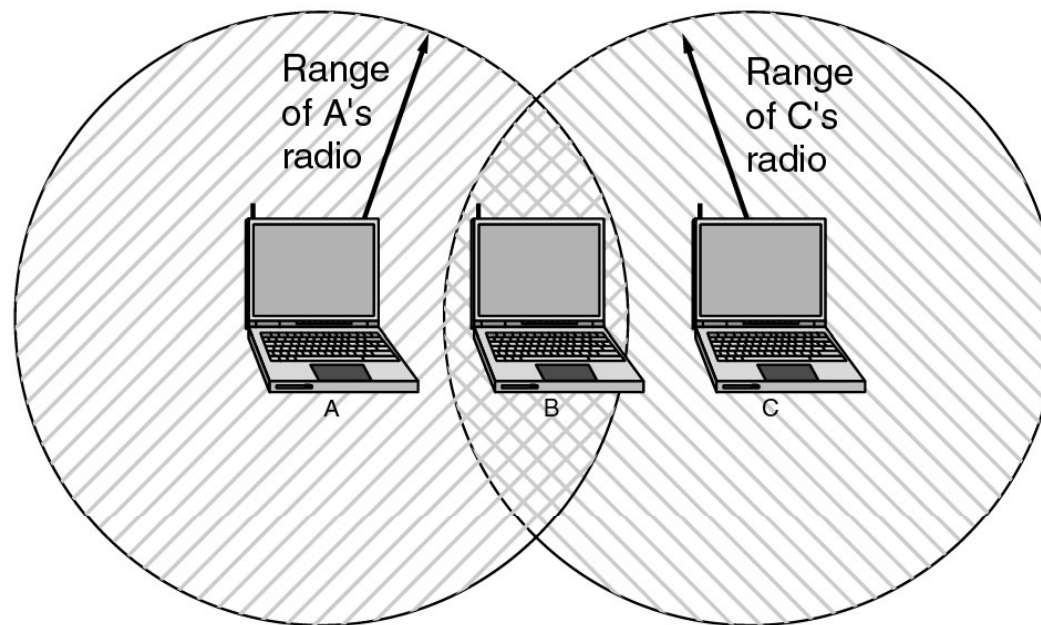
## Infraestructura (Más de un AP)



# IEEE802.11

## Alcance máximo

- El rango de una estación puede no cubrir a todo el sistema



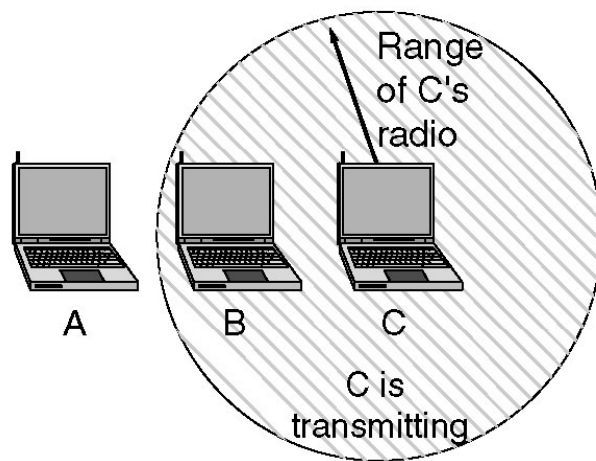


# IEEE802.11

## Capa MAC

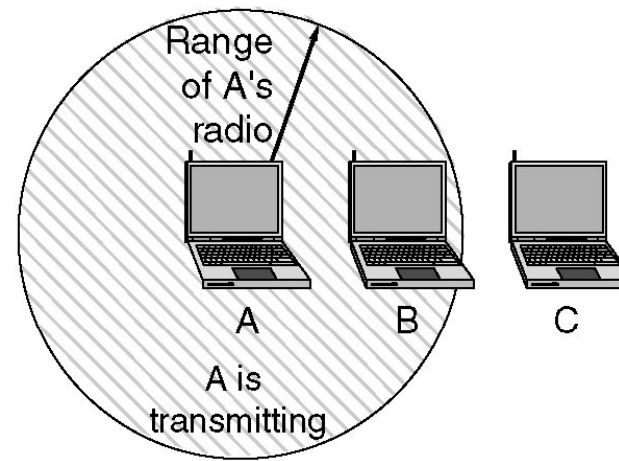
- Nuevos problemas de transmisión que producen colisiones
  - Problema de la estación oculta
  - Problema de la estación expuesta

A wants to send to B  
but cannot hear that  
B is busy



(a)

B wants to send to C  
but mistakenly thinks  
the transmission will fail



(b)



## IEEE802.11

# Mecanismos de acceso al medio

- Función de coordinación puntual (FCP)
  - Se utiliza una estación base para controlar toda la actividad de la celda
- Función de Coordinación distribuida (FCD)
  - No utiliza ningún tipo de control central
  - Existen dos versiones:
    - Similar al usado en Ethernet pero que emite la trama completa y se tarda más en detectar las colisiones
    - MACAW (*Multiple Access with Collision Avoidance for Wireless*). Define canales virtuales



## IEEE802.11

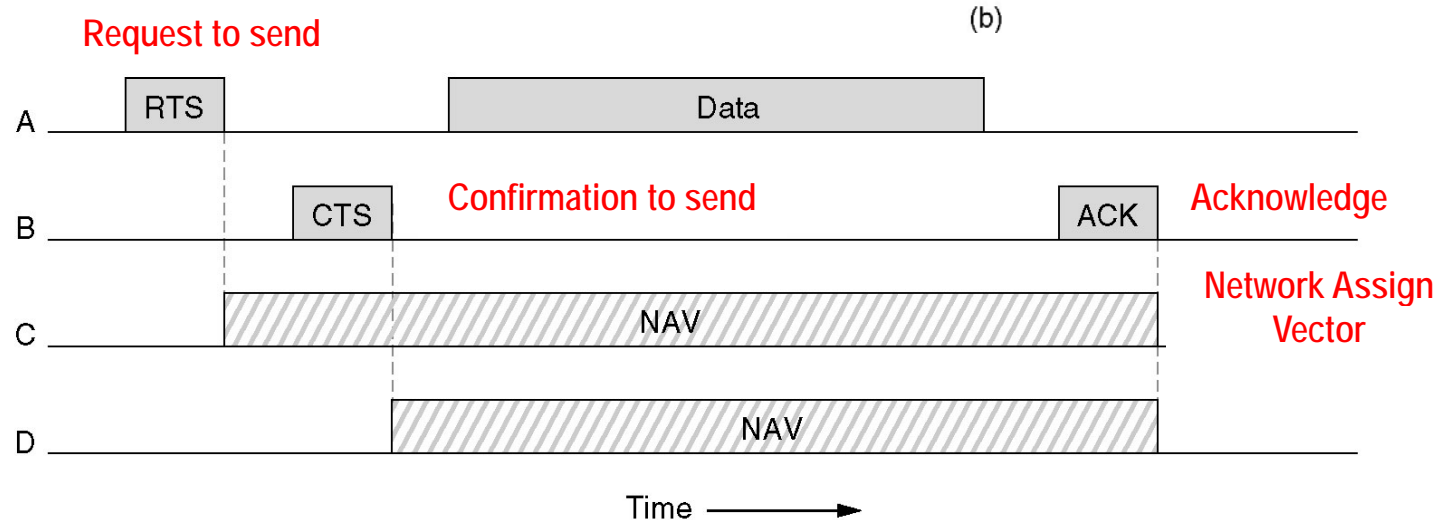
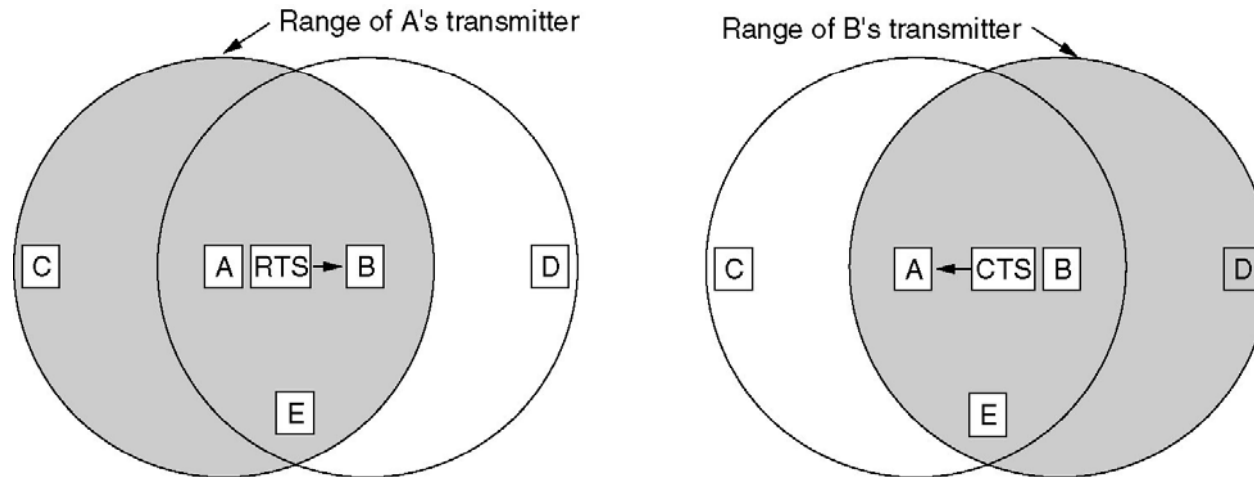
# Mecanismos de acceso al medio (MAC)

### ■ Uso de CSMA/CA:

1. Escuchar para asegurarse de que el medio no está ocupado (no se detectan ondas de radio en las frecuencias que se van a utilizar)
2. Establecer un temporizador de espera aleatorio antes de enviar una trama (para reducir la posibilidad de que todos intenten enviar simultáneamente)
3. Al expirar el temporizador, volver a escuchar el medio para comprobar que no está ocupado. Si no lo está, enviar la trama, si lo está volver a 2.
4. Una vez enviada la trama esperar acuse de recibo (ACK)
5. Si no se recibe ACK volver a enviar la trama

# IEEE802.11

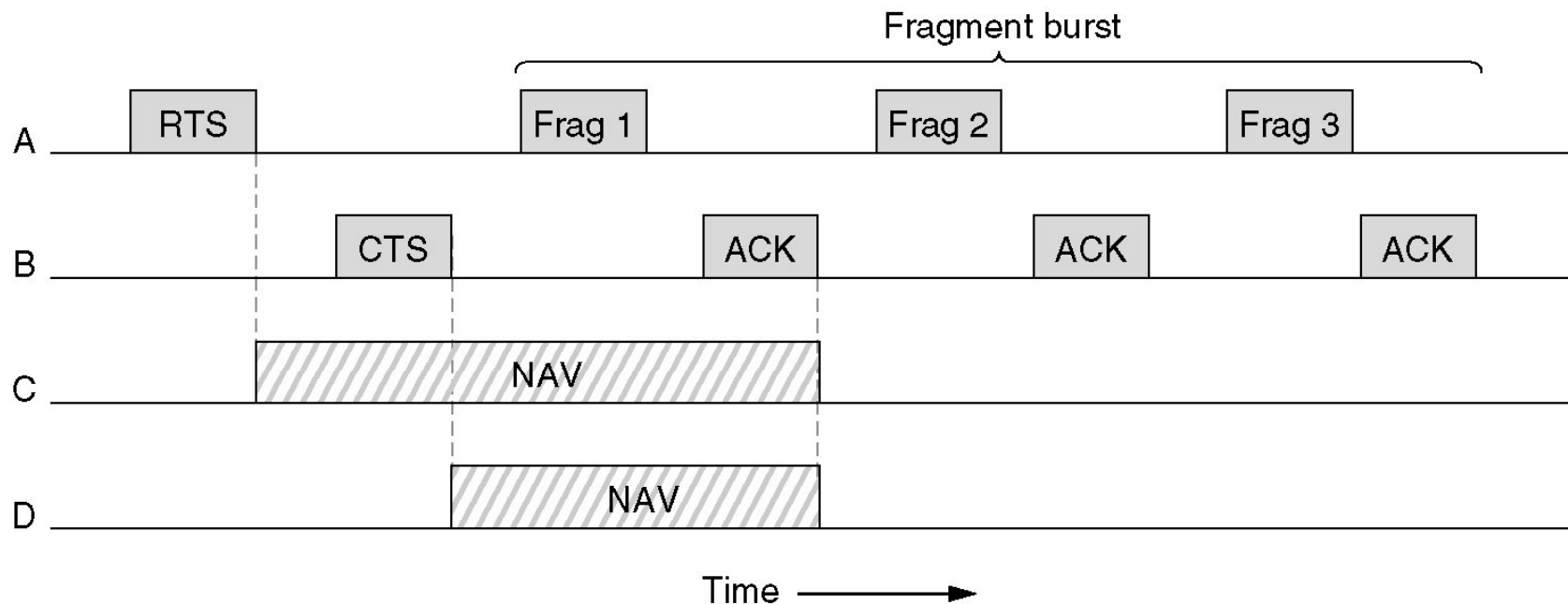
## Funcionamiento MACAW



# IEEE802.11

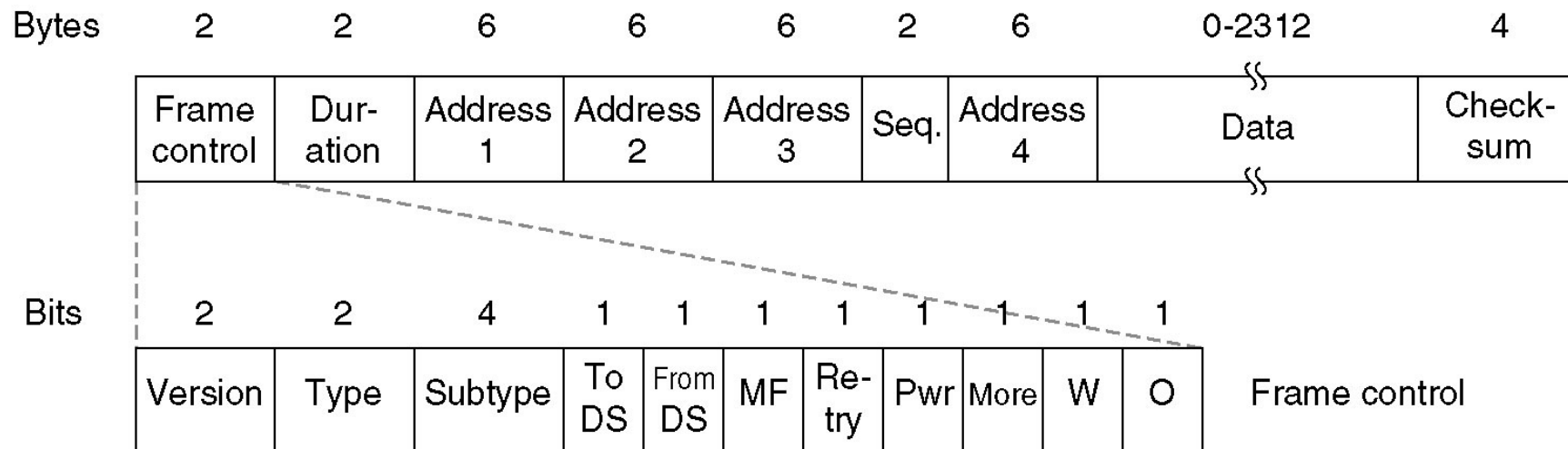
## MACAW

- La tasa de errores en redes inalámbricas es mucho mayor que en redes cableadas
  - Se utilizan mecanismos de corrección de errores
  - Se fragmentan los paquetes para conseguir una mejor tasa de transmisión efectiva



# IEEE802.11

## Formato de las tramas





## IEEE802.11

# Formato de las tramas (Trama de control)

- ❑ **Version:** Permite coexistir varios protocolos en una celda
- ❑ **Type:** Datos / Control / Administración
- ❑ **Subtype:** RTS (*Request to Send*) / CTS (*Confirmation to send*)/ otros..
- ❑ **To / From DS** (*Distribution System*): La trama va de un sistema de una celda a otra
- ❑ **MF** (*More Fragments*): Siguen más fragmentos
- ❑ **Retry:** Retransmisión de una trama enviada previamente
- ❑ **Pwr:** Administración de energía. Se usa para poner a hibernar o activar un dispositivo de la red
- ❑ **More:** Indica que el emisor tiene más tramas para el receptor
- ❑ **W:** Indica que el contenido de la trama (*Data*) se ha codificado usando el algoritmo WEP
- ❑ **O** (*Order*): Indica que la secuencia de tramas debe procesarse en orden estricto



## IEEE802.11

### Formato de las tramas (Resto)

- ❑ **Duration:** Indica cuánto tiempo ocuparán el canal la trama y la confirmación de recepción (ACK)
- ❑ **Address 1-4:** Direcciones origen y destino. Las otras dos direcciones se usan para gestionar el tráfico entre celdas
- ❑ **Seq:** Permite numerar las tramas
- ❑ **Data:** Contenido de la trama
- ❑ **Checksum:** Control de errores





## IEEE802.11

# SSID (*Service Set Identifier*)

- ¿Qué es el SSID?
  - ❑ Es un nombre incluido en todos los paquetes de la red inalámbrica.
  - ❑ A menudo se le conoce como el nombre de la red
  - ❑ Máximo de 32 caracteres
  - ❑ Definen una red lógica: Todos los dispositivos que se comunican entre sí deben compartir el mismo SSID
  - ❑ Se pueden proteger las redes desactivando la difusión (*broadcast*) del SSID, de forma que no aparece como una red en uso
  - ❑ Debe combinarse con otros métodos de defensa para proteger una red inalámbrica.
  - ❑ Se suelen usar diferentes métodos de cifrado y autenticación



# Seguridad

## Problemas de seguridad


- Las redes inalámbricas son más vulnerables que las redes cableadas por tanto requieren mayores niveles de seguridad
  - ☐ Robo de información
  - ☐ Acceso a los hosts de la parte cableada de la red
  - ☐ Denegación de servicios
  - ☐ Suplantación de identidades
  - ☐ Etc.



# Seguridad

## Principales Vulnerabilidades de las WLAN

- **War drivers:** El atacante busca una conexión gratuita a Internet. Se buscan aquellos AP sin seguridad o con seguridad débil
- **Hackers:** Buscan encontrar información o denegar servicios.  
Objetivo: Comprometer los hosts de la red cableada sin pasar por los cortafuegos
  - *Denial of Service (DoS)*
- **Técnicos:** Cuidado con las configuraciones por defecto (sin seguridad o con niveles de seguridad bajos)
- **AP falso:** El atacante captura los paquetes de la WLAN para buscar el SSID y romper las contraseñas (si se usan). Después el atacante sustituye el AP con un AP propio (con la misma configuración de red) para capturar el tráfico y analizarlo offline
  - The man in the middle (MITM)



# Seguridad

## Soluciones

- Autenticación mutua:
  - **Asegurar que cada nodo es quien dice ser**
  - Autenticación entre el cliente y el AP. Se usan contraseñas secretas (clave) tanto en el cliente como en el AP. Hace uso de algoritmos matemáticos complejos (p.e. clave privada / pública) para evitar enviar las claves por el aire. Evita la suplantación del AP.
- Cifrado:
  - El cifrado usa una clave secreta y un algoritmo matemático para desordenar el contenido de la trama WLAN.
- Herramientas de intrusión:
  - Sistemas de detección de intrusión
  - Sistemas de prevención de intrusión



# Seguridad

## Estándares de seguridad WLAN

Nombre	Año	Definido por:
Privacidad equivalente al cableado ( <i>Wired Equivalent Privacy - WEP</i> )	1997	IEEE
Acceso Protegido Wi-Fi ( <i>Wi-Fi Protected Access, WPA</i> )	2003	Alianza Wi-Fi
IEEE802.11i / WPA2	2005	IEEE



## Seguridad

# Criptografía simétrica vs. Asimétrica

- **Criptografía simétrica:** Se usa la misma clave para cifrar y descifrar mensajes. Los dos extremos acuerdan de antemano la clave a usar. El remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.
- **Criptografía asimétrica:** Se usan un par de claves para el envío de mensajes. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez.
- **Criptografía híbrida:** Utiliza criptografía asimétrica para la distribución de las claves y criptografía simétrica para la encriptación de los mensajes.



# Seguridad WEP

- Estándar de seguridad 802.11 original
- Proporciona servicios de autenticación y cifrado
- Nivel de seguridad débil
  - **Claves precompartidas estáticas:** El valor de la clave se configura en cada cliente y AP. Frecuentemente las claves no se cambian regularmente.
  - **Claves fáciles de reventar:** WEP usa claves cortas. Es posible obtener la clave a partir de las tramas copiadas de la WLAN.
  - **Hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos.**
- Mejoras de seguridad
  - **Enmascaramiento del SSID:** El AP no envía el SSID para que los clientes se conecten
  - **Filtrado de direcciones MAC:** El AP puede configurarse para que sólo acepte tramas de un conjunto de direcciones MAC.




# Seguridad

## WPA

- Resuelve muchos problemas de WEP
- Estándar de seguridad multifabricante. Estándar industrial de facto
- Encriptación:
  - TKIP (*Temporal Key Integrity Protocol*): Protocolo que permite el intercambio dinámico de claves
  - AES (*Advanced Encryption Standard*): Criptografía simétrica. Usa un esquema de cifrado por bloques.
- Autenticación de usuarios:
  - Mediante un servidor que almacena las credenciales y contraseñas de los usuarios (IEEE802.1X) - WPA - Enterprise
  - En base a claves precompartidas – WPA - Personal
- Ventajas:
  - Mejora mucho la seguridad en comparación con WEP
  - Gran soporte por parte de las empresas





# Seguridad

## WPA-2

- Implementa el estándar IEEE802.11i
- No es compatible con WPA
- Principales características:
  - Intercambio dinámico de clave
  - Cifrado mucho más fuerte (AES, basado en el algoritmo de Rijndael, 2005)
  - Autenticación de usuarios
- Permite usar AES: Mayor seguridad que WEP
- Ventajas:
  - Mejora mucho la seguridad en comparación con WEP
  - Gran soporte por parte de las empresas