

Redes de computadoras

Introducción

Objetivos

- Fortalecer los conceptos básicos de las redes modernas de comunicaciones
- Identificar los principales retos y tendencias de las redes informáticas
- Configurar y desplegar redes de comunicaciones contemporáneas

Evolución de las redes de computadoras

ARPANET, in full Advanced Research Projects Agency Network, experimental computer network that was the forerunner of the Internet. The Advanced Research Projects Agency (ARPA), an arm of the U.S. Defense Department, funded the development of the Advanced Research Projects Agency Network (ARPANET) in the late 1960s. Its initial purpose was to link computers at Pentagon-funded research institutions over telephone lines.

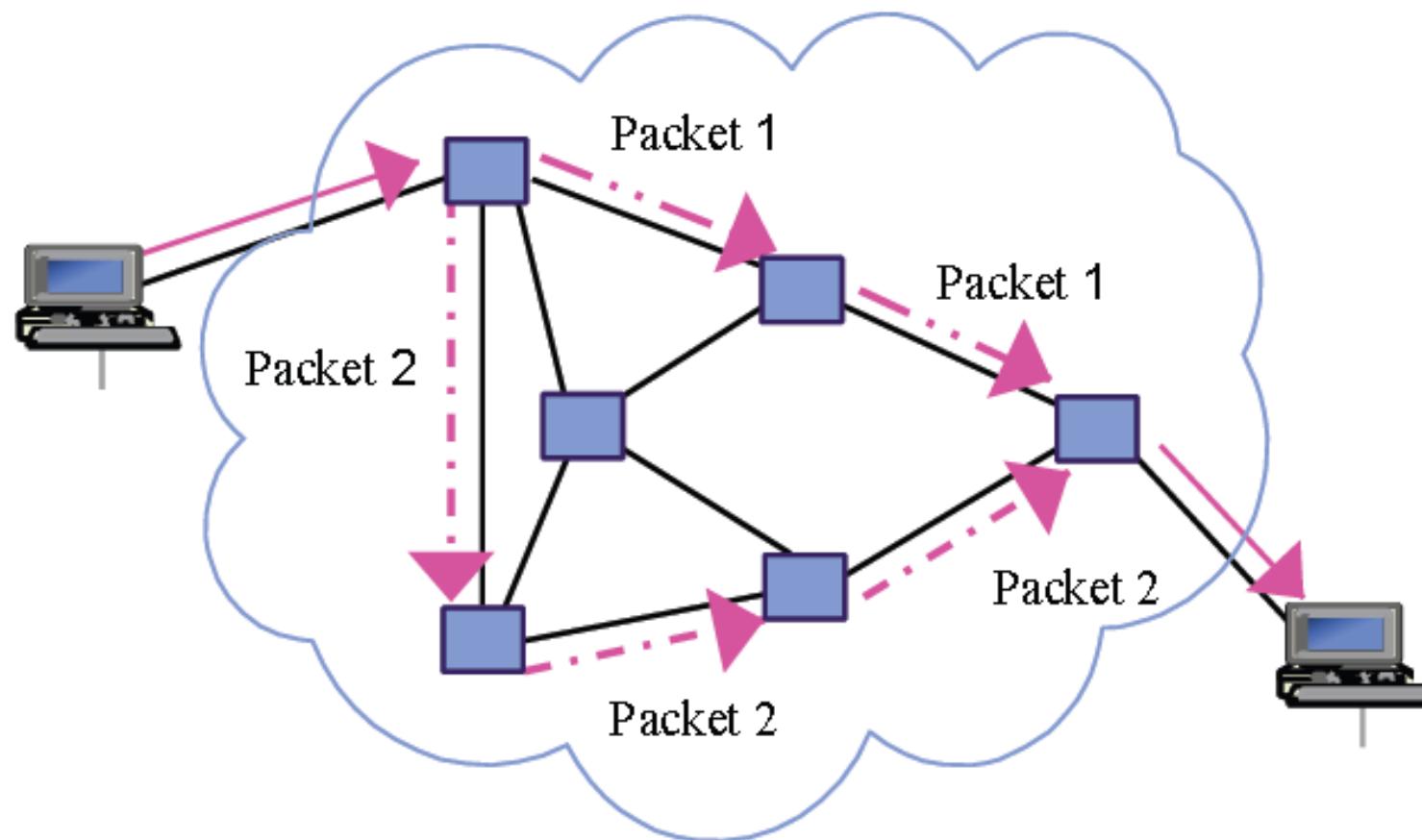
Fuente: Encyclopaedia Britannica.

Comunicación de paquetes

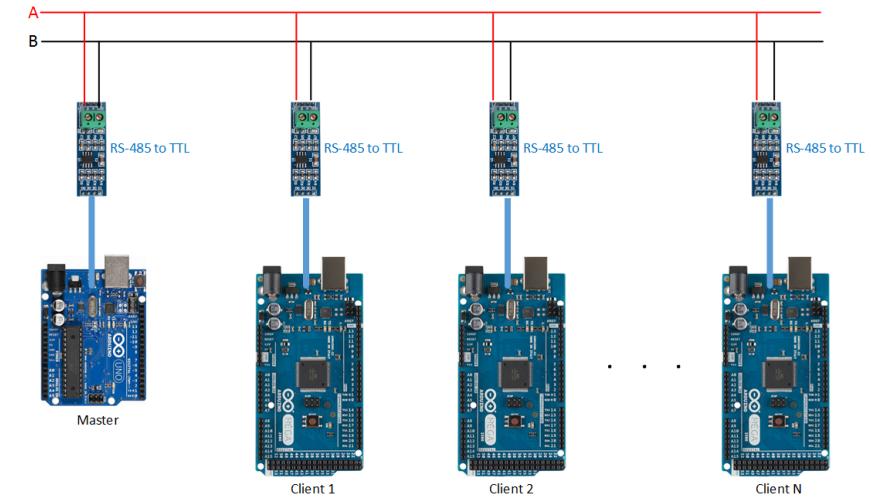
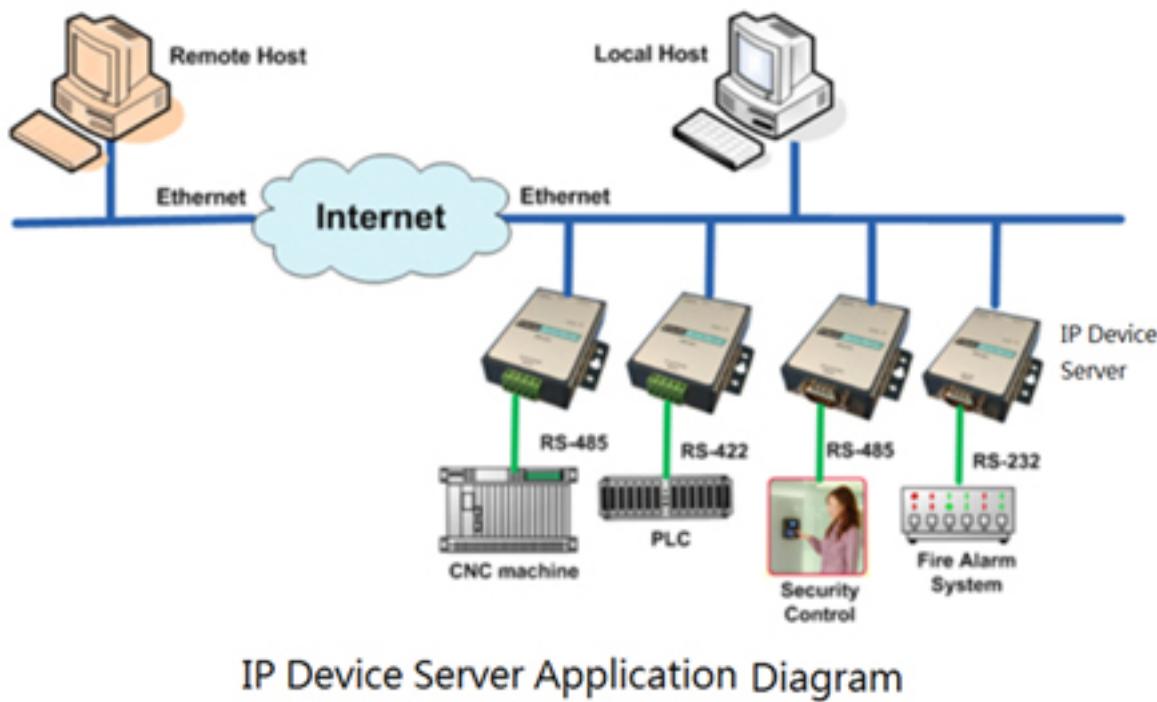
Paul Baran, a researcher at the RAND Corporation think tank, first introduced the idea. Baran was instructed to come up with a plan for a computer communications network that could survive nuclear attack and continue functioning. He came up with a process that he called “hot-potato routing,” which later became known as packet switching.



Comunicación de paquetes.



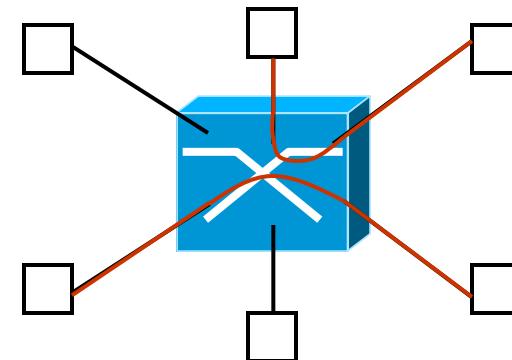
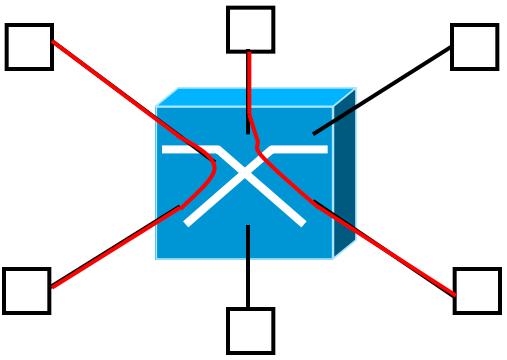
Redes de datos.



Internet de las cosas



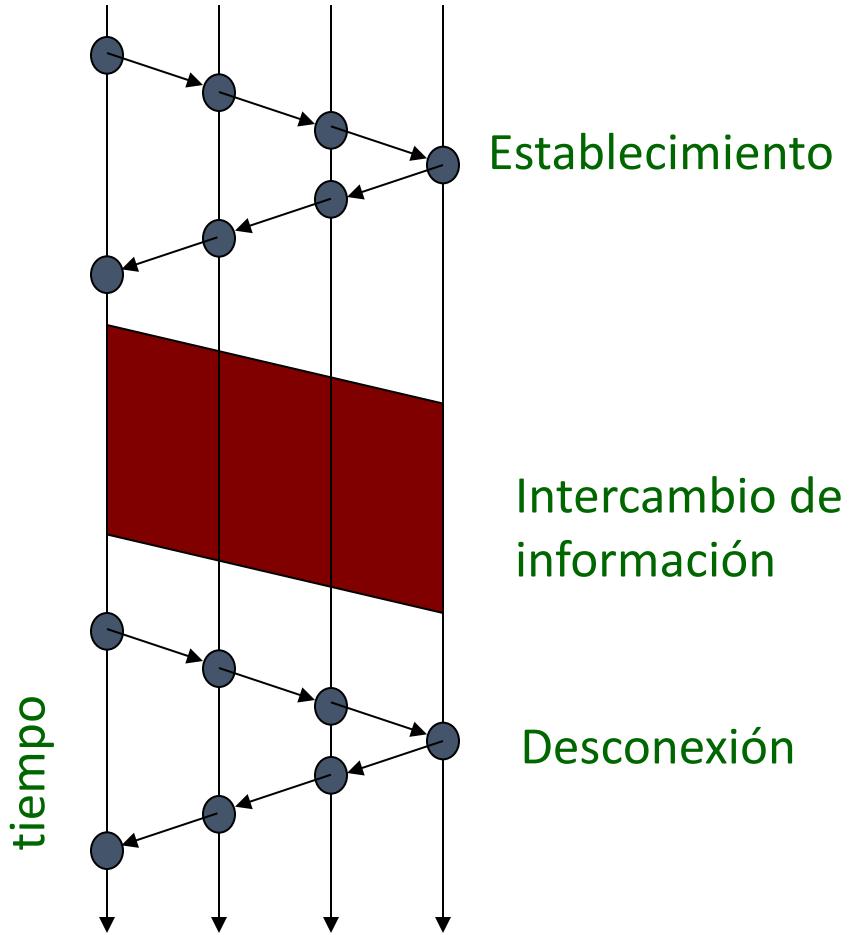
Commutación



Commutación

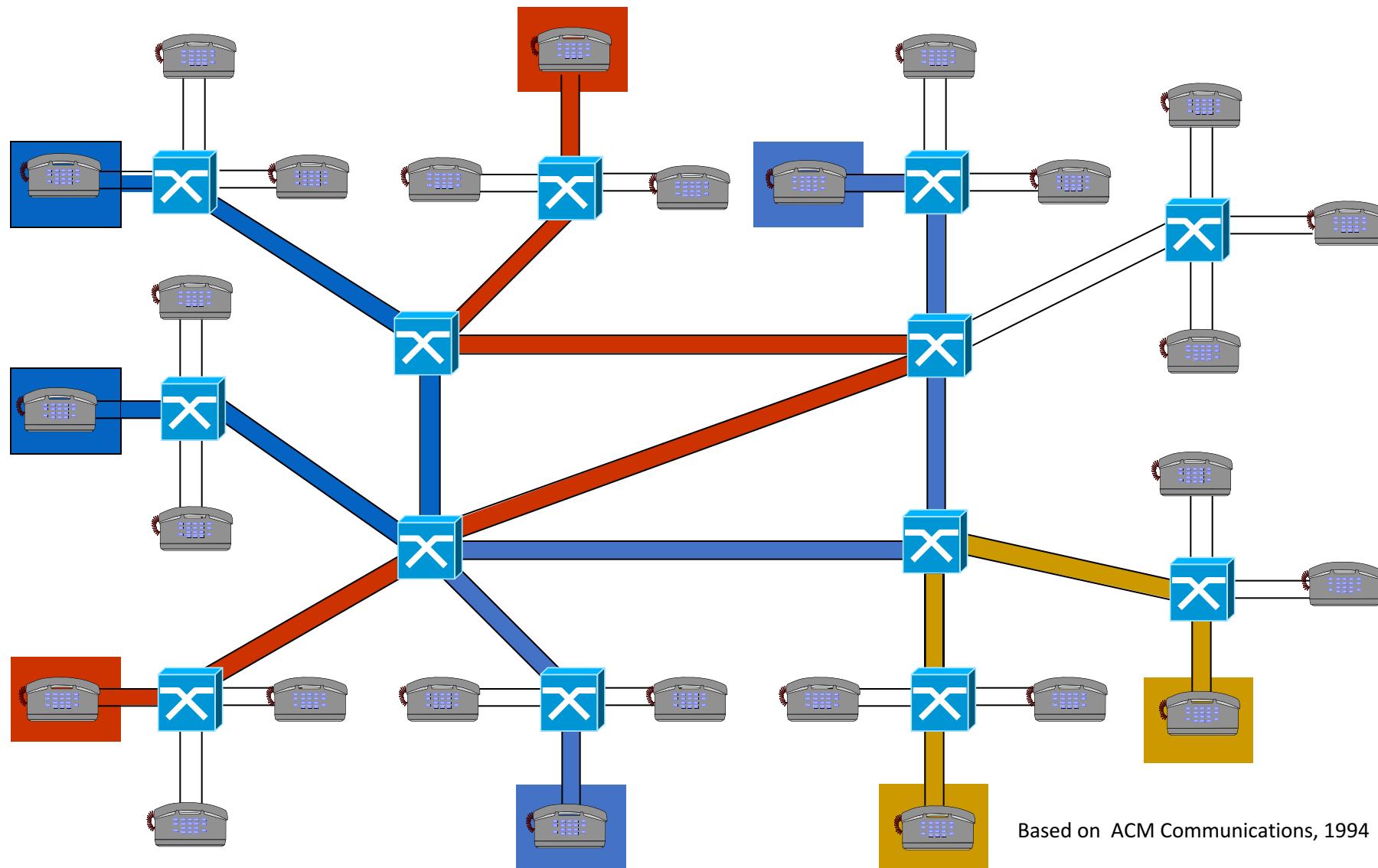
- **Circuitos:** se dedica una ruta y se reservan recursos durante la comunicación
- **Mensajes:** se forma un mensaje que incluye dirección del destinatario y se envía sin establecer una conexión. El mensaje se almacena y retransmite de nodo en nodo
- **Paquetes:** similar a la commutación de mensajes, pero éste se divide en segmentos llamados paquetes, cada uno de los cuales es transmitido individualmente
 - Circuitos Virtuales
 - Datagramas

Commutación de circuitos



- Mecanismos de señalización establecen una trayectoria a través de la cual se transfiere información
 - Reservación de recursos
 - QoS bien definida
- Una vez terminada la conversación, una fase de desconexión permite liberar los recursos reservados

Commutación de circuitos

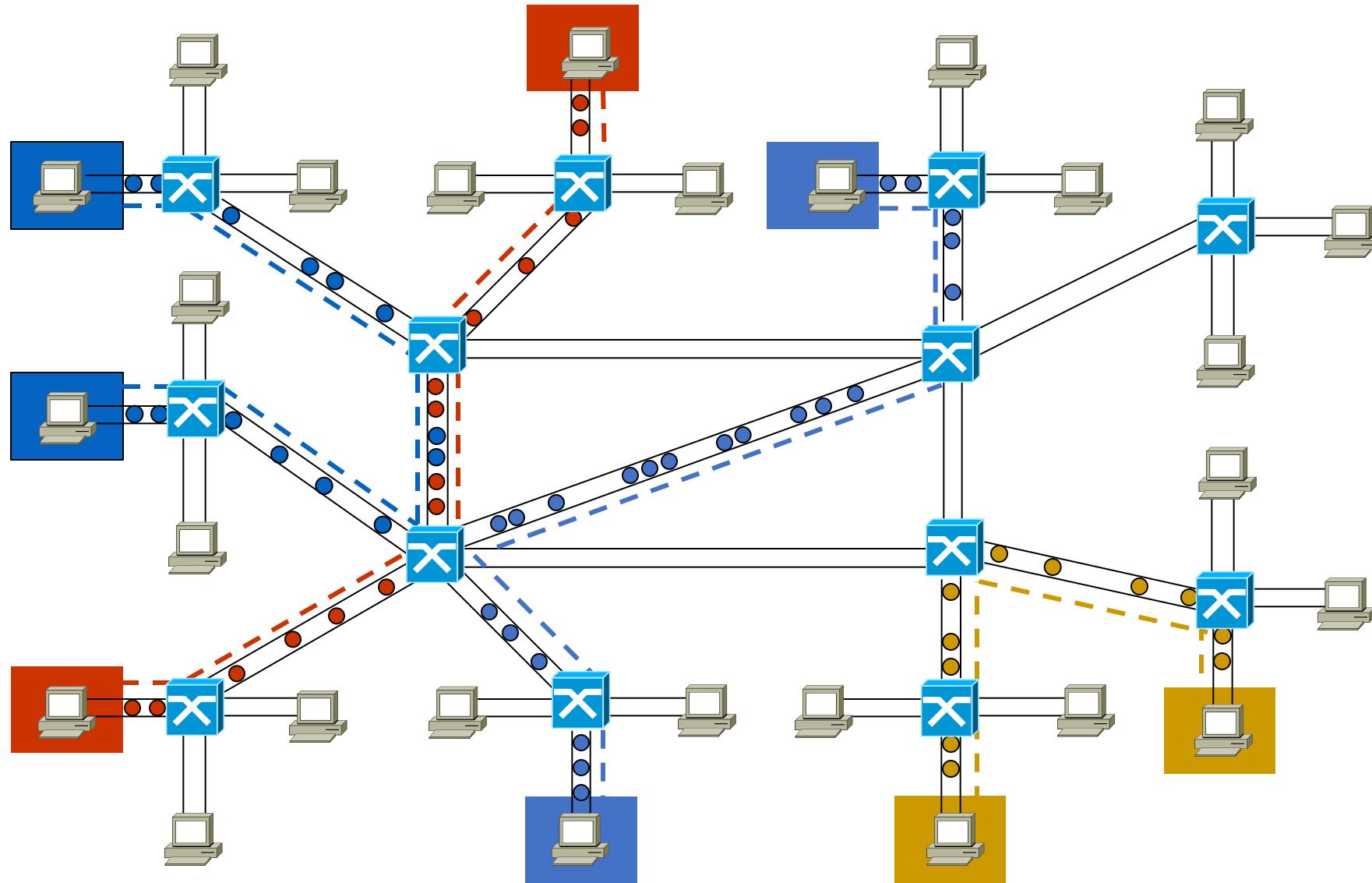


Based on ACM Communications, 1994

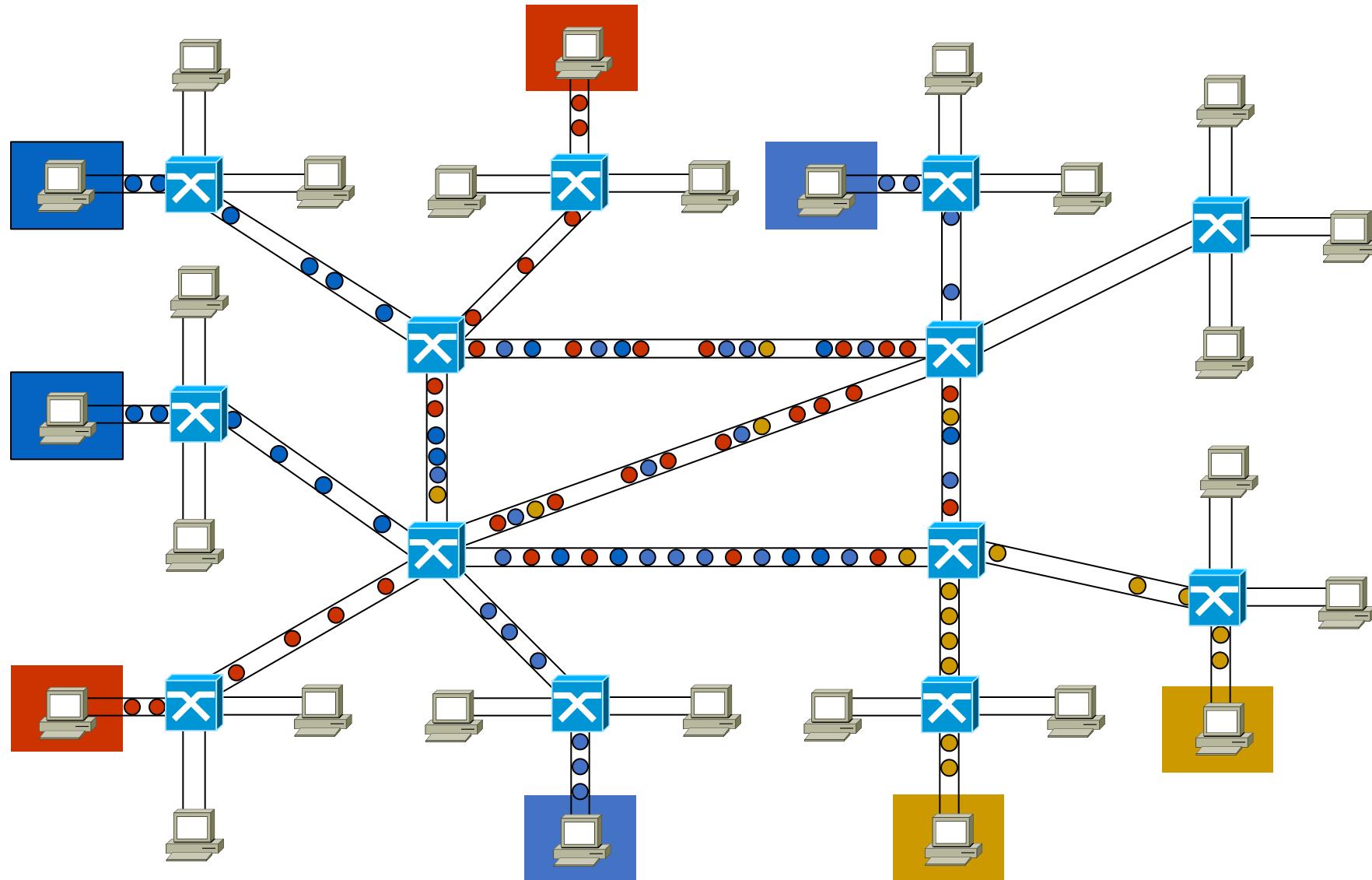
Commutación de circuitos

- Trayectoria dedicada para el flujo
- Ancho de banda y retraso definidos e invariantes
- Ideal para flujos a tasa constante con fuertes restricciones temporales (por ejemplo, conversaciones de voz)
- Reservación de recursos = alto costo independientemente del volumen intercambiado
- Inapropiado para tráfico en ráfagas (típico en servicios de datos)

Commutación de paquetes (circuitos virtuales)



Comunicación de paquetes (datagramas)



Commutación de paquetes

- Nodos de almacenamiento y re-envío
 - Retraso variable en caso de congestión
- Con datagramas, la trayectoria puede cambiar dinámicamente
- Puerto de salida determinado por tablas de commutación o enrutamiento
 - Estático o dinámico
 - Encabezado en el paquete para consultar tablas

Circuitos virtuales y datagramas

- Circuito virtual
 - Se establece una trayectoria durante la configuración del circuito. Es virtual porque los recursos físicos son compartidos, no dedicados
 - Cada paquete tiene un identificador de circuito virtual (VCI)
 - Los paquetes llegan en orden
 - Es común tener mecanismos de control de flujo
- Datagrama
 - Encabezado tiene la dirección destino final. Decisiones de ruteo basadas en este campo
 - Cada paquete se encamina de forma independiente
 - Los paquetes pueden llegar en desorden. El destino final es responsable de reordenarlos

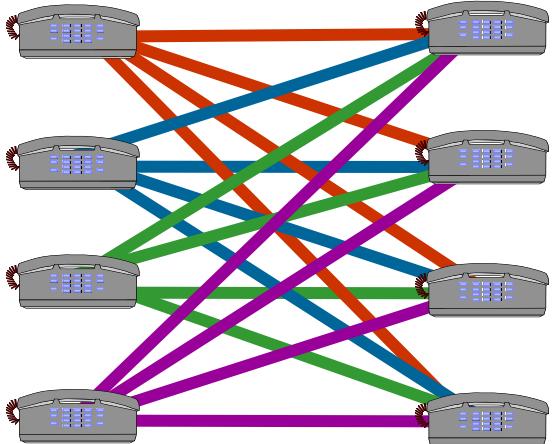
Comunicación de paquetes. Algunas ventajas

- Eficiencia
 - Enlaces compartidos por varios flujos
 - Paquetes encolados y retransmitidos tan pronto como sea posible
 - Los flujos son admitidos y transportados aún bajo condiciones de ligera congestión
- Conversión de tasas de transmisión automática
 - Puertos de entrada y salida no necesariamente operan a la misma velocidad

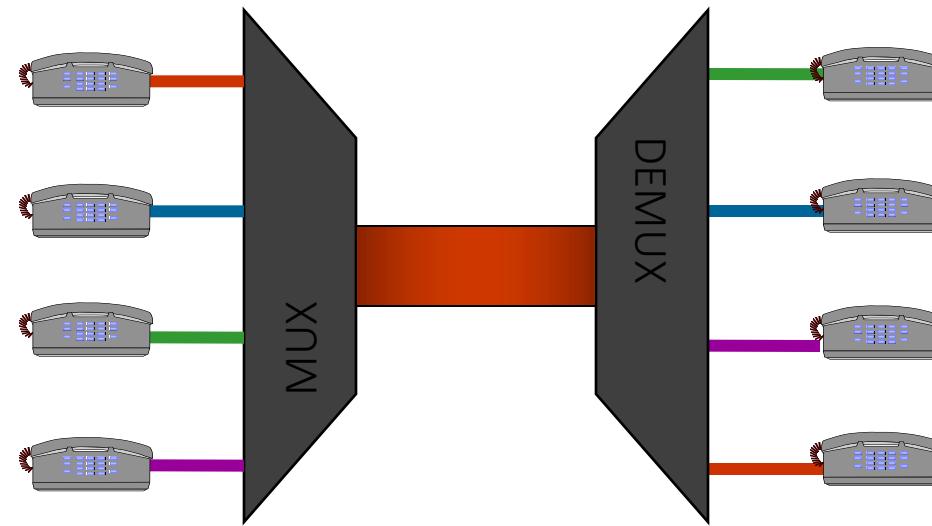
Multiplexaje

Permite la compartición de un medio de comunicación (recurso) entre varios usuarios.

Sin multiplexaje



Un canal
cuatro conexiones

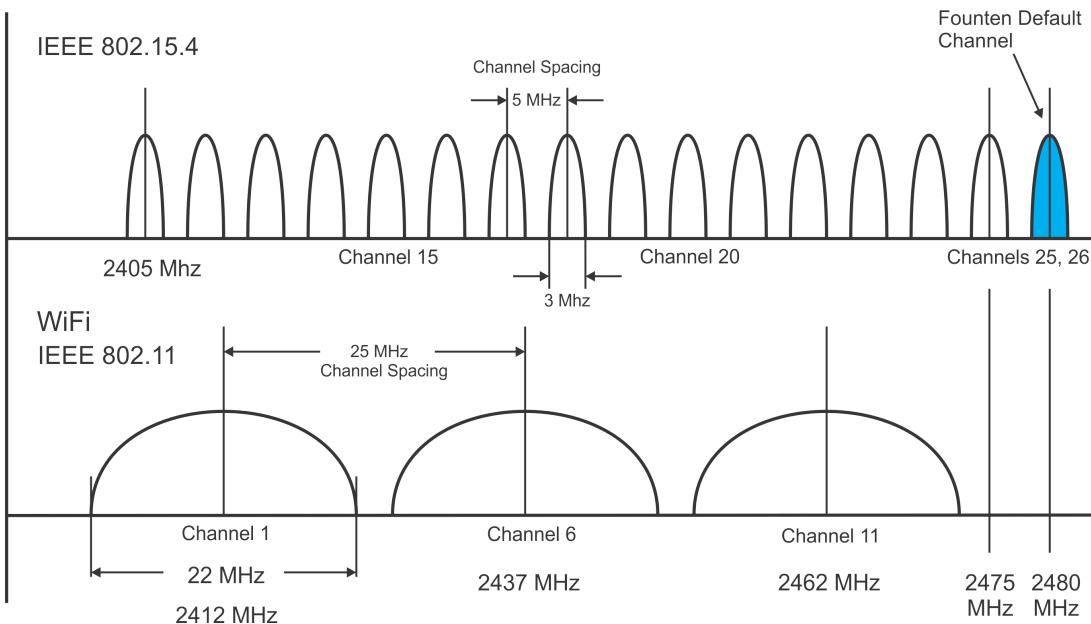


Dominios de multiplexaje

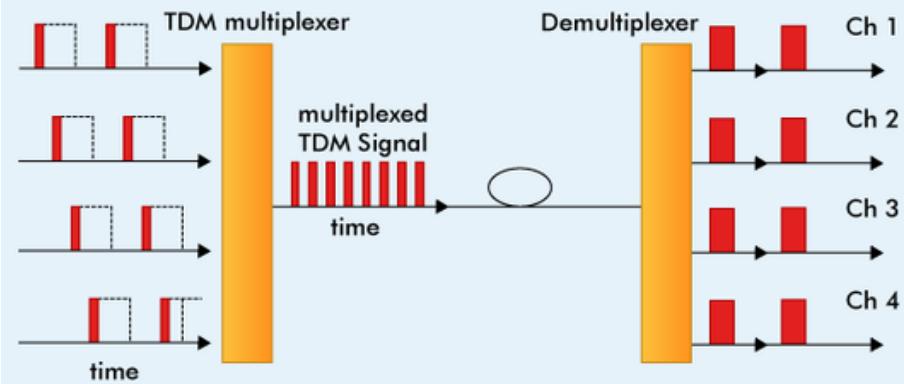
- En frecuencia: FDM
 - ... y longitud de onda: WDM
- En el tiempo: TDM
 - Síncrono
 - Asíncrono, estadístico
- Por código: CDM
- En el espacio: SDM

Multiplexaje en frecuencia

A cada comunicación (canal) se le asigna un rango de frecuencia (ancho de banda) distinto.

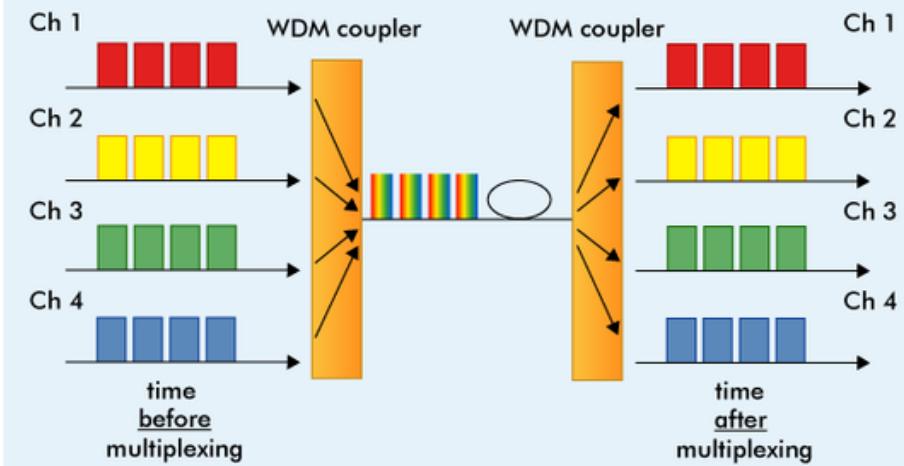


TDM (Time Division Multiplexing)



Multiplexaje en tiempo

WDM (Wavelength Division Multiplexing)



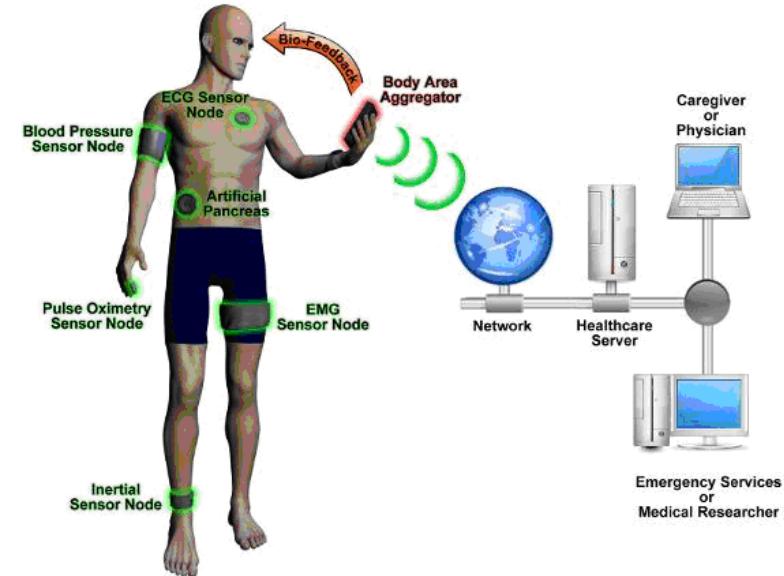
Multiplexaje en longitud de onda

Clasificación de redes

- Por el servicio que ofrecen
 - Telefonía fija y móvil, televisión, intercambio de datos, *trunking*
- Por su función en la arquitectura
 - Redes de acceso, redes de transporte
- Por la población de usuarios que las utilizan
 - redes públicas, privadas, corporativas, para el hogar
- Por su cobertura geográfica
 - BAN, PAN, LAN, CAN, MAN, WAN, GAN

Redes de área corporal (BAN)

- Cobertura de un par de metros
- Medio físico: piel o inalámbrico
- Baja velocidad
- Monitoreo de pacientes,
- Interconexión de dispositivos,
- Autenticación



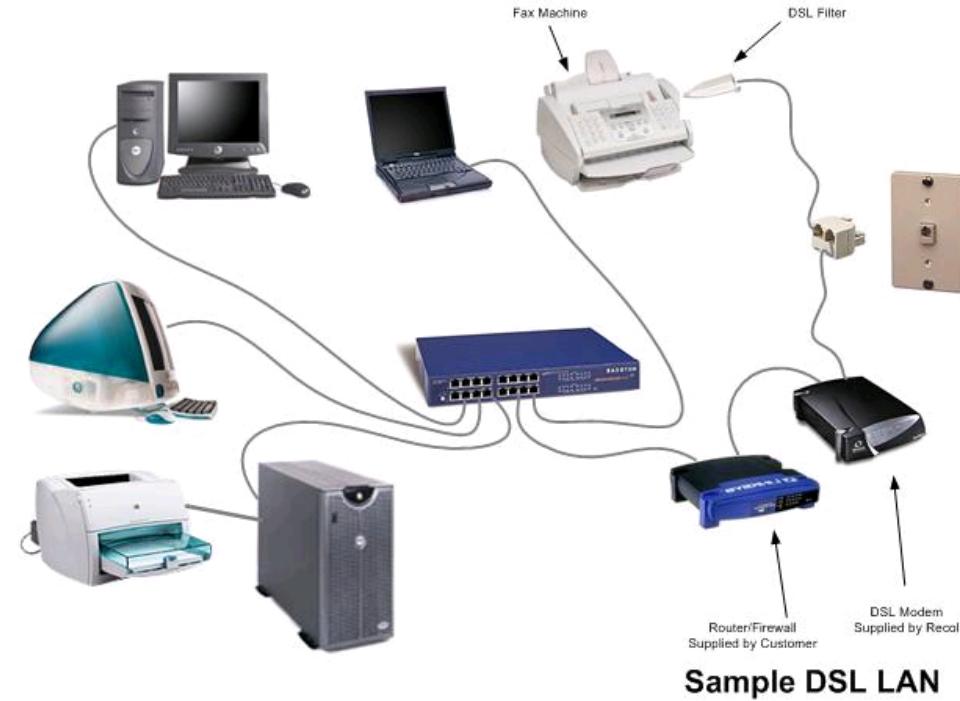
Redes de área personal (PAN)

- Cobertura diez metros
- Medio inalámbrico
- Velocidad 2.4 kb/s a 110 Mb/s
- Interconexión de dispositivos
- Ejemplos
 - Bluetooth
 - ZigBee
 - WUSB

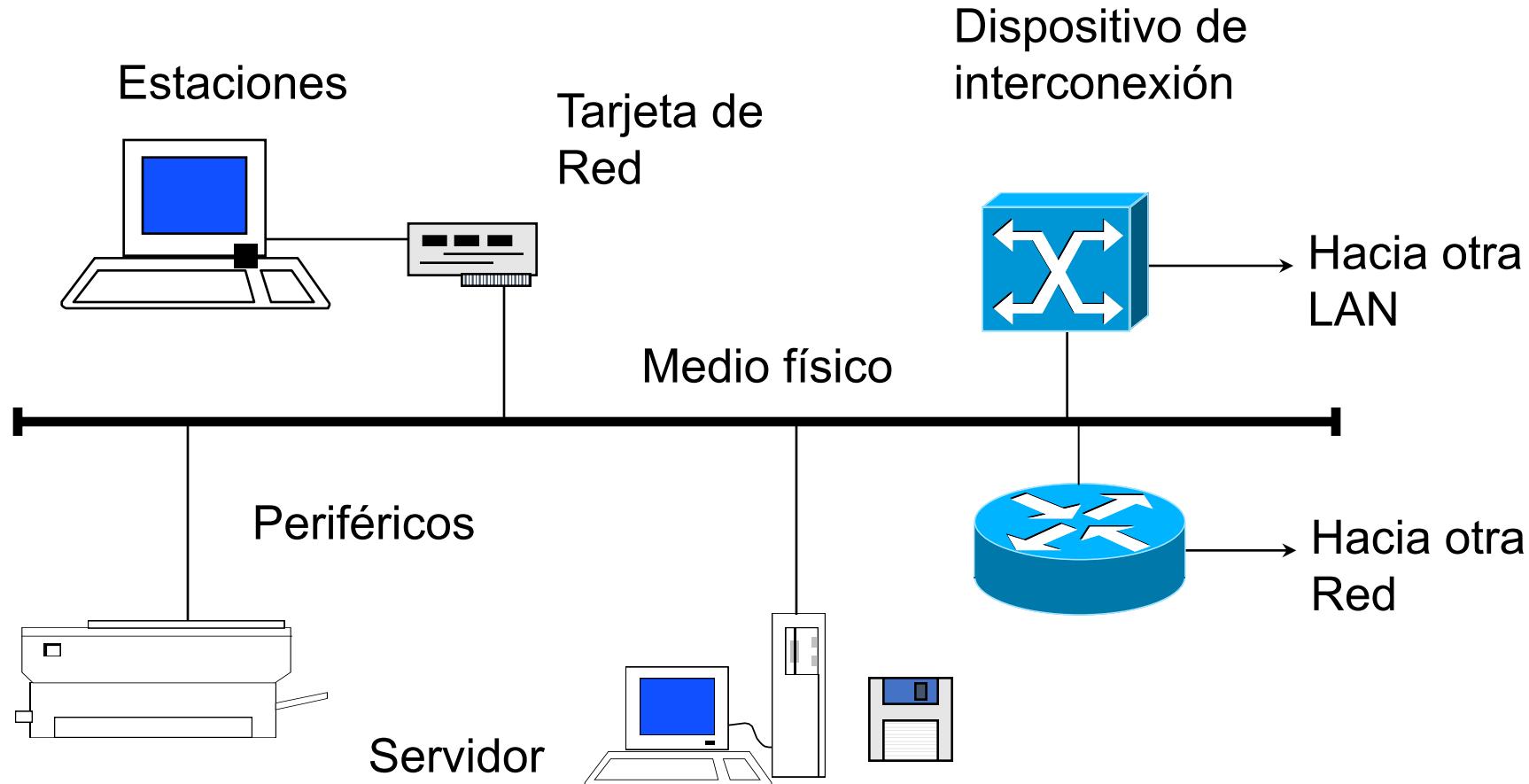


Red de área local (LAN)

- Cobertura de cientos de metros a algunos kilómetros
- Medio alambrado (cobre, fibra) e inalámbrico
- Velocidades 10 Mb/s a 10 Gb/s
- Ejemplos
 - Ethernet, 802.3
 - Token ring

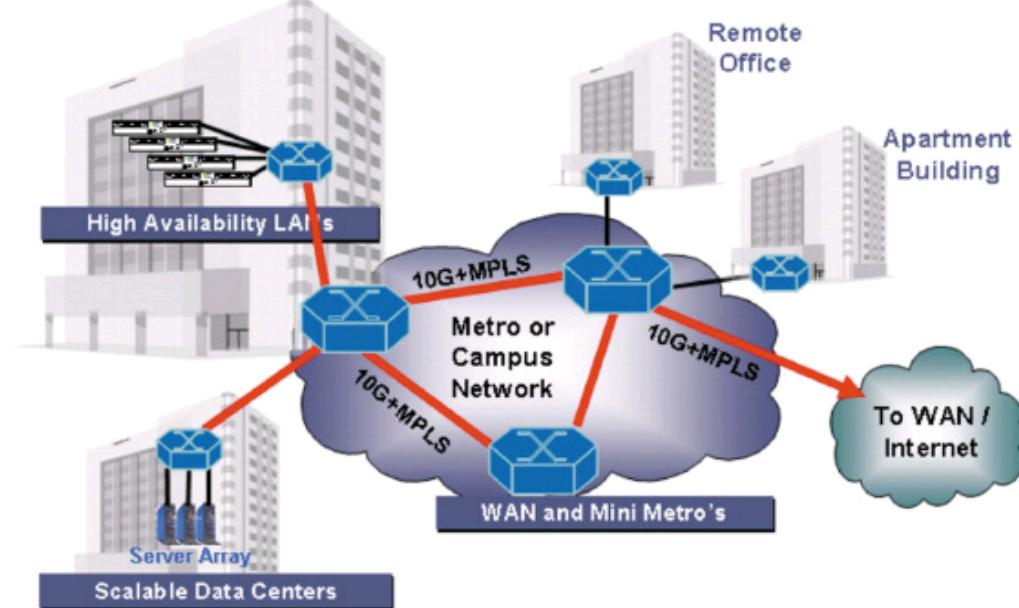


Componentes de una LAN



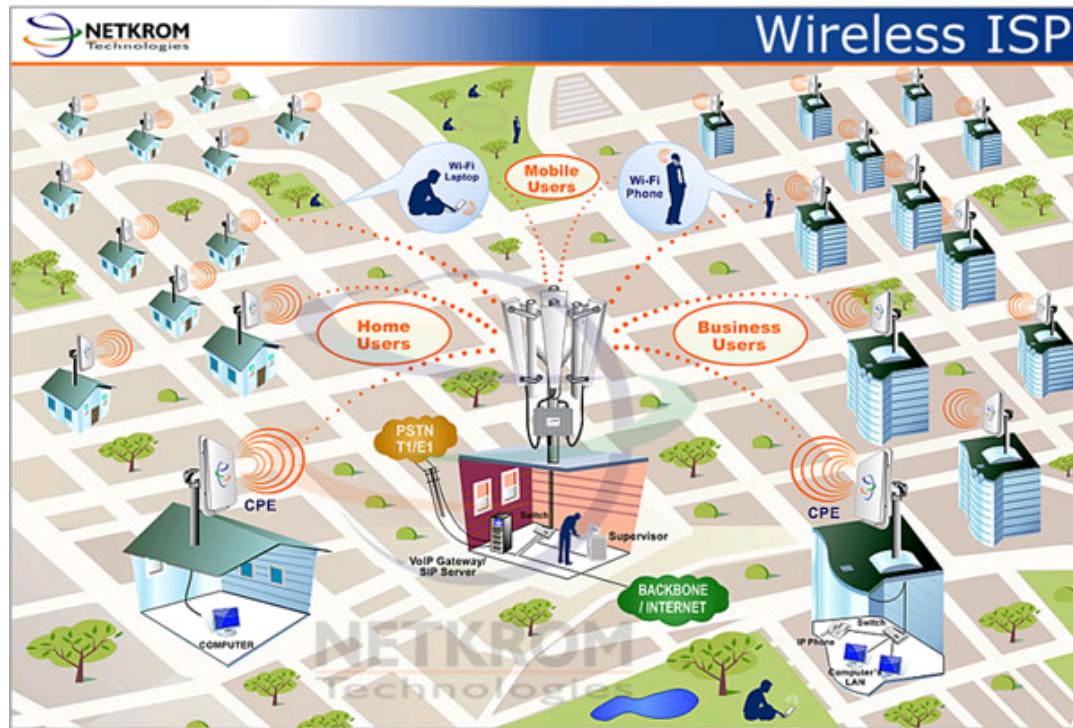
Red de área de campus (CAN)

- Cobertura de algunos kilómetros
- Medio alambrado (fibra)
- Velocidades 100 Mb/s a 10 Gb/s
- Interconecta redes locales en edificios, campus, hospitales
- Ejemplos Ethernet, ATM, FDDI



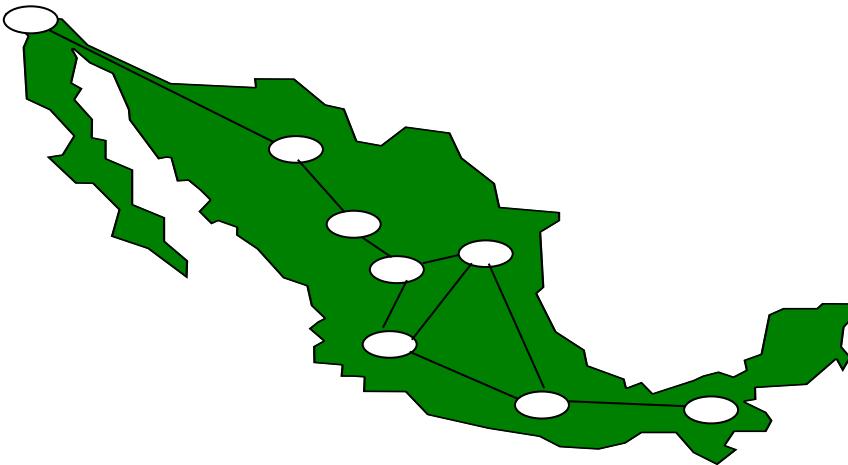
Red de área metropolitana (MAN)

- Cobertura de decenas de Km
- Medio alambrado (fibra, cobre) e inalámbrico
- Amplio rango de velocidades
- Interconecta redes locales en edificios, Redes de acceso
- Ejemplos:
MetroEthernet
WiMAX
PLC

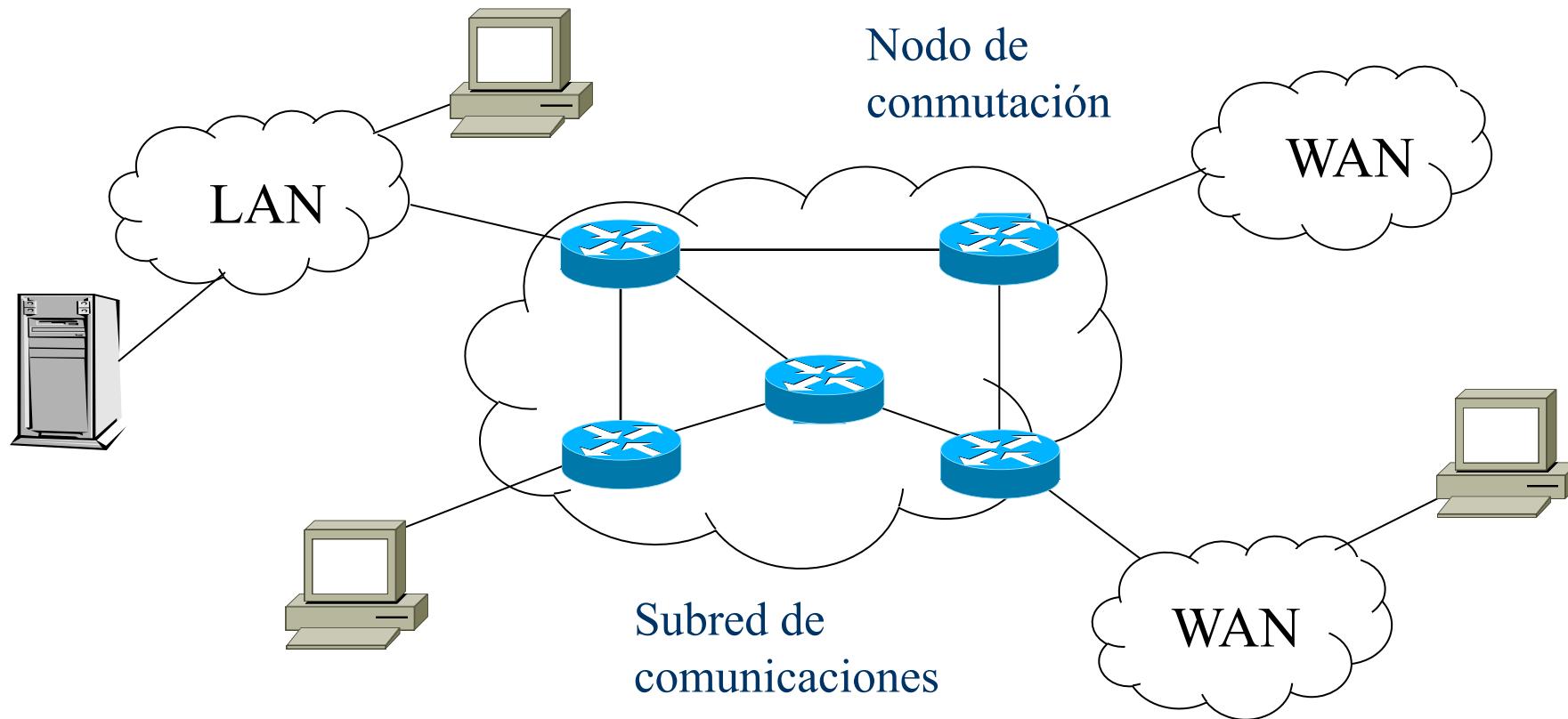


Red de área amplia (WAN)

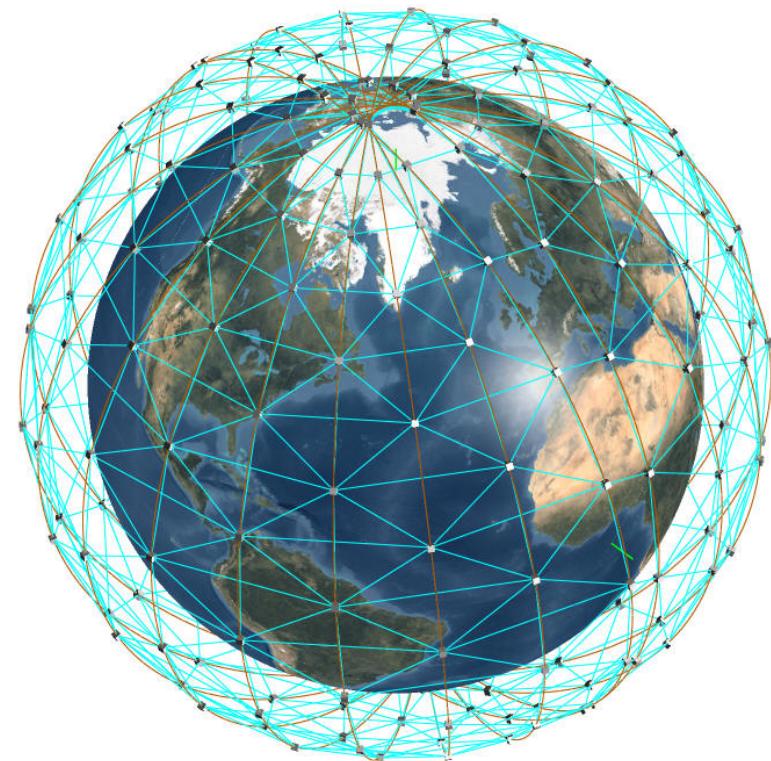
- Interconecta redes en grandes extensiones
- Muy alta velocidad con tecnologías recientes
- Ejemplos
 - SDH
 - Frame relay
 - ATM
 - DWDM



Componentes de una WAN



Redes de área global (GAN) - Internet

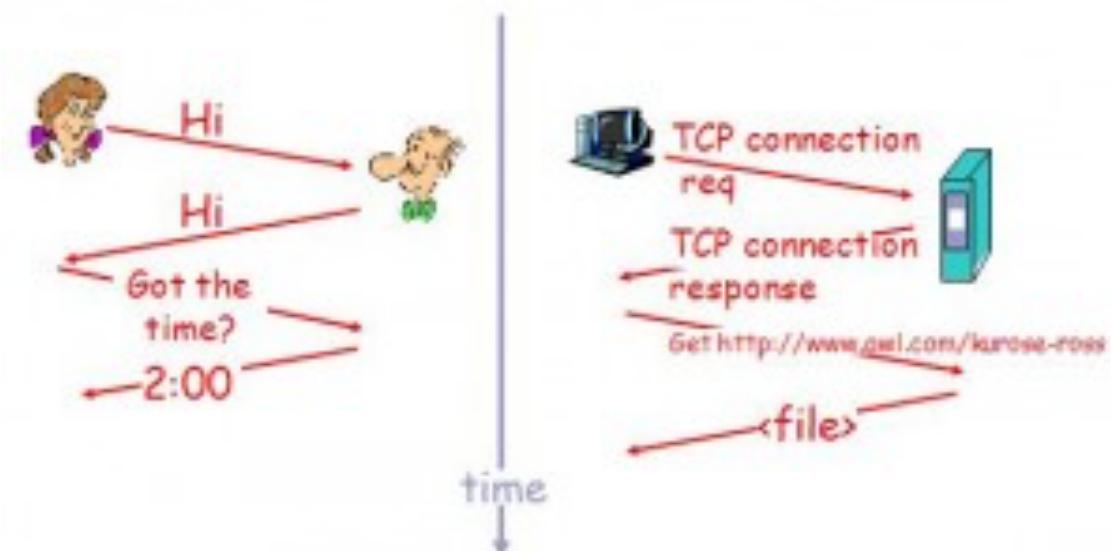


Redes de computadoras

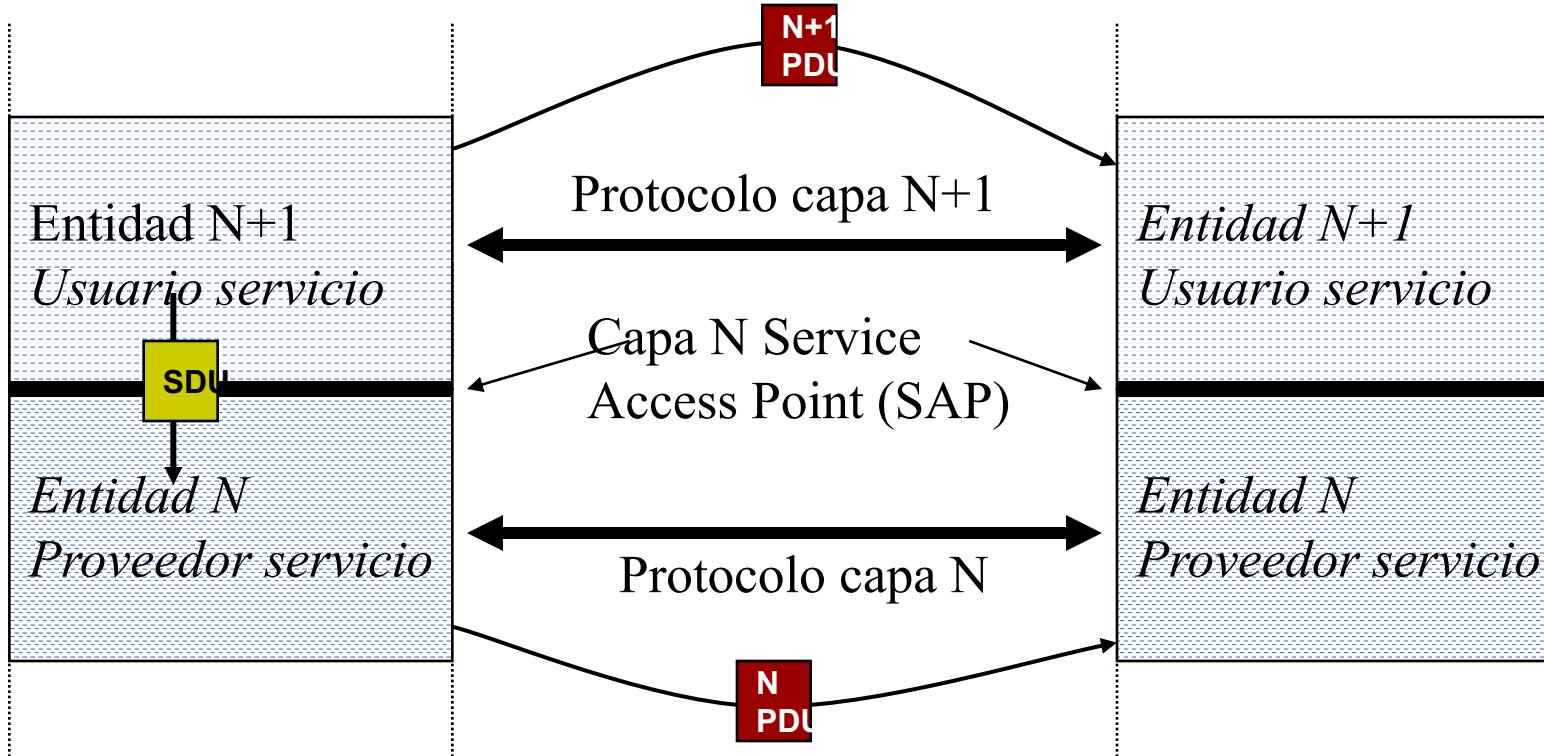
Modelos de referencia

Protocol

a human protocol and a computer network protocol:



Capas, protocolos, interfaces y servicios



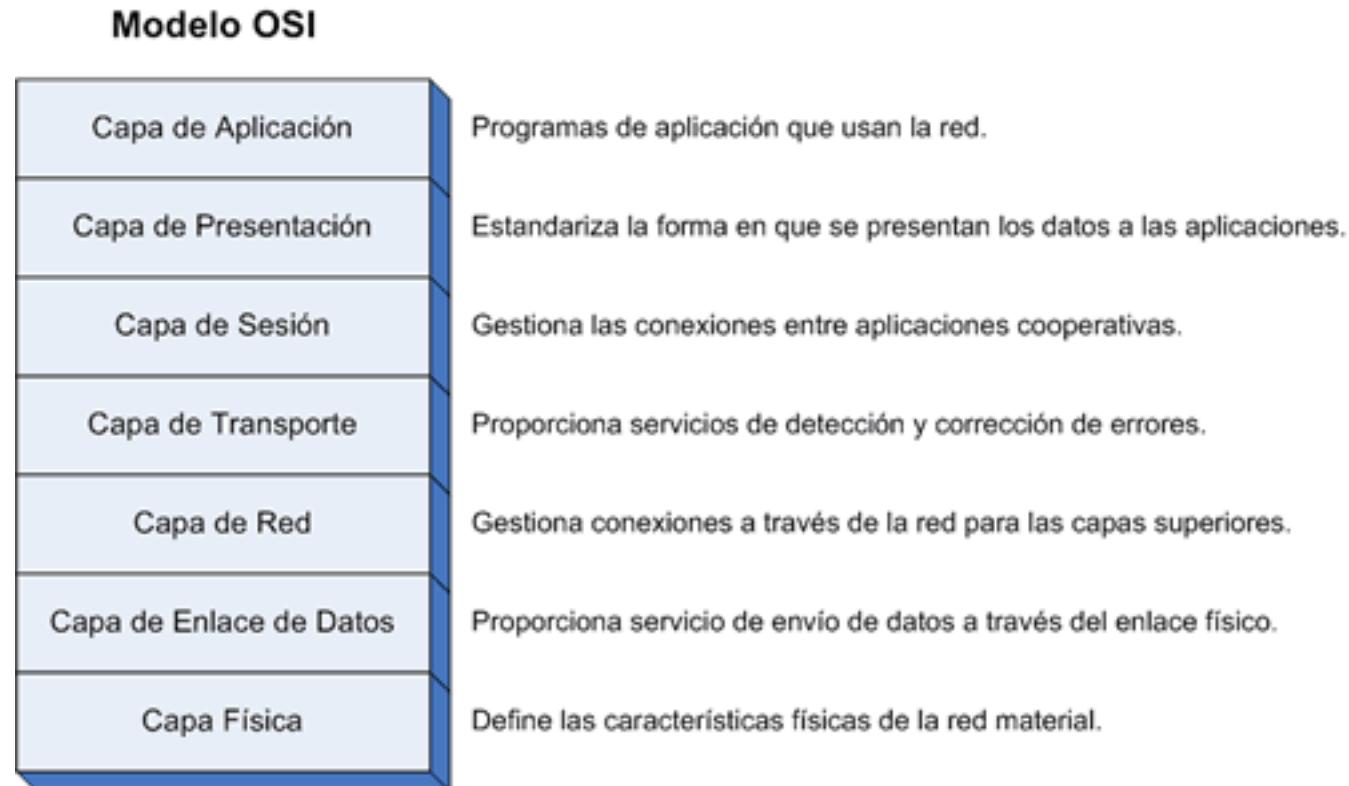
PDU - Protocol Data Unit
SDU - Service Data Unit

Separación en capas

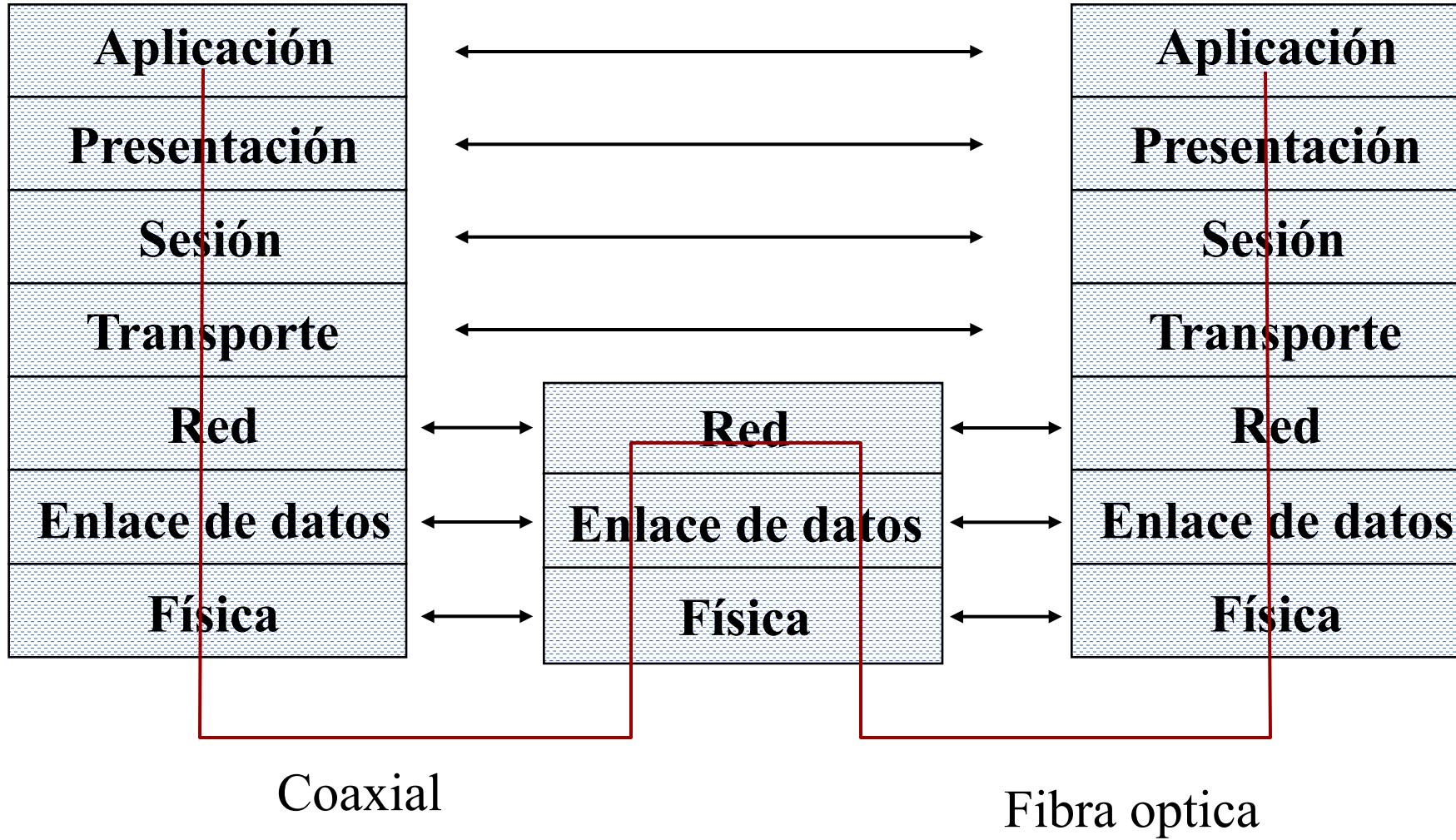
- Modularidad - Cada módulo desempeña una función particular en el desempeño global del sistema
- Cada capa ofrece un **servicio** a la capa superior enriqueciendo los servicios que ella recibe de la capa inferior
- La comunicación entre capas del mismo nivel entre dos sistemas (*entidades pares*), está definida por un **protocolo**

Modelo de referencia OSI

Modelo de *Interconexión de Sistemas Abiertos* propuesto por la Organización Internacional de Estándares (ISO) para establecer una referencia de estándares para redes.

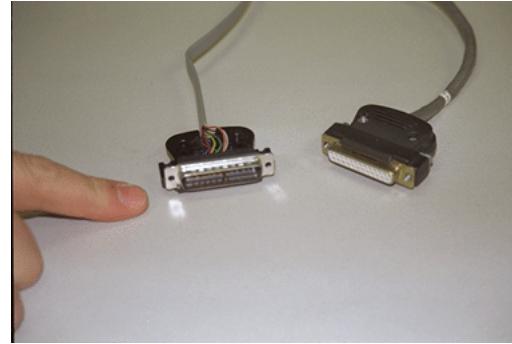


Independencia de capas



Capa física

- Se encarga de la transmisión de cadenas de bits en el medio físico. Se ocupa de las características
 - Mecánicas
 - Eléctricas
 - Estructuras
 - Procedimientoque establecen la transmisión



Capa de enlace de datos

Se encarga de:

- entramado de datos
- sincronización y control de acceso al medio
- transferencia de información fiable punto a punto (a través del medio físico)



Capa de red

- Establece rutas para encaminar los *paquetes* desde su origen hasta su destino final
- Acepta *paquetes* entrantes de la capa de transporte y *paquetes* en tránsito de la capa de enlace de datos y los dirige hacia la salida adecuada

Capa de transporte

- Segmentación y re-ensamblado de *mensajes* en *paquetes*
- Comunicación confiable extremo a extremo
- En algunas arquitecturas, p.e. Internet, control de flujo y control de congestión

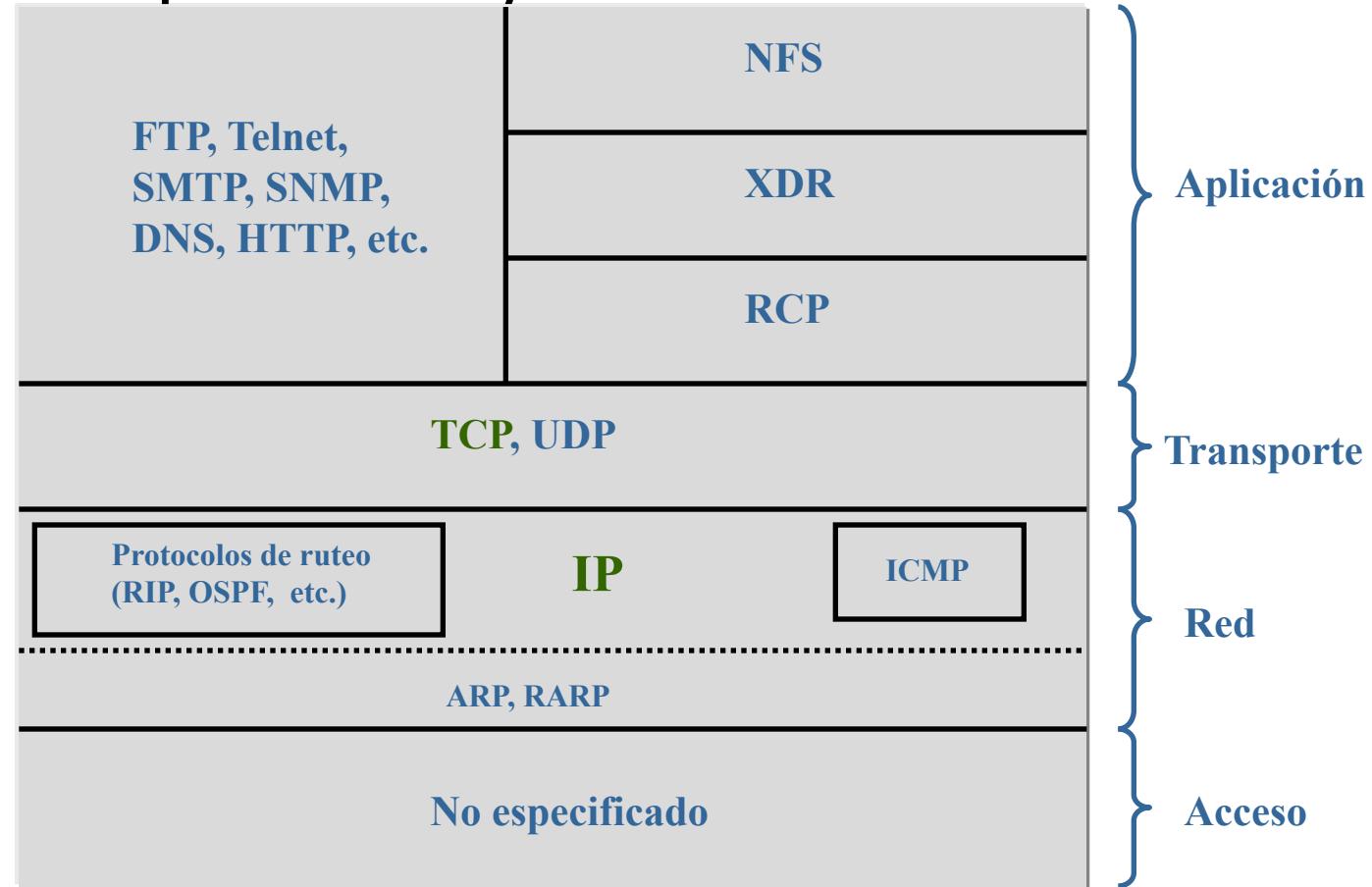
Capas de sesión y presentación

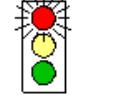
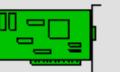
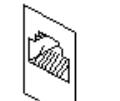
- Estructura de control para comunicaciones entre aplicaciones, administra y establece sesiones. Asigna derechos de acceso, funciones de cobro
- Realiza transformaciones útiles en los datos. Las funciones más importantes son
 - Cifrado
 - Compresión
 - Representación normalizada de datos

Capa de aplicación

- Servicios a los usuarios del ambiente de red. Se encarga de transacciones entre los usuarios
- Ejemplos
 - FTP
 - Navegación WWW
 - Correo electrónico
 - Administración de redes

Modelo de capas TCP/IP

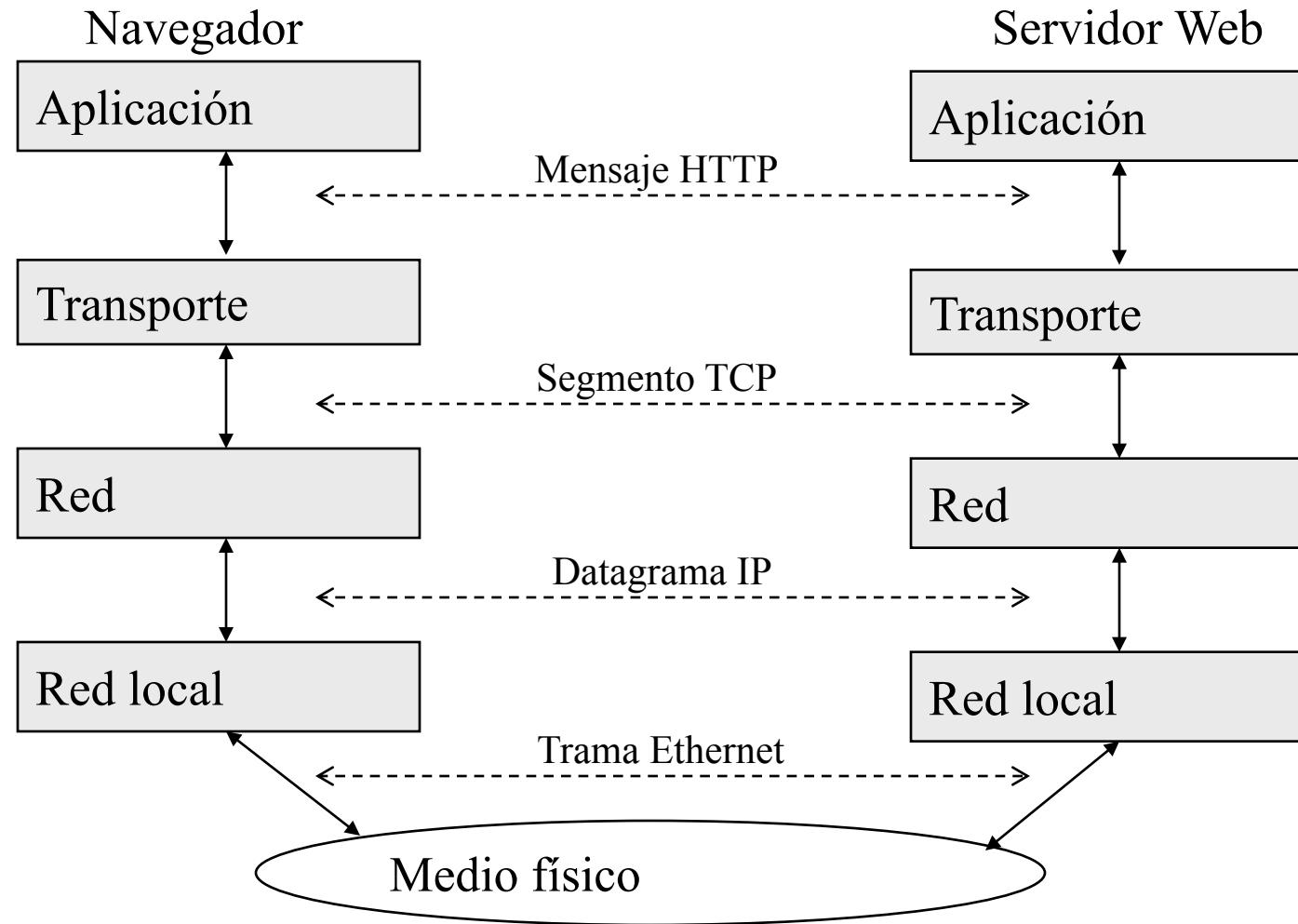


OSI MODEL		
7		Application Layer Type of communication: E-mail, file transfer, client/server.
6		Presentation Layer Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.
5		Session Layer Starts, stops session. Maintains order.
4		Transport Layer Ensures delivery of entire file or message.
3		Network Layer Routes data to different LANs and WANs based on network address.
2		Data Link (MAC) Layer Transmits packets from node to node based on station address.
1		Physical Layer Electrical signals and cabling.

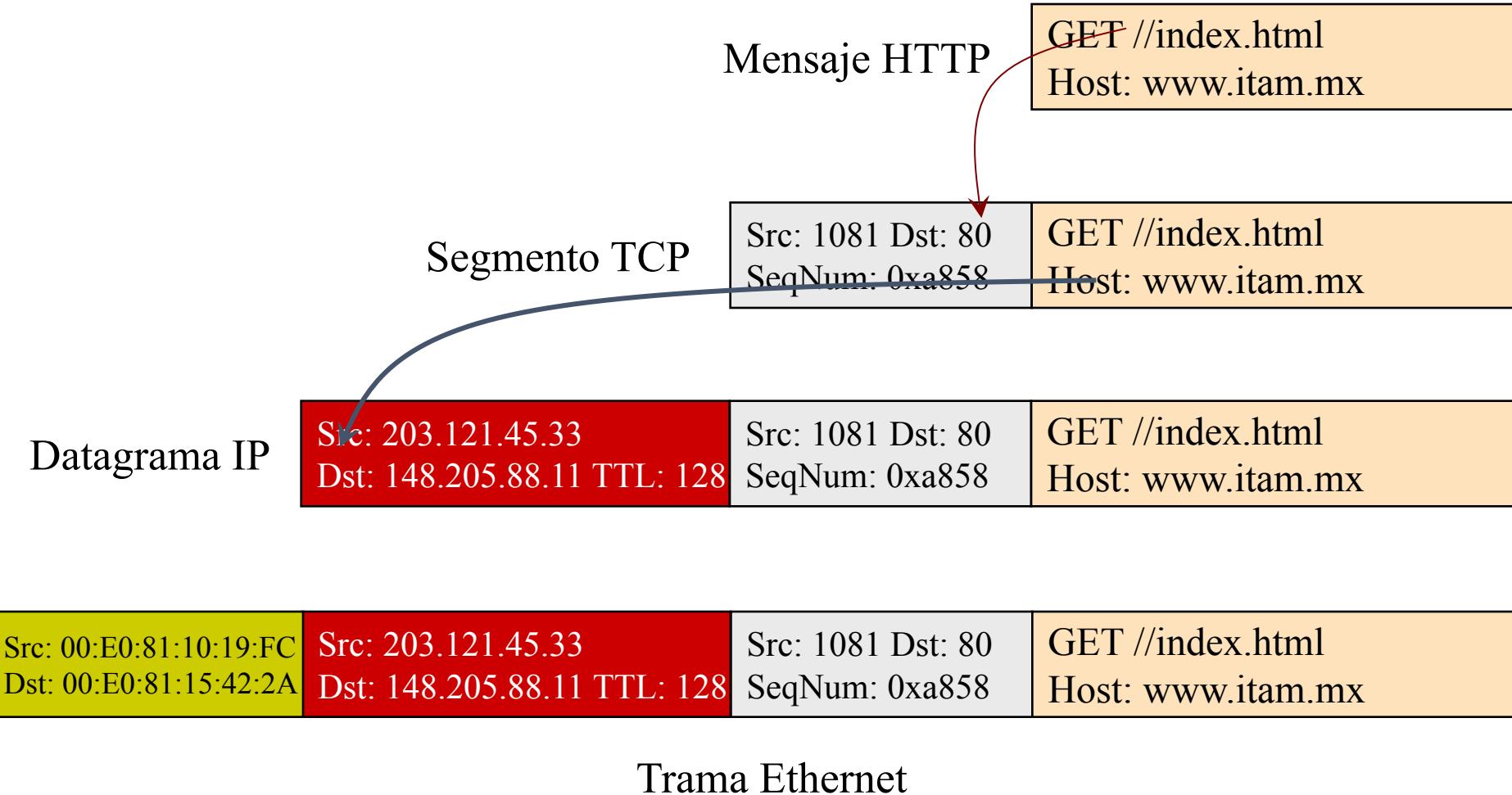
TCP / IP
FTP, Telnet, HTTP, SNMP, DNS, OSPF, RIP, Ping, Traceroute
TCP <small>(delivery ensured)</small>
UDP <small>(delivery NOT ensured)</small>
IP <small>(ICMP, IGMP, ARP, RARP)</small>



Arquitectura en capas



Protocolos de red



Capa física

Medios de transmisión

Contenido

- Conceptos generales
- Medios guiados
 - Par trenzado
 - Cable coaxial
 - Fibra óptica
- Medios libres
 - Medios inalámbricos
 - Microondas
 - Satélites

Medios de transmisión

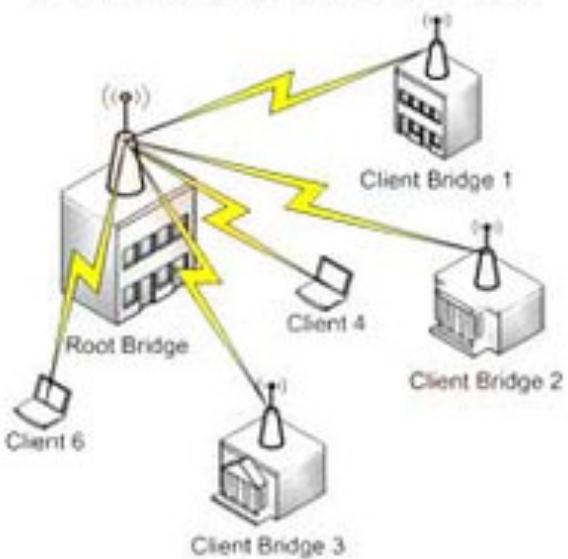
- Camino físico a través del cual se transmite información entre dos dispositivos
- Características
 - Tipo de conexión
 - Modo de transmisión
 - Características de transmisión
 - Características de propagación
 - Cobertura
 - Costo

Tipos de conexión

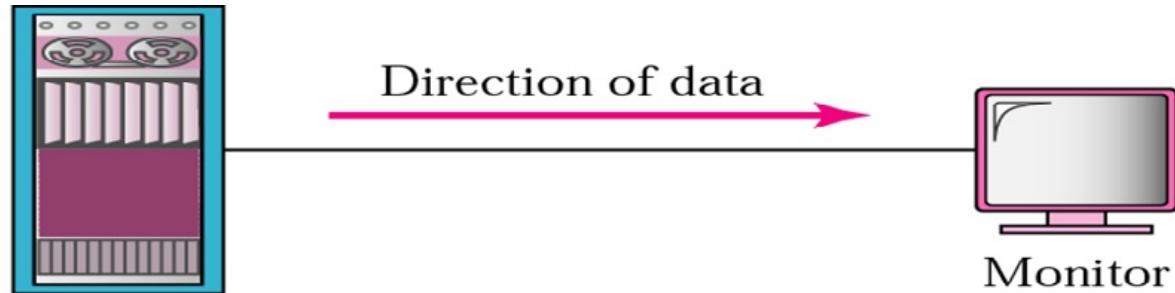
Point to Point connection:



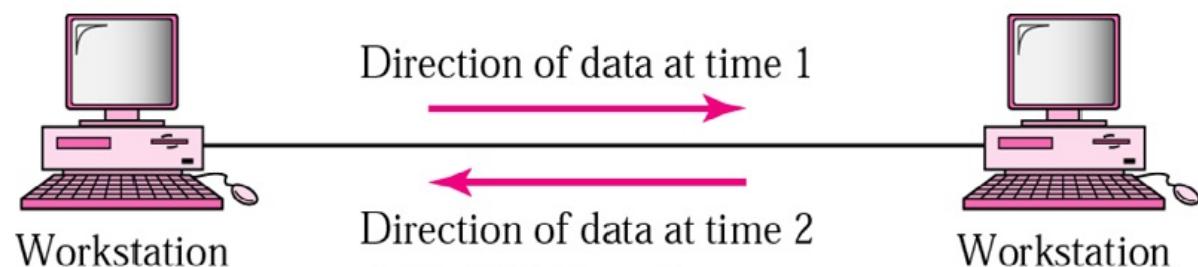
Point to Multipoint connection:



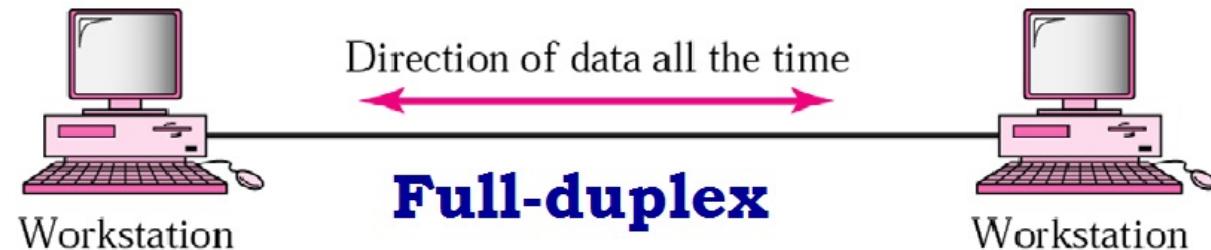
Modos de transmisión



Mainframe **Simplex Mode**



Half-duplex



Transmisión de datos

- Las señales transmitidas pueden
 - Alterarse por ruido
 - Atenuarse
 - Distorsionarse
- La atenuación y la distorsión dependen de:
 - El medio de transmisión
 - El ancho de banda
 - La velocidad de transmisión
 - La distancia
- El medio determina
 - El ancho de banda
 - La tasa de bits

Características de transmisión

- Atenuación
 - La potencia de la señal disminuye con la distancia.
 - Dependiente del medio, pero en general, a mayor frecuencia, mayor atenuación
- Distorsión
 - La señal recibida es distinta de la transmitida. La atenuación es distinta para distintos componentes de frecuencia
 - Distorsión por retardo
 - La velocidad de propagación varía con la frecuencia
 - Efecto de trayectorias múltiples
 - Distorsión por ruido.

Capacidades de los medios

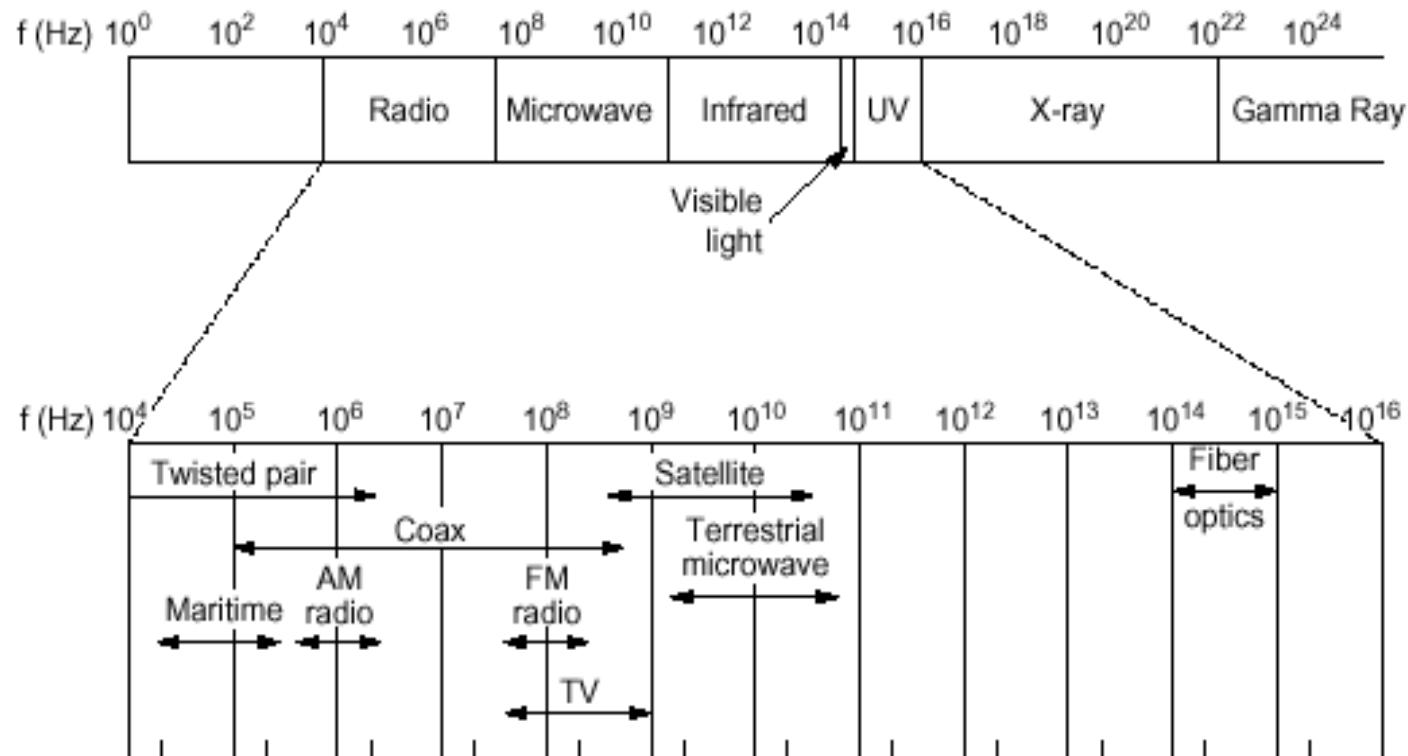
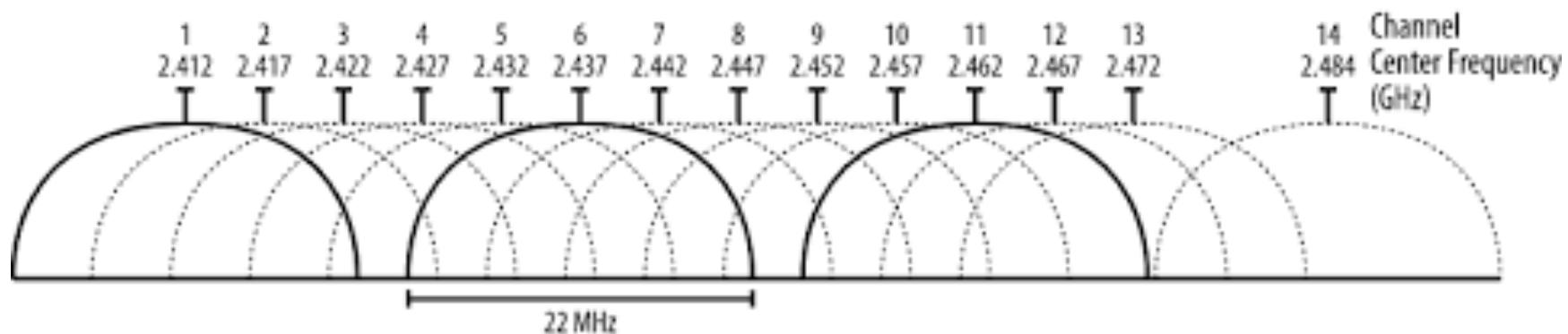


Fig. 2-11. The electromagnetic spectrum and its uses for communication.

Ancho de banda

- Rango de frecuencias en las que opera un sistema de comunicación.
- Ejemplo WiFi



WiFi

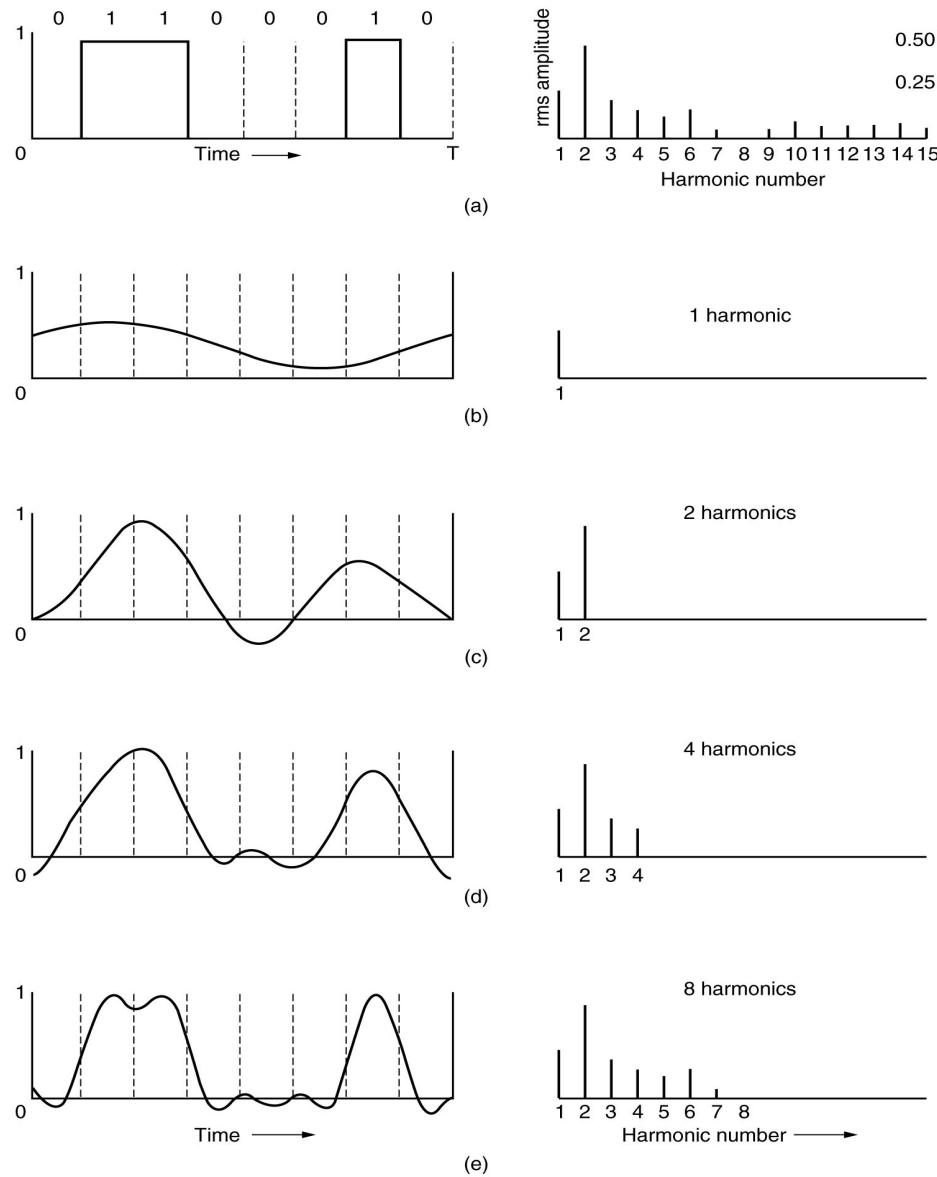
2.4GHZ BAND CHANNEL NUMBERS & FREQUENCIES

CHANNEL NUMBER	LOWER FREQUENCY MHZ	CENTER FREQUENCY MHZ	UPPER FREQUENCY MHZ
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

Velocidad o tasa de transmisión

- Tasa de transmisión de símbolos. Es el número de símbolos transmitidos por segundo (bauds)
- Tasa de transmisión de bits. Es el número de bits que se transmiten por segundo (bps)

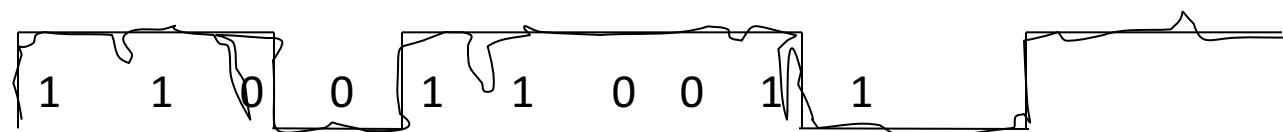
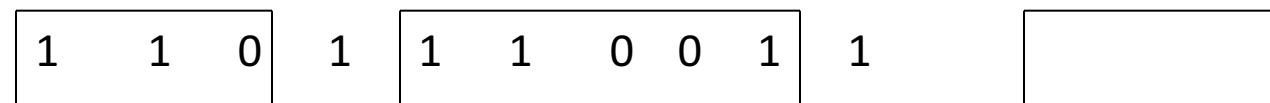
Ejemplo:
Transmisión de la letra “b”



Fuente: Tanenbaum

Velocidad de transmisión

- Fórmula de Nyquist
 - Si un canal tiene un ancho de banda B
 - $C = 2B$ bps Dos niveles por elemento
 - Caso general (ideal)
 - $C = 2B \log_2 (M)$ bps M = Niveles por elemento
 - Sin embargo, la velocidad se reduce porque la transmisión no es perfecta. Hay ruido

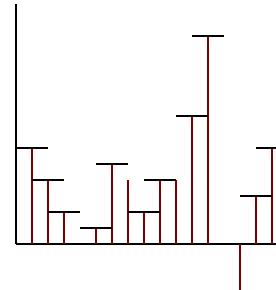
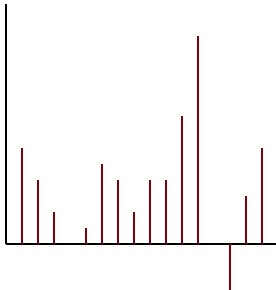
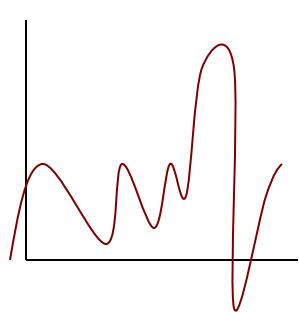
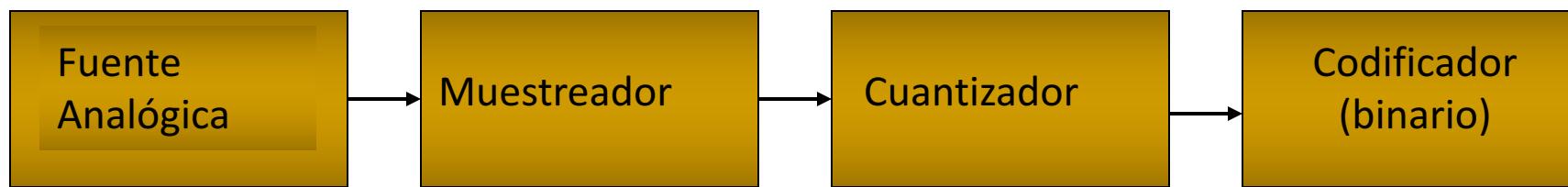


Teorema de Shannon

$$C = B \log_2 \left(1 + \frac{S}{N} \right)$$

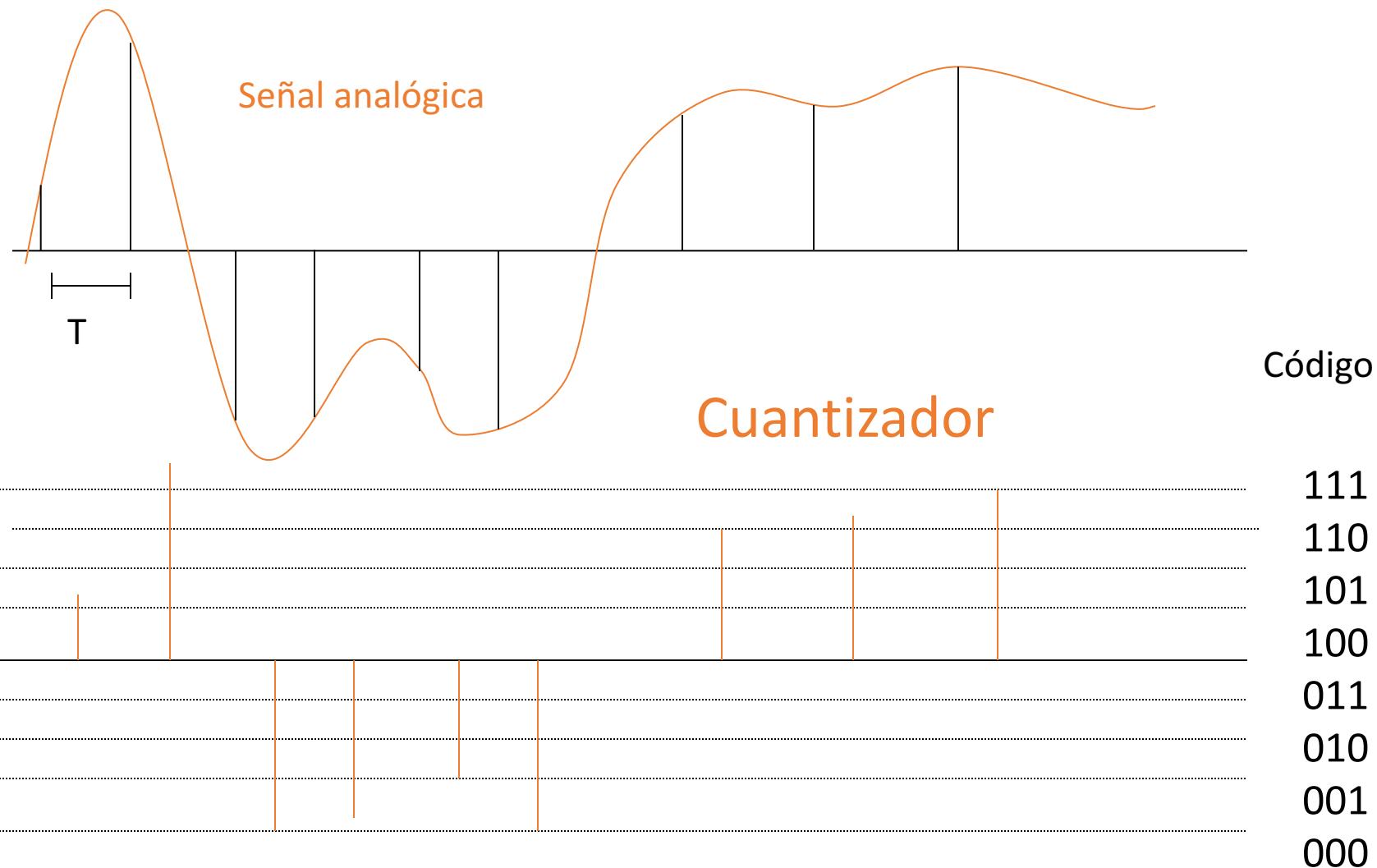
- Capacidad de un medio de transmisión
 - Relación señal a ruido = 422
 - Ancho de banda = 3300 Hz
 - C se acerca a 28.8 kbps
 - ¿Cómo trabaja un módem a 56 kbps? 228558-1

Conversión de analógica a digital (A/D)

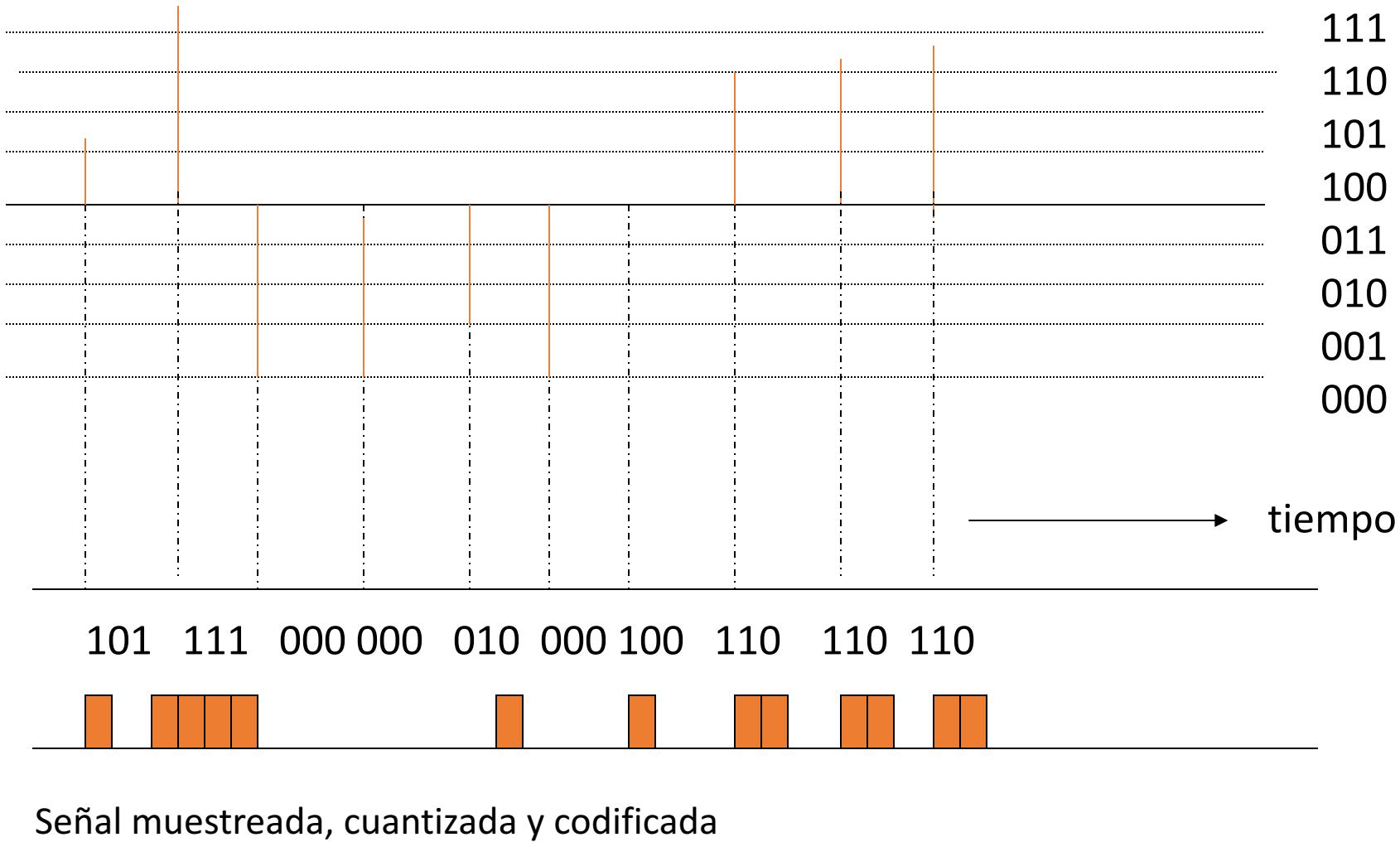


0110...

Conversión A/D: muestreo y cuantización

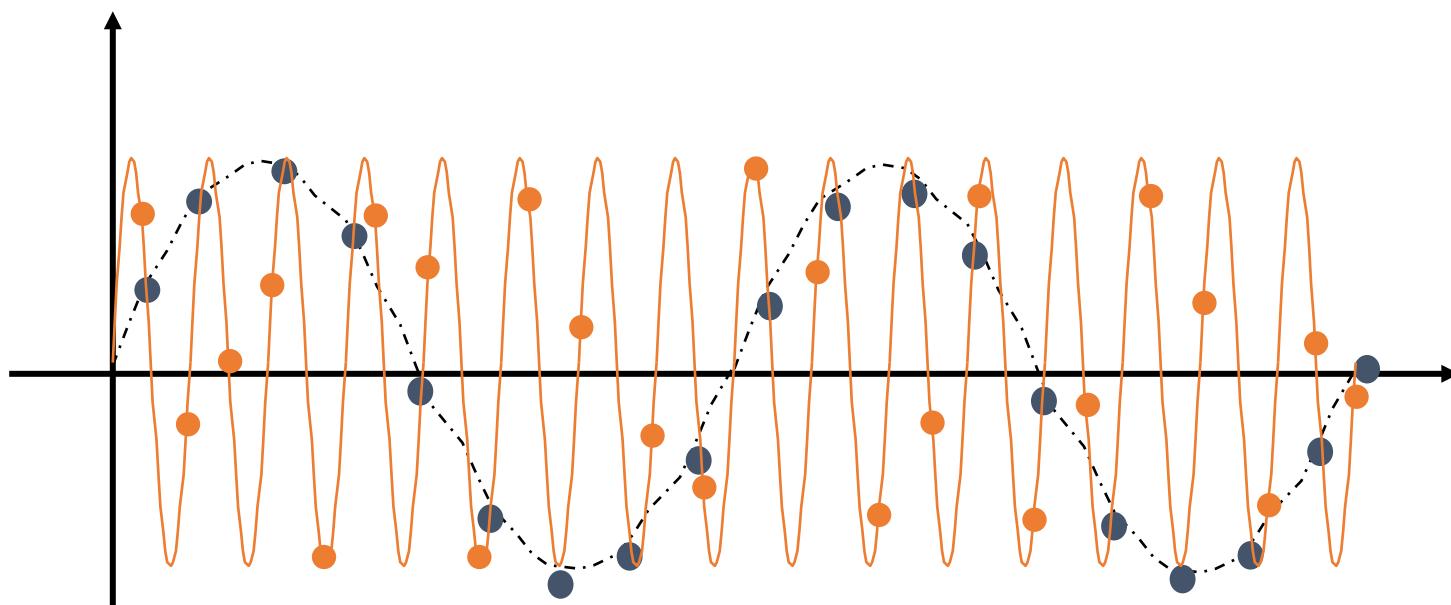


Conversión A/D: cuantización y codificación



Frecuencia de muestreo

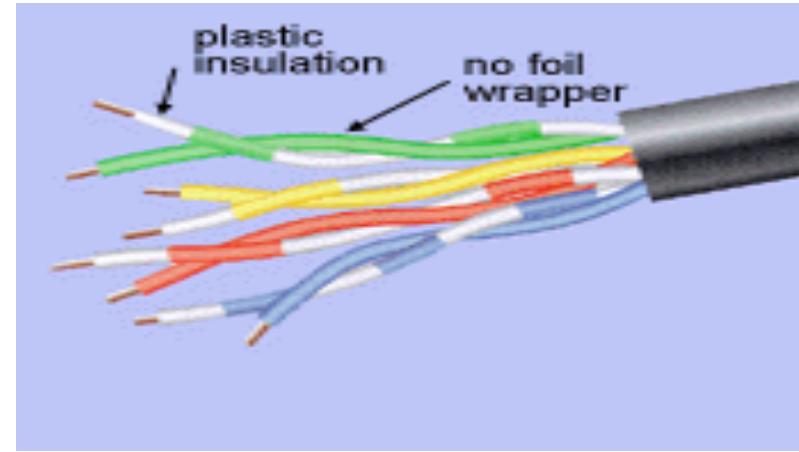
- El teorema de muestreo de Nyquist indica que deben tomarse al menos $2B$ muestras, donde B es la frecuencia máxima de la señal.



Medios guiados

Par trenzado

- Par de conductores de cobre aislados trenzados entre sí
- Económico, flexible y sumamente difundido en redes telefónicas (bucle de abonado) y redes locales
- Tres tipos:
 - no blindado (UTP)
 - Recubierto (FTP)
 - blindado (STP)



Par trenzado

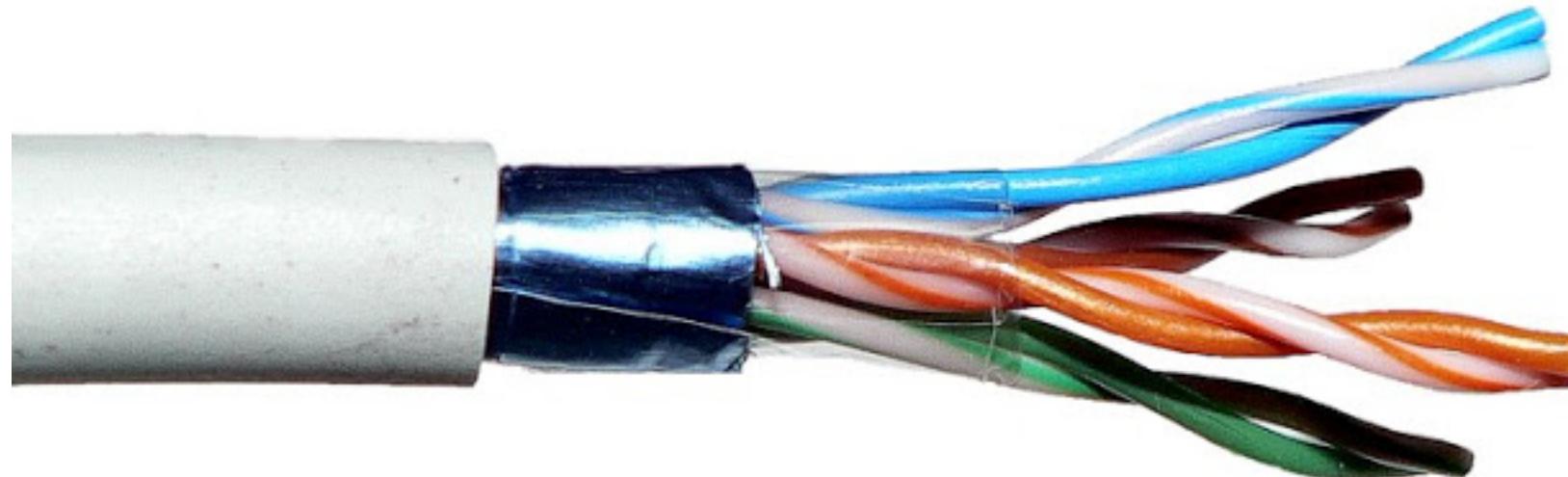
- Cada par es un canal de comunicación
- Diámetro de cada cable < 1mm
- El trenzado reduce la interferencia entre cables adyacentes (diafonía)
- Alcance depende de la frecuencia, pero limitado a distancias relativamente cortas: atenuación 3dB/km@1kHz
 - Amplificadores cada 5 a 6 km (analógico) y repetidores cada 2 ó 3 km (digital)
- Susceptible al ruido pues no se eliminan todas las interferencias (sobre todo en UTP)

UTP – Estándar EIA/TIA - 568

- Categoría 1: Comunicaciones telefónicas únicamente
- Categoría 2: Transmisión de datos a 4 MHz
- Categoría 3: Tasas hasta 16 MHz
- Categoría 4: Tasas hasta 20 MHz
- Categoría 5: Tasas hasta 100 MHz
- Categoría 6: Tasas hasta 200 MHz
- Categoría 7: Tasas hasta 600 MHz

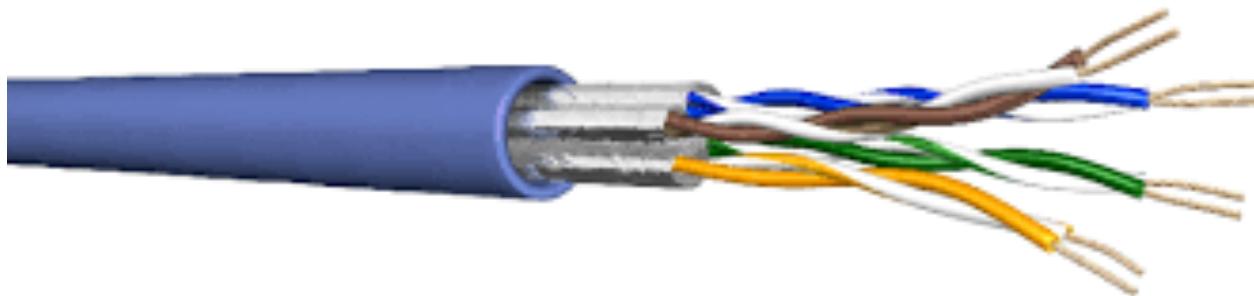
Cable FTP

Cable FTP (Foiled Twisted Pair)

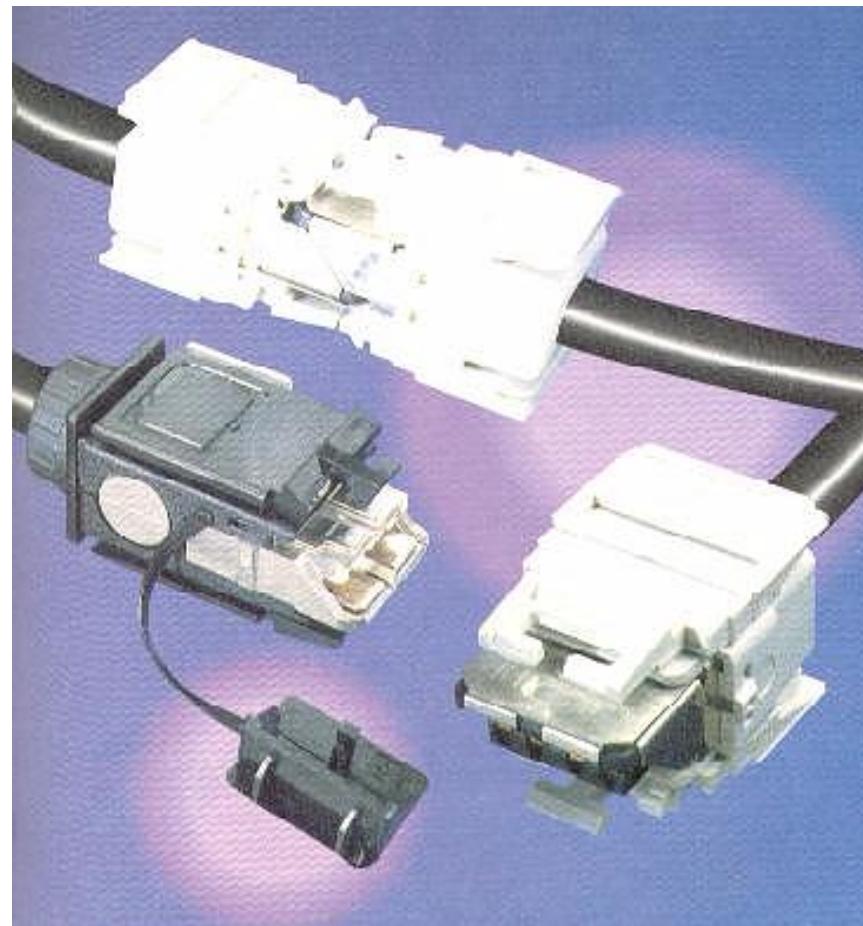


STP

- Pares de cobre recubiertos con malla metálica
- El recubrimiento reduce la interferencia y el ruido eléctrico
- Más costoso y menos flexible que UTP

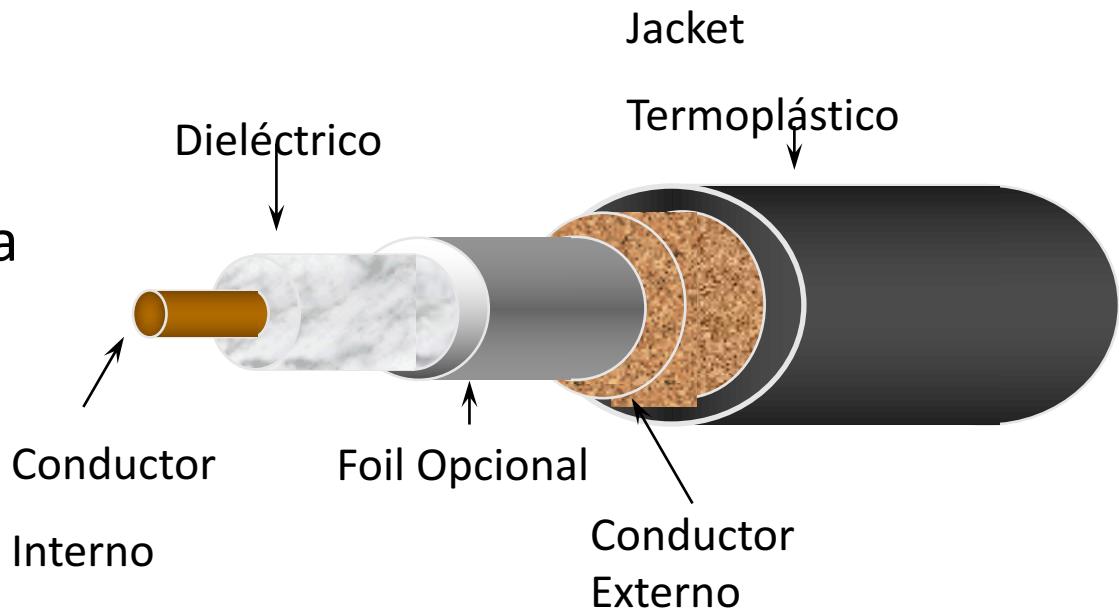


STP-A: Sistema Blindado 150 Ohms



Cable coaxial

- Conductor central de cobre rodeado por otro conductor en forma de malla circular y separados por un medio dieléctrico.
- Mayor inmunidad que par trenzado, puede cubrir mayores distancias a mayores frecuencias
- Dos clases:
 - Banda base: transmisión digital
 - Banda amplia: transmisión analógica



Cable coaxial

- La frecuencia depende de la distancia y de las características del cable
 - 1 a 2 GHz para 1 km
 - 300 MHz para 100 km
- Transmisión digital en configuración de banda amplia requiere generalmente de un par de cables unidireccionales
- Más costoso y difícil de instalar y manipular, ha sido ampliamente sustituido por UTP categoría 5 en redes locales

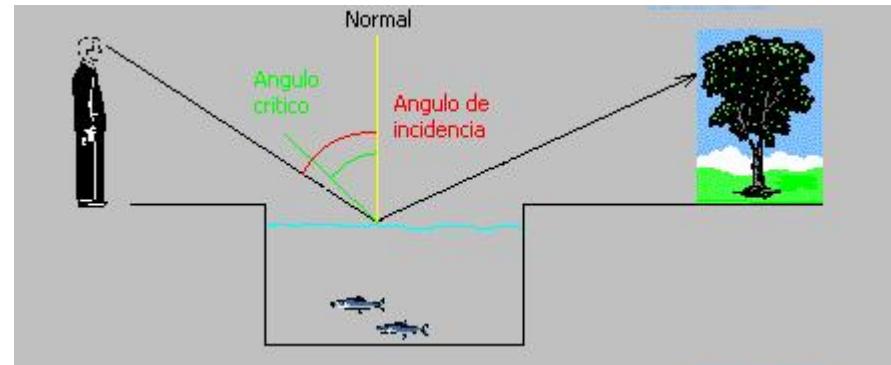
Fibra óptica

- Fibra de vidrio o plástico (núcleo) a través de la cual se transmite la señal en forma de energía luminosa
- El núcleo está rodeado por un revestimiento, también de vidrio o plástico con un índice de refracción menor
- Es una forma de guía de onda en la que la señal óptica se propaga por la reflexión interna entre el núcleo y el revestimiento



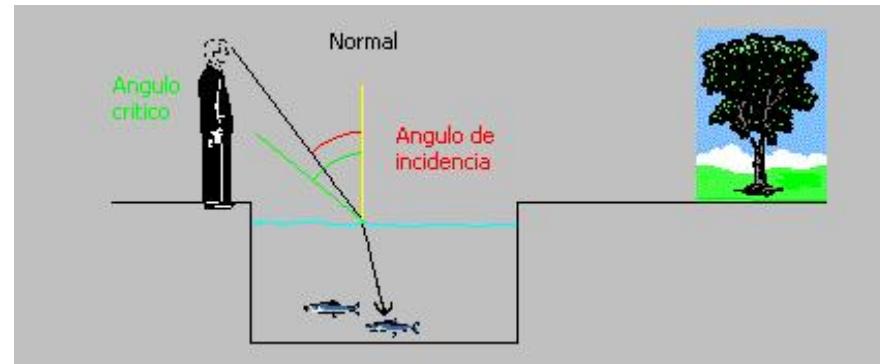
Principio de transmisión

- Ángulo de incidencia mayor al ángulo crítico
- $n_1 > n_2$



Reflexión

- Ángulo de incidencia menor al ángulo crítico
- $n_1 > n_2$
- n es el índice de refracción



Refracción

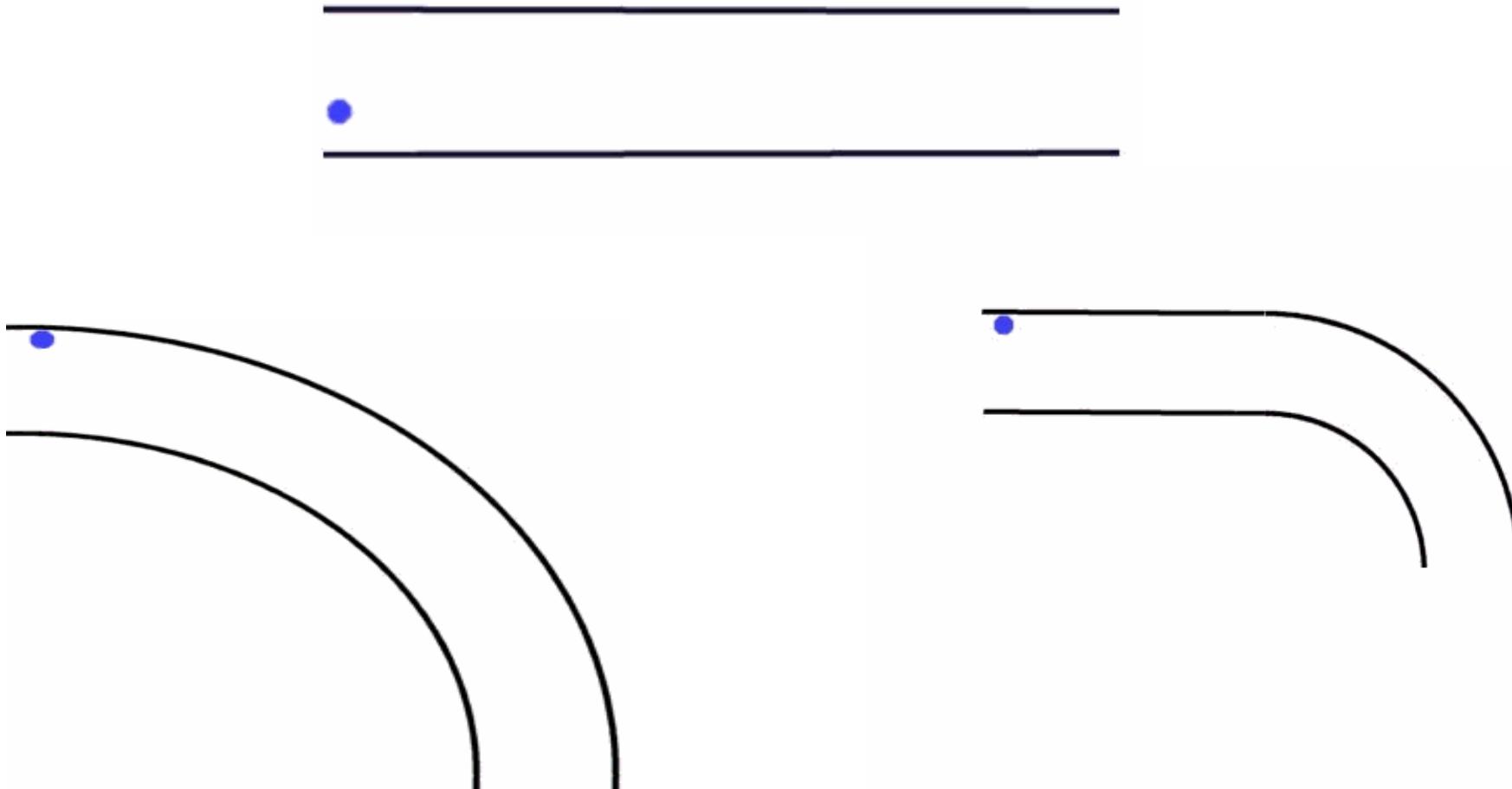
Características

- Menor atenuación que par trenzado y coaxial, permite transmitir señales a distancias mucho mayores sin necesidad de amplificación
- Transmite luz, por lo que es inmune a interferencias electromagnéticas
- Inmune a factores ambientales (oxidación, tormentas eléctricas, etc.)
- Capacidad de transmitir 500 Gbps con una sola longitud de onda.
- Más delgada y más ligera que el par trenzado
- Seguridad: muy difícil de intervenir

Características (cont.)

- Atenuación
 - Absorción por calor, fugas, impurezas, dobleces, vibración atómica
- Muy costosa
 - Instalación, mantenimiento, interfaces (sobre todo monomodal)
- Poco flexible: no soporta dobleces con grandes ángulos
- Relativamente frágil
- Usos: Enlaces larga distancia, redes metropolitanas, backbone redes LAN

Angulo crítico de flexión



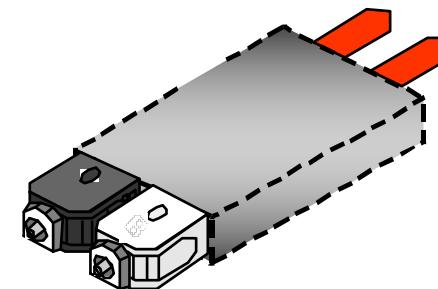
Conectores 568ST



Conectores 568SC



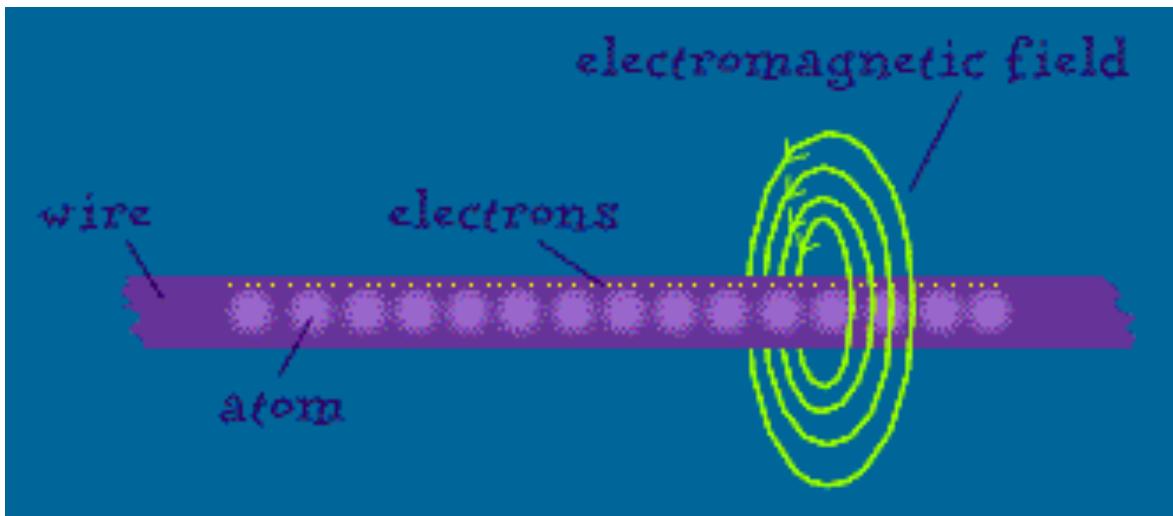
Conectores 568-SC



Medios no guiados

Ondas electromagnéticas

- La corriente eléctrica genera un campo eléctrico que induce un campo magnético que a su vez genera un campo eléctrico...
- Principio de radiación de las antenas



Medios no guiados

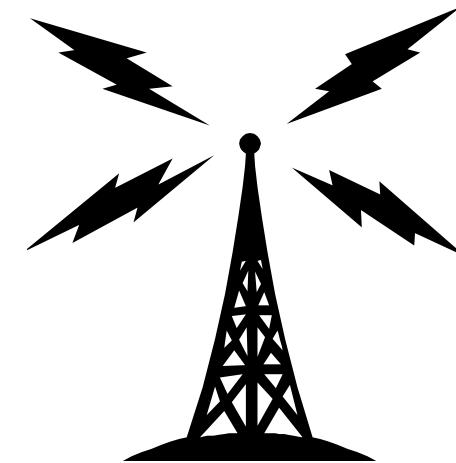
- El espacio o el aire es el medio de propagación de las ondas electromagnéticas. No se requiere de conexión física
- Emisor y receptor pueden ser fijos o móviles
- Amplia gama de espectro: servicios con requerimientos grandes de ancho de banda o limitados
- Puede implementarse rápidamente
- Propenso a interferencias
- Estricto control de acceso y utilización del medio

Aplicaciones

- Radiodifusión (radio, TV, datos)
- Redes locales y metropolitanas
- Telefonía celular
- Servicios de *trunking*
- Aplicaciones ICM y de entretenimiento
- Radiolocalización
- Navegación
- ...

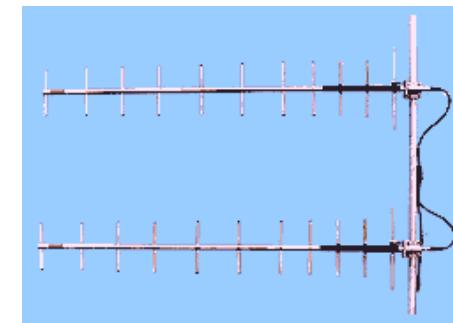
Radiodifusión

- Propagación omnidireccional de señales terrenas
- Antenas relativamente sencillas sin necesidad de alineación muy precisa
- Difusión de radio AM, FM
- Difusión de televisión VHF, UHF
- Servicios de datos

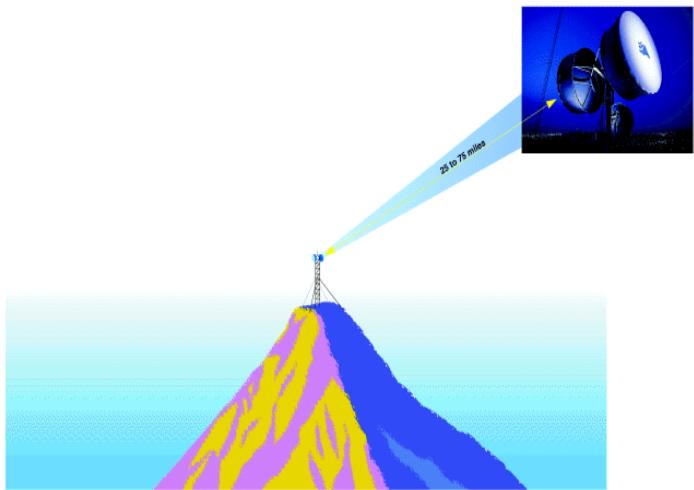


Microondas

- Propagación en línea de vista, requiere de alineación muy precisa
- Utiliza antenas altamente direccionales para minimizar interferencia
- Frecuencias dedicadas y reguladas por COFETEL
- Señales de microondas pueden atravesar paredes y barreras físicas
- Exposición a radiaciones es nociva para la salud
- Propensa a interferencia de otras fuentes



Microondas terrestres

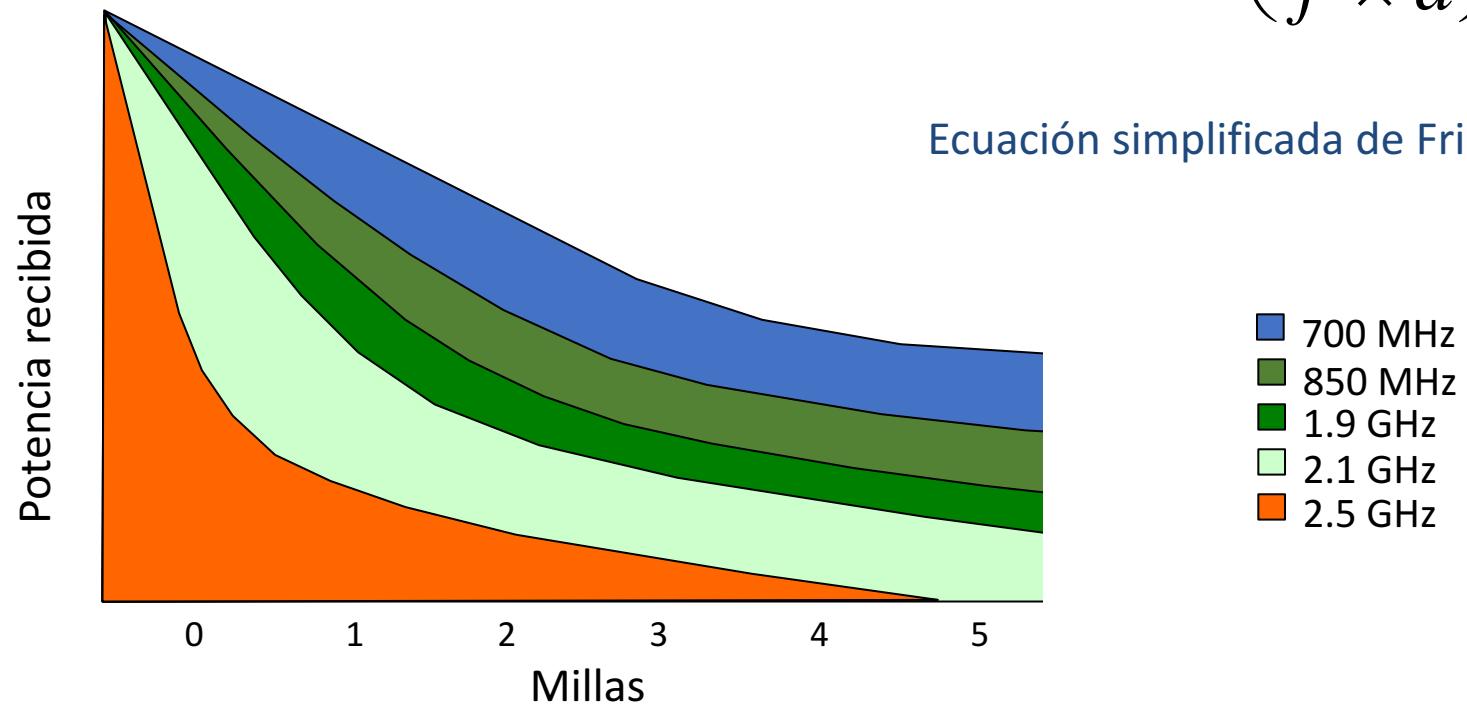


- Rangos de frecuencia de 2 a 40 GHz
- Relativamente cara aunque puede resultar la tecnología más económica en el corto plazo o cuando la instalación física no es viable
- Distancia entre repetidores de 40 km a 100 km
- Tasas de transmisión de decenas de Mbps, aunque 500 Mbps son factibles
- Telecomunicaciones de media y larga distancia
- Enlaces punto a punto entre edificios
- Voz, televisión y redes de datos privadas

Frecuencia vs cobertura

$$P_{rx} = P_{tx} \left(\frac{1}{f \times d} \right)^2$$

Ecuación simplificada de Friis



Fuente: Propia con datos de Morgan Stanley

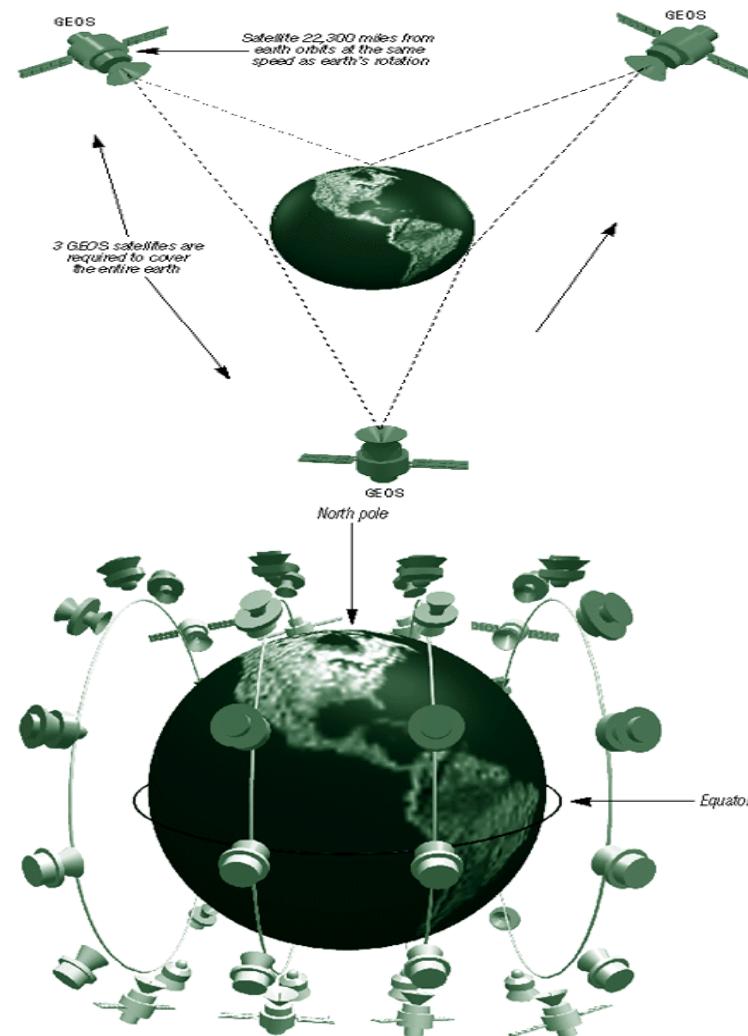
Frecuencia vs cobertura

Frecuencia (GHz)	Distancia (km)
2	60
4-6	50
7-8	45
11	40
13	35
15	20
20	10
30	5
60	0.5

Para una potencia fija

Enlaces satelitales

- Estación de relevo de microondas en el espacio, funciona como un amplificador o como un repetidor
- Conectividad
 - punto a punto para enlazar dos estaciones terrenas
 - Punto multipunto para servicios de difusión
- Huella puede ser amplia o angosta
- Categorías
 - LEO, MEO, GEO



Enlaces satelitales

- Anchos de banda de 36 A 72 Mbps en canales de 64 kbps a 512 kbps
- Bandas de frecuencia de operación (transponders):
 - Banda C: 3.7 - 4.2 5.925 - 6.425 GHz
 - Banda Ku: 11.7 - 12.2 14 -14.5 GHz
 - Banda L: 1.6465 - 1.66 1.545 - 1.5585 GHz
- Orbita geoestacionaria
 - Cinturon de Clark: 35,784 km sobre el ecuador
 - Antenas en posición fija

Enlaces satelitales

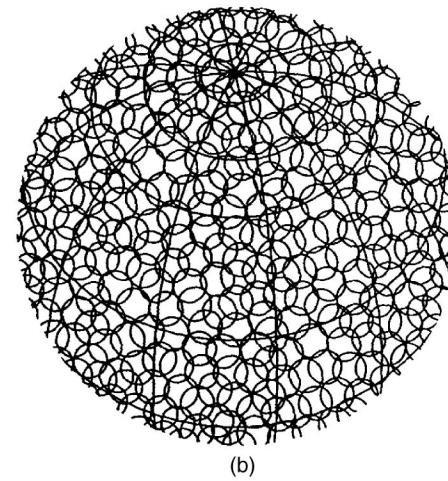
- Usos
 - Difusión de televisión
 - Telefonía larga distancia
 - Redes de datos privadas
- Limitaciones
 - Retraso: satélite geoestacionario 250 ms
 - Seguridad
 - Susceptibilidad a condiciones atmosféricas (> 10GHz)
 - Visibilidad desde la tierra

Satélites de órbita baja

- LEO
- 750 a 1500 Km. de altura
- Ejemplos:
 - Iridium 66 satélites
 - Globalstar 48
 - SkyBridge 80

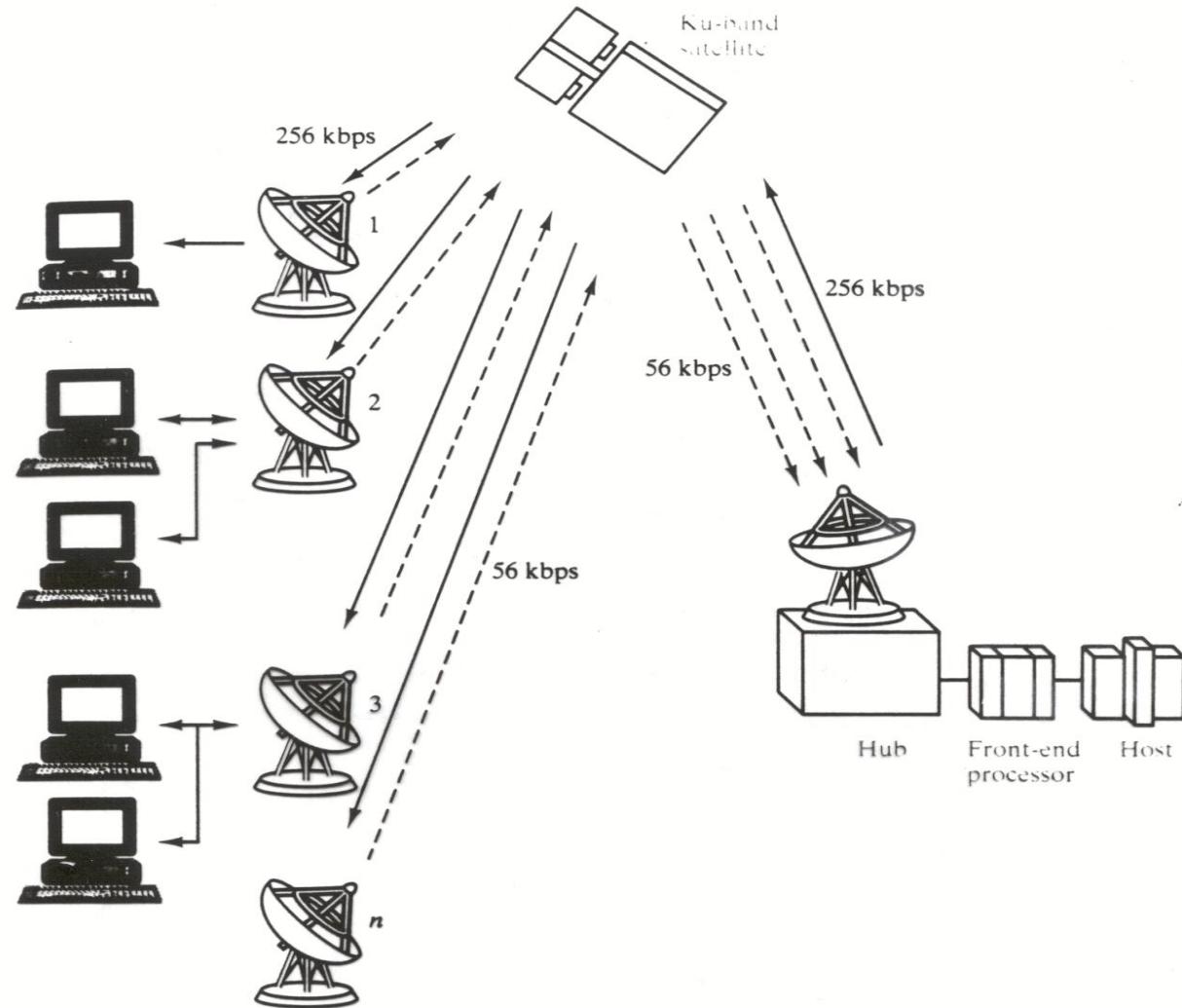


(a)



(b)

VSAT: Very small aperture terminals



VSAT

- Alternativa de bajo costo para empresas
- Comparten satélite para transmitir información hacia un nodo concentrador
- El concentrador coordina la comunicación entre suscriptores
- Transmisión con mucha potencia, permite que las antenas receptoras tengan diámetro pequeño (0.6 a 3.8 m)

Infrarrojo

- Transmisor modula haz de luz infrarroja
- Se requiere línea de vista o reflexión en una superficie clara (por ejemplo, el techo)
- Tasas de transmisión hasta de 20 Mbps
- No requiere licencia
- Cobertura limitada: potencia de emisión restringida para evitar daños
- Conectividad punto a punto
- Inherentemente seguro pues las ondas infrarrojo no penetran las paredes
- Luz ambiental puede ser una fuente de ruido. Necesario filtros ópticos pasa bandas

Comparación entre medios

	P.Trenzado	Coaxial	F. Optica	μOndas	Satélite
Costo	Muy bajo	Bajo	Medio	Alto	Muy alto
Velocidad	Muy baja	Media	Muy alta	Alta	Alta
Disponibilidad	Buena	Buena	Buena	Buena	Media, Buena
Escalabilidad	Media	Buena (local)	Buena	Buena	Buena
Errores	Media	Buena	Muy buena	Media	Media
Seguridad	Media	Media	Muy buena	Mala	Mala
Distancia	Buena	Mala	Buena	Buena	Buena

The Data Link Layer

Chapter 3

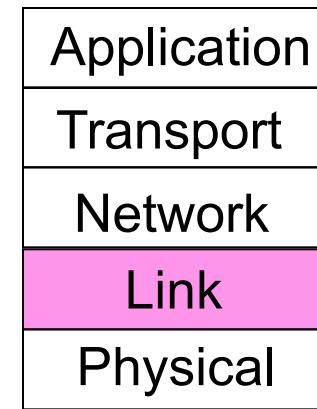
- Data Link Layer Design Issues
- Error Detection and Correction
- Elementary Data Link Protocols
- Sliding Window Protocols
- Example Data Link Protocols

Revised: August 2011

The Data Link Layer

Responsible for delivering frames of information over a single link

- Handles transmission errors and regulates the flow of data

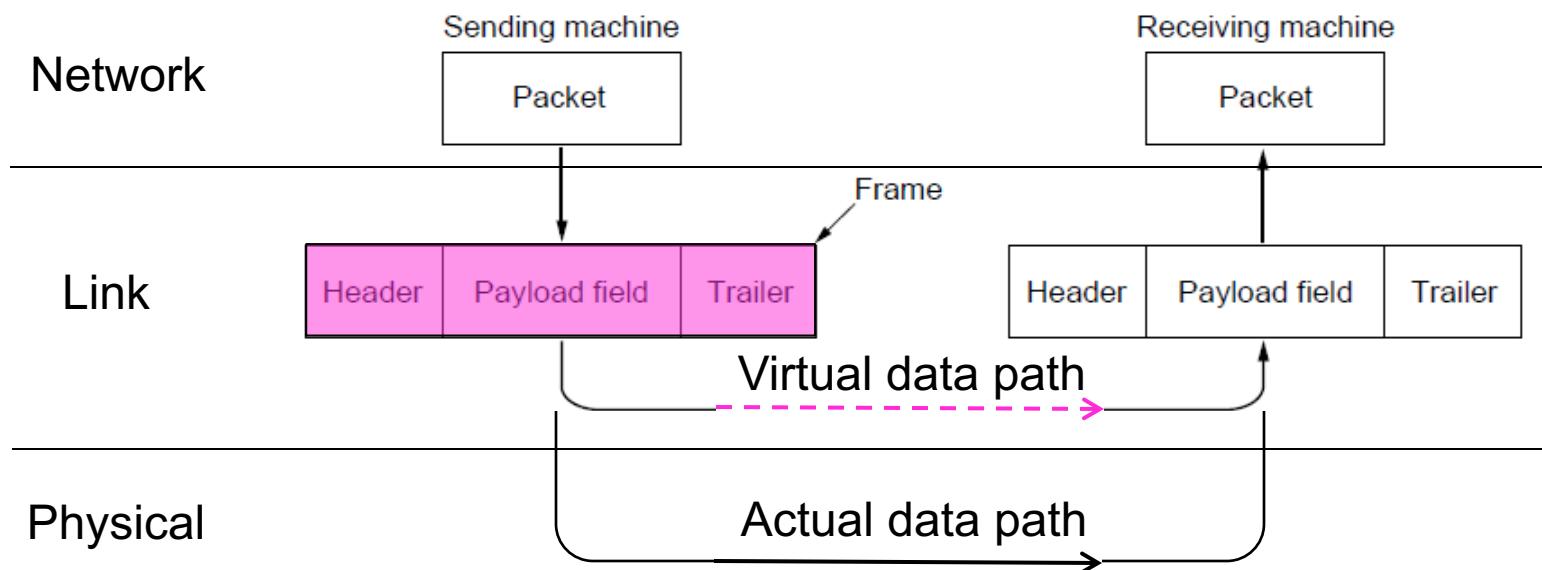


Data Link Layer Design Issues

- Frames »
- Possible services »
- Framing methods »
- Error control »
- Flow control »

Frames

Link layer accepts packets from the network layer, and encapsulates them into frames that it sends using the physical layer; reception is the opposite process



Possible Services

Unacknowledged connectionless service

- Frame is sent with no connection / error recovery
- Ethernet is example

Acknowledged connectionless service

- Frame is sent with retransmissions if needed
- Example is 802.11

Acknowledged connection-oriented service

- Connection is set up; rare

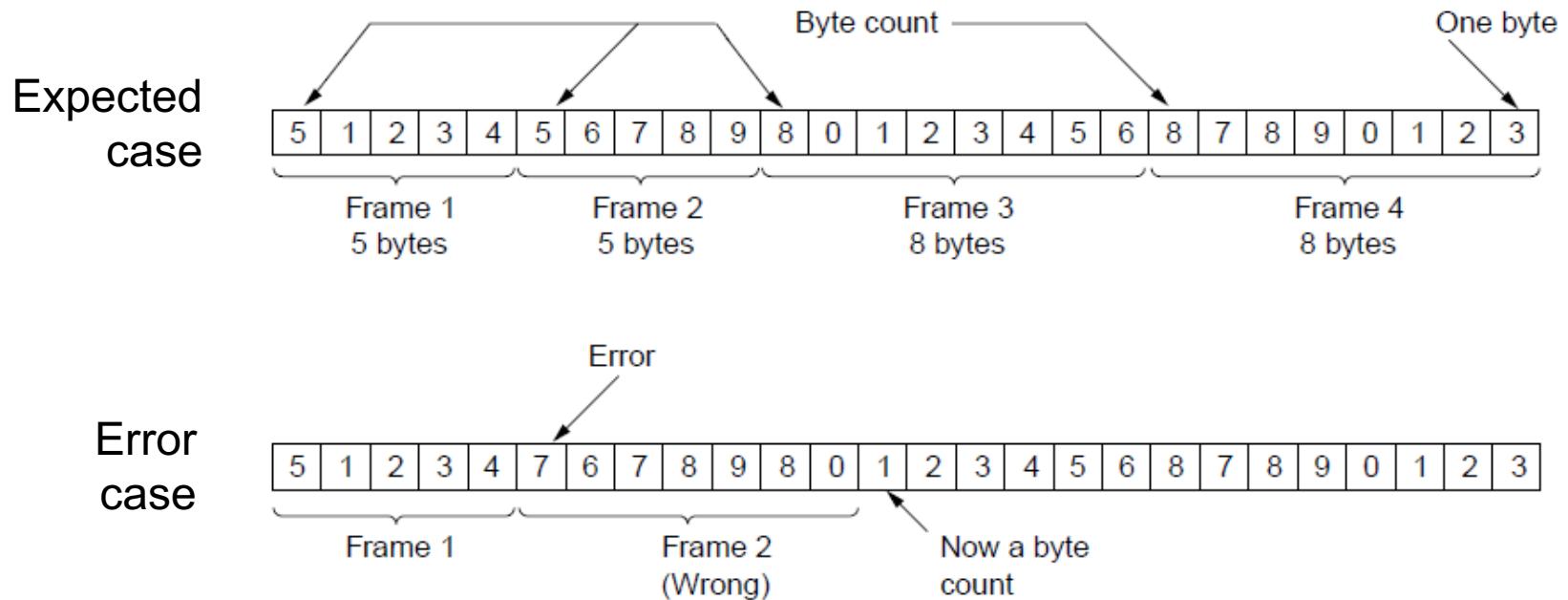
Framing Methods

- Byte count »
- Flag bytes with byte stuffing »
- Flag bits with bit stuffing »
- Physical layer coding violations
 - Use non-data symbol to indicate frame

Framing – Byte count

Frame begins with a count of the number of bytes in it

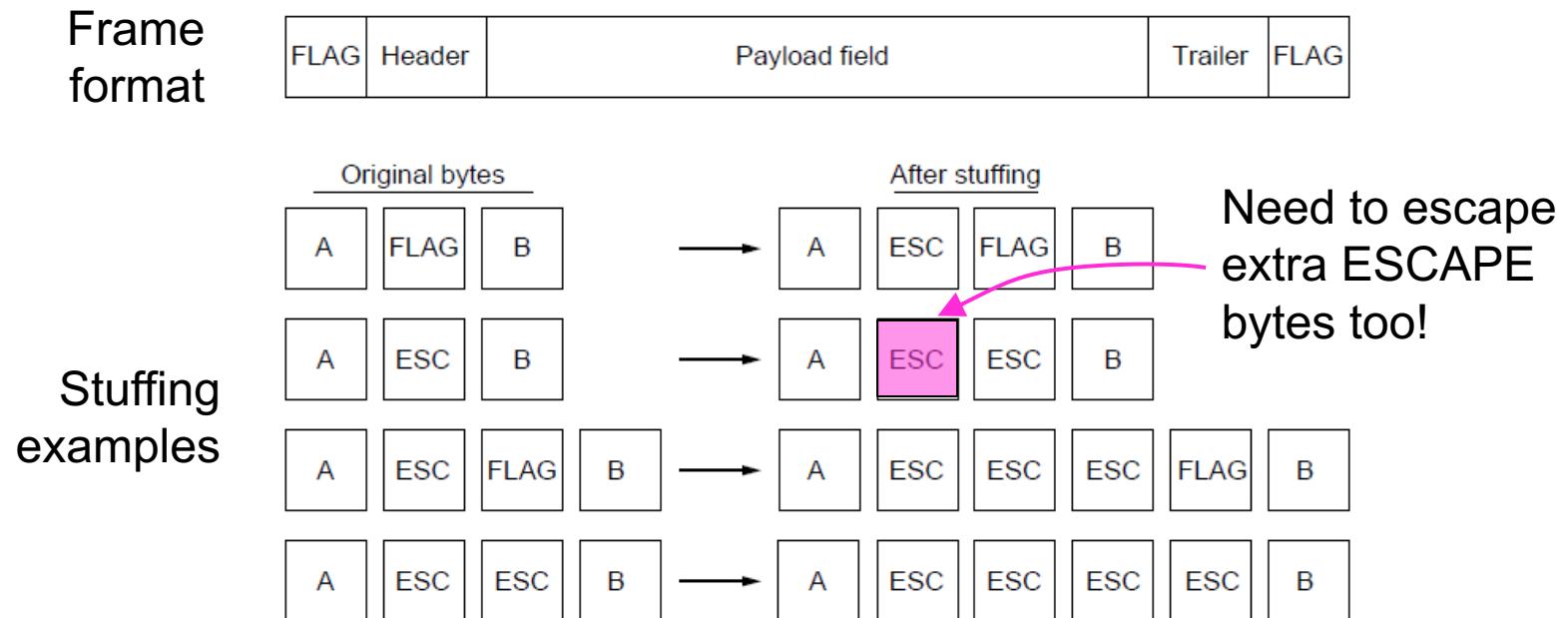
- Simple, but difficult to resynchronize after an error



Framing – Byte stuffing

Special flag bytes delimit frames; occurrences of flags in the data must be stuffed (escaped)

- Longer, but easy to resynchronize after error



Framing – Bit stuffing

Stuffing done at the bit level:

- Frame flag has six consecutive 1s (not shown)
- On transmit, after five 1s in the data, a 0 is added
- On receive, a 0 after five 1s is deleted

Data bits 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

Transmitted bits
with stuffing 0 1 1 0 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0

Stuffed bits

Error Control

Error control repairs frames that are received in error

- Requires errors to be detected at the receiver
- Typically retransmit the unacknowledged frames
- Timer protects against lost acknowledgements

Detecting errors and retransmissions are next topics.

Flow Control

Prevents a fast sender from out-pacing a slow receiver

- Receiver gives feedback on the data it can accept
- Rare in the Link layer as NICs run at “wire speed”
 - Receiver can take data as fast as it can be sent

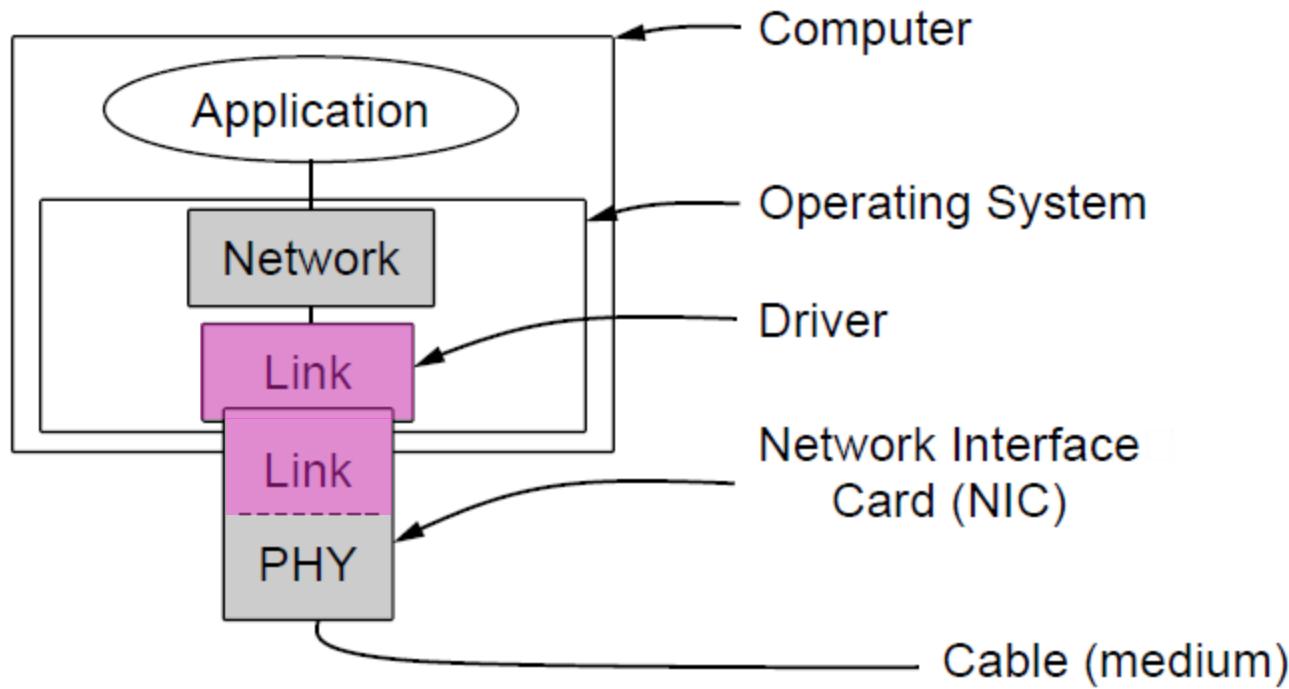
Flow control is a topic in the Link and Transport layers.

Elementary Data Link Protocols

- Link layer environment »
- Utopian Simplex Protocol »
- Stop-and-Wait Protocol for Error-free channel »
- Stop-and-Wait Protocol for Noisy channel »

Link layer environment (1)

Commonly implemented as NICs and OS drivers;
network layer (IP) is often OS software



Utopian Simplex Protocol

An optimistic protocol (p1) to get us started

- Assumes no errors, and receiver as fast as sender
- Considers one-way data transfer

```
void sender1(void)
{
    frame s;
    packet buffer;

    while (true) {
        from_network_layer(&buffer);
        s.info = buffer;
        to_physical_layer(&s);
    }
}
```

Sender loops blasting frames

```
void receiver1(void)
{
    frame r;
    event_type event;

    while (true) {
        wait_for_event(&event);
        from_physical_layer(&r);
        to_network_layer(&r.info);
    }
}
```

Receiver loops eating frames

- That's it, no error or flow control ...

Stop-and-Wait – Error-free channel

Protocol (p2) ensures sender can't outpace receiver:

- Receiver returns a dummy frame (ack) when ready
- Only one frame out at a time – called stop-and-wait
- We added flow control!

```
void sender2(void)
{
    frame s;
    packet buffer;
    event_type event;

    while (true) {
        from_network_layer(&buffer);
        s.info = buffer;
        to_physical_layer(&s);
        wait_for_event(&event);
    }
}
```

Sender waits to for ack after passing frame to physical layer

```
void receiver2(void)
{
    frame r, s;
    event_type event;
    while (true) {
        wait_for_event(&event);
        from_physical_layer(&r);
        to_network_layer(&r.info);
        to_physical_layer(&s);
    }
}
```

Receiver sends ack after passing frame to network layer

Stop-and-Wait – Noisy channel (1)

ARQ (Automatic Repeat reQuest) adds error control

- Receiver acks frames that are correctly delivered
- Sender sets timer and resends frame if no ack)

For correctness, frames and acks must be numbered

- Else receiver can't tell retransmission (due to lost ack or early timer) from new frame
- For stop-and-wait, 2 numbers (1 bit) are sufficient

Sliding Window Protocols

- Sliding Window concept »
- One-bit Sliding Window »
- Go-Back-N »
- Selective Repeat »

Sliding Window concept (1)

Sender maintains window of frames it can send

- Needs to buffer them for possible retransmission
- Window advances with next acknowledgements

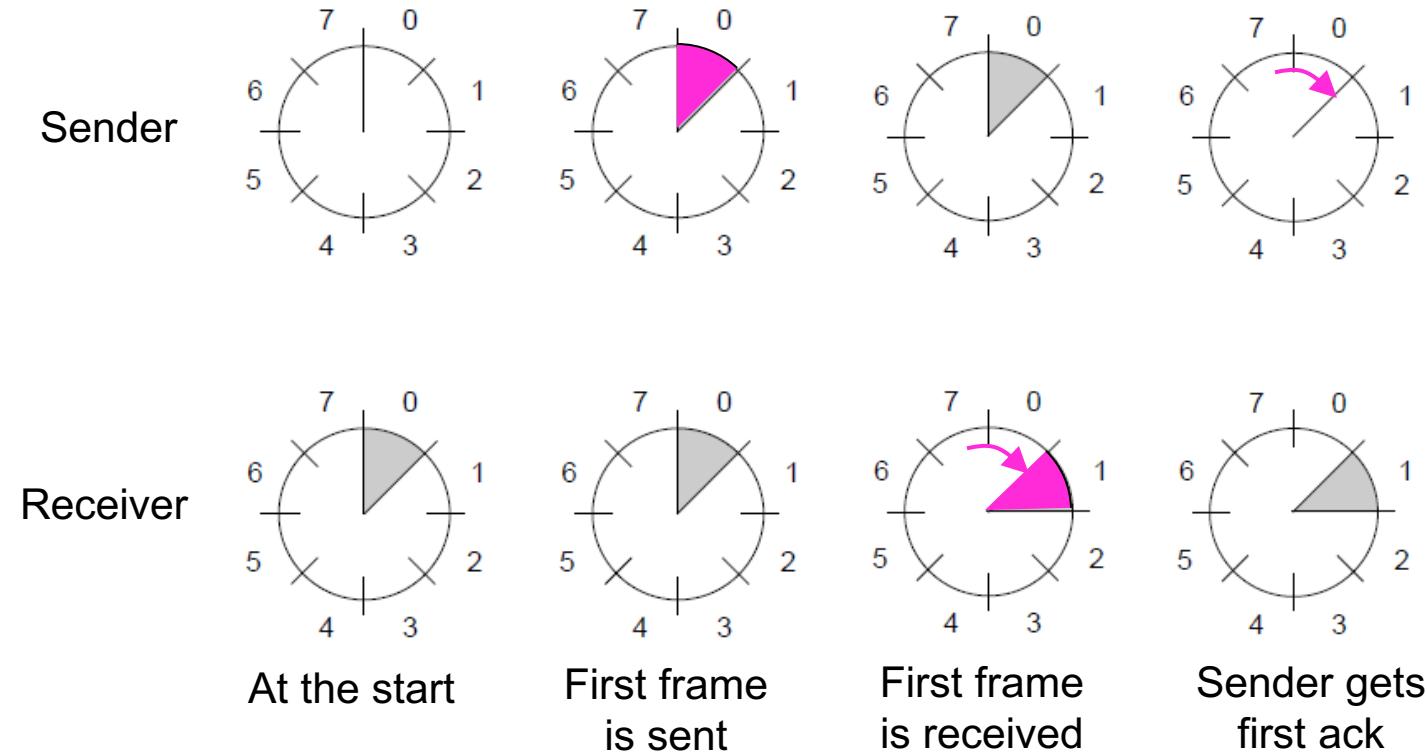
Receiver maintains window of frames it can receive

- Needs to keep buffer space for arrivals
- Window advances with in-order arrivals

Sliding Window concept (2)

A sliding window advancing at the sender and receiver

- Ex: window size is 1, with a 3-bit sequence number.



Sliding Window concept (3)

Larger windows enable pipelining for efficient link use

- Stop-and-wait ($w=1$) is inefficient for long links
- Best window (w) depends on bandwidth-delay (BD)
- Want $w \geq 2BD+1$ to ensure high link utilization

Pipelining leads to different choices for errors/buffering

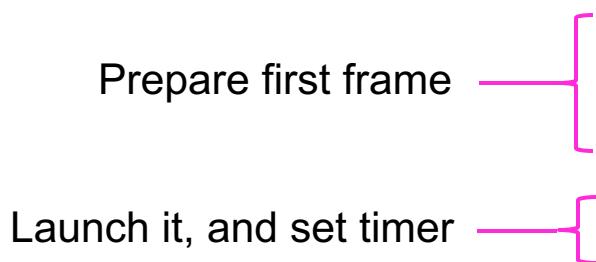
- We will consider Go-Back-N and Selective Repeat

One-Bit Sliding Window (1)

Transfers data in both directions with stop-and-wait

- Piggybacks acks on reverse data frames for efficiency
- Handles transmission errors, flow control, early timers

Each node is sender
and receiver (p4):



```
void protocol4 (void) {  
    seq_nr next_frame_to_send;  
    seq_nr frame_expected;  
    frame r, s;  
    packet buffer;  
    event_type event;  
    next_frame_to_send = 0;  
    frame_expected = 0;  
    from_network_layer(&buffer);  
    s.info = buffer;  
    s.seq = next_frame_to_send;  
    s.ack = 1 - frame_expected;  
    to_physical_layer(&s);  
    start_timer(s.seq);  
    . . .
```

One-Bit Sliding Window (2)

Wait for frame or timeout

If a frame with new data
then deliver it

If an ack for last send then
prepare for next data frame

(Otherwise it was a timeout)

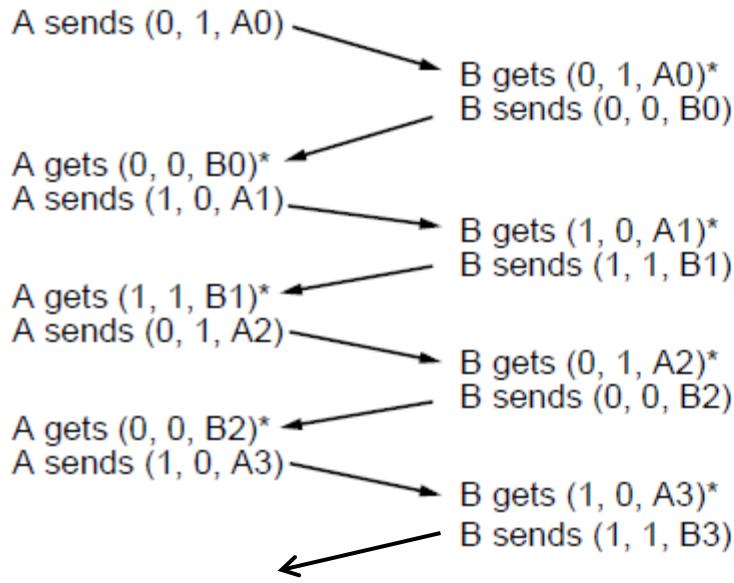
Send next data frame or
retransmit old one; ack
the last data we received

```
    . . .
while (true) {
    → wait_for_event(&event);
    if (event == frame_arrival) {
        from_physical_layer(&r);
        if (r.seq == frame_expected) {
            to_network_layer(&r.info);
            inc(frame_expected);
        }
        if (r.ack == next_frame_to_send) {
            stop_timer(r.ack);
            from_network_layer(&buffer);
            inc(next_frame_to_send);
        }
    }
    s.info = buffer;
    s.seq = next_frame_to_send;
    s.ack = 1 - frame_expected;
    → to_physical_layer(&s);
    start_timer(s.seq);
}
```

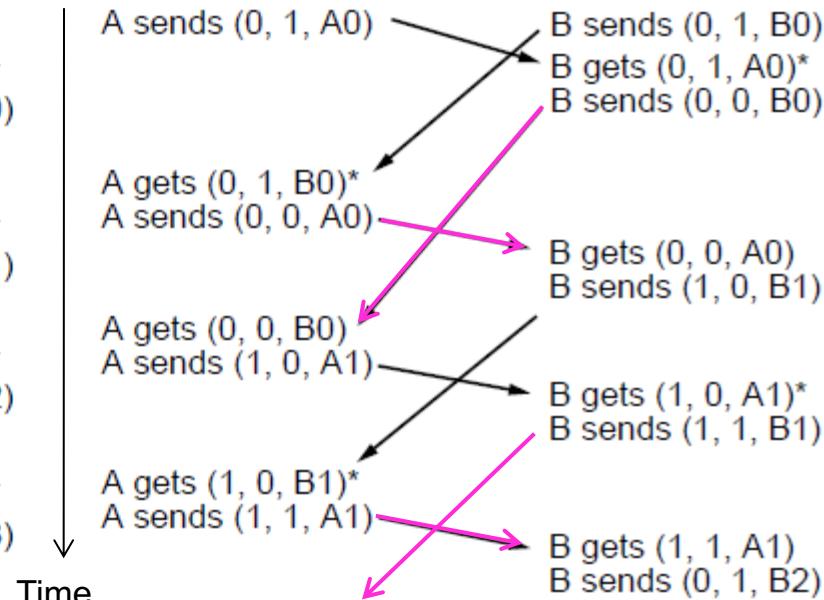
One-Bit Sliding Window (3)

Two scenarios show subtle interactions exist in p4:

- Simultaneous start [right] causes correct but slow operation compared to normal [left] due to duplicate transmissions.



Normal case

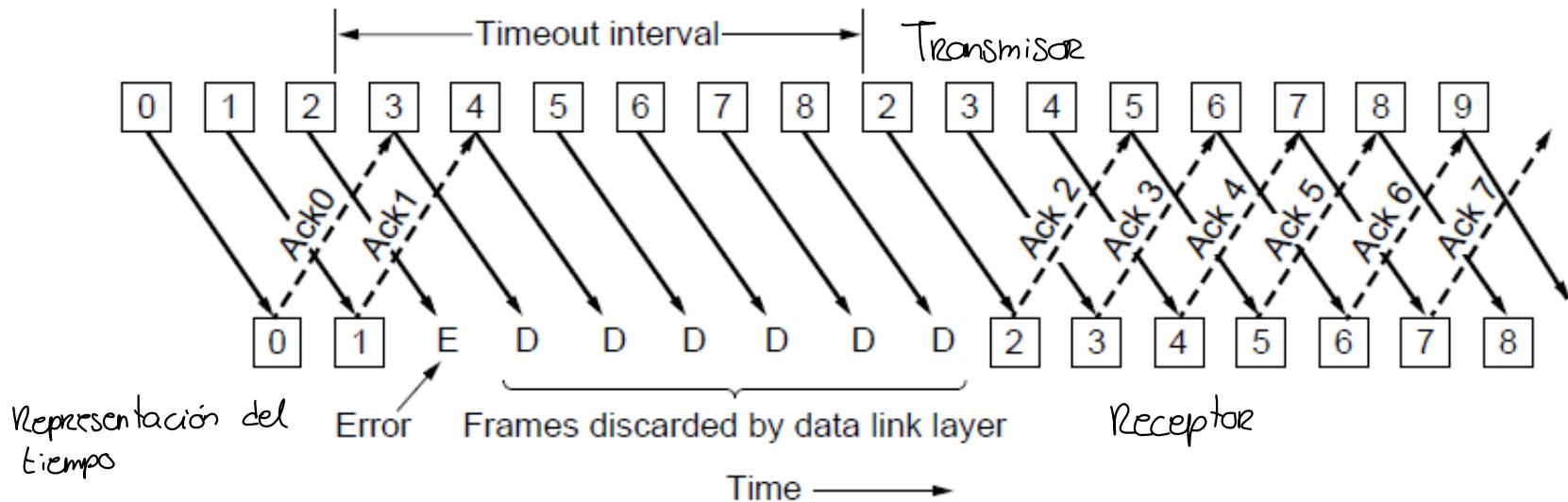


Correct, but poor performance

Go-Back-N (1)

Receiver only accepts/acks frames that arrive in order:

- Discards frames that follow a missing/errored frame
- Sender times out and resends all outstanding frames



Go-Back-N (2)

Tradeoff made for Go-Back-N:

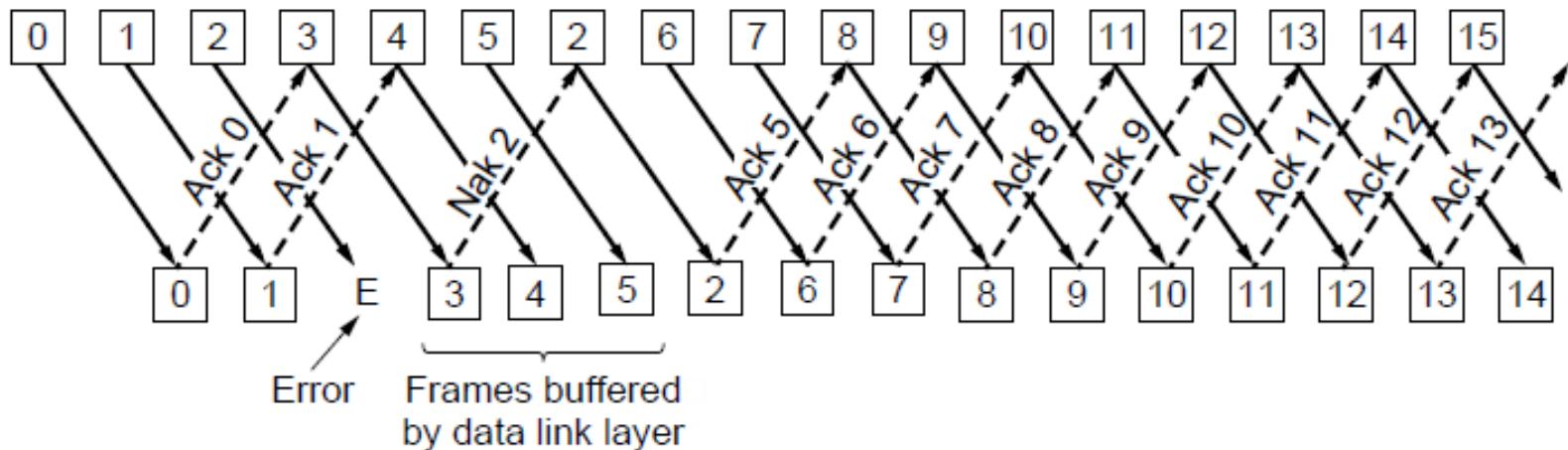
- Simple strategy for receiver; needs only 1 frame
- Wastes link bandwidth for errors with large windows; entire window is retransmitted

Implemented as p5 (see code in book)

Selective Repeat (1)

Receiver accepts frames anywhere in receive window

- Cumulative ack indicates highest in-order frame
- NAK (negative ack) causes sender retransmission of a missing frame before a timeout resends window



Selective Repeat (2)

Tradeoff made for Selective Repeat:

- More complex than Go-Back-N due to buffering at receiver and multiple timers at sender
- More efficient use of link bandwidth as only lost frames are resent (with low error rates)

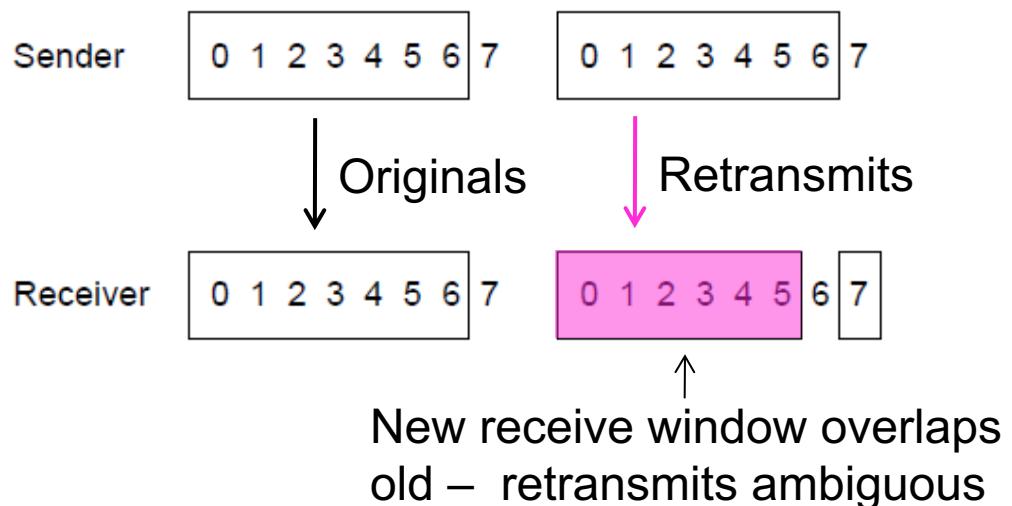
Implemented as p6 (see code in book)

Selective Repeat (3)

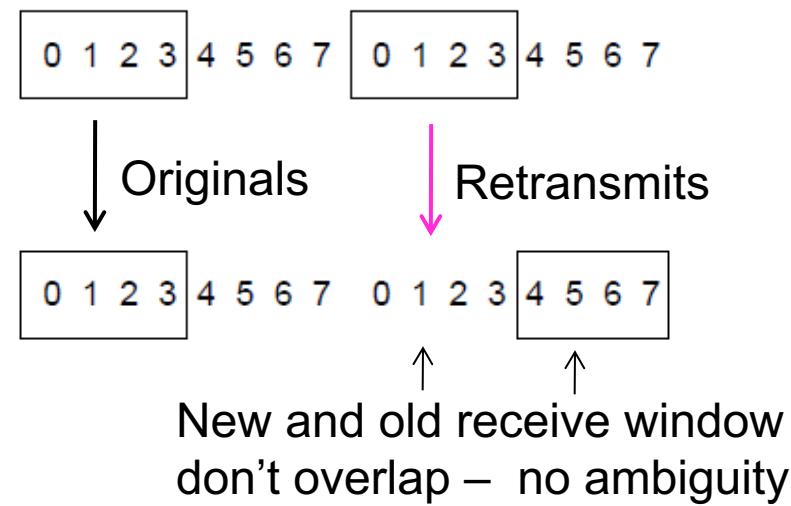
For correctness, we require:

- Sequence numbers (s) at least twice the window (w)

Error case ($s=8$, $w=7$) – too few sequence numbers



Correct ($s=8$, $w=4$) – enough sequence numbers



CRC

Cálculo del CRC con MATLAB

Ejemplo

Calcula el CRC de la secuencia de bits (trama) 1001 usando el CRC-3 GSM (0x3)

```
>> p = 2; %GF(2)
```

Los datos representados por un polinomio (invertimos el orden) y agregamos tres ceros

```
>> b = [ 0 0 0 1 0 0 1];
```

```
>> gfpoly(b);
```

Polinomio divisor (0x3 -> 11 -> 1011)

```
>> a = [1 1 0 1];
```

```
>> gfpoly(a);
```

Calcula la división de b entre a

```
>> [q,r] = gfdeconv(b,a,p)
```

```
q = 0 1 0 1
```

```
r = 0 1 1
```

El cociente es q y el residuo r (CRC)

```
>> gfpoly(r);
```

La trama completa sería los bits originales+CRC = 1001110

Los últimos tres bits corresponden al CRC (orden inverso)

Comprobación del CRC

- Trama

```
>> c = [0 1 1 1 0 0 1]  
>> [q,r] = gfdeconv(c,a,p)  
q = 0 1 0 1  
r = 0
```

Ejercicios.

- Realiza el cálculo del CRC para las siguientes tramas y estándares. Para los casos más sencillos se sugiere realizar el cálculo manualmente y posteriormente comprobar los resultados en MATLAB.

Trama/estándar CRC

- 1 1 1 1 /CRC-3-GSM
- 0 1 1 0 1 1 0 / CRC-4-ITU
- 1 0 0 0 0 1 / CRC-4-ITU
- 1 0 1 0 1 0 0 1 1 /CRC-5-EPC
- 0xA012/CRC-8-CCITT

Ejercicios.

- Comprueba si las siguientes tramas están libres de errores

- 1 1 0 0 1 1 1 1 1 0 1 1/CRC-4
- 1 0 1 1 0 1 0 0 1 1 0 0/CRC-4
- 1 0 1 1 1 1 1/CRC-5-ITU

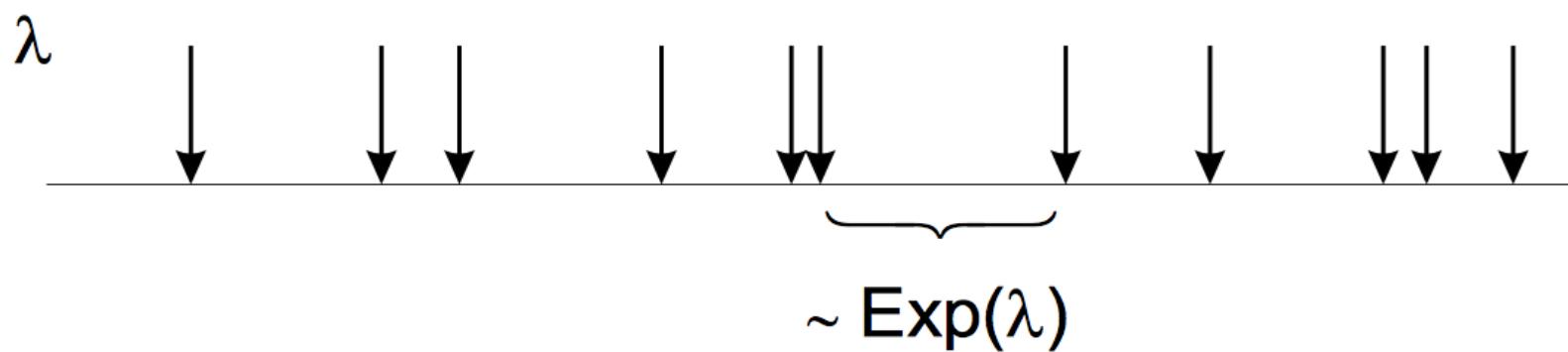
Distribución Poisson

Redes de Computadoras.

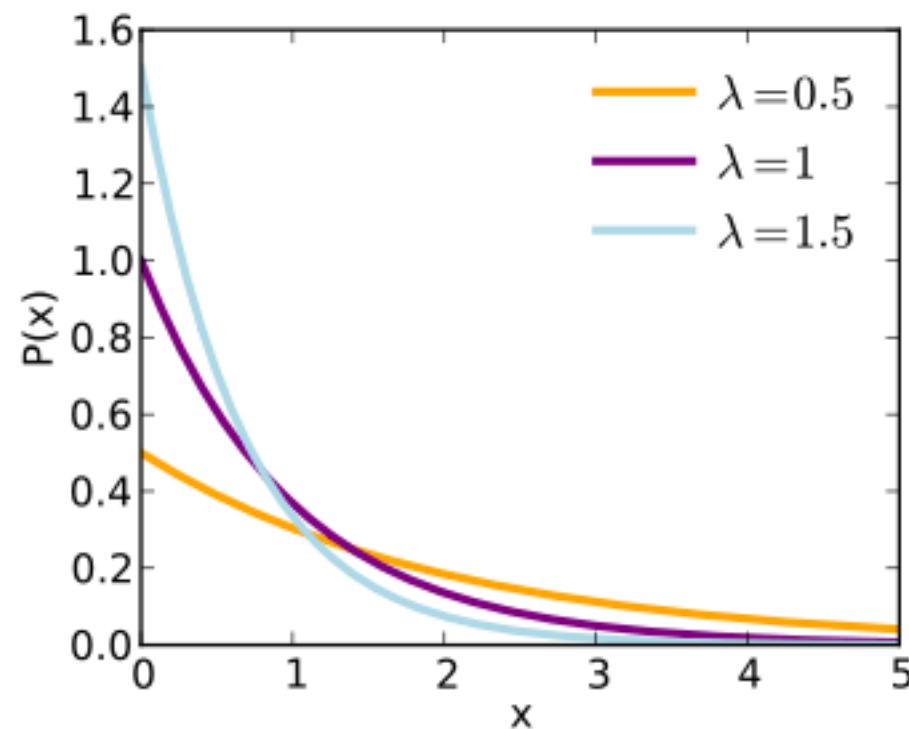
Definición

Los tiempos entre llegadas (interarrival time) son independientes y obedecen a una distribución exponencial.

$$P\{\text{interarrival time} > t\} = e^{-\lambda t}$$



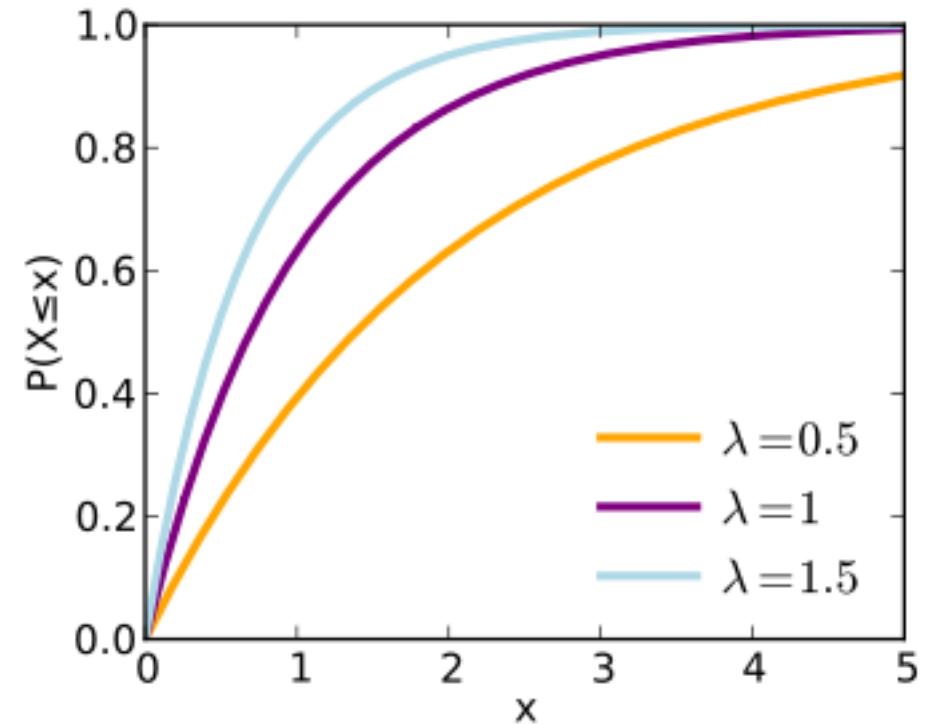
Distribución exponencial



Función de distribución acumulada

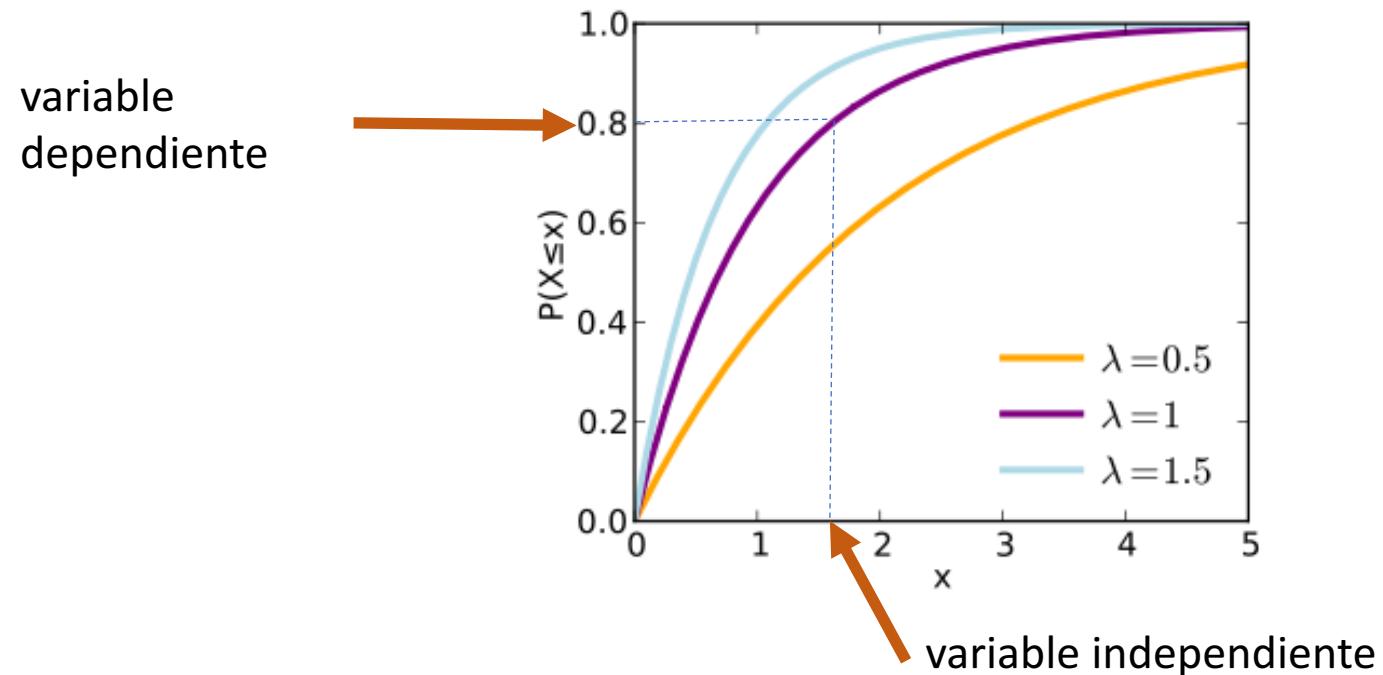
$$F(x) = P(X \leq x) = \begin{cases} 0 & \text{para } x < 0 \\ 1 - e^{-\lambda x} & \text{para } x \geq 0 \end{cases}$$

$$E[X] = \frac{1}{\lambda}, \quad V(X) = \frac{1}{\lambda^2}$$



Generación de un proceso aleatorio con distribución Poisson

Partiremos de una variable aleatoria distribuida uniformemente (variable dependiente), deseamos encontrar el valor correspondiente de la variable independiente de la distribución de probabilidad acumulada.



Generación de un proceso aleatorio con distribución Poisson

El problema consiste en encontrar la función inversa de la función exponencial $F(x)$ a partir de una variable uniformemente distribuida $u = U(0,1)$

$$F(x) = P(X \leq x) = \begin{cases} 0 & \text{para } x < 0 \\ 1 - e^{-\lambda x} & \text{para } x \geq 0 \end{cases}$$

Función inversa:

$$x = -\frac{1}{\lambda} \ln(1 - u)$$

Como $1-u$, es nuevamente una variable uniformemente distribuida

$$x = -\frac{1}{\lambda} \ln(u)$$

Implementaciones. Python

```
import math
import random
def nextTime(rateParameter):
    return -math.log(1.0 - random.random()) / rateParameter
```

En python existe la biblioteca `random.expovariate(lambda)`

<https://docs.python.org/3/library/random.html#random.expovariate>

Implementaciones. C

```
#include <math.h>
#include <stdlib.h>
float nextTime(float rateParameter)
{
    return -logf(1.0f - (float) random() / (RAND_MAX + 1)) / rateParameter;
}
```

Medium Access Control Sublayer

Chapter 4

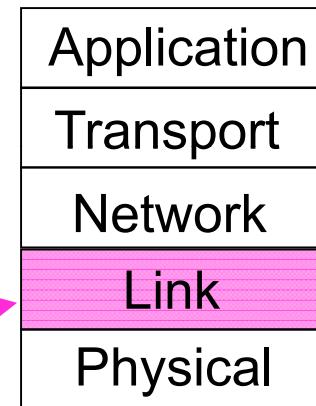
- Channel Allocation Problem
- Multiple Access Protocols
- Ethernet
- Wireless LANs
- Broadband Wireless
- Bluetooth
- RFID
- Data Link Layer Switching

Revised: August 2011

The MAC Sublayer

Responsible for deciding who sends next on a multi-access link

- An important part of the link layer, especially for LANs



MAC is in here!

Channel Allocation Problem (1)

For fixed channel and traffic from N users

- Divide up bandwidth using FTM, TDM, CDMA, etc.
- This is a static allocation, e.g., FM radio

This static allocation performs poorly for bursty traffic

- Allocation to a user will sometimes go unused

Channel Allocation Problem (2)

Dynamic allocation gives the channel to a user when they need it. Potentially N times as efficient for N users.

Schemes vary with assumptions:

Assumption	Implication
Independent traffic	Often not a good model, but permits analysis
Single channel	No external way to coordinate senders
Observable collisions	Needed for reliability; mechanisms vary
Continuous or slotted time	Slotting may improve performance
Carrier sense	Can improve performance if available

Si el canal se encuentra libre o no

Multiple Access Protocols

- ALOHA » método que nació de Hawaii. Estación base con diferentes islas
- CSMA (Carrier Sense Multiple Access) »
- Collision-free protocols »
- Limited-contention protocols »
- Wireless LAN protocols »

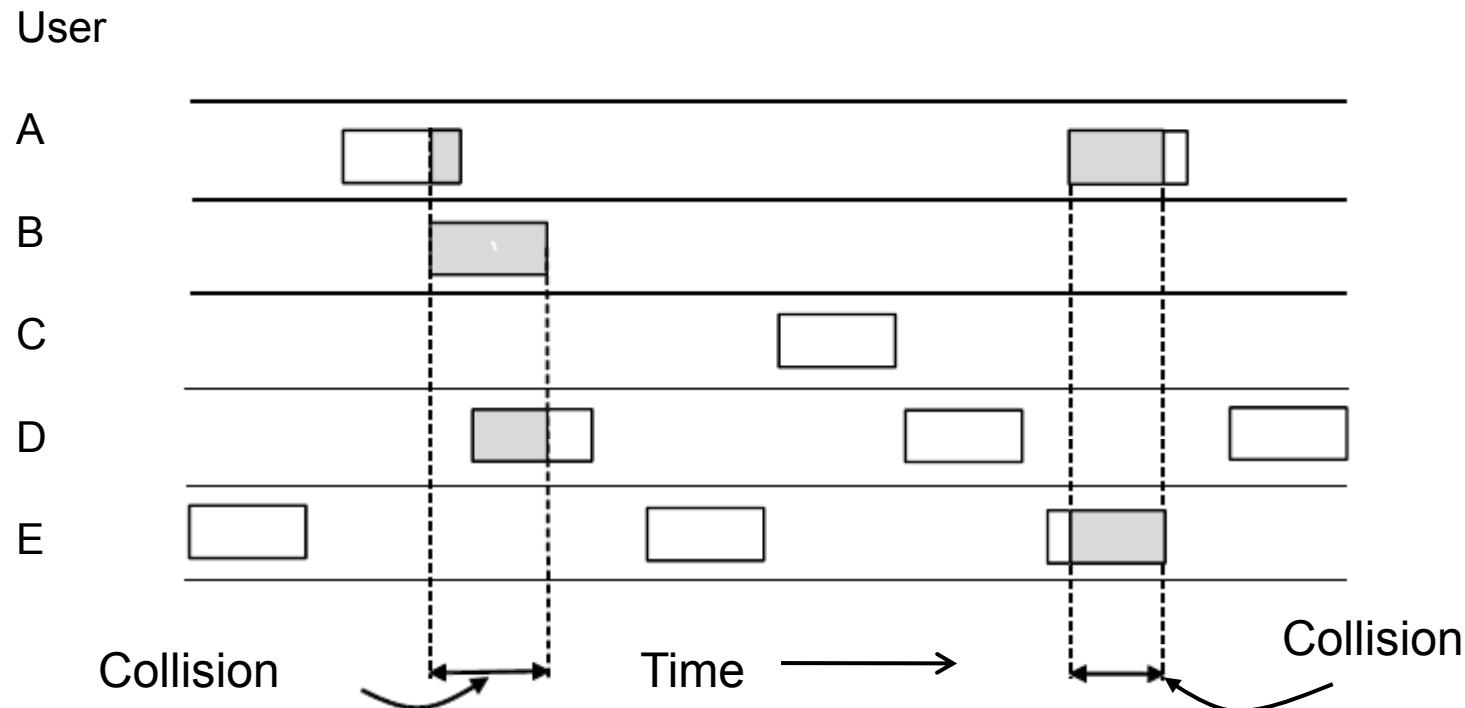
ALOHA (1)

Retransmisión? → los que tienen acuse de recibo. negativo

Control de flujo retransmisiones: cuando pasa un intervalo de tiempo

In pure ALOHA, users transmit frames whenever they have data; users retry after a random time for collisions

- Efficient and low-delay under low load



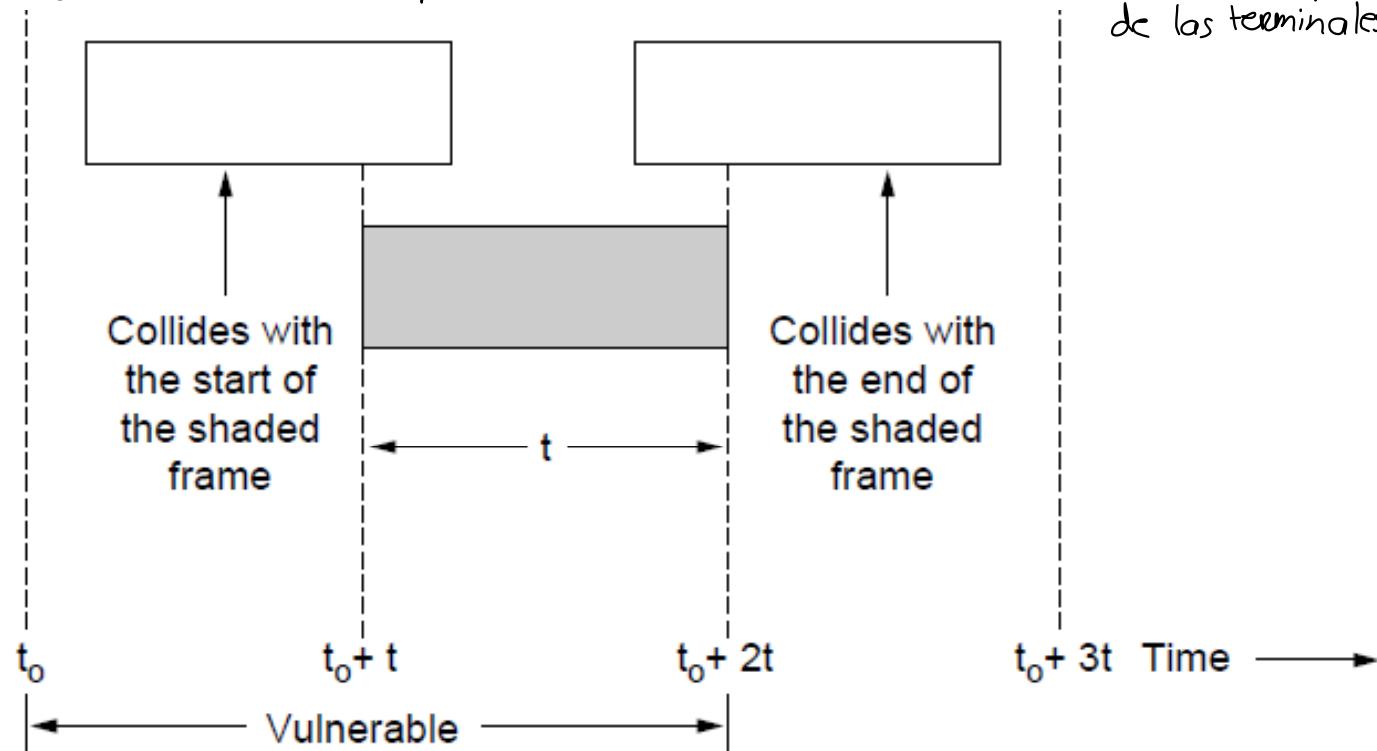
ALOHA (2)

Collisions happen when other users transmit during a vulnerable period that is twice the frame time

- Synchronizing senders to slots can reduce collisions

Bits de info se traslapan con el otro bit.

Colisión depende de la distancia de los terminales.



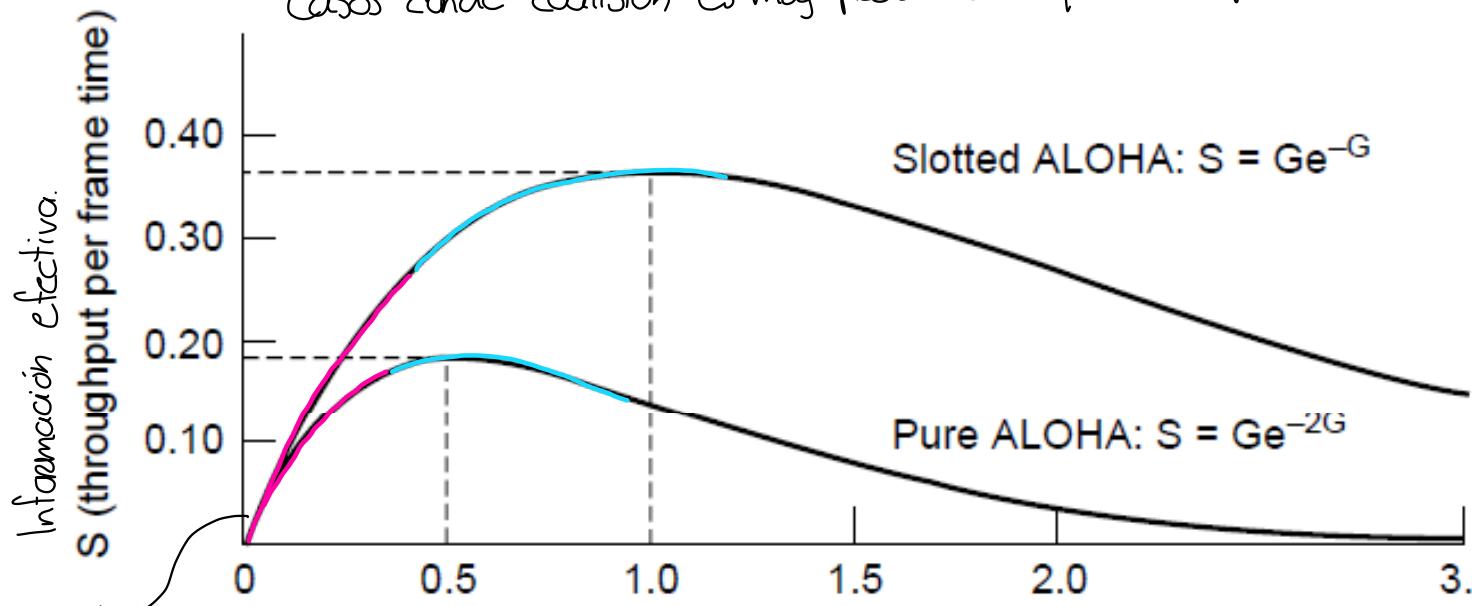
ALOHA (3)

Versión mejorada. ALOHA randomizado. Tramas empiezan en tiempo predefinido

Slotted ALOHA is twice as efficient as pure ALOHA

- Low load wastes slots, high loads causes collisions
- Efficiency up to $1/e$ (37%) for random traffic models

(casos donde colisión es muy probable → quitar los peores casos)



tráfico aumenta con menos velocidad el crecimiento de la red.
Info efectiva.

máximo: al llegar al máximo empieza a decrecer el throughput.

CSMA (1)

CSMA improves on ALOHA by sensing the channel!

- User doesn't send if it senses someone else

Dispositivos pueden escuchar el canal antes de transmitir.

Dispositivos no tienen que moverse, solo esperan a que el canal esté libre.

Variations on what to do if the channel is busy:

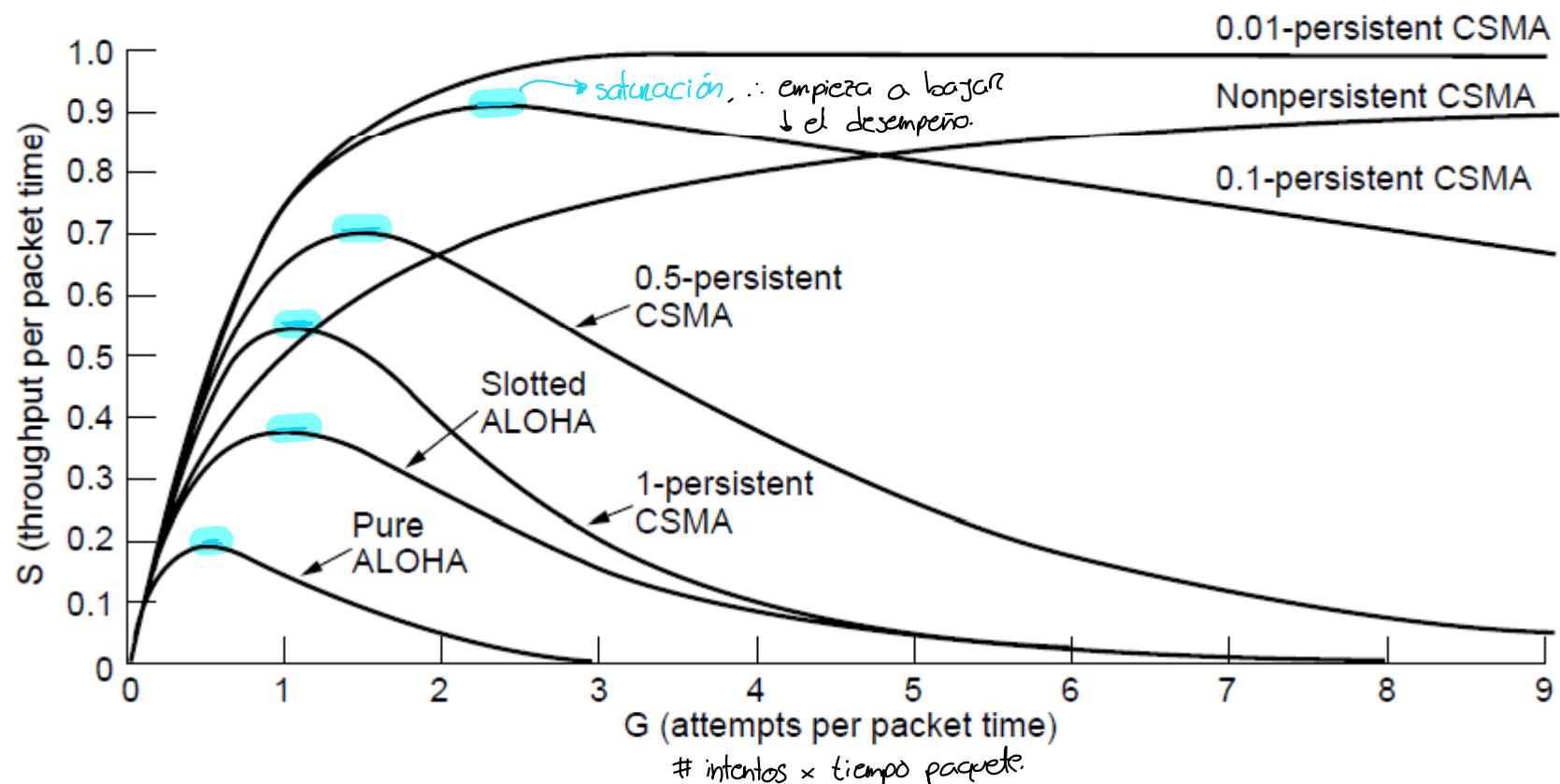
- 1-persistent (greedy) sends as soon as idle
- Nonpersistent waits a random time then tries again
- p-persistent sends with probability p when idle

cuando el canal está libre
empieza a transmitir.

Inconveniente: Si hay varios escuchando, al momento de liberarse, todos van a querer transmitir y provoca saturación.

CSMA (2) – Persistence

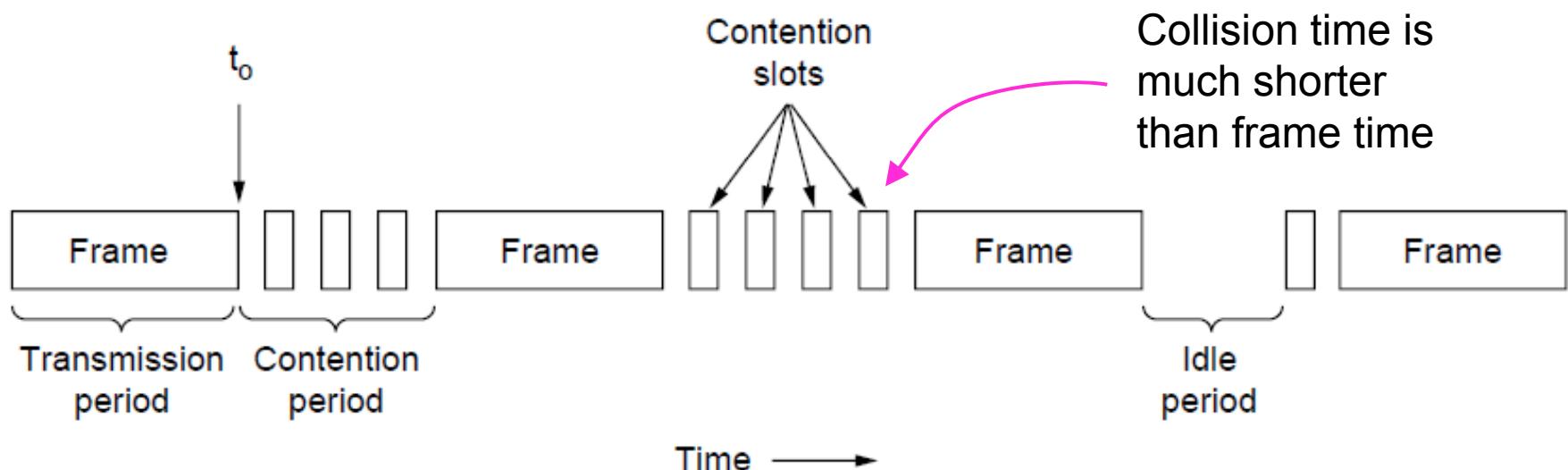
CSMA outperforms ALOHA, and being less persistent is better under high load



CSMA (3) – Collision Detection

CSMA/CD improvement is to detect/abort collisions

- Reduced contention times improve performance



Primero se verifica que este libre el medio (carrier sense), luego transmite la trama y al mismo tiempo estoy recibiendo.

Ranuras de contención: espacios donde se busca separar el medio en una transmisión.

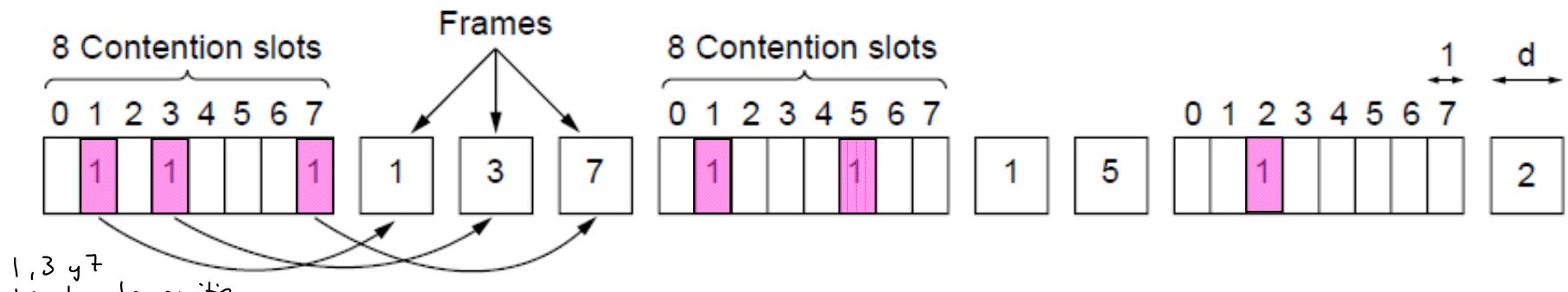
Collision-Free (1) – Bitmap

Collision-free protocols avoid collisions entirely

- Senders must know when it is their turn to send

The basic bit-map protocol:

- Sender set a bit in contention slot if they have data
- Senders send in turn; everyone knows who has data



1, 3 y 7
intento transmitir

Primeros reservan el lugar a donde transmitir y luego transmite. Cuando transmite todos, se puede volver a reservar.
de estaciones debe contener a todos los que quieren transmitir

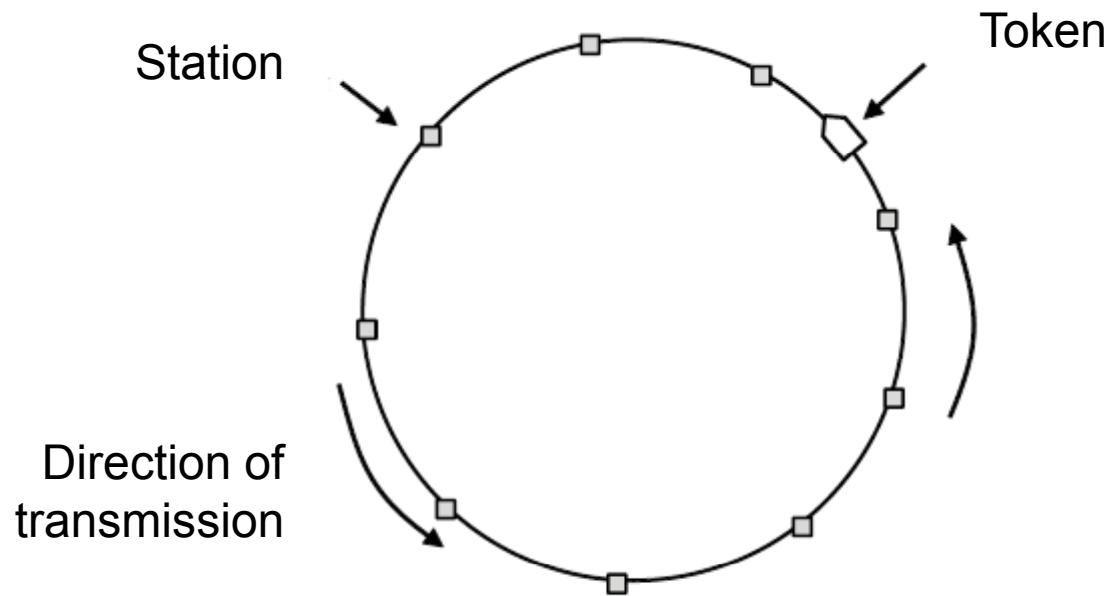
Ventaja: No hay colisiones.

Collision-Free (2) – Token Ring

estafeta.

Token sent round ring defines the sending order

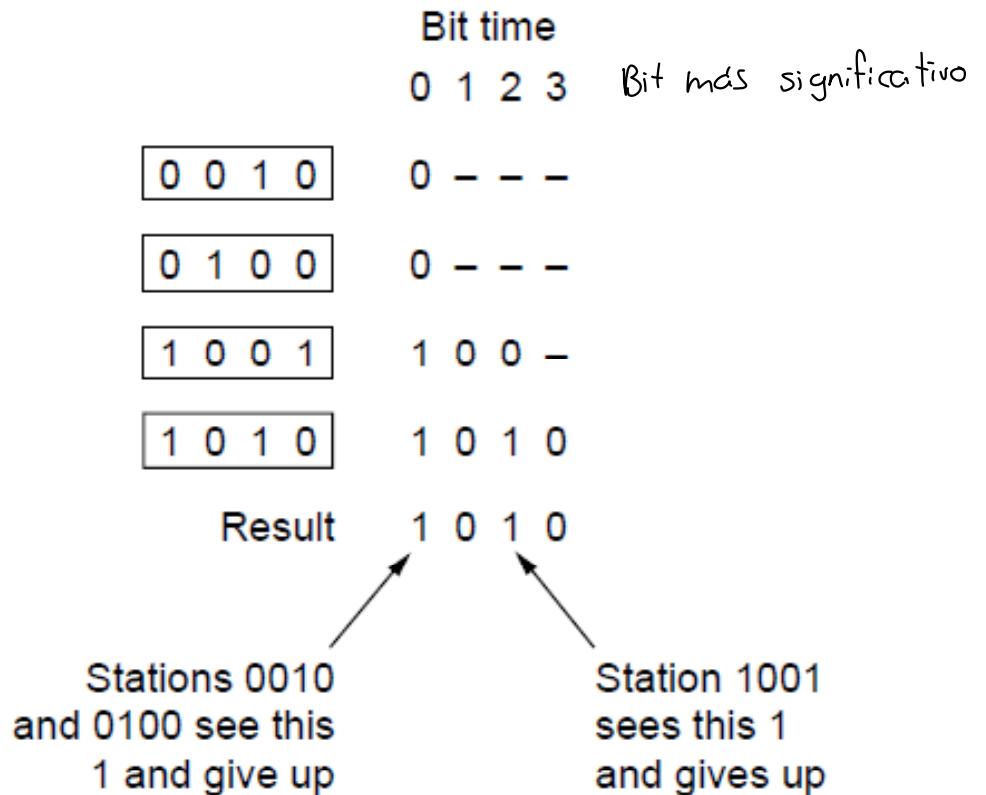
- Station with token may send a frame before passing
- Idea can be used without ring too, e.g., token bus



Collision-Free (3) – Countdown

Binary countdown improves on the bitmap protocol

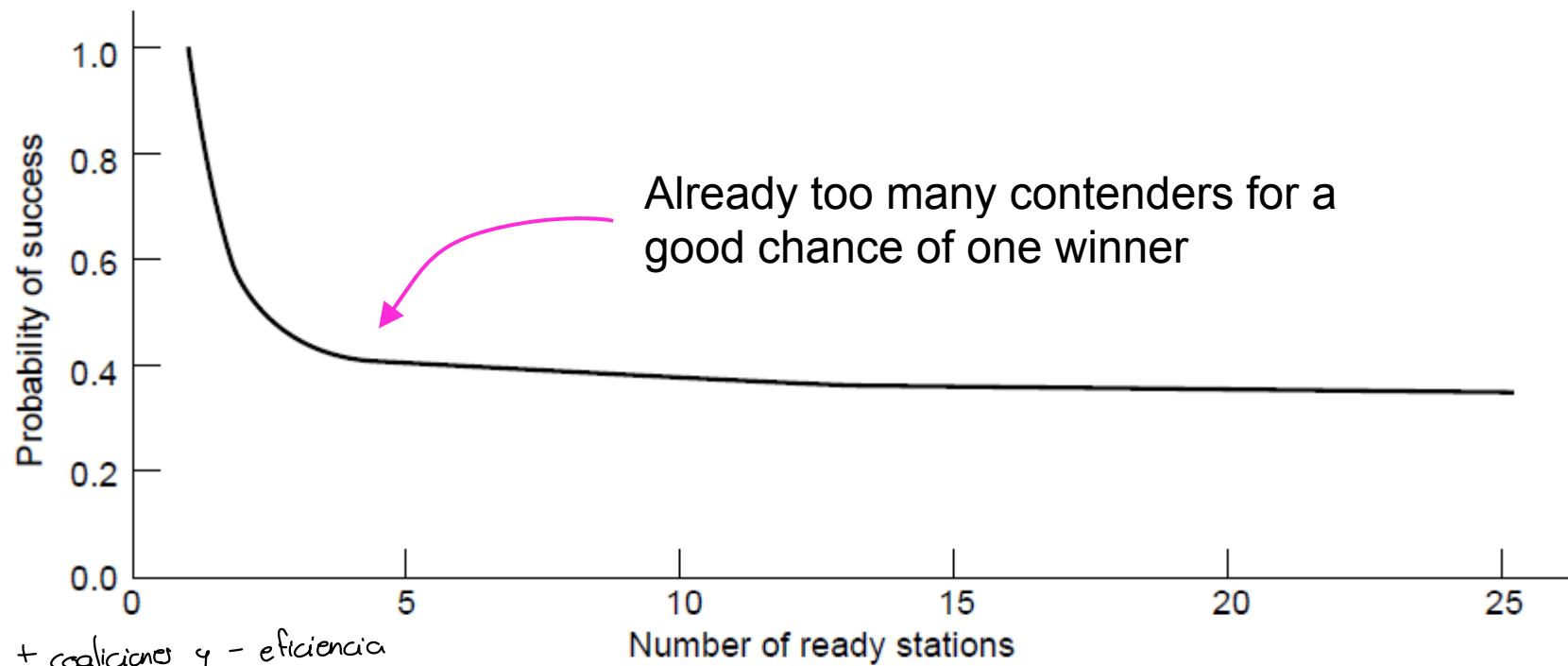
- Stations send their address in contention slot ($\log N$ bits instead of N bits)
- Medium ORs bits; stations give up when they send a “0” but see a “1”
- Station that sees its full address is next to send



Limited-Contention Protocols (1)

Idea is to divide stations into groups within which only a very small number are likely to want to send

- Avoids wastage due to idle periods and collisions

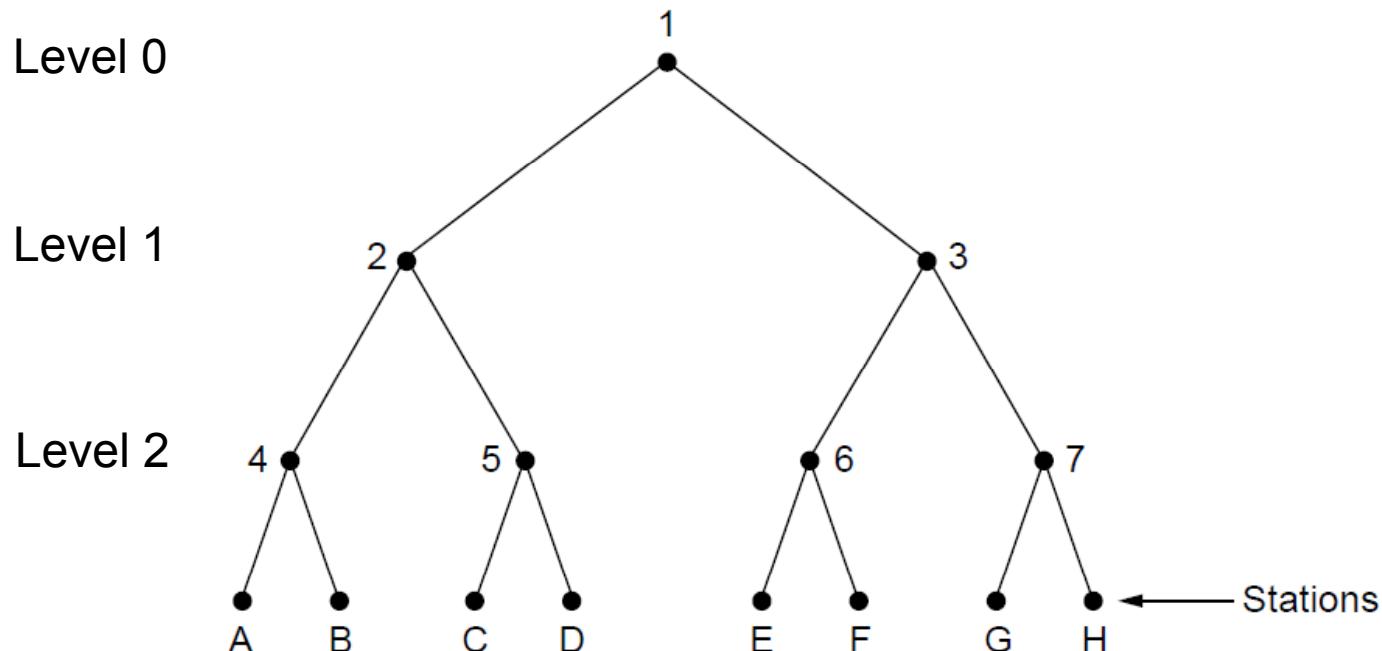


+ estaciones = + colisiones y - eficiencia
se limitan el # de estaciones

Limited Contention (2) –Adaptive Tree Walk

Tree divides stations into groups (nodes) to poll

- Depth first search under nodes with poll collisions
- Start search at lower levels if >1 station expected



Wireless LAN Protocols (1)

Medio inalámbrico permite más libertad de los elementos.

Wireless has complications compared to wired.

Nodes may have different coverage regions

- Leads to hidden and exposed terminals

Nodes can't detect collisions, i.e., sense while sending

- Makes collisions expensive and to be avoided

Wireless LANs (2) – Hidden terminals

Terminal Oculta:

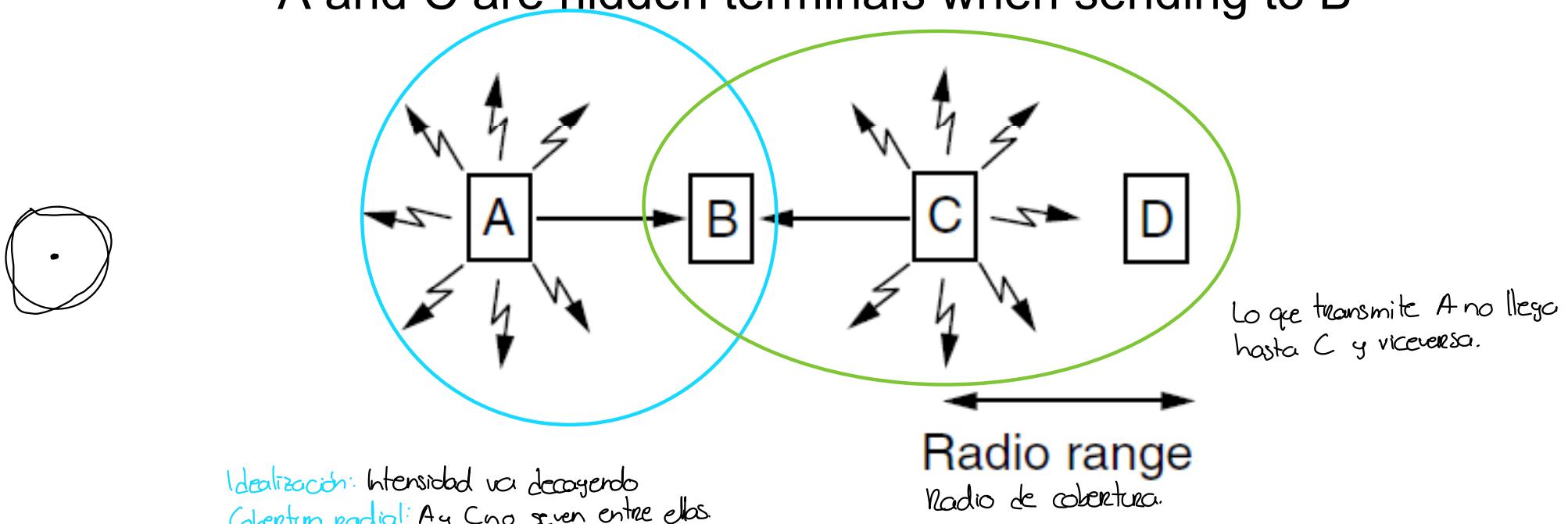
Clave de todo está dado por la cobertura.

Sistemas inalámbricos no garantizan que a mayor distancia menor eficiencia.

Antenas omnidireccionales → todas las direcciones.

Hidden terminals are senders that cannot sense each other but nonetheless collide at intended receiver

- Want to prevent; loss of efficiency
- A and C are hidden terminals when sending to B



Idealización: Intensidad va decayendo

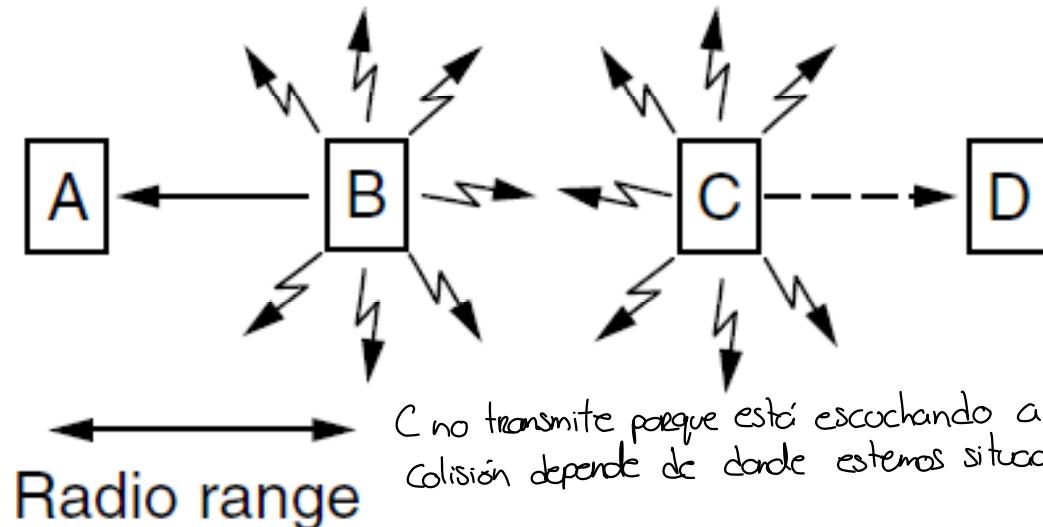
Cobertura radial: A y C no se ven entre ellos.

CSMA: Cada vez sense, nunca va a escuchar entre A y C.

Wireless LANs (3) – Exposed terminals

Exposed terminals are senders who can sense each other but still transmit safely (to different receivers)

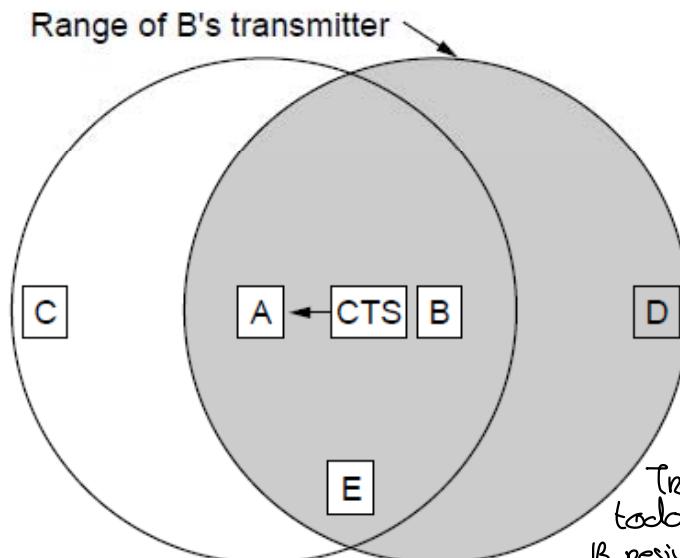
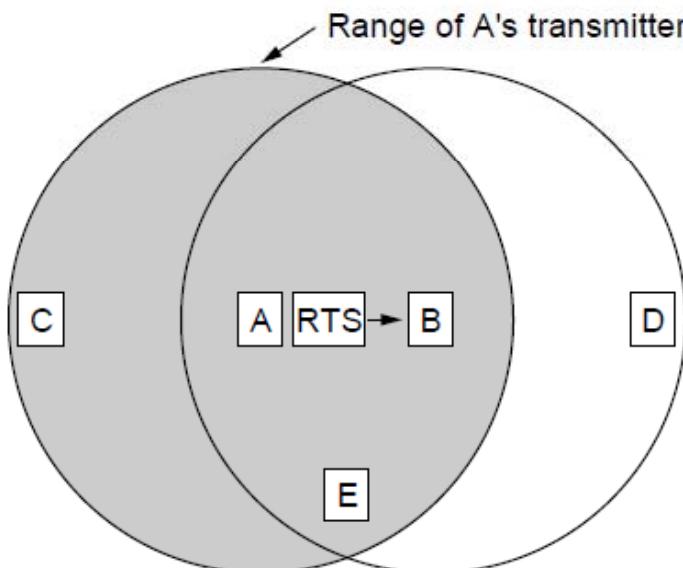
- Desirably concurrency; improves performance
- $B \rightarrow A$ and $C \rightarrow D$ are exposed terminals



Wireless LANs (4) – MACA

MACA protocol grants access for A to send to B:

- A sends RTS to B [left]; B replies with CTS [right]
- A can send with exposed but no hidden terminals



Tramo de aviso hacia todo el entorno de que B resuena una trama.

Aviso de envío.

A sends RTS to B; C and E
hear and defer for CTS

B replies with CTS; D and
E hear and defer for data

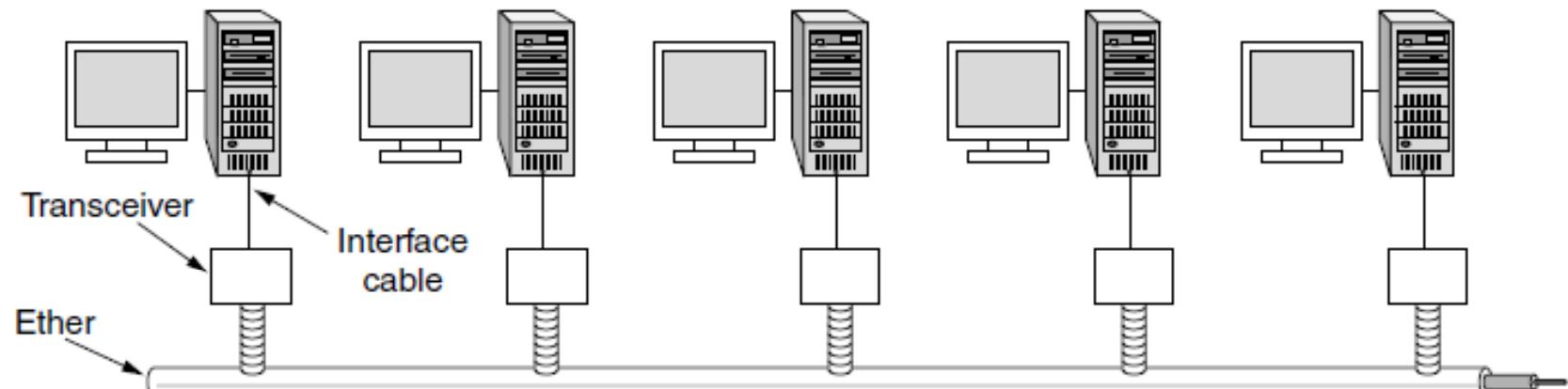
Ethernet

- Classic Ethernet »
- Switched/Fast Ethernet »
- Gigabit/10 Gigabit Ethernet »

Classic Ethernet (1) – Physical Layer

One shared coaxial cable to which all hosts attached

- Up to 10 Mbps, with Manchester encoding
- Hosts ran the classic Ethernet protocol for access



Este método ya se dejó de utilizar

Classic Ethernet (2) – MAC

MAC protocol is 1-persistent CSMA/CD (earlier)

- Random delay (backoff) after collision is computed with BEB (Binary Exponential Backoff)
- Frame format is still used with modern Ethernet.

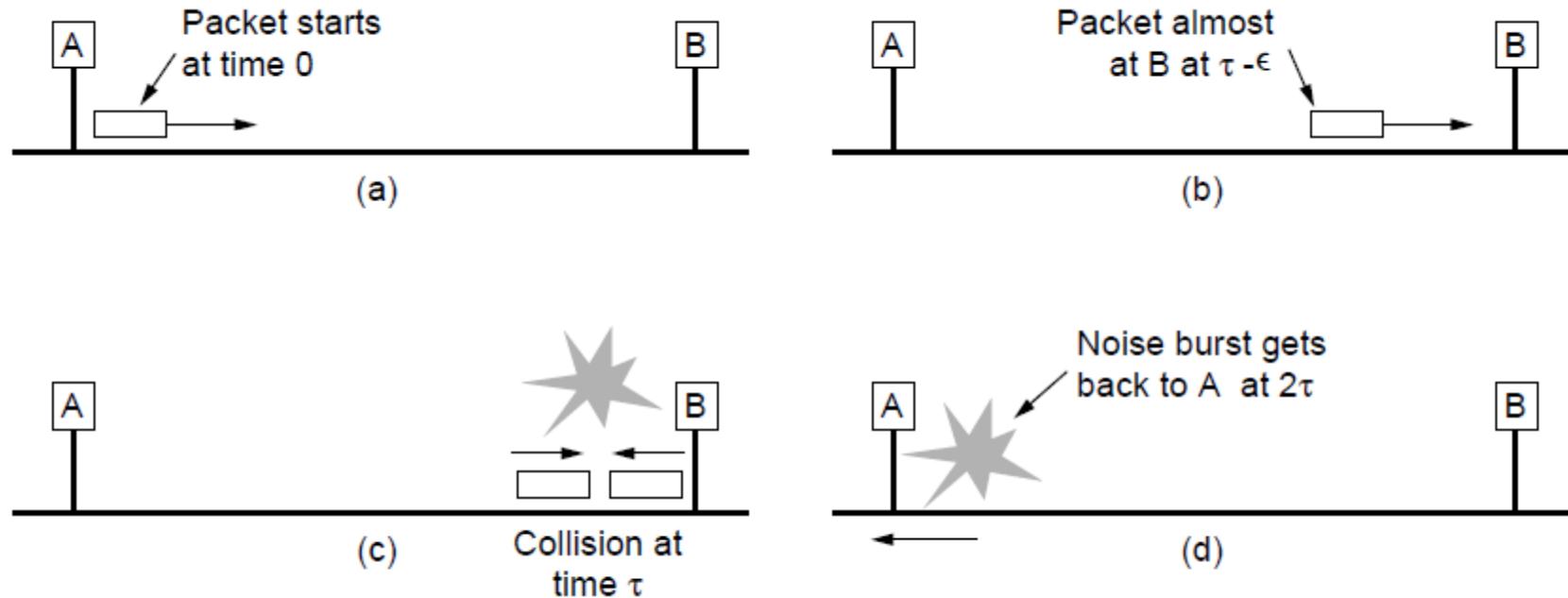
	Bytes	8	6	6	2	0-1500	0-46	4	
Ethernet (DIX)		Preamble	Destination address	Source address	Type	Data	Pad	Check-sum	equivalente al CRC
Red local con Ethernet	IEEE 802.3	Preamble	S O F	Destination address	Source address	Length	Data	Pad	Check-sum

Indica donde empieza la trama. Tasa de transmisión

Classic Ethernet (3) – MAC

Collisions can occur and take as long as 2τ to detect

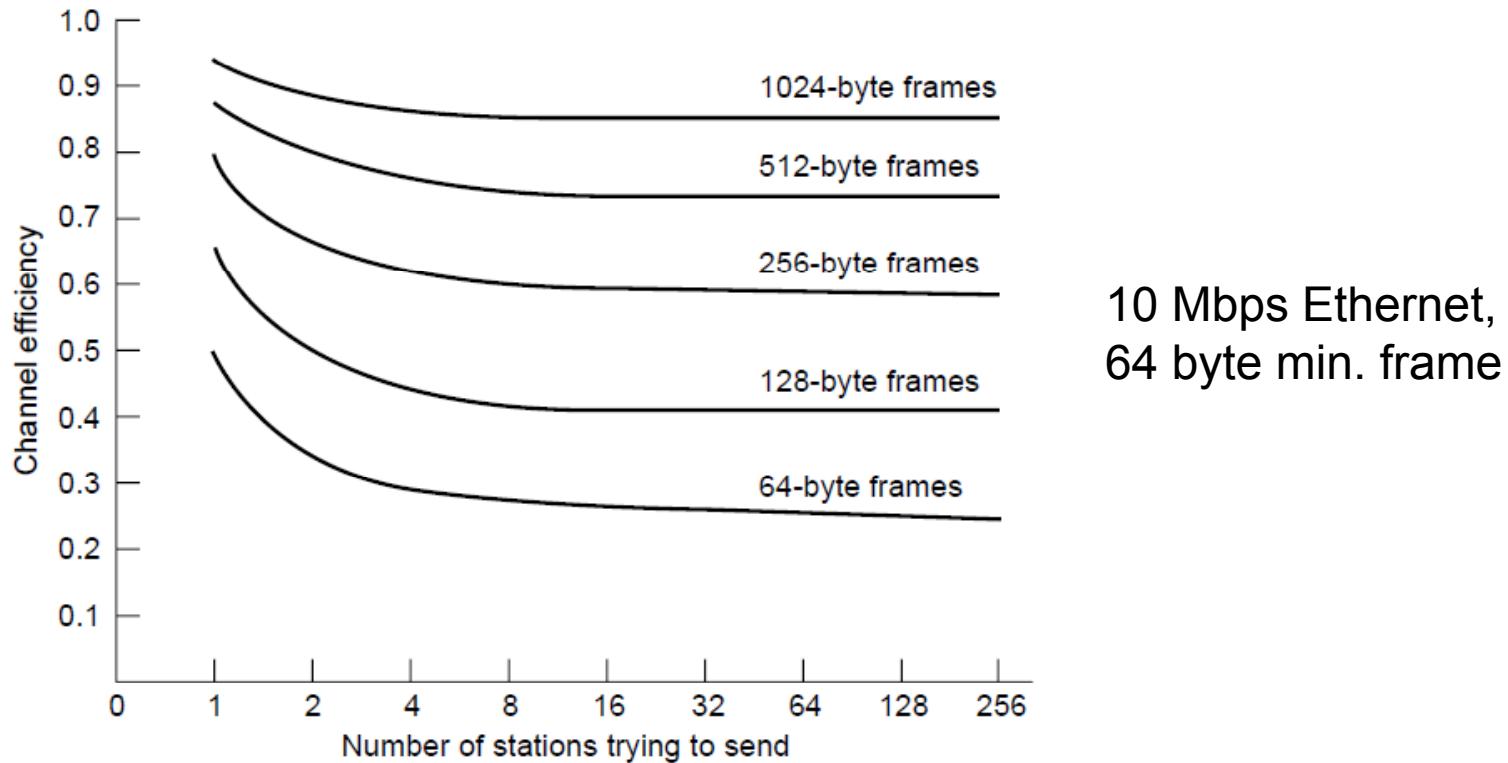
- τ is the time it takes to propagate over the Ethernet
- Leads to minimum packet size for reliable detection



Classic Ethernet (4) – Performance

Efficient for large frames, even with many senders

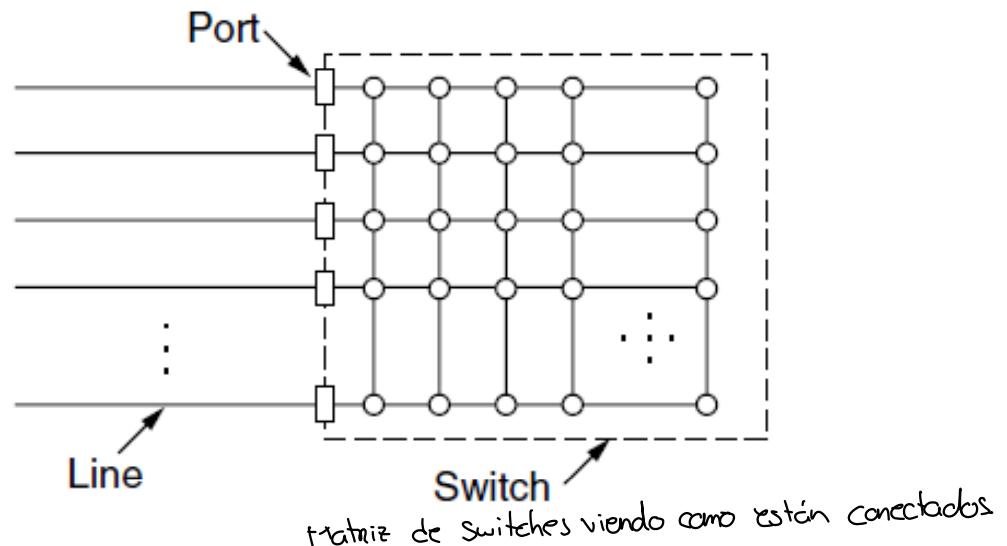
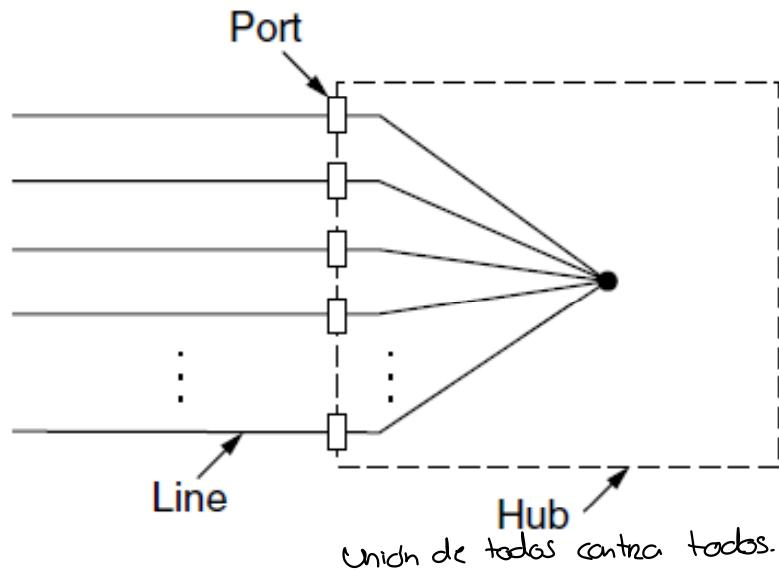
- Degrades for small frames (and long LANs)



Switched/Fast Ethernet (1)

Ethernet clásico

- Hubs wire all lines into a single CSMA/CD domain
- Switches isolate each port to a separate domain
 - Much greater throughput for multiple ports
 - No need for CSMA/CD with full-duplex lines

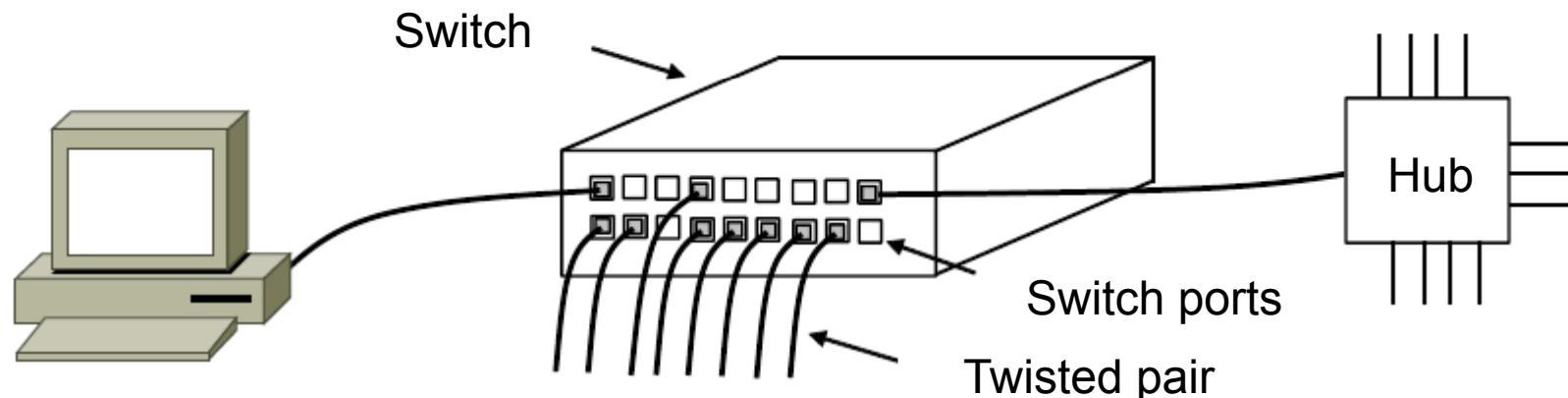


Switched/Fast Ethernet (2)

Se emplean actualmente. Medio de transmisión. Debemos usar más switch que hubs.

Switches can be wired to computers, hubs and switches

- Hubs concentrate traffic from computers
- More on how to switch frames the in 4.8



Switched/Fast Ethernet (3)

Fast Ethernet extended Ethernet from 10 to 100 Mbps

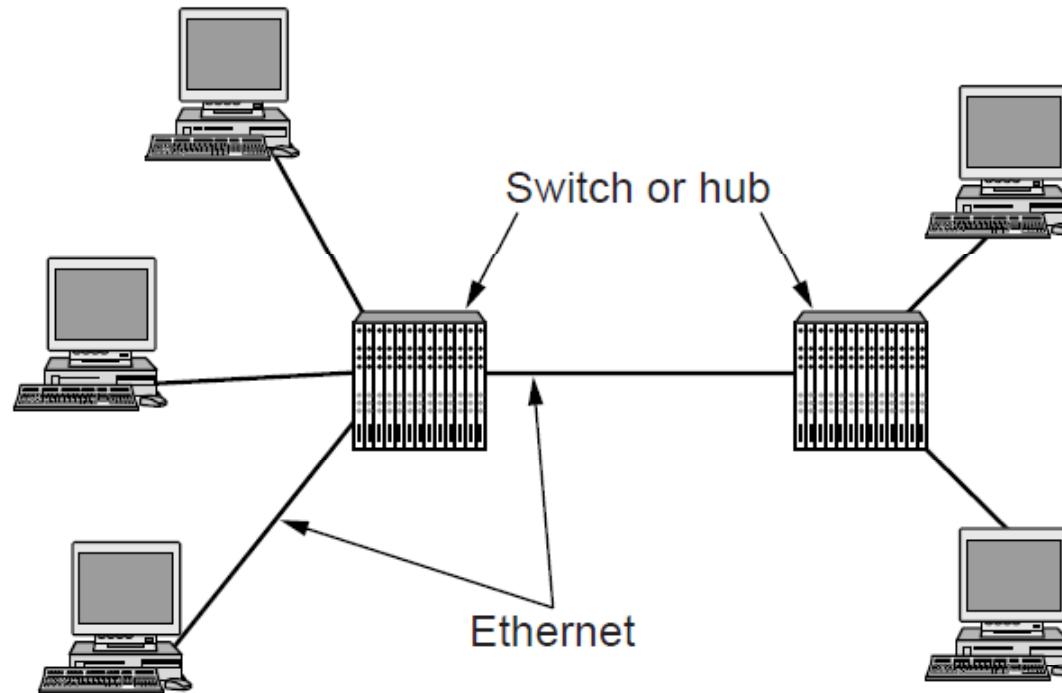
- Twisted pair (with Cat 5) dominated the market

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 (Cat 5 UTP)
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Gigabit / 10 Gigabit Ethernet (1)

Switched Gigabit Ethernet is now the garden variety

- With full-duplex lines between computers/switches



Gigabit / 10 Gigabit Ethernet (1)

- Gigabit Ethernet is commonly run over twisted pair

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 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

- 10 Gigabit Ethernet is being deployed where needed

Name	Cable	Max. segment	Advantages
10GBase-SR	Fiber optics	Up to 300 m	Multimode fiber (0.85 μ)
10GBase-LR	Fiber optics	10 km	Single-mode fiber (1.3 μ)
10GBase-ER	Fiber optics	40 km	Single-mode fiber (1.5 μ)
10GBase-CX4	4 Pairs of twinax	15 m	Twinaxial copper
10GBase-T	4 Pairs of UTP	100 m	Category 6a UTP

- 40/100 Gigabit Ethernet is under development

Wireless LANs

- 802.11 architecture/protocol stack »
- 802.11 physical layer »
- 802.11 MAC »
- 802.11 frames »

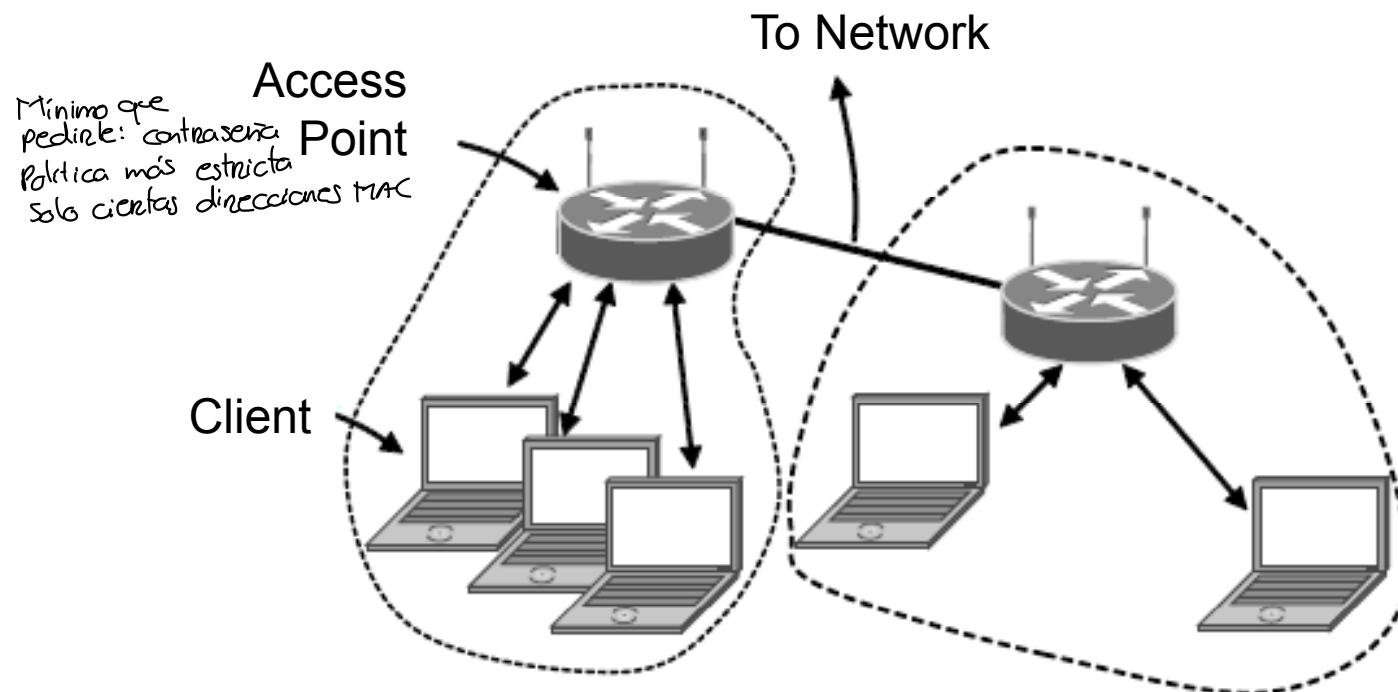
802.11 Architecture/Protocol Stack (1)

Estación que transmite hasta los demás dispositivos.

Política de conexión de clientes.

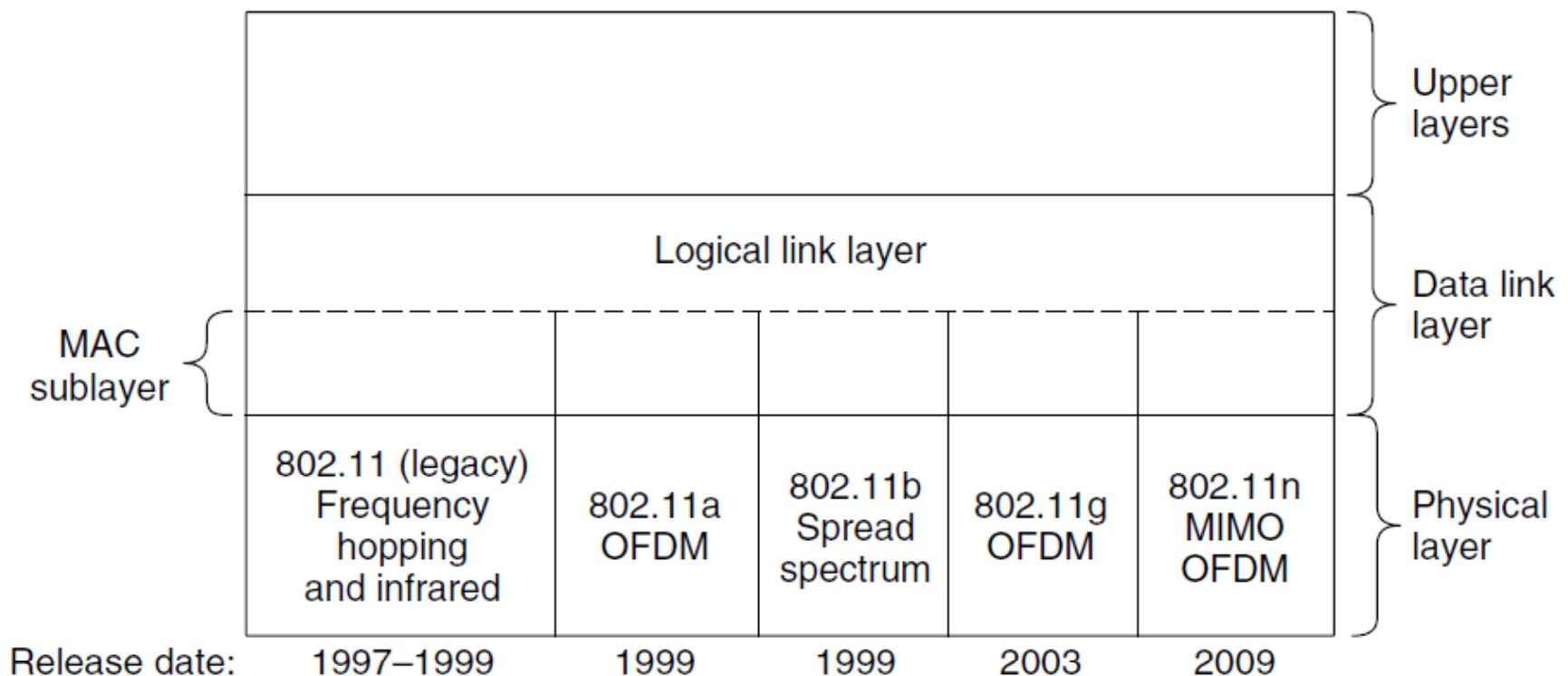
Wireless clients associate to a wired AP (Access Point)

- Called infrastructure mode; there is also ad-hoc mode with no AP, but that is rare.



802.11 Architecture/Protocol Stack (2)

MAC is used across different physical layers



802.11 physical layer

- NICs are compatible with multiple physical layers
 - E.g., 802.11 a/b/g

Name	Technique	Max. Bit Rate
802.11b	Spread spectrum, 2.4 GHz	11 Mbps
802.11g	OFDM, 2.4 GHz	54 Mbps
802.11a	OFDM, 5 GHz	54 Mbps
802.11n	OFDM with MIMO, 2.4/5 GHz	600 Mbps

$0, 2^{k-1}$
0, 3

0, 1, 2, 3

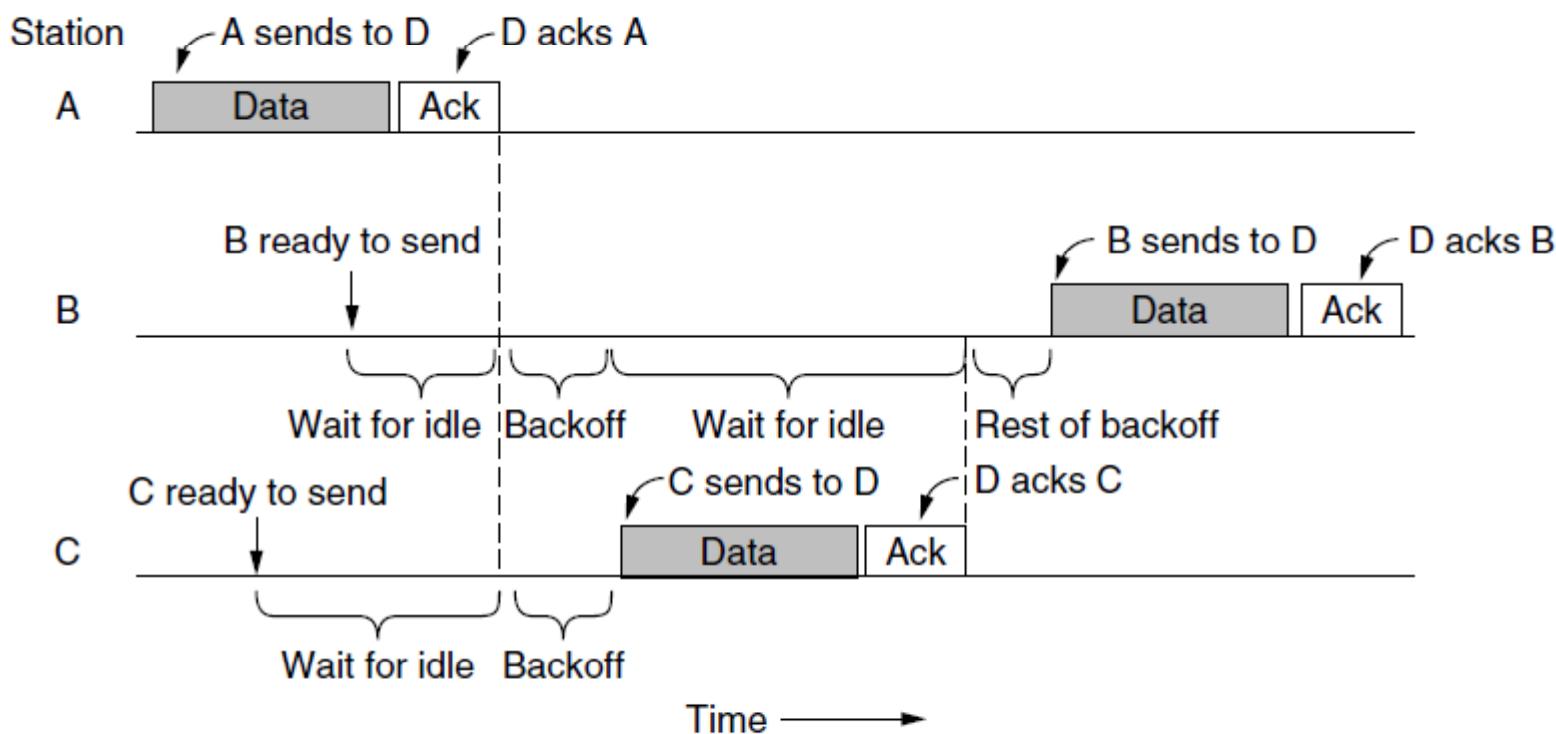
0 1 2 3

mas posibilidades
colisión menos probable

802.11 MAC (1)

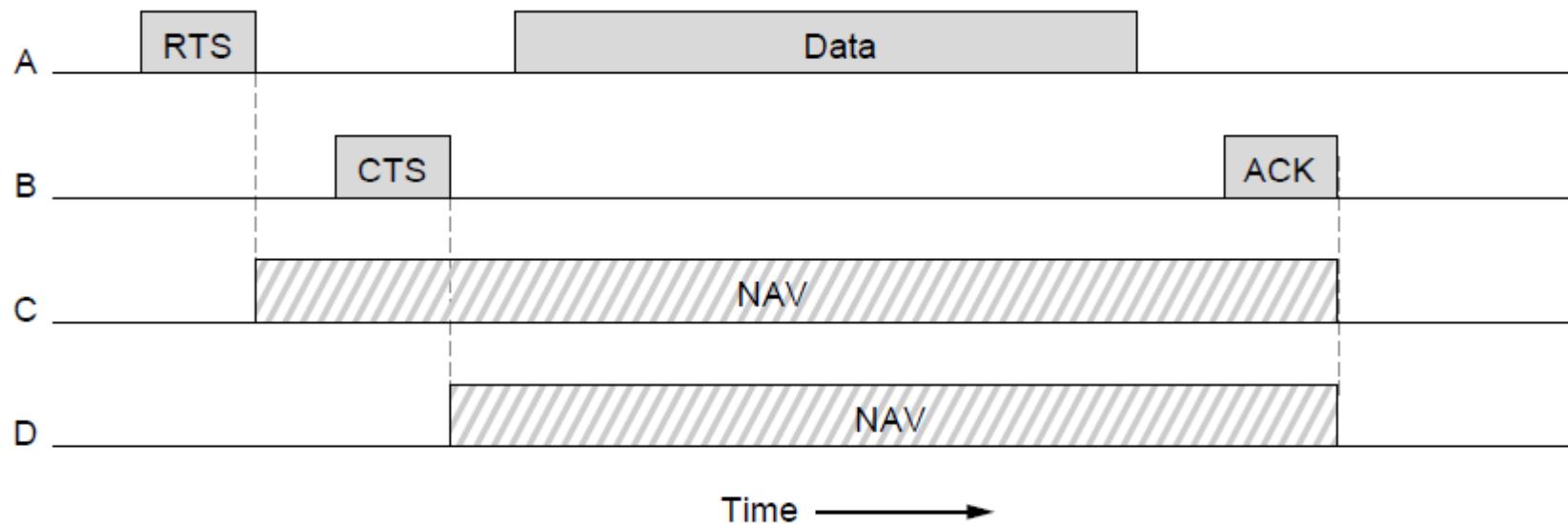
Posibilidad de retransmisión.
Tiempo que se espera para retransmisión va a ir cambiando

- CSMA/CA inserts backoff slots to avoid collisions
- MAC uses ACKs/retransmissions for wireless errors



802.11 MAC (2)

Virtual channel sensing with the NAV and optional RTS/CTS (often not used) avoids hidden terminals

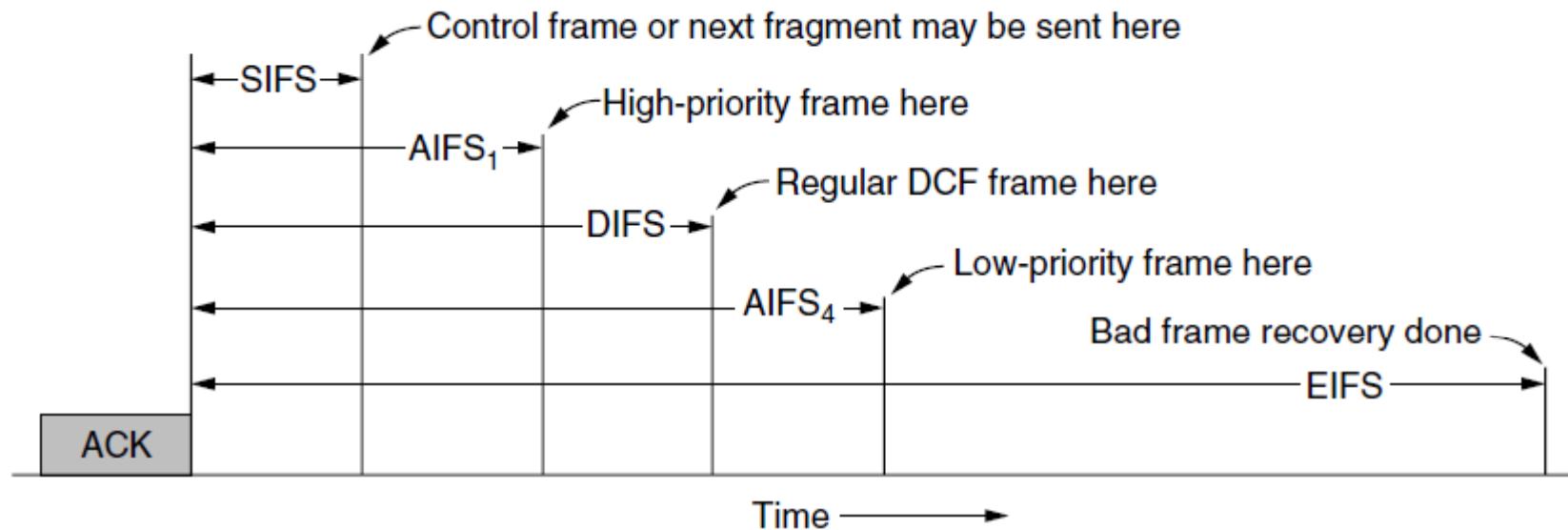




802.11 MAC (3)

valor mínimo de backoff= ?
Calidad de servicio → tamaño de delay

- Different backoff slot times add quality of service
 - Short intervals give preferred access, e.g., control, VoIP
- MAC has other mechanisms too, e.g., power save





802.11 Frames

- Frames vary depending on their type (Frame control)
- Data frames have 3 addresses to pass via APs

Bytes	2	2	6	6	6	2	0–2312	4
	Frame control	Duration	Address 1 (recipient)	Address 2 (transmitter)	Address 3	Sequence	Data	Check sequence
Bits	2	2	4	1	1	1	1	1

A dashed line connects the 'Frame control' field in the first row to the 'Version = 00' field in the second row.

Version = 00	Type = 10	Subtype = 0000	To DS	From DS	More frag.	Retry	Pwr. mgt.	More data	Protected	Order
--------------	-----------	----------------	-------	---------	------------	-------	-----------	-----------	-----------	-------

802.11

MAC layer

DCF (Distributed coordination function)

- The IEEE 802.11 uses DCF as the distributed medium access protocol .
- Based on CSMA/CA. (RTS/CTS)
- In DCF, a station will monitor the channel before transmit.
- A station must sense the medium before initiating transmission
 - If the medium is idle for a time interval greater than a distributed interframe space (DIFS), the station transmits
 - Else, transmission is deferred and the station starts a backoff process
 - which delays the transmission by a random backoff time [0, contention window CW]
 - Timer is decremented if the medium is idle

DCF

- If the channel is still free, it will transmit a request to send (RTS) to the destination. The destination will respond with a clear to send (CTS) if it is available to receive data
- 802.11 Distributed Coordination Function (DCF) maximizes throughput while preventing packet collisions

Network allocation vector (NAV)

- NAV is used to inform other nodes how long the current node will need the channel.
- Any nodes overhearing the NAV know that they have no need of sensing the channel for the time indicated.
- Idle sensing of the channel is one of the biggest uses of energy in a network
- NAV reduces the amount of idle sensing required at any nodes which can overhear it, thus saving energy at all nodes in the network.

Point Coordination function

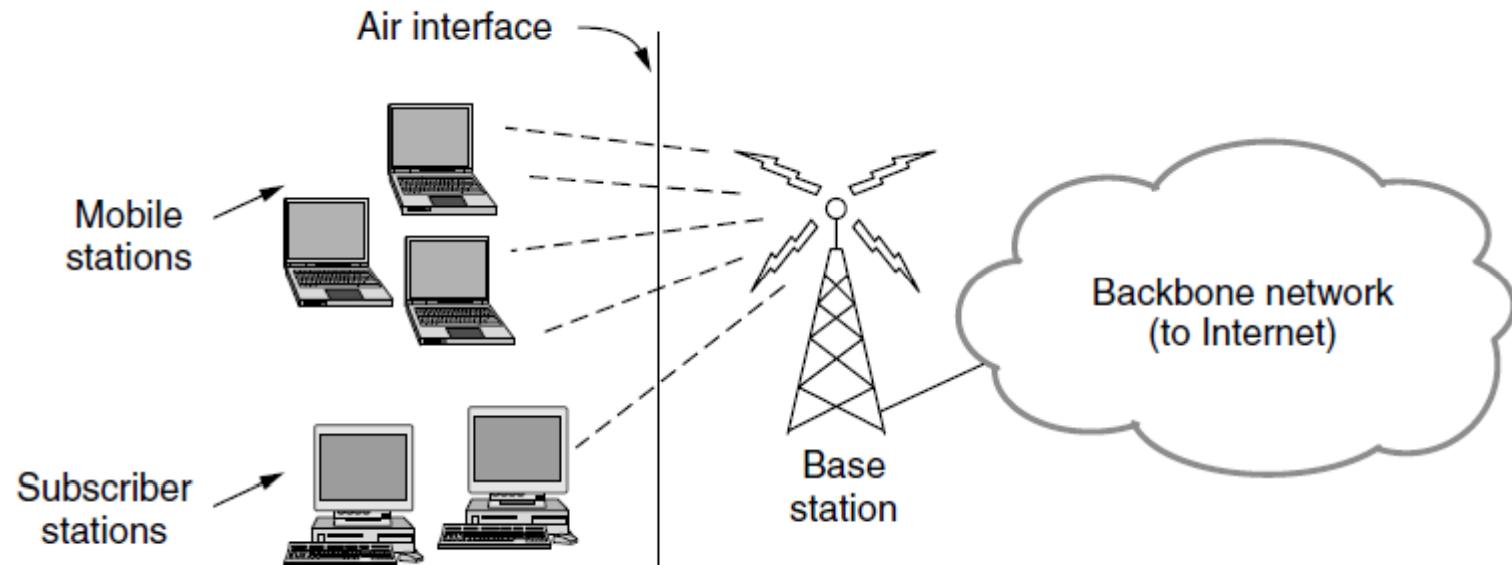
- Polling access method
- A point coordinator which cyclically polls wireless stations
- Centralized method
- The PCF is located directly above the distributed coordination function (DCF), in the IEEE 802.11 MAC Architecture.
- Contention free

Broadband Wireless

- 802.16 Architecture / Protocol Stack »
- 802.16 Physical Layer »
- 802.16 MAC »
- 802.16 Frames »

802.16 Architecture/Protocol Stack (1)

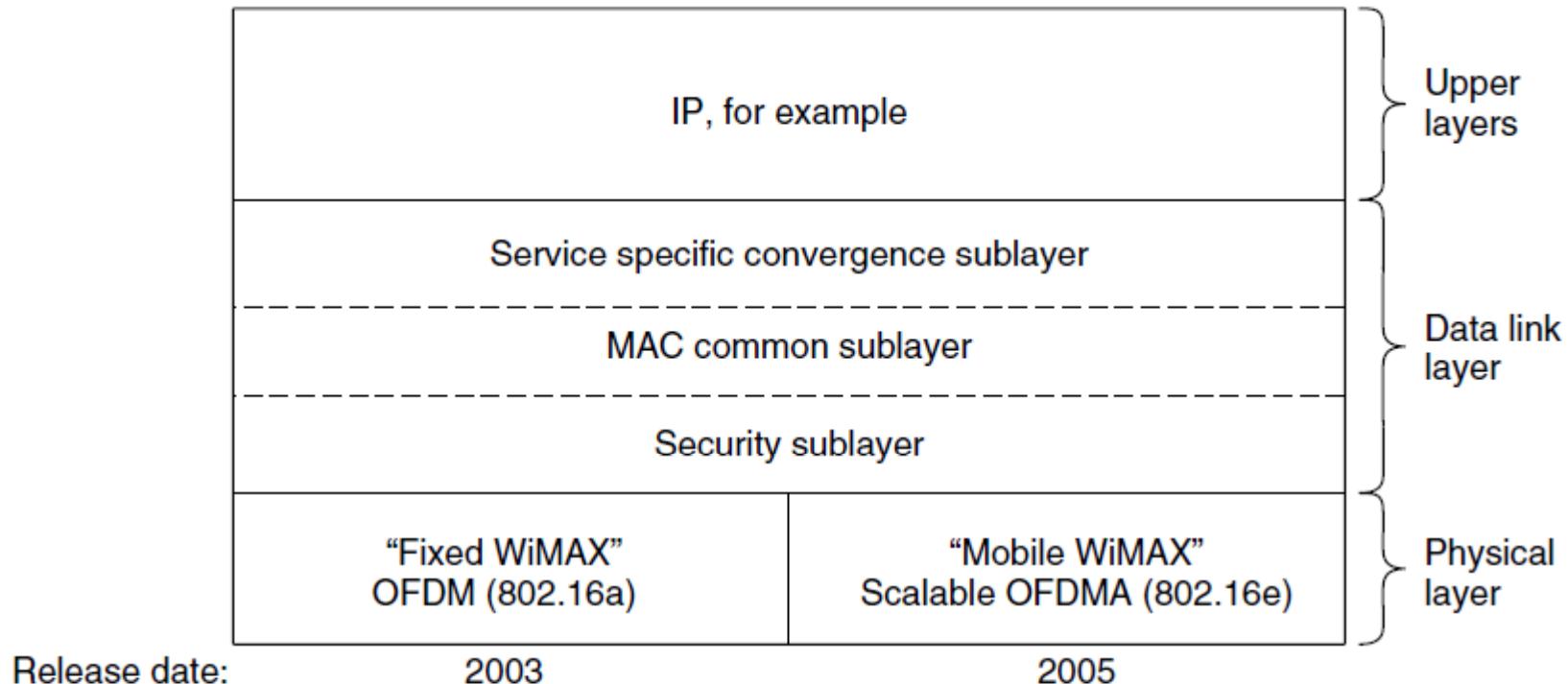
Wireless clients connect to a wired basestation (like 3G)



802.16 Architecture/Protocol Stack (2)

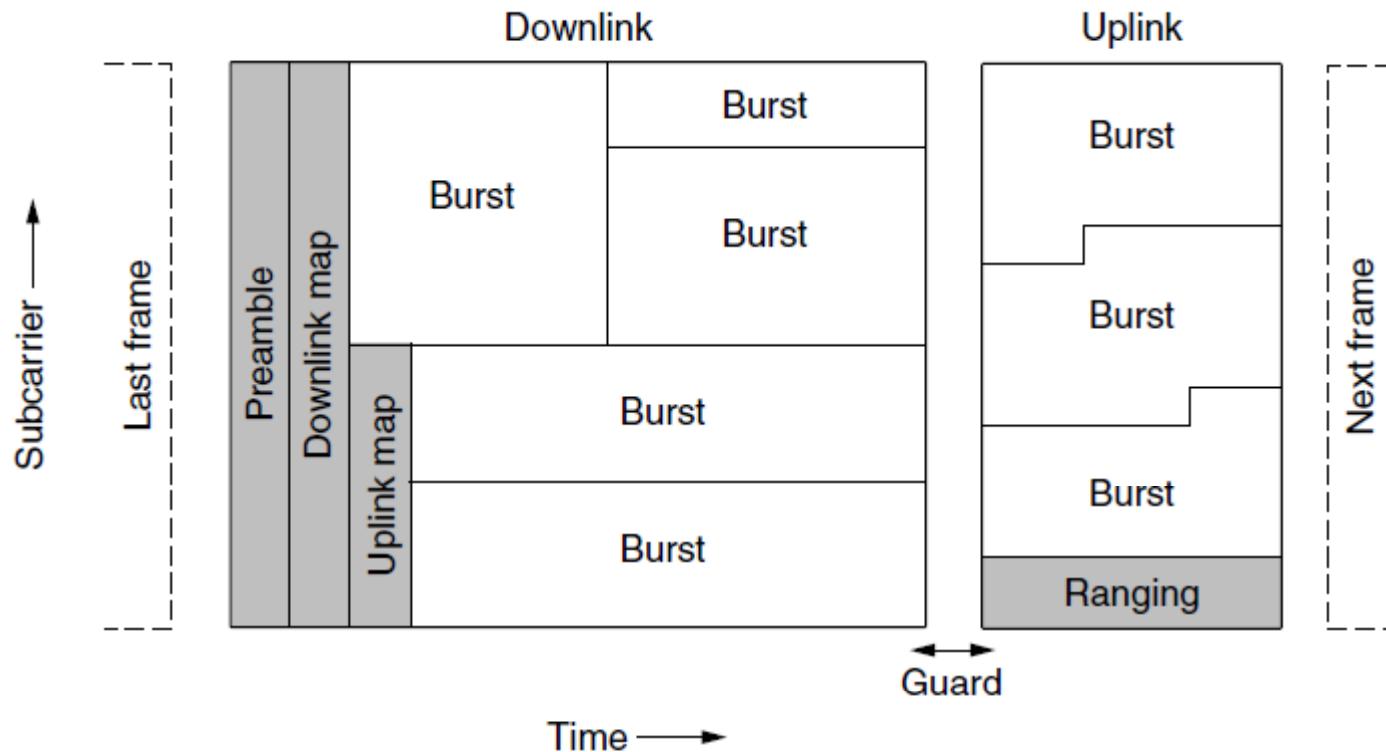
MAC is connection-oriented; IP is connectionless

- Convergence sublayer maps between the two



802.16 Physical Layer

Based on OFDM; base station gives mobiles bursts (subcarrier/time frame slots) for uplink and downlink



802.16 MAC

Connection-oriented with base station in control

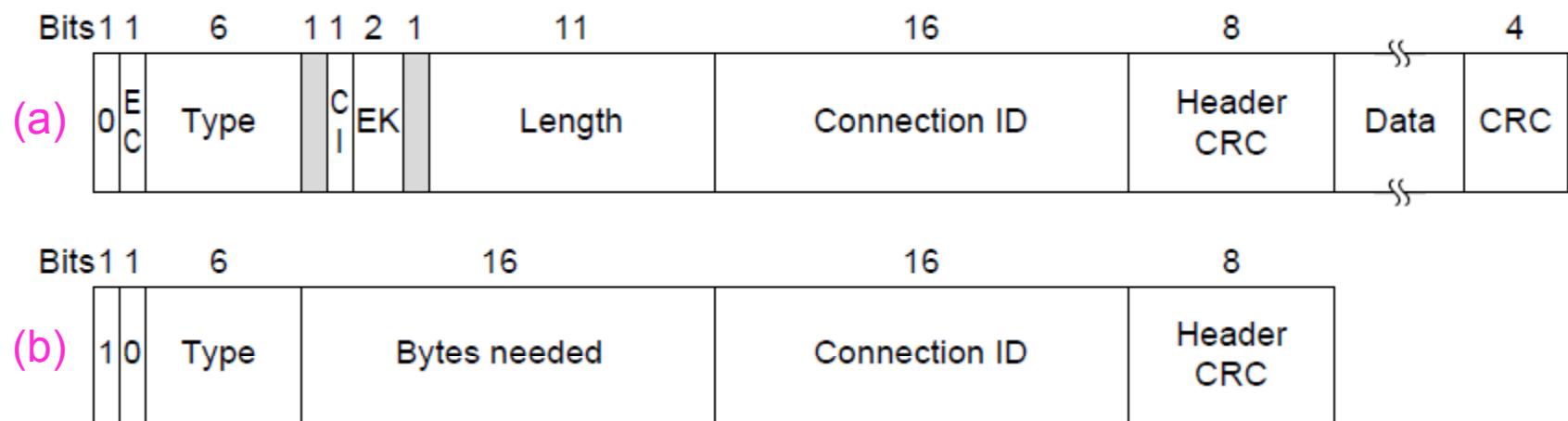
- Clients request the bandwidth they need

Different kinds of service can be requested:

- Constant bit rate, e.g., uncompressed voice
- Real-time variable bit rate, e.g., video, Web
- Non-real-time variable bit rate, e.g., file download
- Best-effort for everything else

802.16 Frames

- Frames vary depending on their type
- Connection ID instead of source/dest addresses

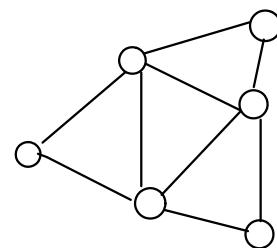
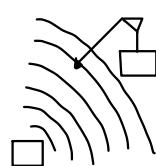


(a) A generic frame. (b) A bandwidth request frame

Bluetooth

- Bluetooth Architecture »
- Bluetooth Applications / Protocol »
- Bluetooth Radio / Link Layers »
- Bluetooth Frames »

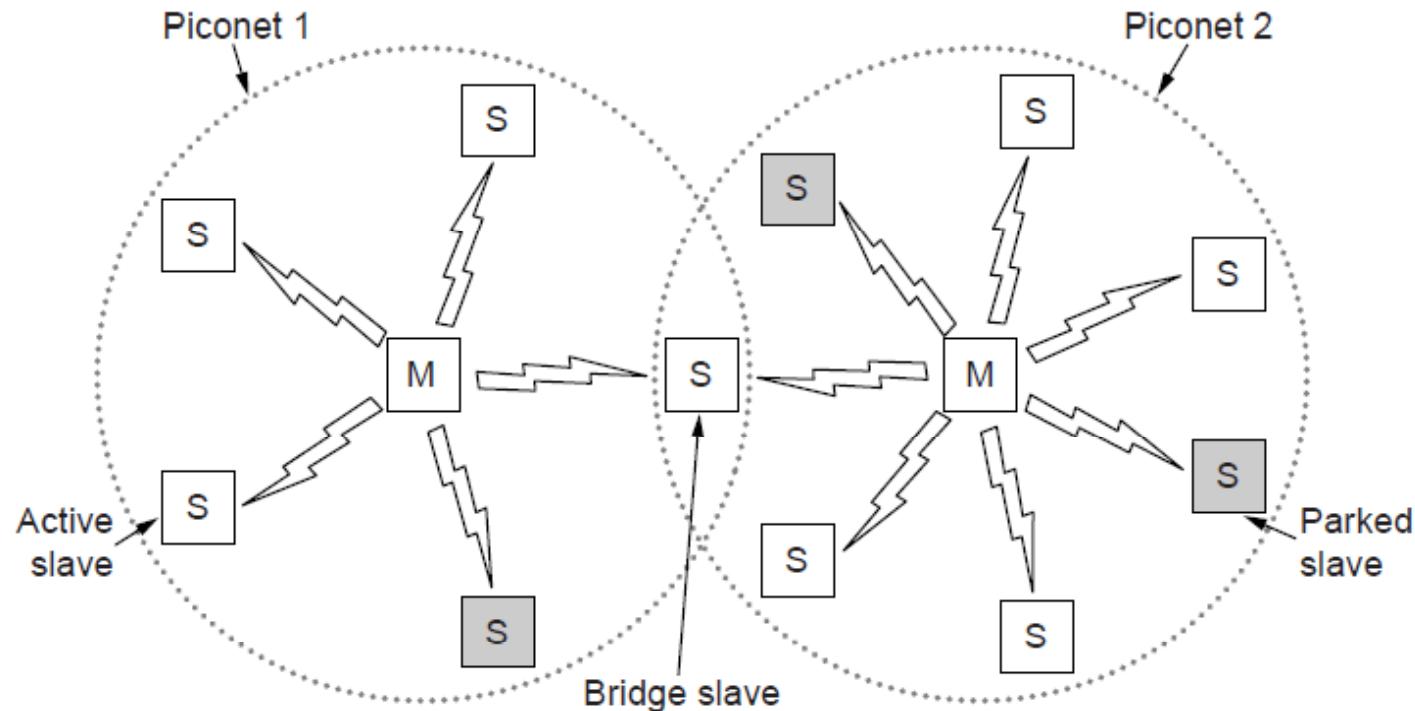
Ha ido evolucionando, hoy muchas versiones. Se quería que no usara mucha energía
Pueden determinar el ángulo de arriba
No se debe emplear toda la energía.



Bluetooth Architecture

Piconet master is connected to slave wireless devices

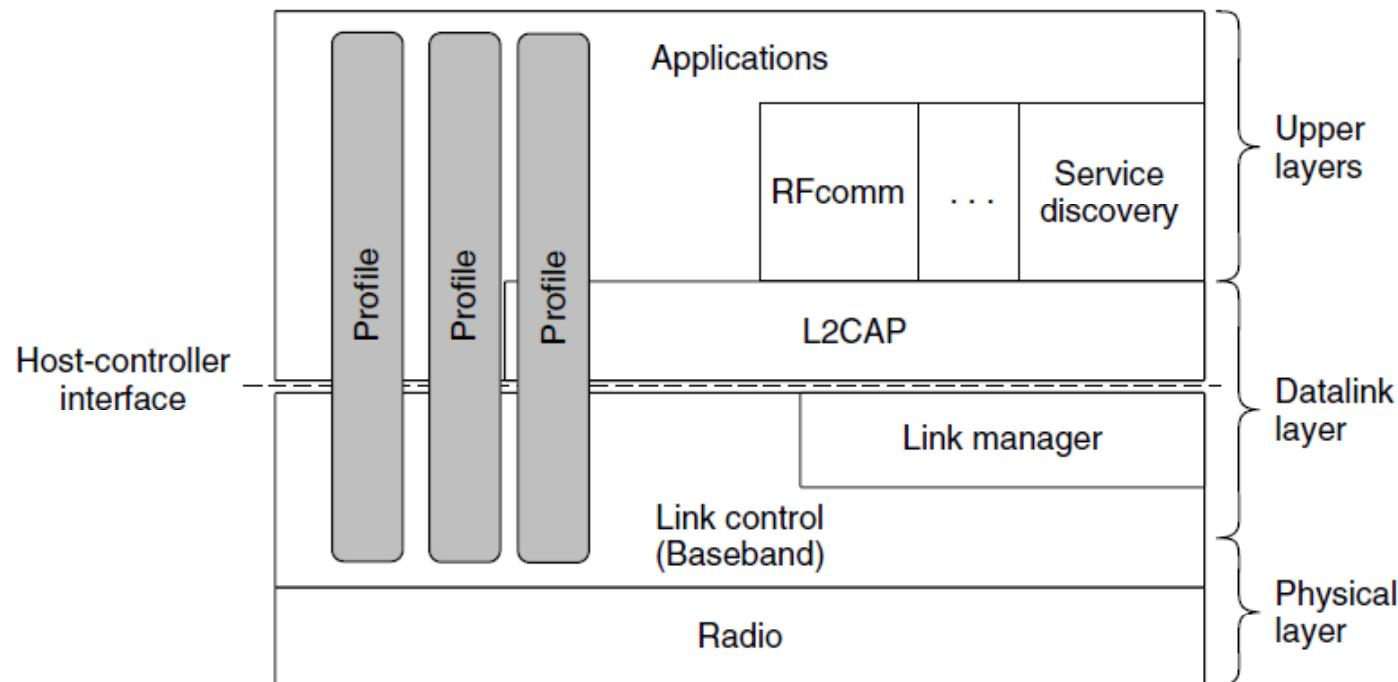
- Slaves may be asleep (parked) to save power
- Two piconets can be bridged into a scatternet



Bluetooth Applications / Protocol Stack

Profiles give the set of protocols for a given application

- 25 profiles, including headset, intercom, streaming audio, remote control, personal area network, ...



Bluetooth Radio / Link Layers

Radio layer

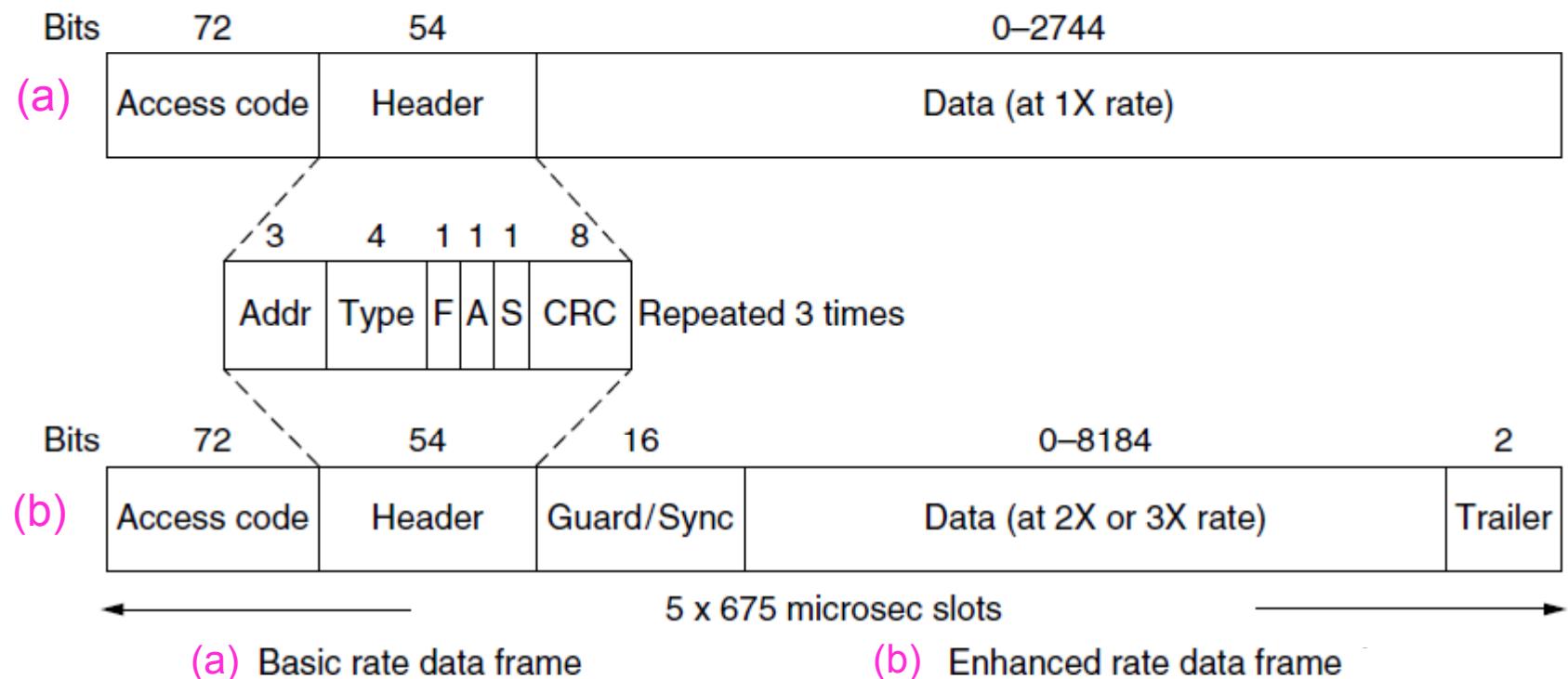
- Uses adaptive frequency hopping in 2.4 GHz band

Link layer

- TDM with timeslots for master and slaves
- Synchronous CO for periodic slots in each direction
- Asynchronous CL for packet-switched data
- Links undergo pairing (user confirms passkey/PIN) to authorize them before use

Bluetooth Frames

Time is slotted; enhanced data rates send faster but for the same time; addresses are only 3 bits for 8 devices

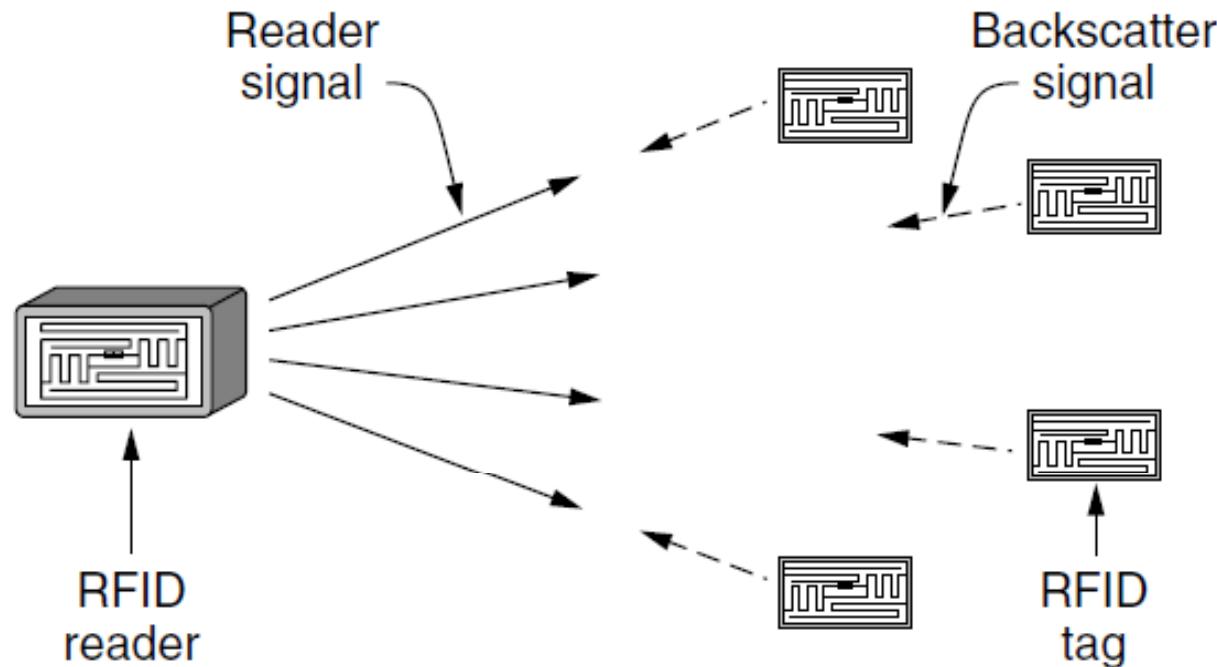


RFID

- Gen 2 Architecture »
- Gen 2 Physical Layer »
- Gen 2 Tag Identification Layer »
- Gen 2 Frames »

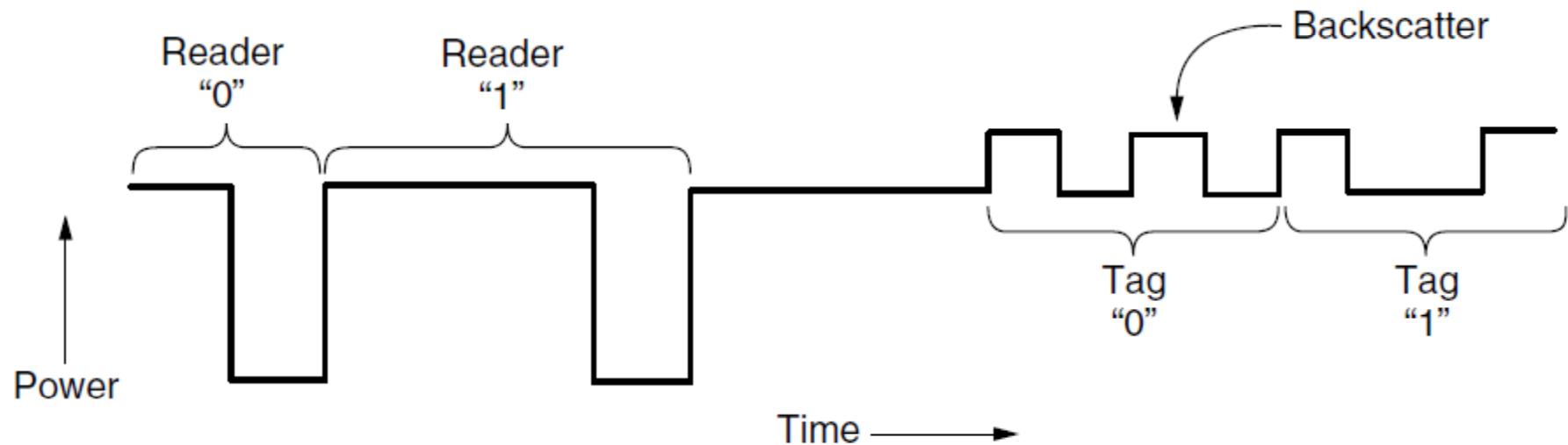
Gen 2 Architecture

Reader signal powers tags; tags reply with backscatter



Gen 2 Physical Layer

- Reader uses duration of on period to send 0/1
- Tag backscatters reader signal in pulses to send 0/1



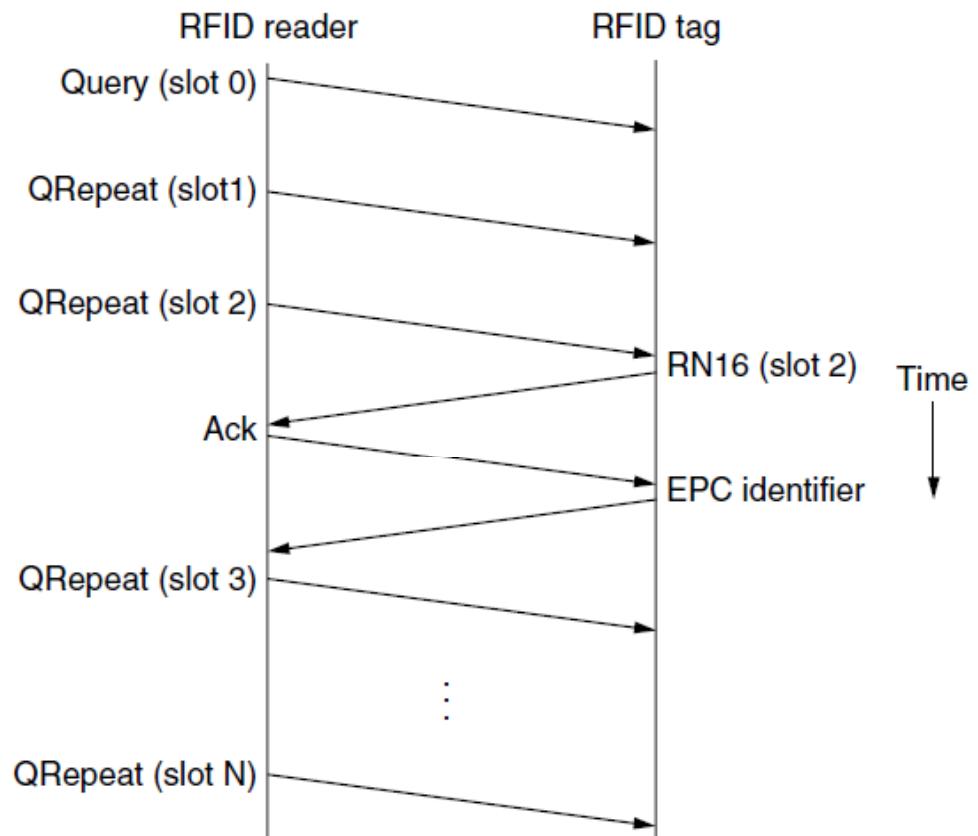
Gen 2 Tag Identification Layer

Reader sends query and sets slot structure

Tags reply (RN16) in a random slot; may collide

Reader asks one tag for its identifier (ACK)

Process continues until no tags are left



Gen 2 Frames

- Reader frames vary depending on type (Command)
 - Query shown below, has parameters and error detection
- Tag responses are simply data
 - Reader sets timing and knows the expected format



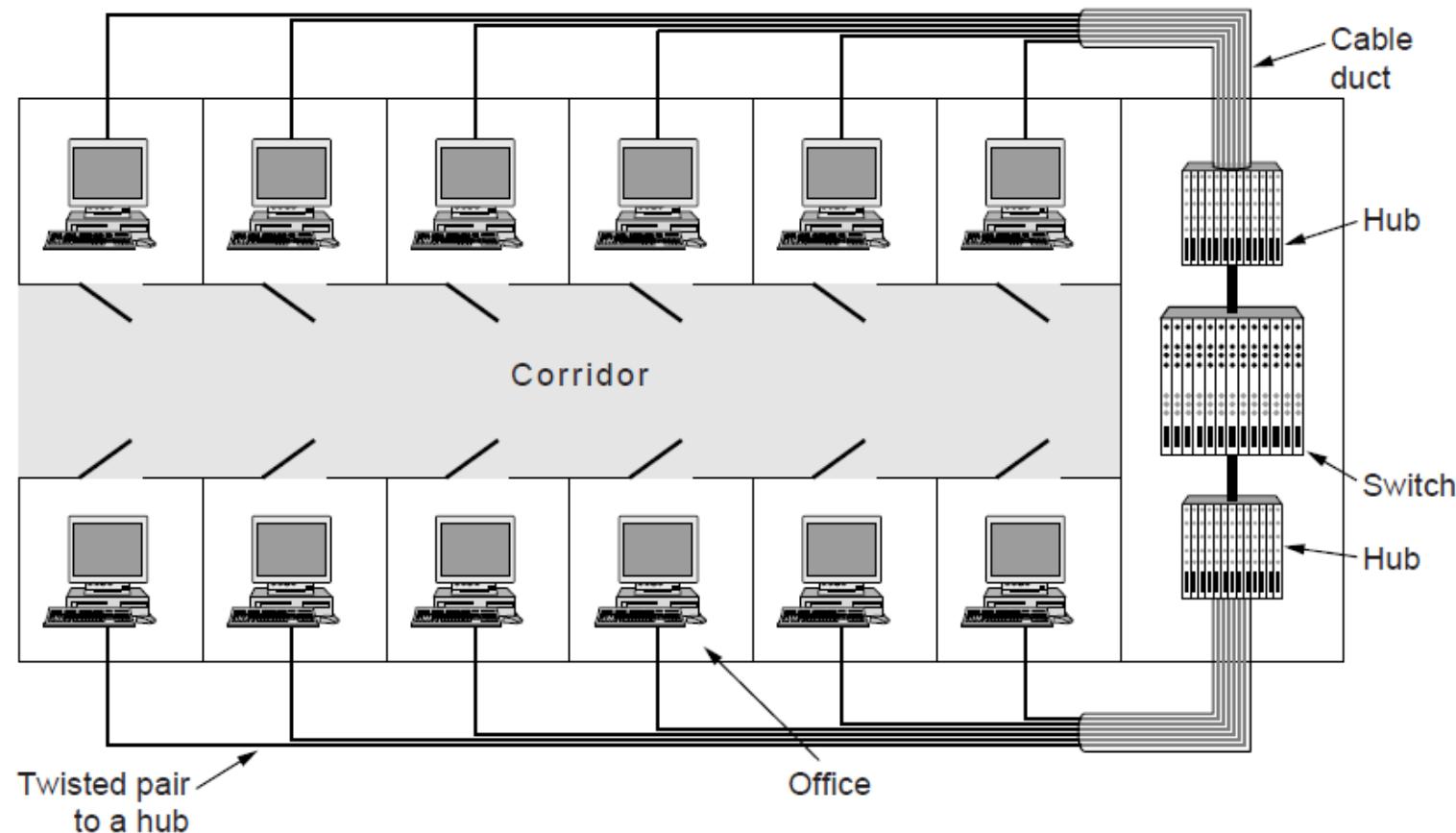
Data Link Layer Switching

- Uses of Bridges »
- Learning Bridges »
- Spanning Tree »
- Repeaters, hubs, bridges, .., routers, gateways »
- Virtual LANs »

Uses of Bridges

Common setup is a building with centralized wiring

- Bridges (switches) are placed in or near wiring closets

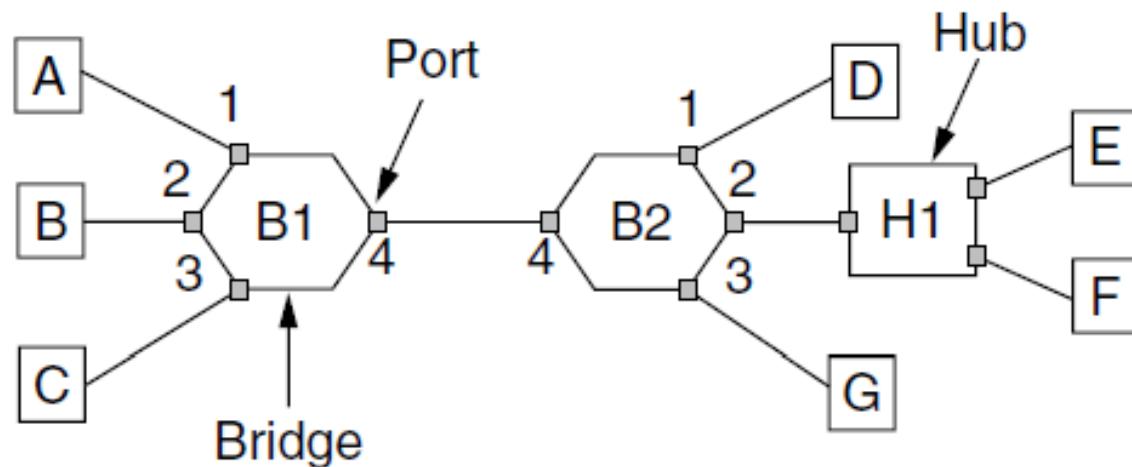


Learning Bridges (1)

Entre más computadoras se quieren interconectar, más compleja su conexión

A bridge operates as a switched LAN (not a hub)

- Computers, bridges, and hubs connect to its ports



Learning Bridges (2)

Backward learning algorithm picks the output port:

- Associates source address on frame with input port
- Frame with destination address sent to learned port
- Unlearned destinations are sent to all other ports

Needs no configuration

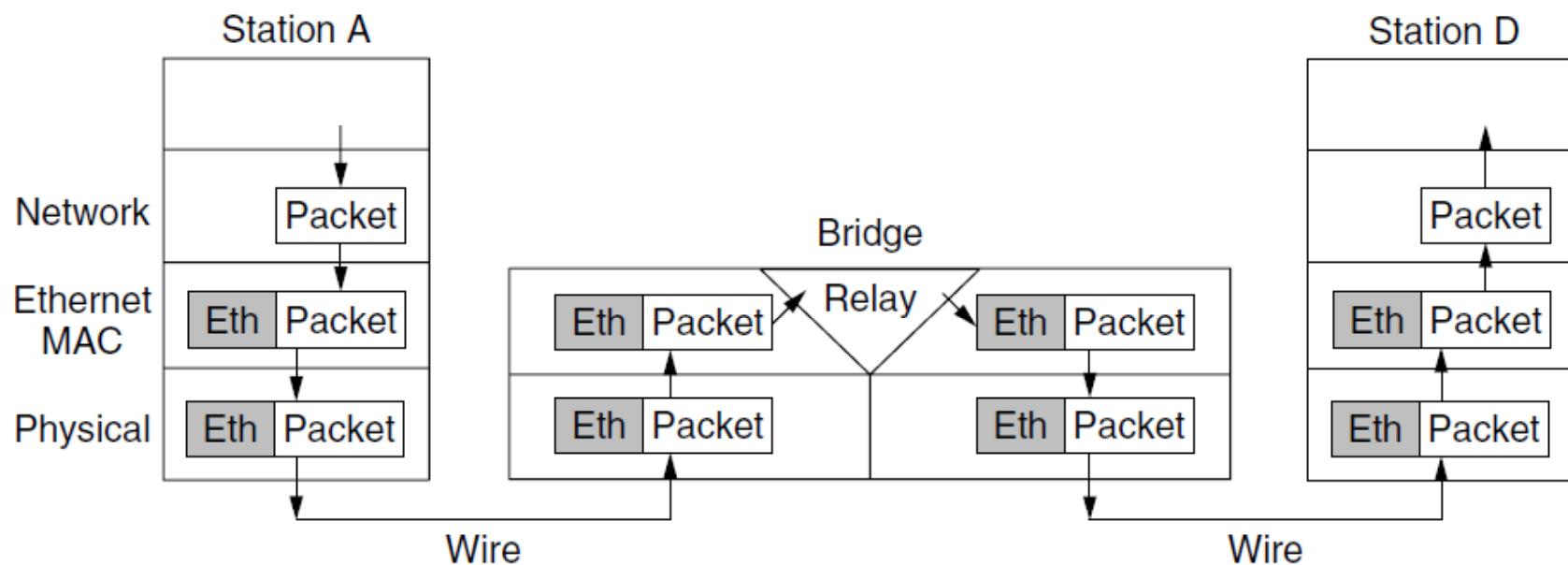
- Forget unused addresses to allow changes
- Bandwidth efficient for two-way traffic

Learning Bridges (3)

Ya no estamos usando un medio compartido

Bridges extend the Link layer:

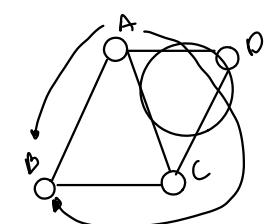
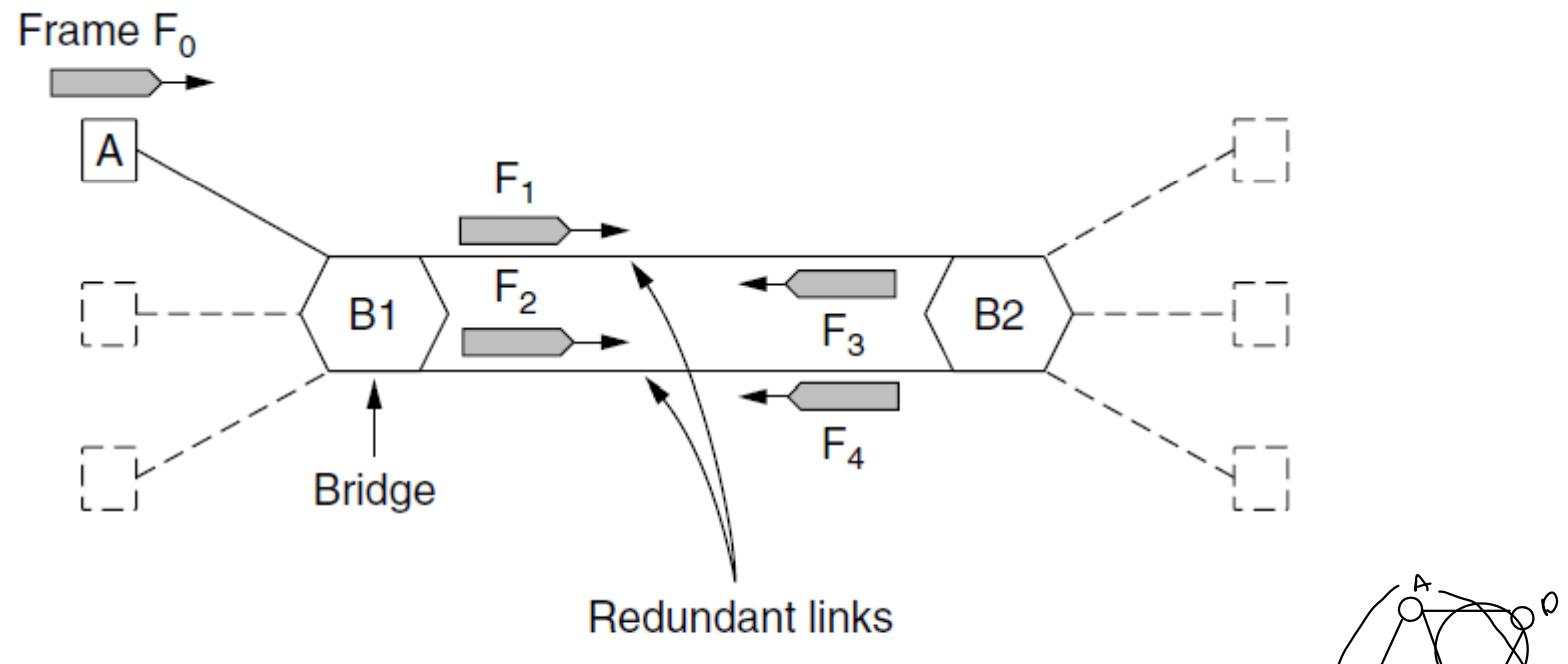
- Use but don't remove Ethernet header/addresses
- Do not inspect Network header



Spanning Tree (1) – Problem

Bridge topologies with loops and only backward learning will cause frames to circulate for ever

- Need spanning tree support to solve problem



Spanning Tree (2) – Algorithm

- Subset of forwarding ports for data is used to avoid loops
- Selected with the spanning tree distributed algorithm by Perlman

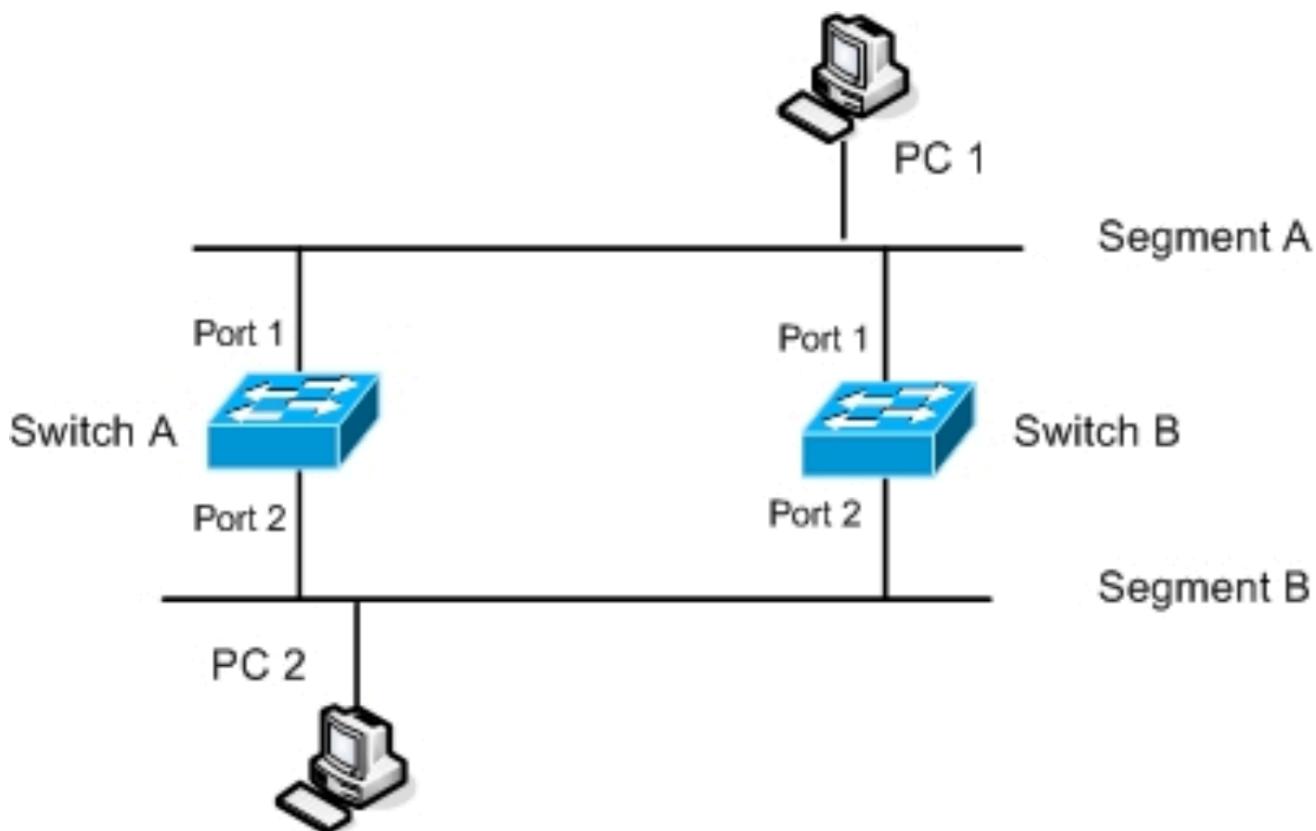
*I think that I shall never see
A graph more lovely than a tree.
A tree whose crucial property
Is loop-free connectivity.
A tree which must be sure to span.
So packets can reach every LAN.
First the Root must be selected
By ID it is elected.
Least cost paths from Root are traced
In the tree these paths are placed.
A mesh is made by folks like me
Then bridges find a spanning tree.*

– Radia Perlman, 1985.

Spanning tree protocol

Referencia: Cisco CCNA

Problemas de bucles



Un paquete de la PC 2 será retransmitido por A y B, ambos paquetes llegarán a B y A respectivamente y nuevamente serán retransmitidos.

Spanning Tree Protocol (STP)

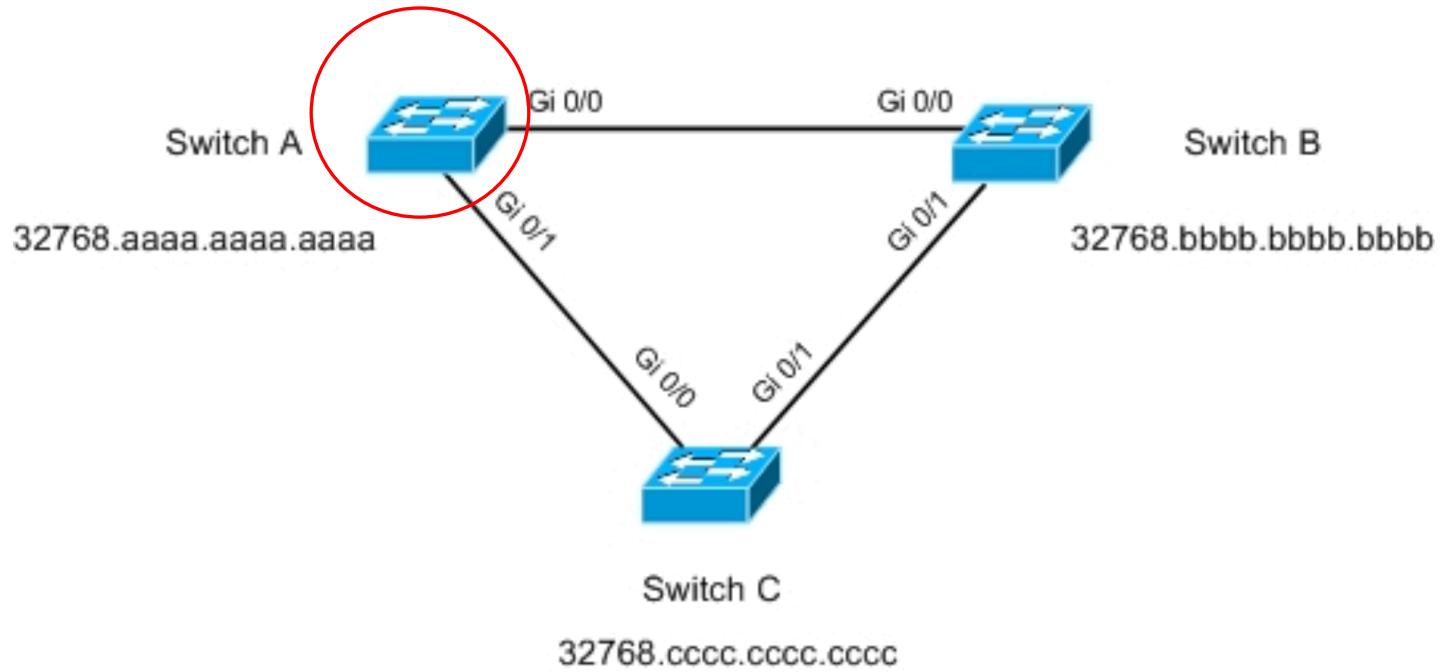
- Elimina los bucles (loops) ocasionados por enlaces redundantes bloqueando dichos enlaces.
- Sin embargo en caso de falla de los enlaces que forman parte del árbol, se desbloquean automáticamente los enlaces redundantes para proveer robustez a la red y mantener el árbol
- Bridge Protocol Data Units (BPDU): unidades de información del STP
- Existirán tres tipos de puertos:
 - I. Root Port
 - II. Designated Port
 - III. Non-Designated/Blocking Port

Pasos del STP

1. Elección del puente raíz (bridge root).
2. Elección de un “root port” en los puentes diferentes al raíz.
3. Elección del “Designated Port” en cada segmento

1. Elección del puente raíz

- Cada puente tiene un ID de 8 bytes formado por: 2 bytes de prioridad+6 bytes dirección MAC
- La raíz del árbol se elige como el menor ID
- Cada puente “anuncia” que es raíz e incluye su ID en el anuncio.
- B y C determinarán que A es raíz porque tiene menor ID



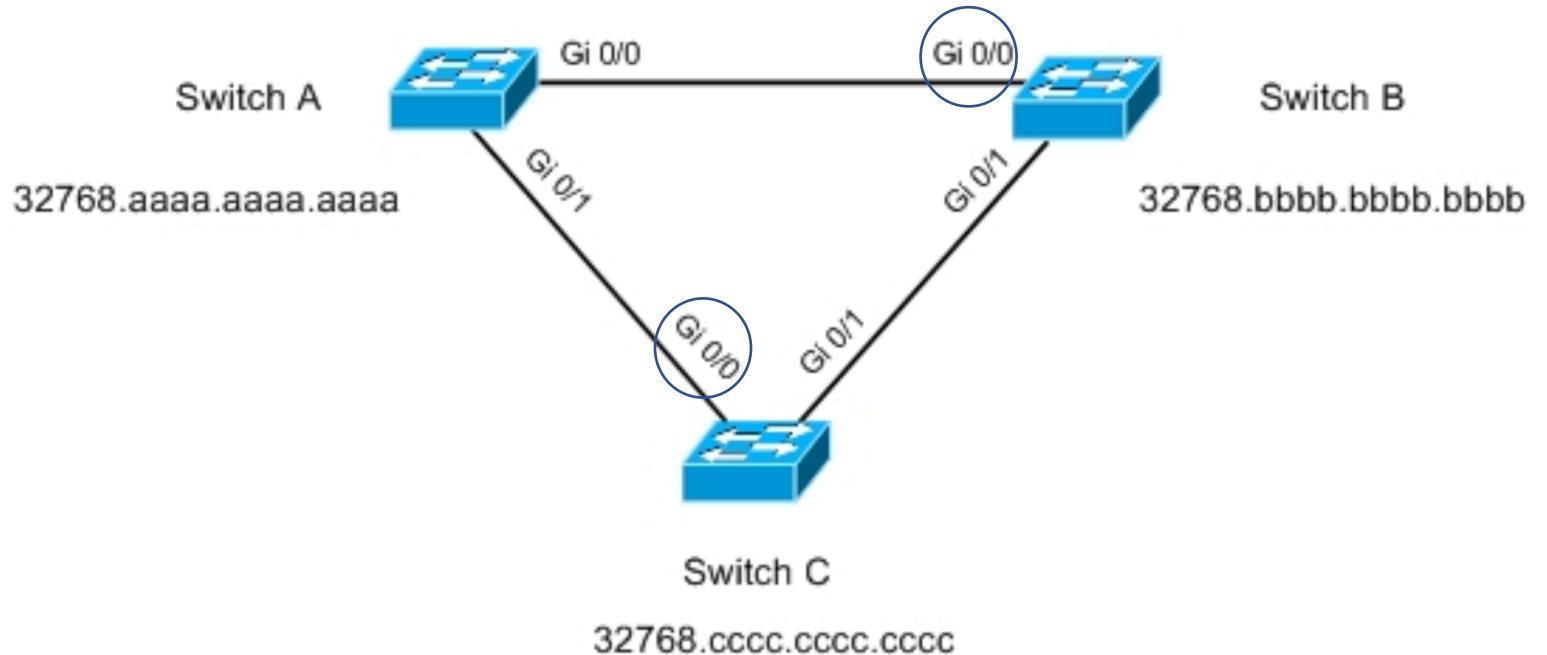
2. Elección del “root port” en los puentes

- El “root port” en cada puente (excepto el raíz) es aquel puerto que presenta el menor costo acumulativo hacia el puente raíz.
- Se puede considerar que el “root port” apunta (upstream) al puente raíz.
- Costos de acuerdo al estándar IEEE 802.1D

Link Bandwidth	STP Cost
4 Mbps	250
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

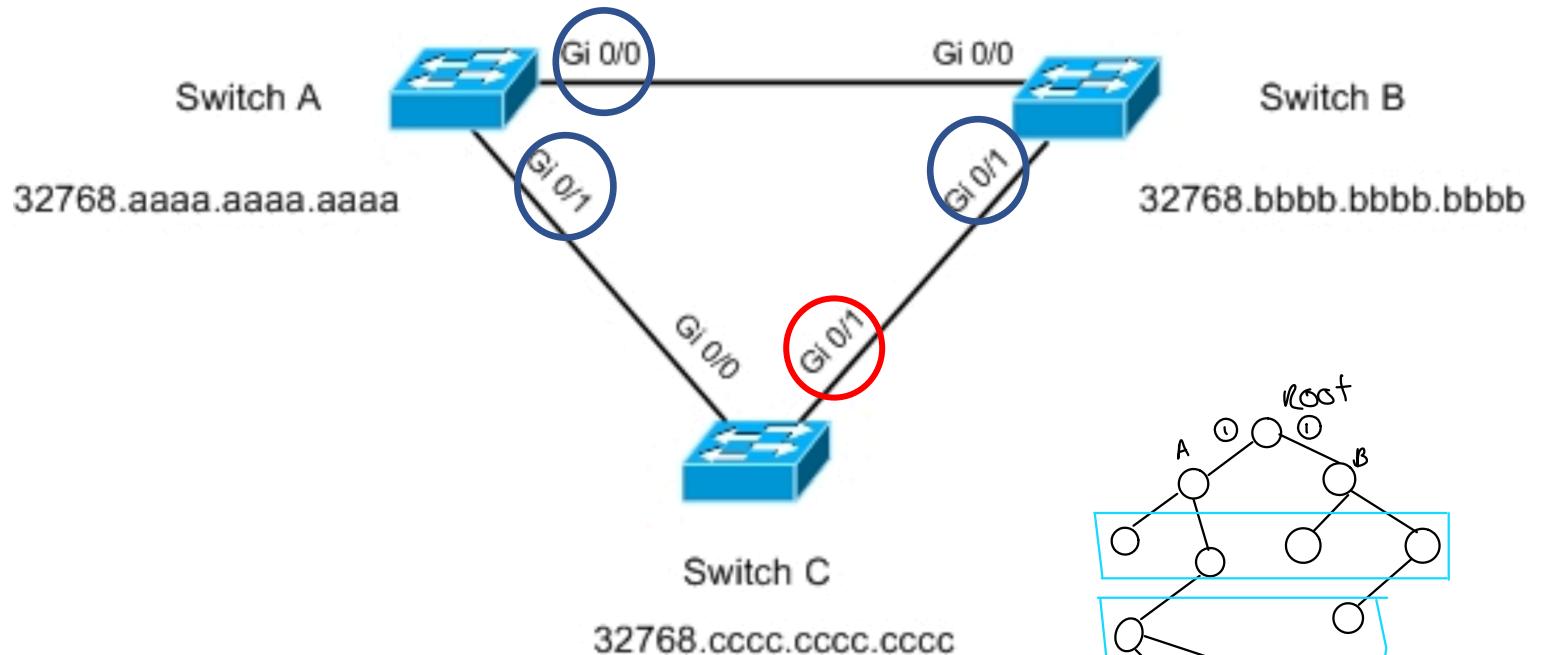
2. Elección del “root port” en los puentes

- A enviará periódicamente el costo de la ruta al raíz, cero en este caso.
- B y C incluirán un costo de 4 a la ruta en los puertos Gi 0/0, adicionalmente B y C tendrán rutas de costo 8 en sus puertos Gi 0/1.
- Por lo tanto el root port será Gi 0/0 tanto en B como en C



3. Elección del “Designated port” en cada segmento

- Es el puerto en un segmento que anuncia la ruta de menor costo al raíz.
- En el segmento BC ambos puentes anuncian el mismo costo de 4, en este caso de empate la elección será el puerto Gi 0/1 perteneciente a B, debido a que B tiene el menor ID.
- El puerto Gi 0/1 de C por lo tanto se bloquea para evitar bucles.



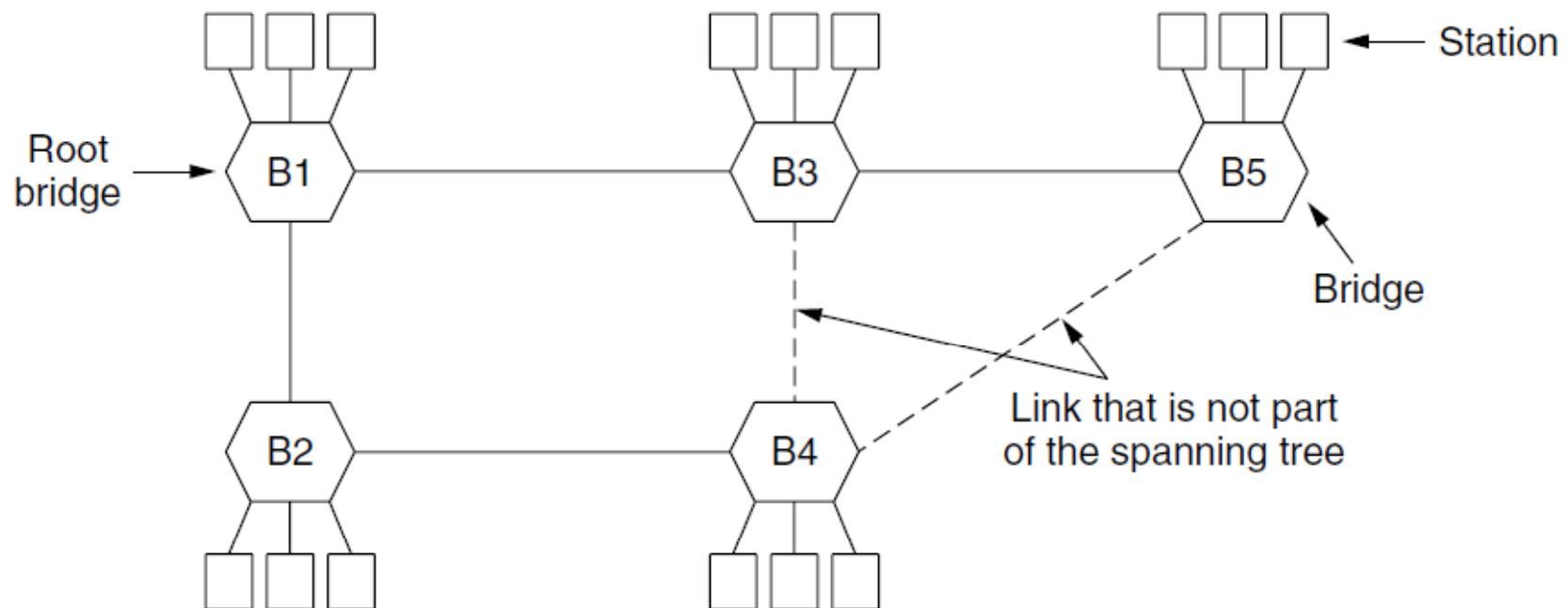
Estados de los puertos

- Disabled. Desactivado o deshabilitado.
- Blocking. Al habilitar el puerto se cambia a estado de bloqueo (no cursa tráfico) para evitar bucles. Solamente recibe BPDU (no participa activamente en el STP)
- Listening. Participa activamente en el STP (está en capacidad de enviar BPDU)
- Learning. Además de las funciones de “listening” puede aprender las direcciones MAC
- Forwarding. Puerto completamente funcional, puede cursar tráfico.

Spanning Tree (3) – Example

After the algorithm runs:

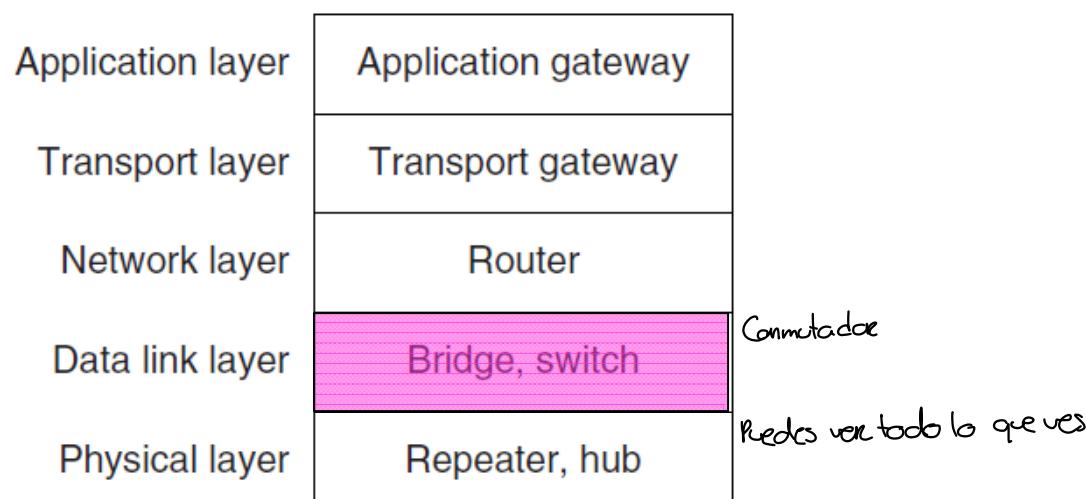
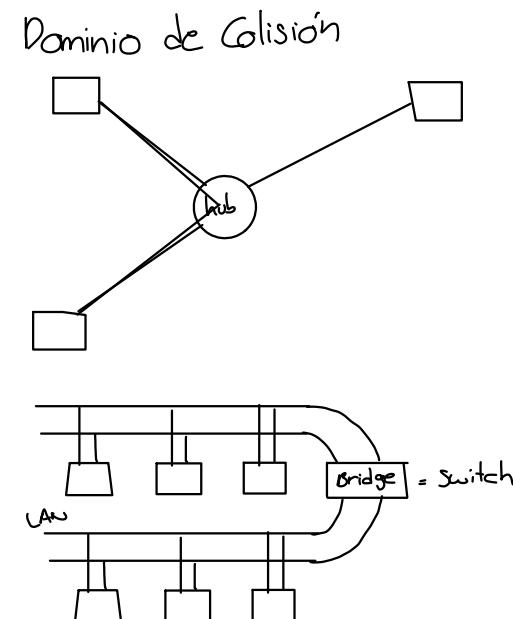
- B1 is the root, two dashed links are turned off
- B4 uses link to B2 (lower than B3 also at distance 1)
- B5 uses B3 (distance 1 versus B4 at distance 2)



Repeaters, Hubs, Bridges, Switches, Routers, & Gateways

Devices are named according to the layer they process

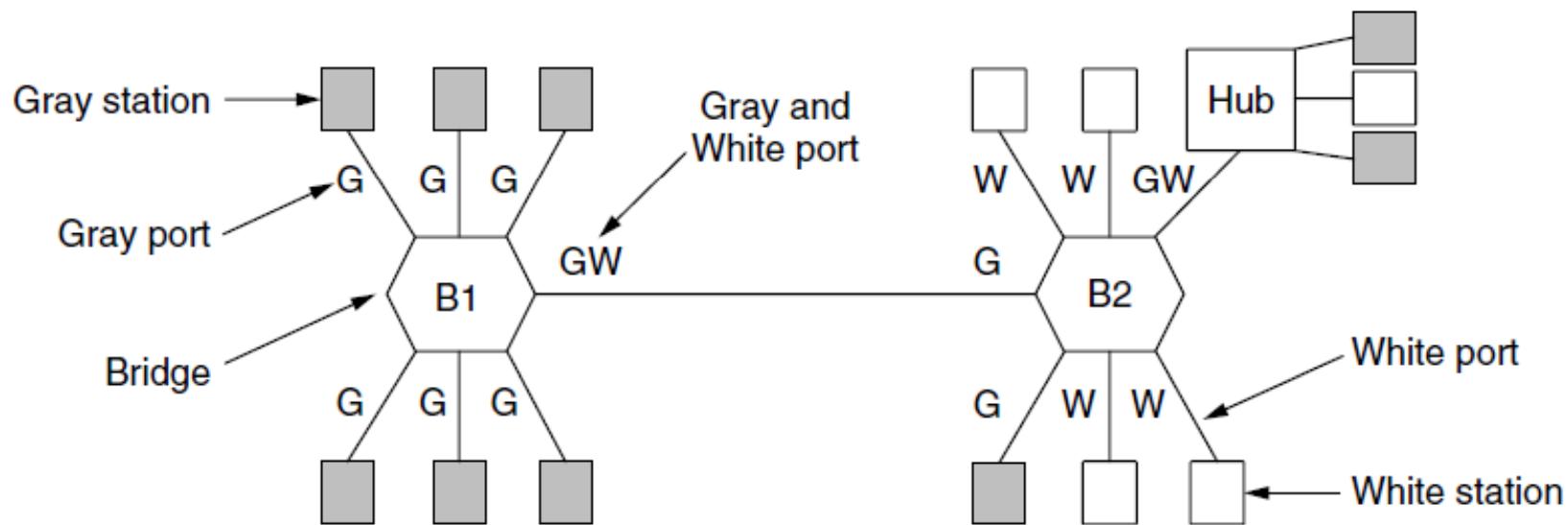
- A bridge or LAN switch operates in the Link layer



Virtual LANs (1)

VLANs (Virtual LANs) splits one physical LAN into multiple logical LANs to ease management tasks

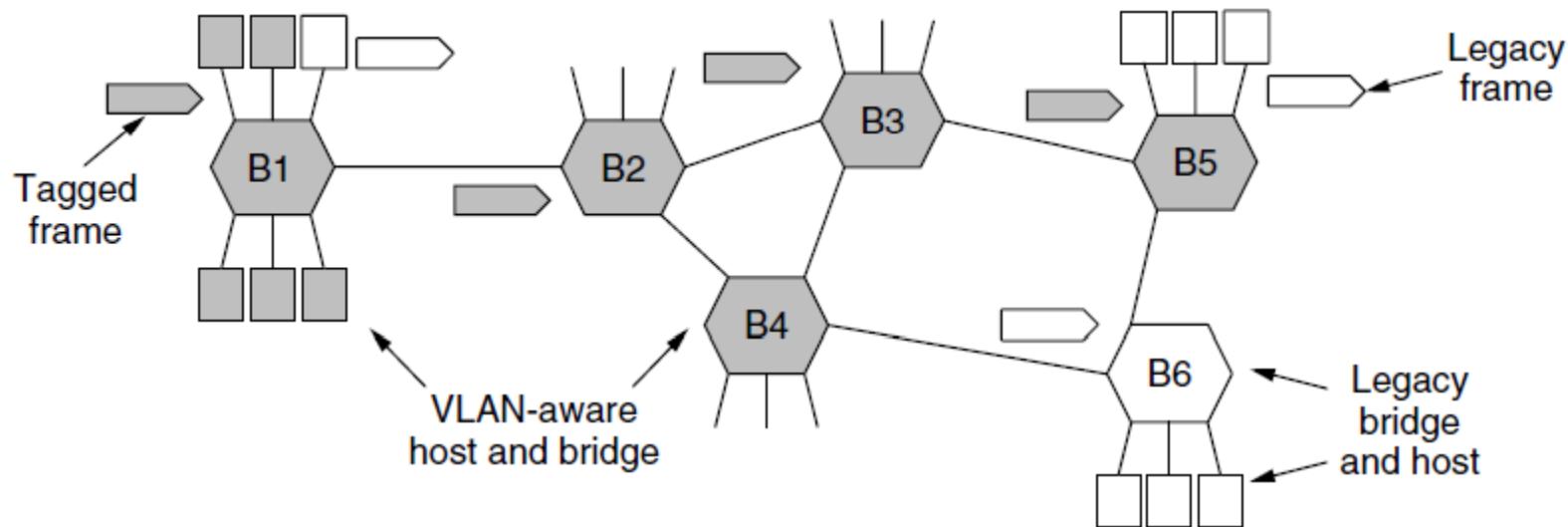
- Ports are “colored” according to their VLAN



Virtual LANs (2) – IEEE 802.1Q

Bridges need to be aware of VLANs to support them

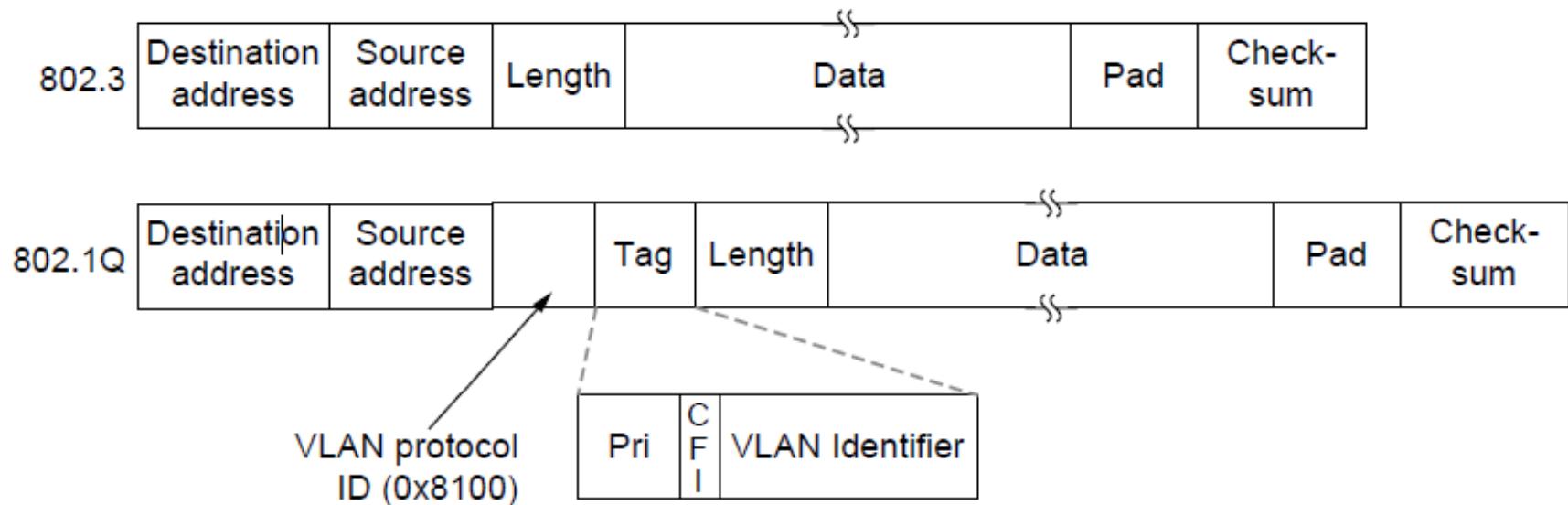
- In 802.1Q, frames are tagged with their “color”
- Legacy switches with no tags are supported



Virtual LANs (3) – IEEE 802.1Q

802.1Q frames carry a color tag (VLAN identifier)

- Length/Type value is 0x8100 for VLAN protocol



End

Chapter 4

Network Layer

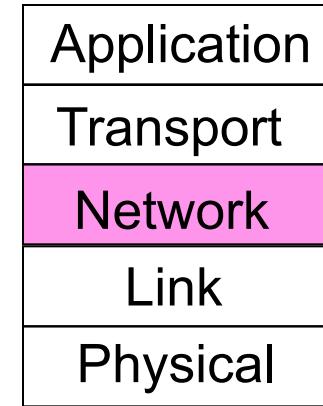
Chapter 5

- Design Issues
- Routing Algorithms
- Congestion Control
- Quality of Service
- Internetworking
- Network Layer of the Internet

Revised: August 2011

The Network Layer

Responsible for delivering packets between endpoints over multiple links

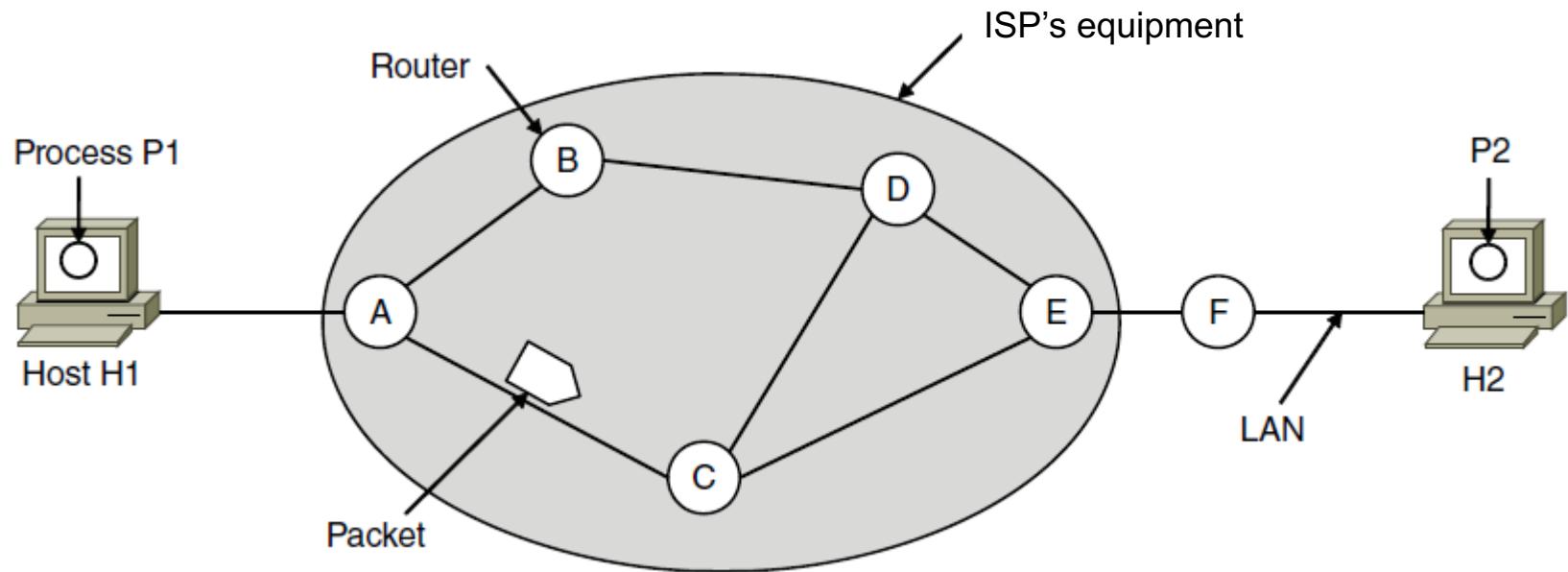


Design Issues

- Store-and-forward packet switching »
- Connectionless service – datagrams »
- Connection-oriented service – virtual circuits »
- Comparison of virtual-circuits and datagrams »

Store-and-Forward Packet Switching

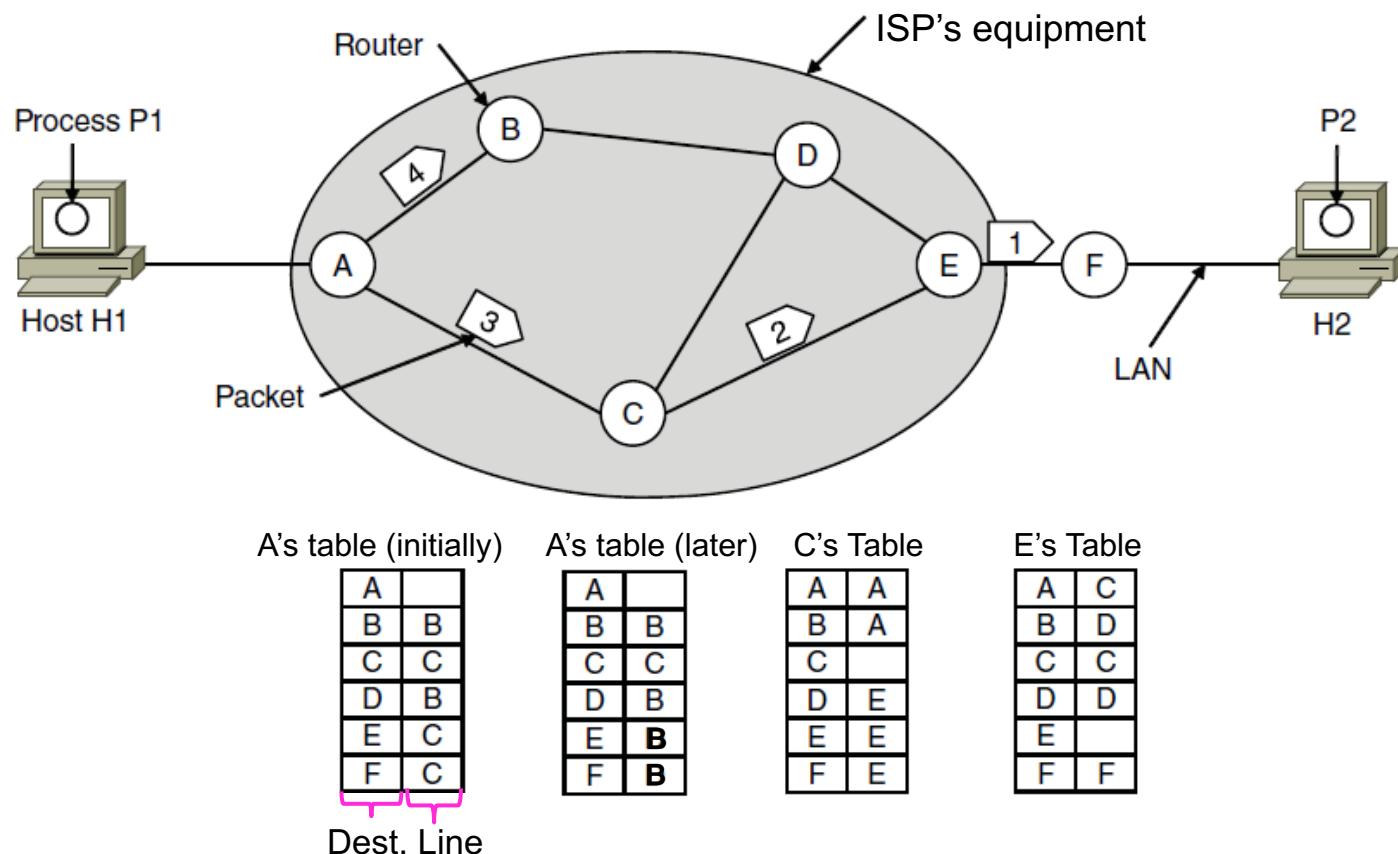
Hosts send packets into the network; packets are forwarded by routers



Connectionless Service – Datagrams

Packet is forwarded using destination address inside it

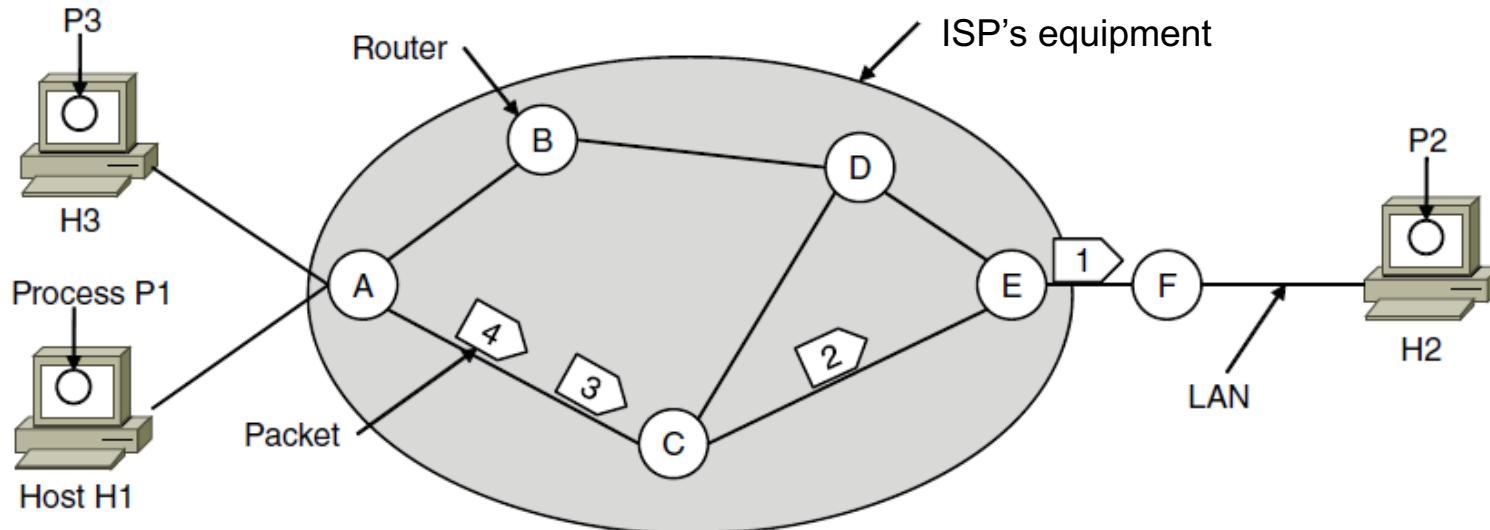
- Different packets may take different paths



Connection-Oriented – Virtual Circuits

Packet is forwarded along a virtual circuit using tag inside it

- Virtual circuit (VC) is set up ahead of time



A's table

H1	1
H3	1
C	1
C	2

C's Table

A	1
A	2
E	1
E	2

E's Table

C	1
C	2
F	1
F	2

In: Line Tag Line Tag: Out

Comparison of Virtual-Circuits & Datagrams

Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

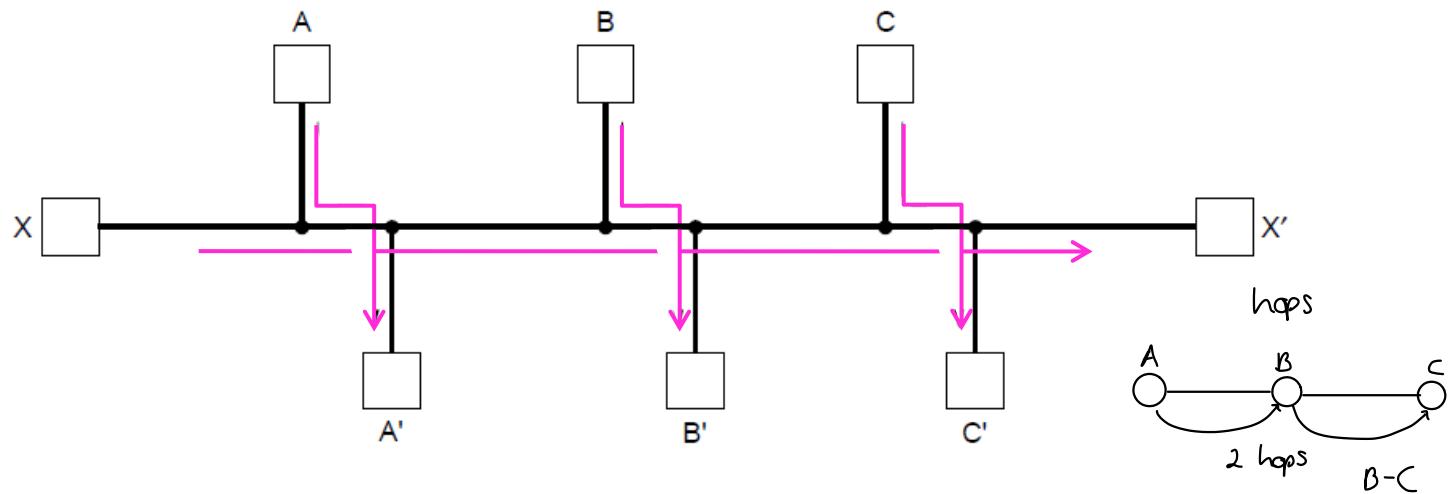
Routing Algorithms (1)

- Optimality principle »
- Shortest path algorithm »
- Flooding »
- Distance vector routing »
- Link state routing »
- Hierarchical routing »
- Broadcast routing »
- Multicast routing »
- Anycast routing »
- Routing for mobile hosts »
- Routing in ad hoc networks »

Routing Algorithms (2)

Routing is the process of discovering network paths

- Model the network as a graph of nodes and links
- Decide what to optimize (e.g., fairness vs efficiency)
- Update routes for changes in topology (e.g., failures)



Forwarding is the sending of packets along a path

Reenvio.

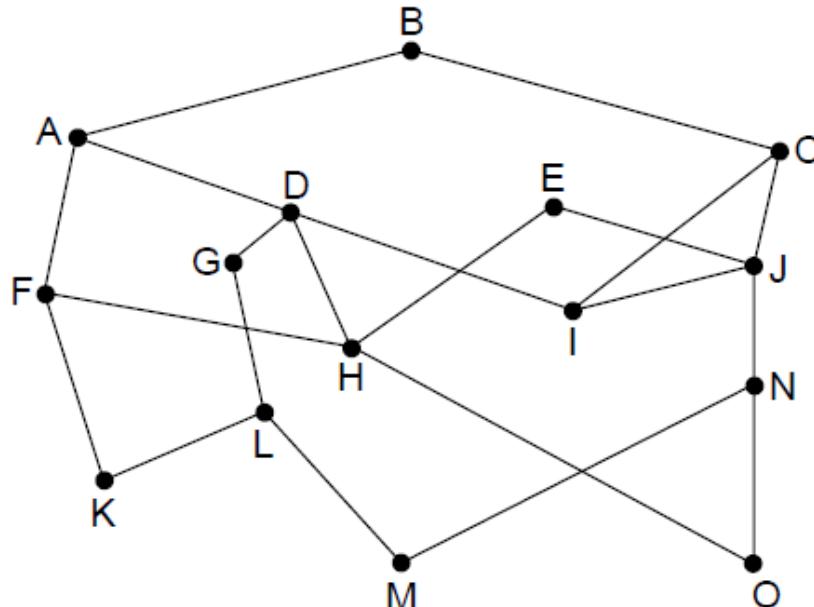
Falta de convergencia. Intermisión.

The Optimality Principle

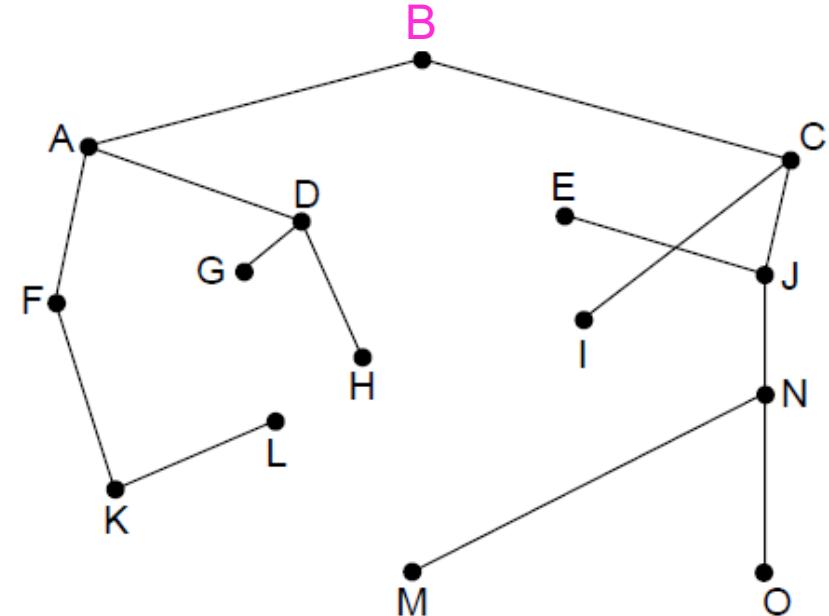
Algoritmo de Dijkstra

Each portion of a best path is also a best path; the union of them to a router is a tree called the sink tree

- Best means fewest hops in the example



Network



Sink tree of best paths to router B

Shortest Path Algorithm (1)

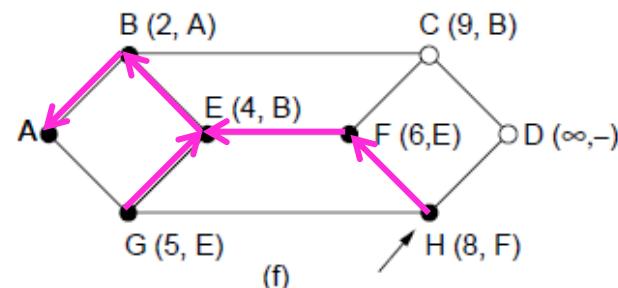
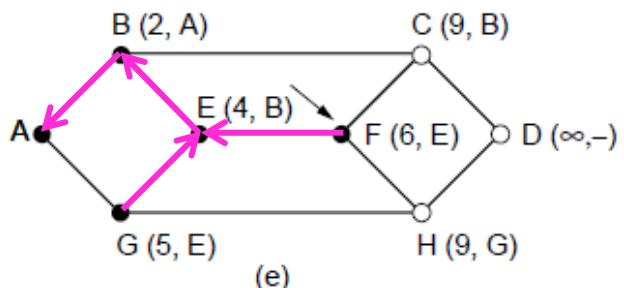
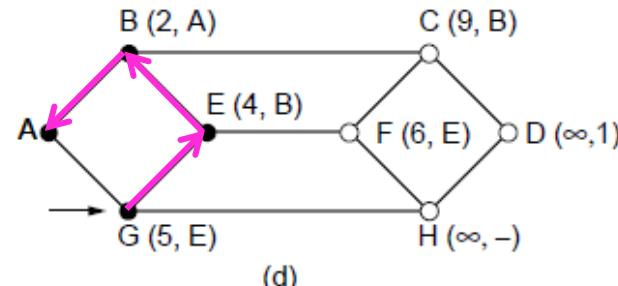
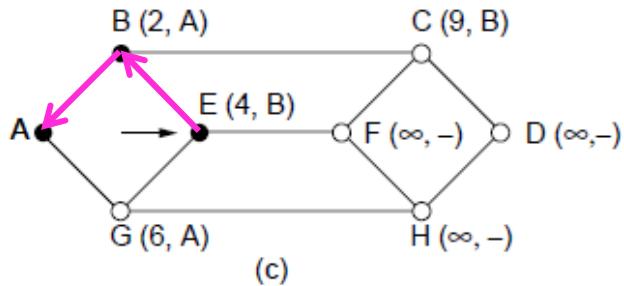
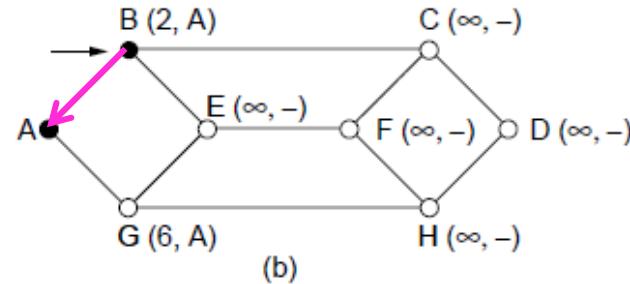
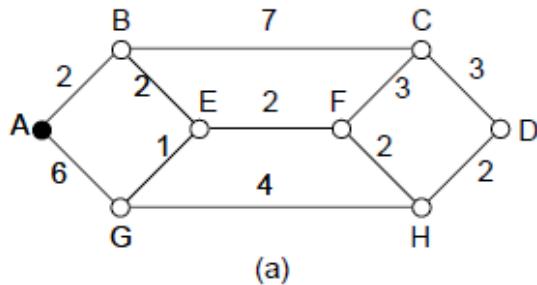
Dijkstra's algorithm computes a sink tree on the graph:

- Each link is assigned a non-negative weight/distance
- Shortest path is the one with lowest total weight
- Using weights of 1 gives paths with fewest hops

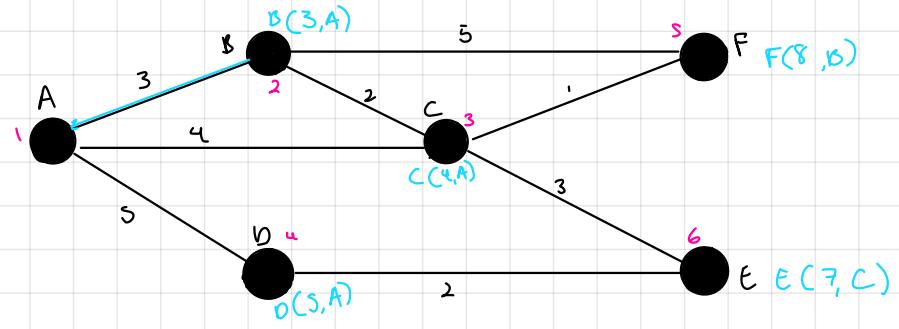
Algorithm:

- Start with sink, set distance at other nodes to infinity
- Relax distance to other nodes
- Pick the lowest distance node, add it to sink tree
- Repeat until all nodes are in the sink tree

Shortest Path Algorithm (2)



A network and first five steps in computing the shortest paths from A to D. Pink arrows show the sink tree so far.



Tomaremos orden de entrada.

Shortest Path Algorithm (3)

```
for (p = &state[0]; p < &state[n]; p++) {  
    p->predecessor = -1;  
    p->length = INFINITY;  
    p->label = tentative;  
}  
state[t].length = 0; state[t].label = permanent;  
k = t;  
do {  
    for (i = 0; i < n; i++)  
        if (dist[k][i] != 0 && state[i].label == tentative) {  
            if (state[k].length + dist[k][i] < state[i].length) {  
                state[i].predecessor = k;  
                state[i].length = state[k].length + dist[k][i];  
            }  
        }  
}
```

} Start with the sink,
all other nodes are
unreachable

} Relaxation step.
Lower distance to
nodes linked to
newest member of
the sink tree

Shortest Path Algorithm (4)

```
    . . .
k = 0; min = INFINITY;
for (i = 0; i < n; i++)
    if (state[i].label == tentative && state[i].length < min) {
        min = state[i].length;
        k = i;
    }
    state[k].label = permanent;
} while (k != s);
```

Find the lowest distance, add it to the sink tree, and repeat until done

Flooding

A simple method to send a packet to all network nodes

Each node floods a new packet received on an incoming link by sending it out all of the other links

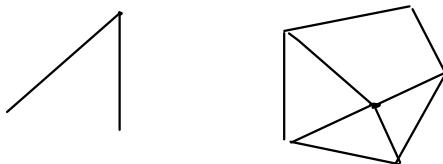
Nodes need to keep track of flooded packets to stop the flood; even using a hop limit can blow up exponentially

Distance Vector Routing (1)

Se contrasta con el enlace estocástico.
Tecnología de red con dispositivos ya fabricados

Distance vector is a distributed routing algorithm

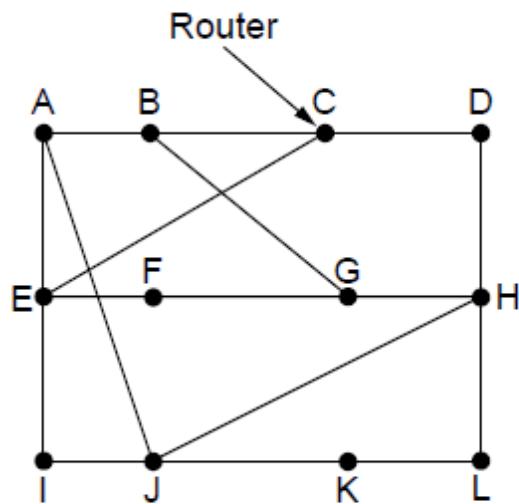
- Shortest path computation is split across nodes



Algorithm:

- Each node knows distance of links to its neighbors
- Each node advertises vector of lowest known distances to all neighbors
- Each node uses received vectors to update its own
- Repeat periodically

Distance Vector Routing (2)



Para dispositivos pequeños
relativamente útil y económico.

Tiempo de convergencia: tiempo de transición
algoritmos que utilizan optimización: complejidad,
convergencia.
Tener rutas alternas que genera el mayor
número de rutas diversas)

New estimated delay from J

↓ Line

To	A	I	H	K	Line
A	0	24	20	21	8 A
B	12	36	31	28	20 A
C	25	18	19	36	28 I
D	40	27	8	24	20 H
E	14	7	30	22	17 I
F	23	20	19	40	30 I
G	18	31	6	31	18 H
H	17	20	0	19	12 H
I	21	0	14	22	10 I
J	9	11	7	10	0 -
K	24	22	22	0	6 K
L	29	33	9	9	15 K

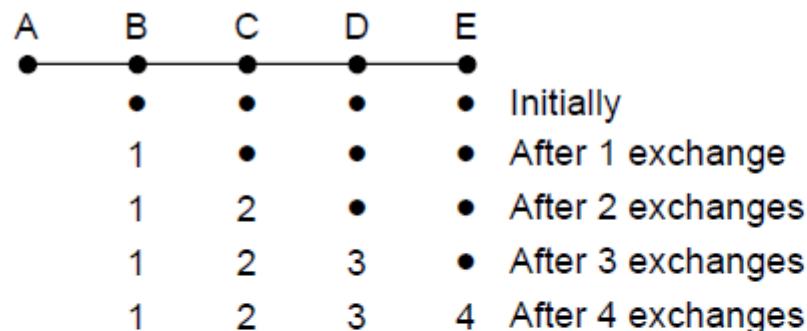
JA delay is 8 JI delay is 10 JH delay is 12 JK delay is 6

Vectors received at J from Neighbors A, I, H and K

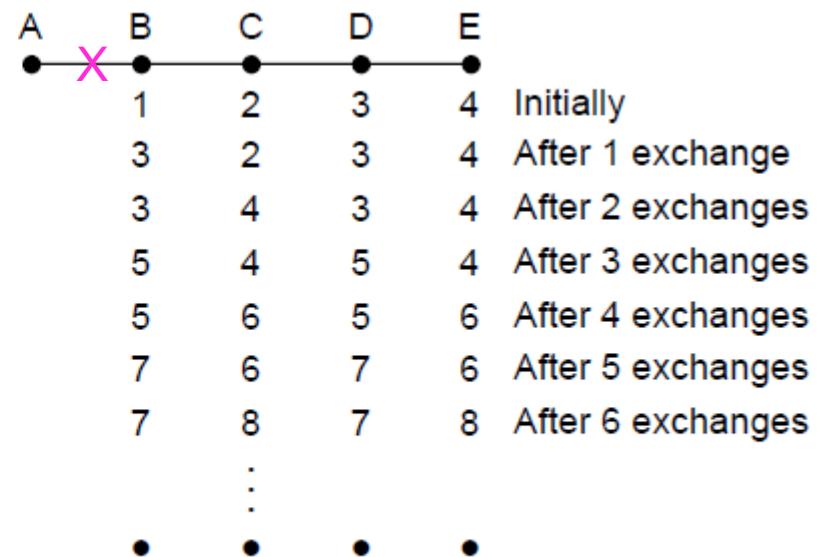
New vector for J

The Count-to-Infinity Problem

Failures can cause DV to “count to infinity” while seeking a path to an unreachable node



Good news of a path to A spreads quickly



Bad news of no path to A is learned slowly

Link State Routing (1)

No hay cuenta al infinito. Si se cae un enlace se recalcula toda la topología y la mejor ruta a cada nodo

Link state is an alternative to distance vector

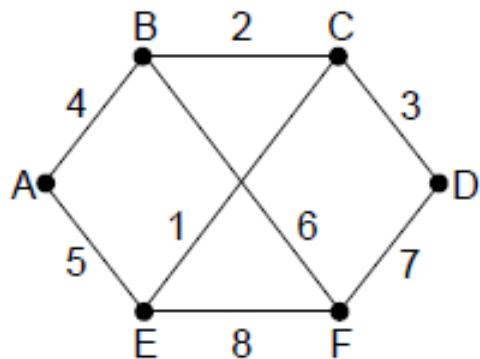
- More computation but simpler dynamics
- Widely used in the Internet (OSPF, ISIS)

Algorithm:

- Each node floods information about its neighbors in LSPs (Link State Packets); all nodes learn the full network graph
- Each node runs Dijkstra's algorithm to compute the path to take for each destination

Link State Routing (2) – LSPs

LSP (Link State Packet) for a node lists neighbors and weights of links to reach them



Network

causa problemas de conteo al infinito.
Dispositivo del internet de las cosas

A	Seq.	B	Seq.	C	Seq.	D	Seq.	E	Seq.	F	Seq.
	Age										
B	4	A	4	B	2	C	3	A	5	B	6
E	5	C	2	D	3	F	7	C	1	D	7
		F	6	E	1			F	8	E	8

LSP for each node

Link State Routing (3) – Reliable Flooding

Romper ciclo y empezar a generar rutas.

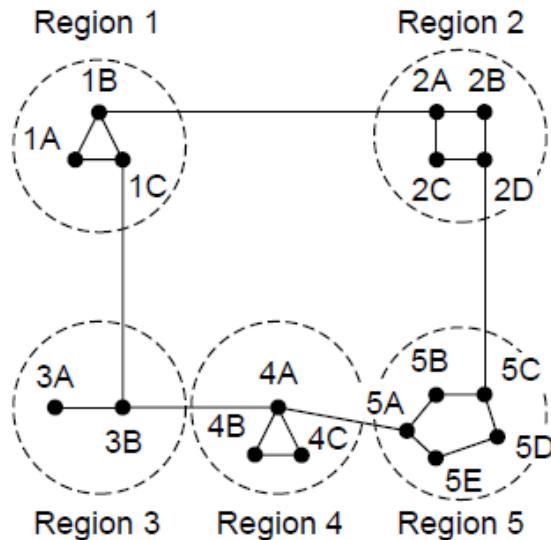
Seq. number and age are used for reliable flooding

- New LSPs are acknowledged on the lines they are received and sent on all other lines
- Example shows the LSP database at router B

Source	Seq.	Age	Send flags			ACK flags			Data
			A	C	F	A	C	F	
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Hierarchical Routing

Hierarchical routing reduces the work of route computation but may result in slightly longer paths than flat routing



Full table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Hierarchical table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

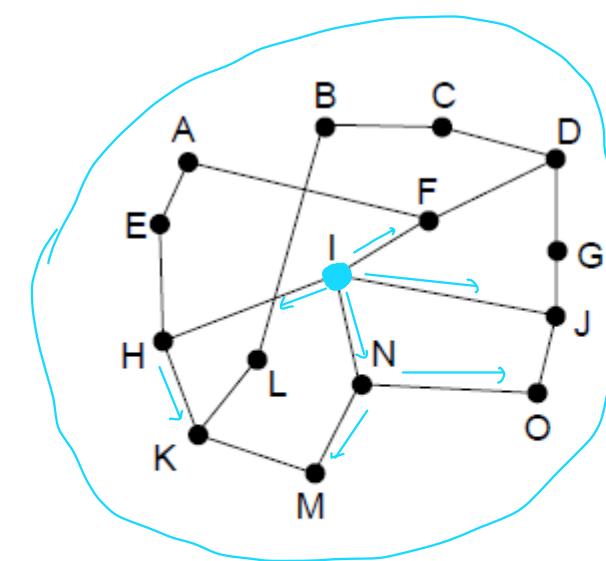


Best choice to reach nodes in 5 except for 5C

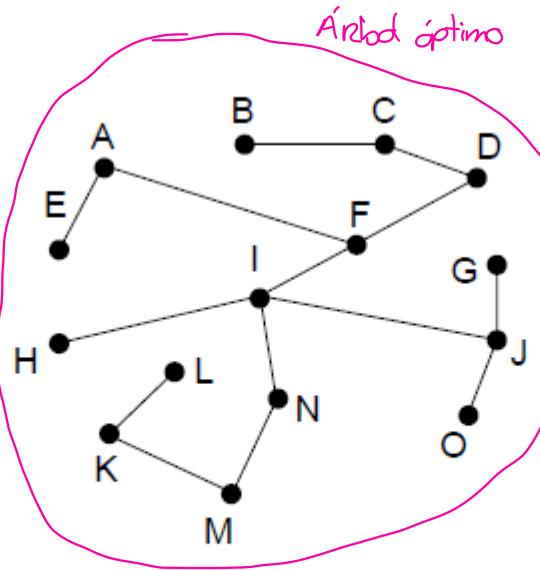
Broadcast Routing

Broadcast sends a packet to all nodes

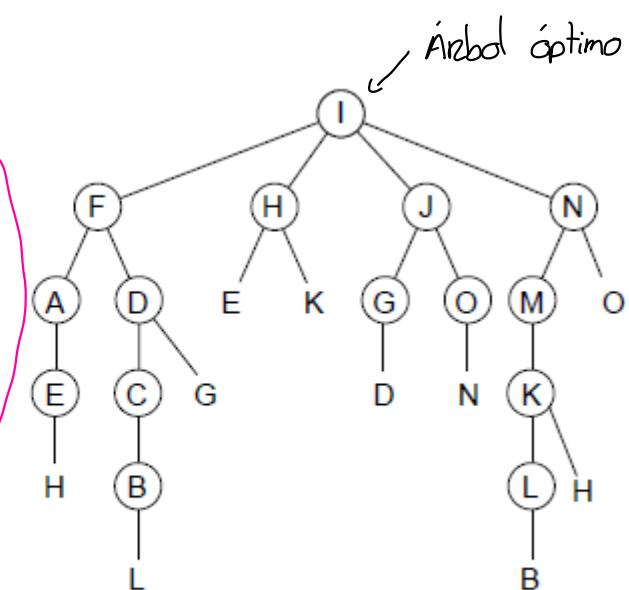
- RPF (Reverse Path Forwarding): send broadcast received on the link to the source out all remaining links
- Alternatively, can build and use sink trees at all nodes



Network



Sink tree for / is
efficient broadcast



RPF from / is larger than
sink tree

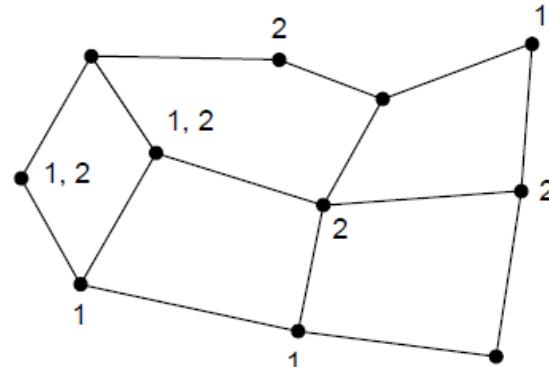
Cuando paquete llega por primera vez es porque usó la ruta más óptima

Multicast Routing (1) – Dense Case

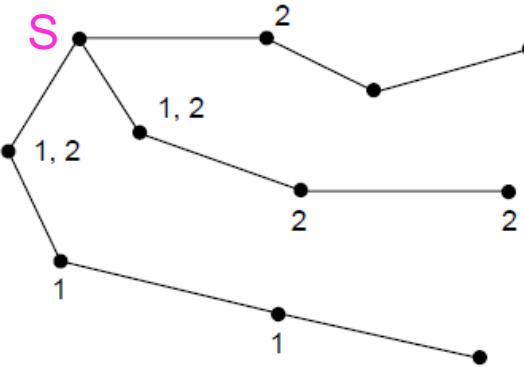
Un grupo o conjunto de grupos

Multicast sends to a subset of the nodes called a group

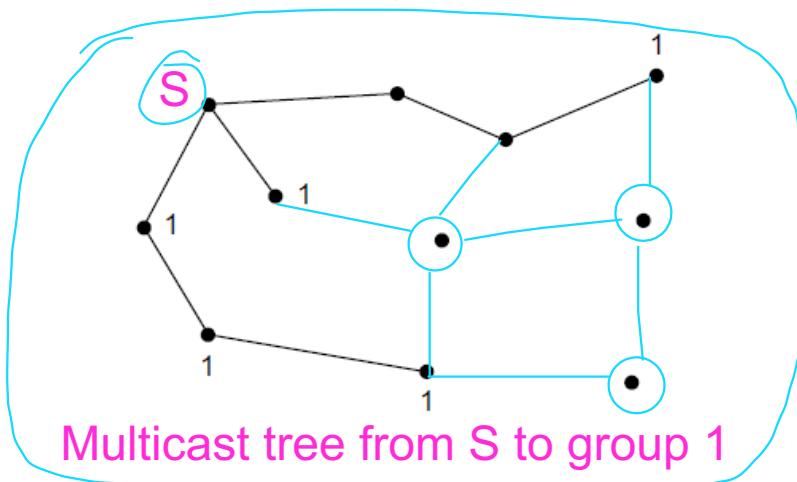
- Uses a different tree for each group and source



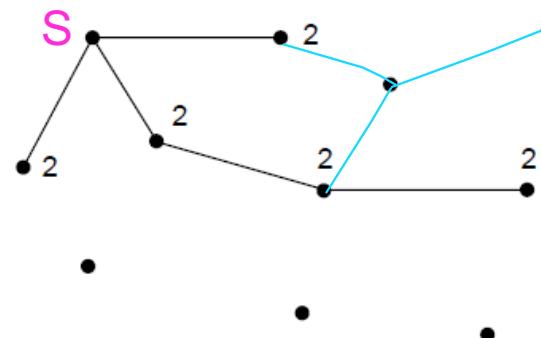
Network with groups 1 & 2



Spanning tree from source S



Multicast tree from S to group 1

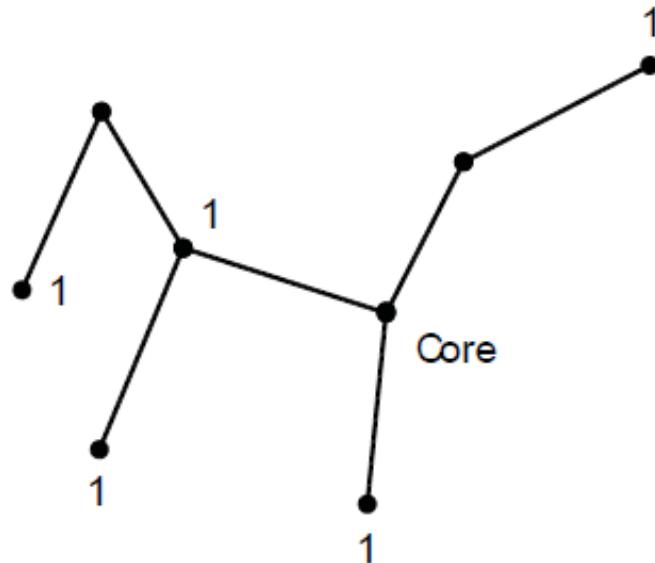


Multicast tree from S to group 2

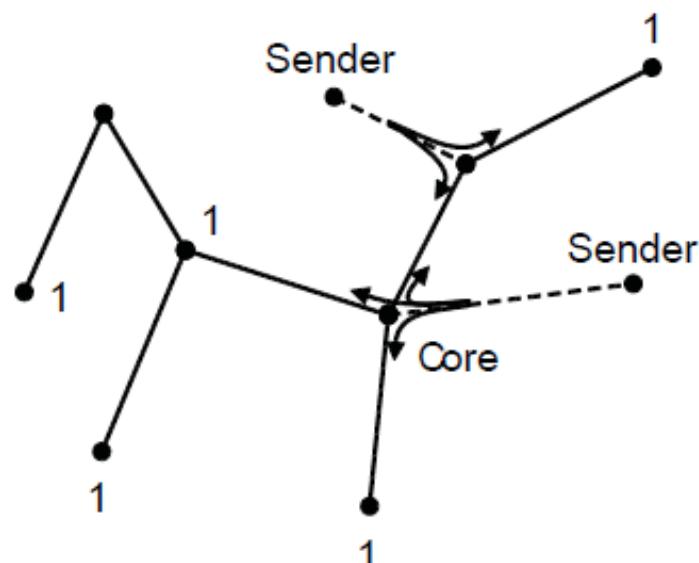
Multicast Routing (2) – Sparse Case

CBT (Core-Based Tree) uses a single tree to multicast

- Tree is the sink tree from core node to group members
- Multicast heads to the core until it reaches the CBT



Sink tree from core to group 1

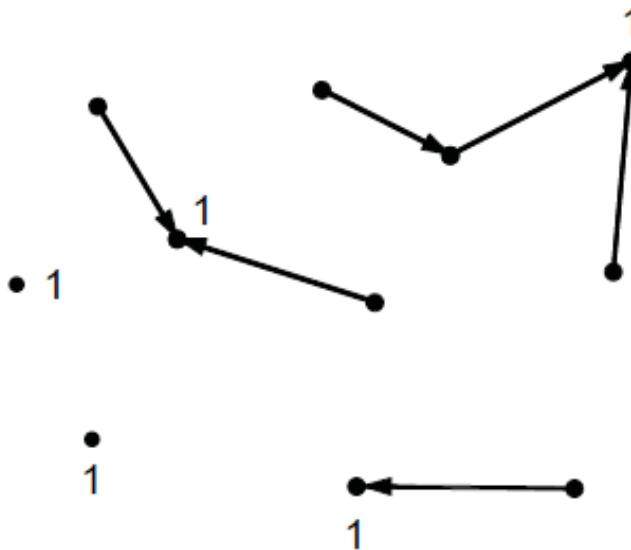


Multicast is send to the core then down when it reaches the sink tree

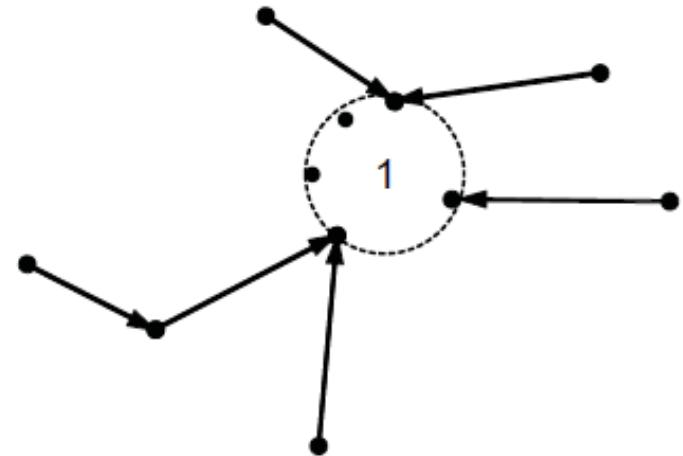
Anycast Routing

Anycast sends a packet to one (nearest) group member

- Falls out of regular routing with a node in many places



Anycast routes to group 1

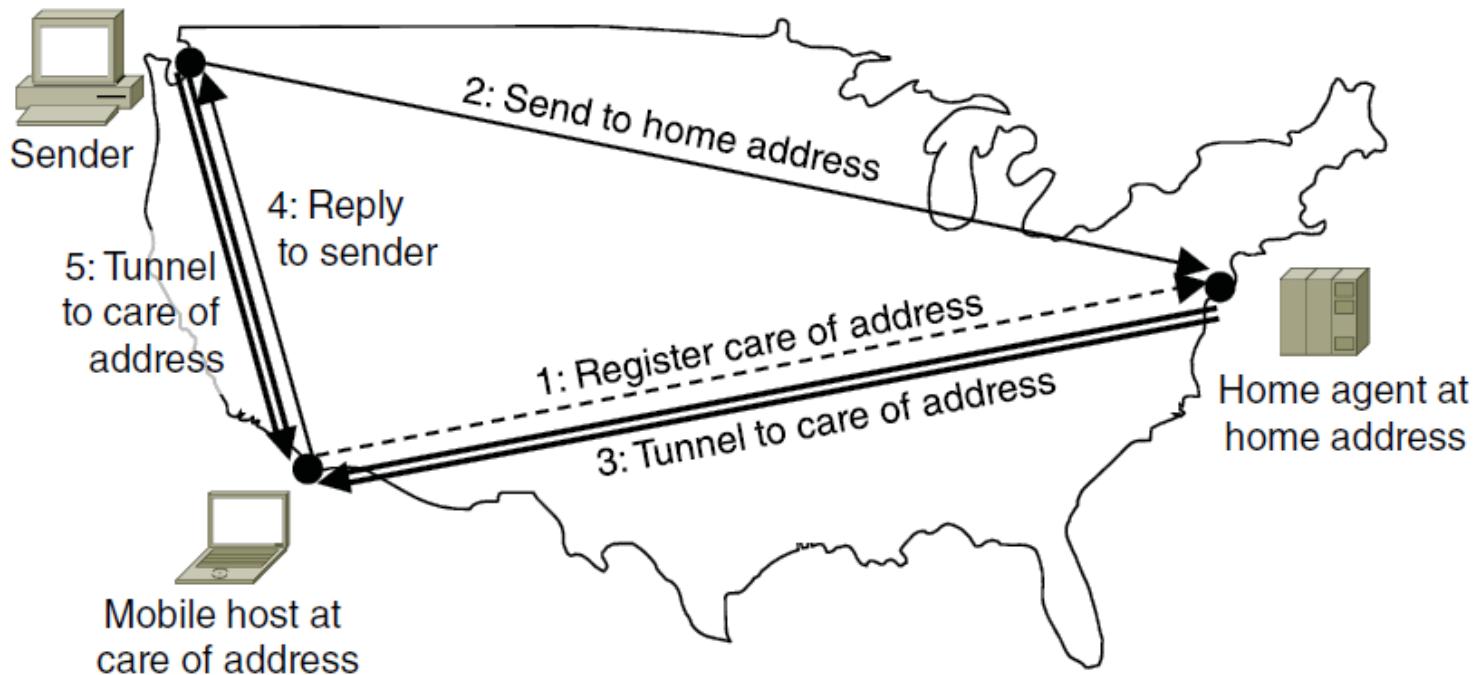


Apparent topology of
sink tree to “node” 1

Routing for Mobile Hosts

Mobile hosts can be reached via a home agent

- Fixed home agent tunnels packets to reach the mobile host; reply can optimize path for subsequent packets
- No changes to routers or fixed hosts

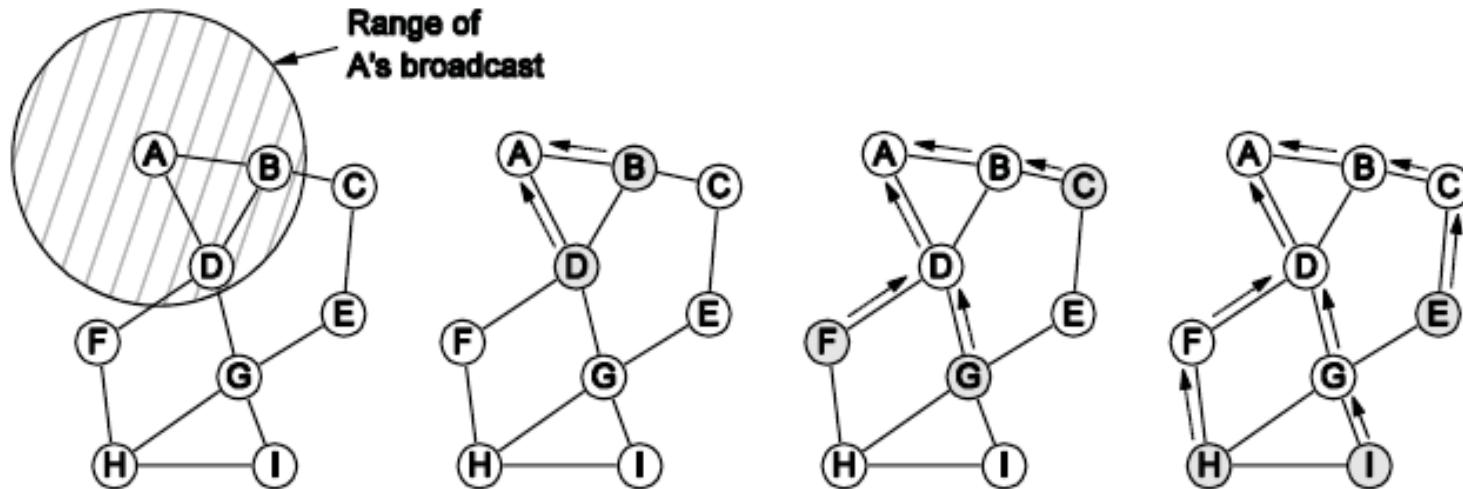


Routing in Ad Hoc Networks

Protocolos que crean las rutas solo cuando las necesita.

The network topology changes as wireless nodes move

- Routes are often made on demand, e.g., AODV (below)



A's starts to
find route to /

A's broadcast
reaches B & D

B's and D's
broadcast
reach C, F & G

C's, F's and G's
broadcast
reach H & I

Recorrer la ruta inversa

Armar las rutas necesarias
Overhead → lo que empleo para
armar la red.

Congestion Control (1)

Redirección de tráfico. No circula. Evitar horas pico. → Control de congestión.
Nivel de red, control de flujo nivel punto a punto

Handling congestion is the responsibility of the Network and Transport layers working together

– We look at the Network portion here

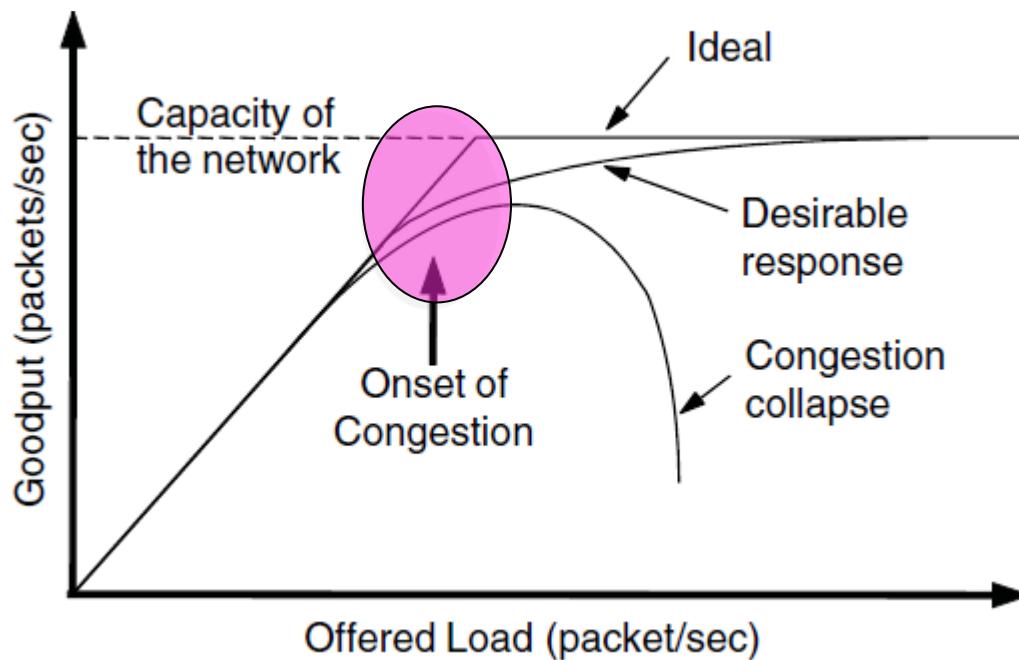
- Traffic-aware routing »
- Admission control »
- Traffic throttling »
- Load shedding »

Congestion Control (2)

Evitar que haya una gran cantidad de paquetes que se interpongan.
No caer en modo de crecimiento, sino ir subiendo

Congestion results when too much traffic is offered; performance degrades due to loss/retransmissions

- Goodput (=useful packets) trails offered load



Congestion Control

- Back Pressure: When a router is congested, it can inform the previous upstream router to reduce the rate of outgoing packets. The action can be recursive all the way to the router before the source.
- Choke Point: A packet sent by a router to the source to inform it of congestion. This type of control is similar to ICMP's source quench packet.
- Implicit Signaling: Source can detect an implicit signal concerning congestion and slow down its sending rate. For example, the mere delay in receiving an acknowledgement can be a signal that the network is congested.
- Explicit Signaling: Routers that experience congestion can send an explicit signal, the setting of a bit in a packet, for example, to inform the sender or the receiver of congestion.
 - Backward Signaling: Bit can be set in a packet moving in the direction opposite to the congestion; indicate the source.
 - Forward Signaling: Bit can be set in a packet moving in the direction of the congestion; indicate the destination.

Open-Loop Congestion control

Open-Loop Congestion Control (rely on other layers for feedback and control)

Retransmission policy - a good policy can reduce congestion

Window policy - sel-reject better than go-back-N; use a bigger window size

Acknowledgment policy - don't ack each packet individually

Discard policy - a good policy by routers may prevent congestion and at the same time may not harm the integrity of the transmission

Admission policy - QOS mechanism

Closed-Loop Congestion Control

Closed-Loop Congestion Control

Backpressure - when a router is congested, it informs the previous upstream router to reduce the rate of outgoing packets

Choke packet of choke point - sent by router to source, similar to ICMP's source quench packet

Implicit signaling - look for delay in some other action

Explicit signaling - router sends an explicit signal

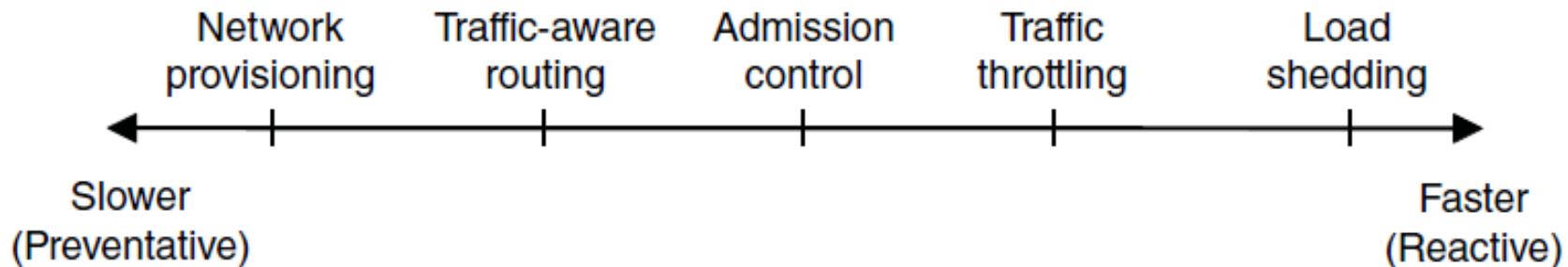
Backward signaling - bit is set in packet moving in the direction opposite to the congestion

Forward signaling - bit is set in packet moving in the direction of congestion. Receiver can use policy such as slowing down acks to alleviate congestion

Congestion Control (3) – Approaches

Network must do its best with the offered load

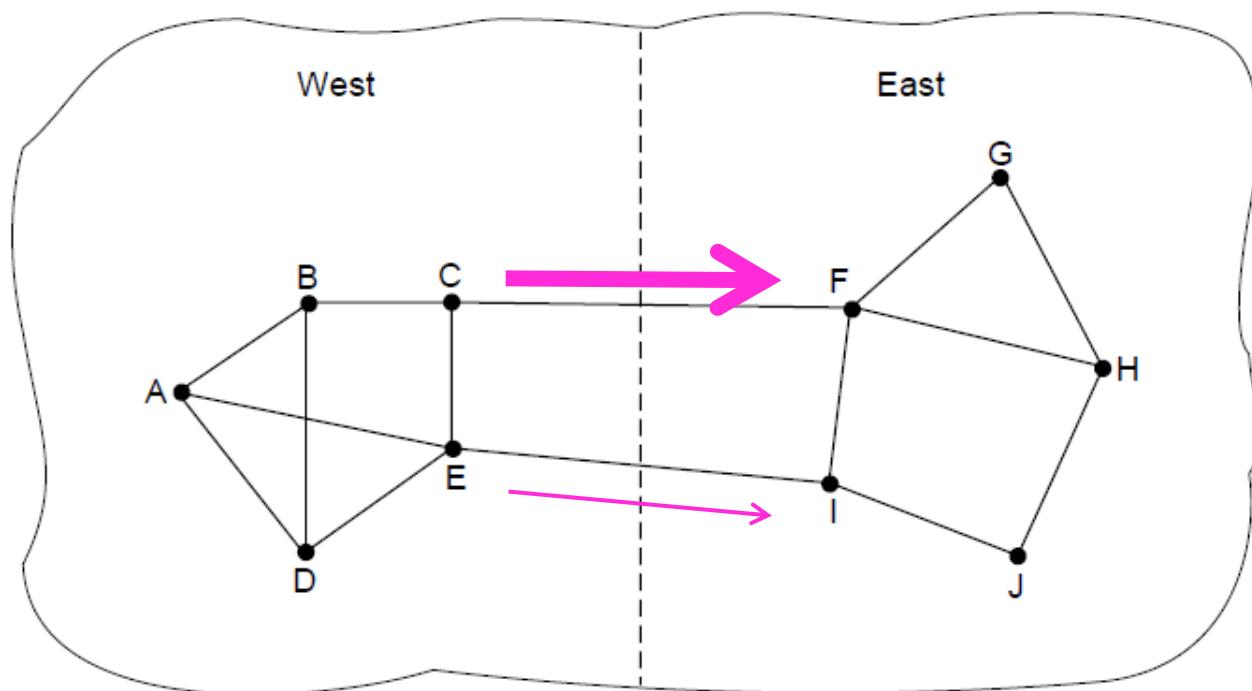
- Different approaches at different timescales
- Nodes should also reduce offered load (Transport)



Traffic-Aware Routing

Choose routes depending on traffic, not just topology

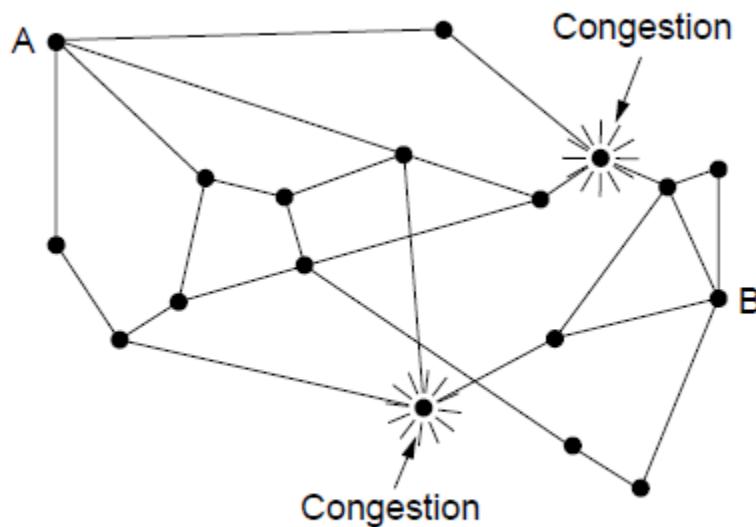
- E.g., use *EI* for West-to-East traffic if *CF* is loaded
- But take care to avoid oscillations



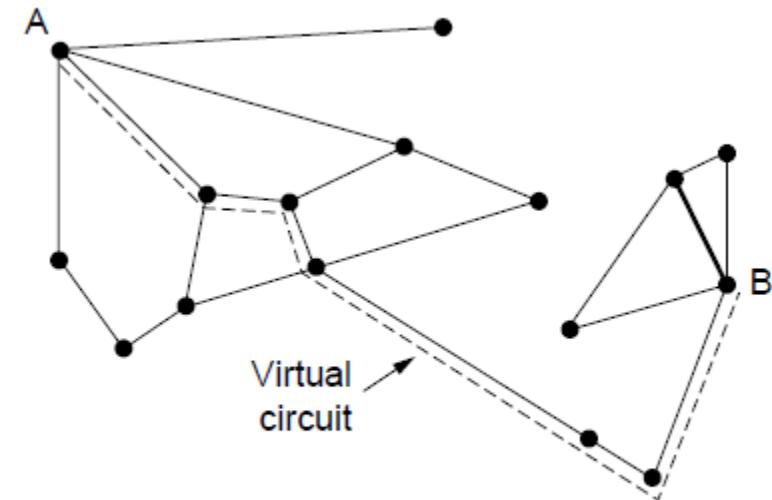
Admission Control

Admission control allows a new traffic load only if the network has sufficient capacity, e.g., with virtual circuits

- Can combine with looking for an uncongested route



Network with some
congested nodes



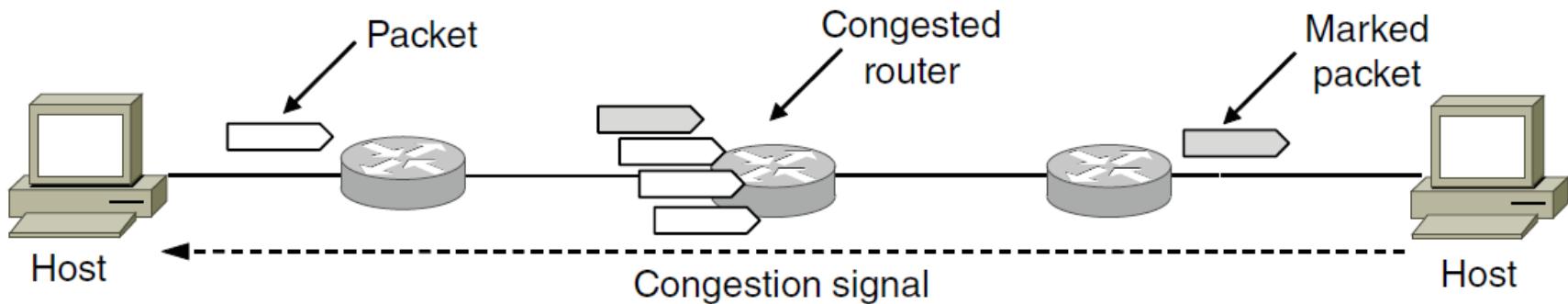
Uncongested portion and
route AB around congestion

Traffic Throttling

Avisa al destino. Conexión a la fuente. Control de congestión y control de flujo abarcan diferentes elementos

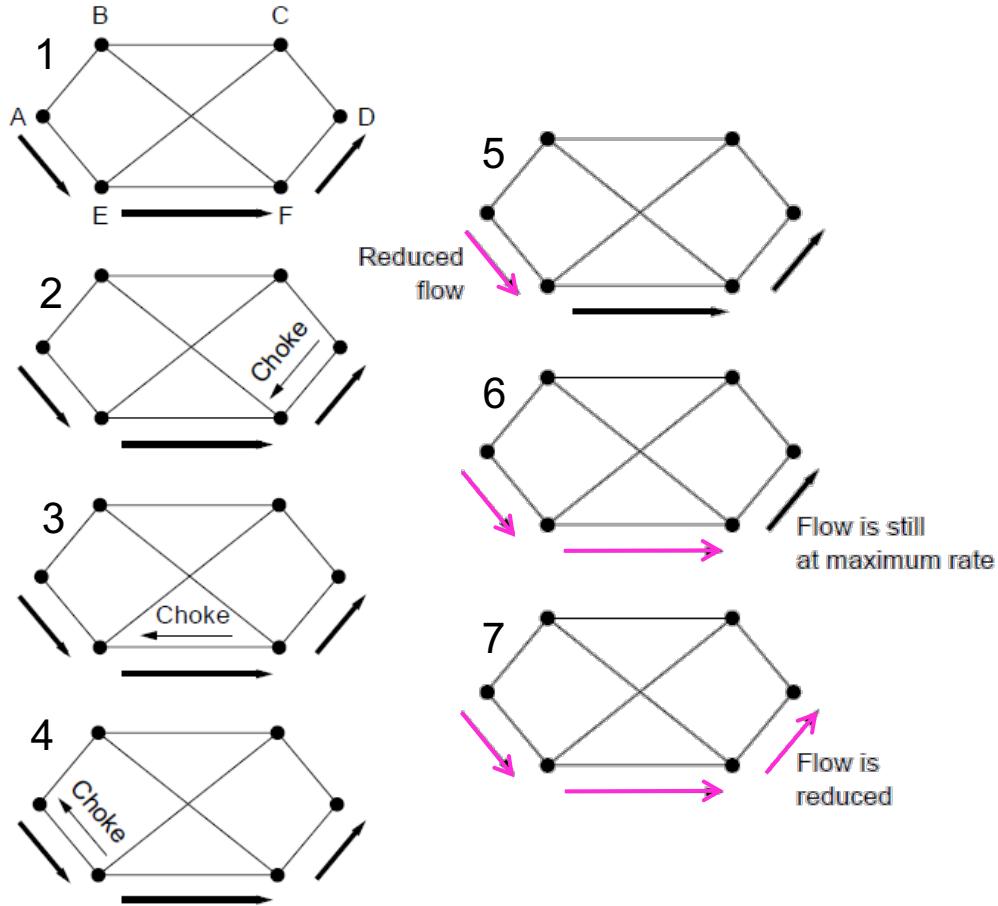
Congested routers signal hosts to slow down traffic

- ECN (Explicit Congestion Notification) marks packets and receiver returns signal to sender



Choke packet

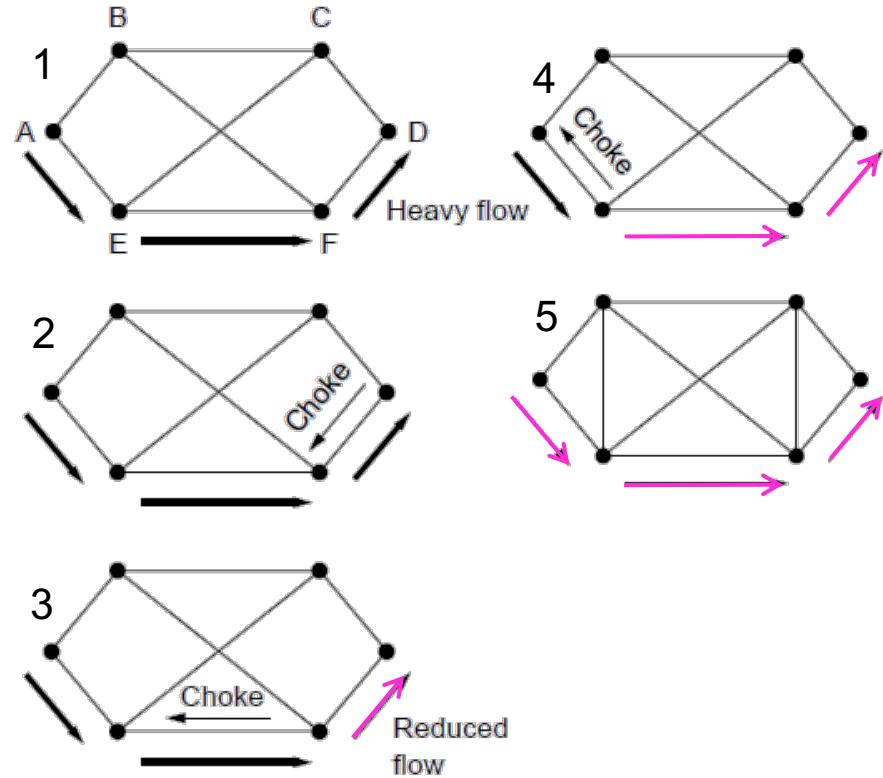
End-to-end (right) takes longer to have an effect



Choke packet

Can be done end-to-end or link-by-link

Link-by-link (right) produces rapid relief



Load Shedding

Load shedding: Wine Vs. Milk

Wine: drop new packets (keep old); good for file transfer

Milk: drop old packets (keep new); good for multimedia

Random Early Detection

When the average queue length exceeds a threshold,
packets are picked at random from the queue and discarded.

Quality of Service

- Application requirements »
- Traffic shaping »
- Packet scheduling »
- Admission control »
- Integrated services »
- Differentiated services »

Application Requirements (1)

Different applications care about different properties

- We want all applications to get what they need

Application	Bandwidth	Delay	Jitter	Loss
Email	Low	Low	Low	Medium
File sharing	High	Low	Low	Medium
Web access	Medium	Medium	Low	Medium
Remote login	Low	Medium	Medium	Medium
Audio on demand	Low	Low	High	Low
Video on demand	High	Low	High	Low
Telephony	Low	High	High	Low
Videoconferencing	High	High	High	Low

“High” means a demanding requirement, e.g., low delay

Jitter

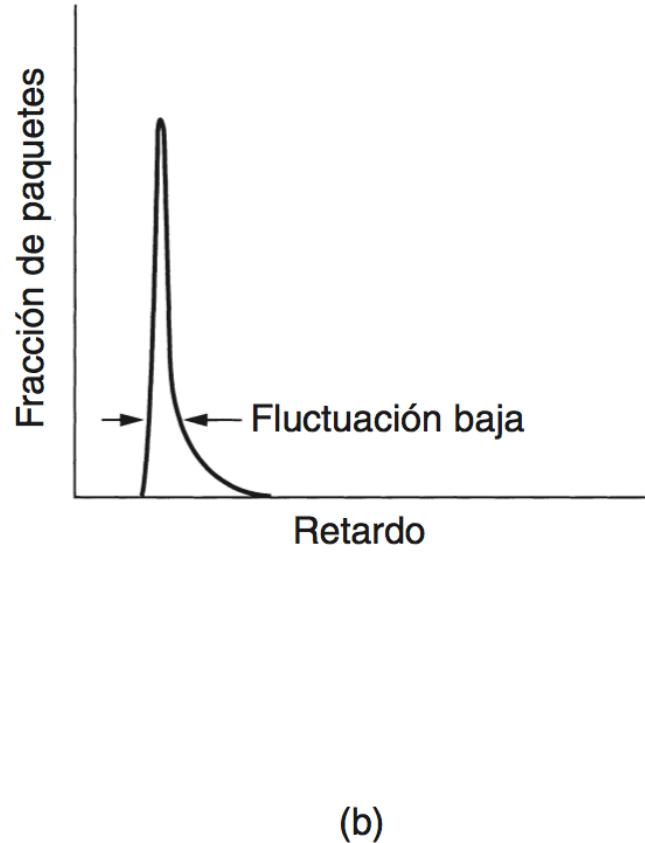
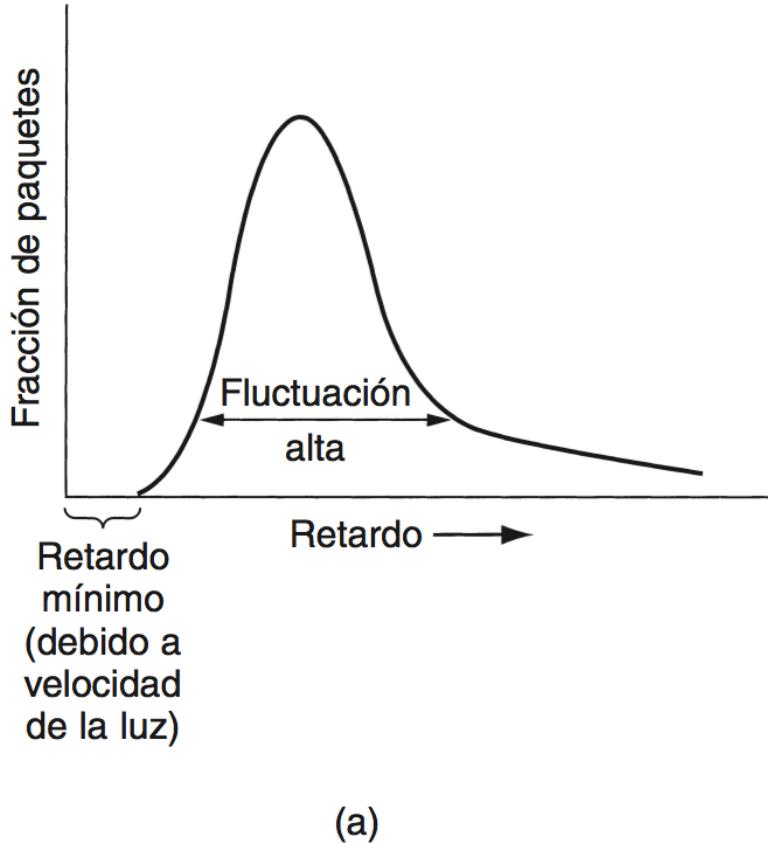


Figura 5-29. (a) Fluctuación alta. (b) Fluctuación baja.

Application Requirements (2)

Network provides service with different kinds of QoS (Quality of Service) to meet application requirements

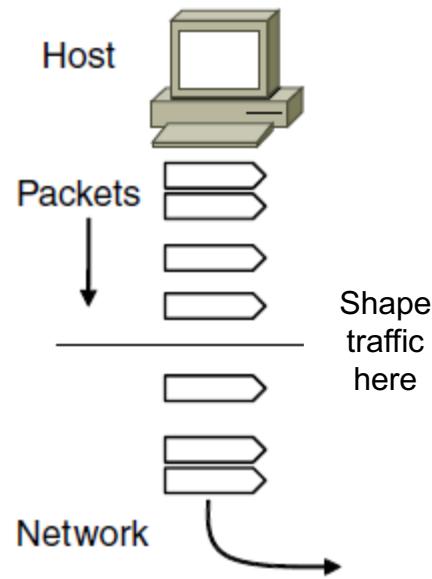
Network Service	Application
Constant bit rate	Telephony
Real-time variable bit rate	Videoconferencing
Non-real-time variable bit rate	Streaming a movie
Available bit rate	File transfer

Example of QoS categories from ATM networks

Traffic Shaping (1)

Traffic shaping regulates the average rate and burstiness of data entering the network

- Lets us make guarantees



Leaky Bucket

Leaky bucket limits both the average rate (R) and short-term burst (B) of traffic

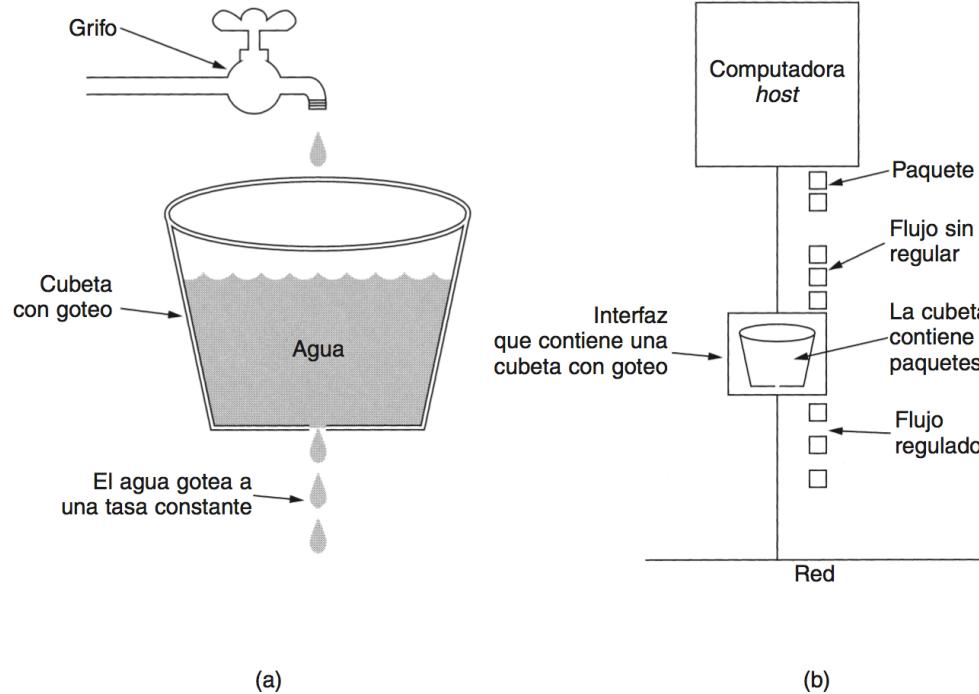
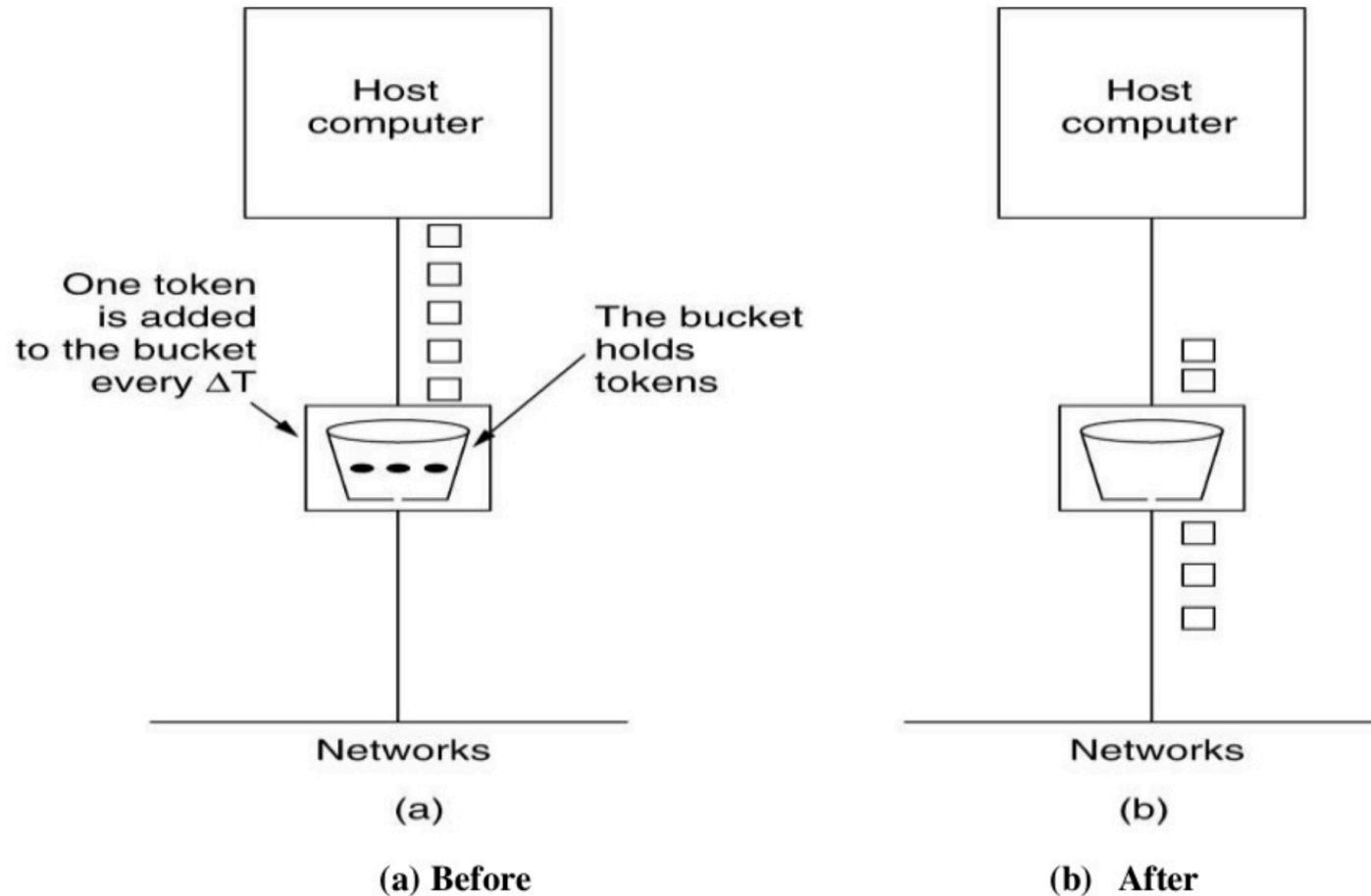
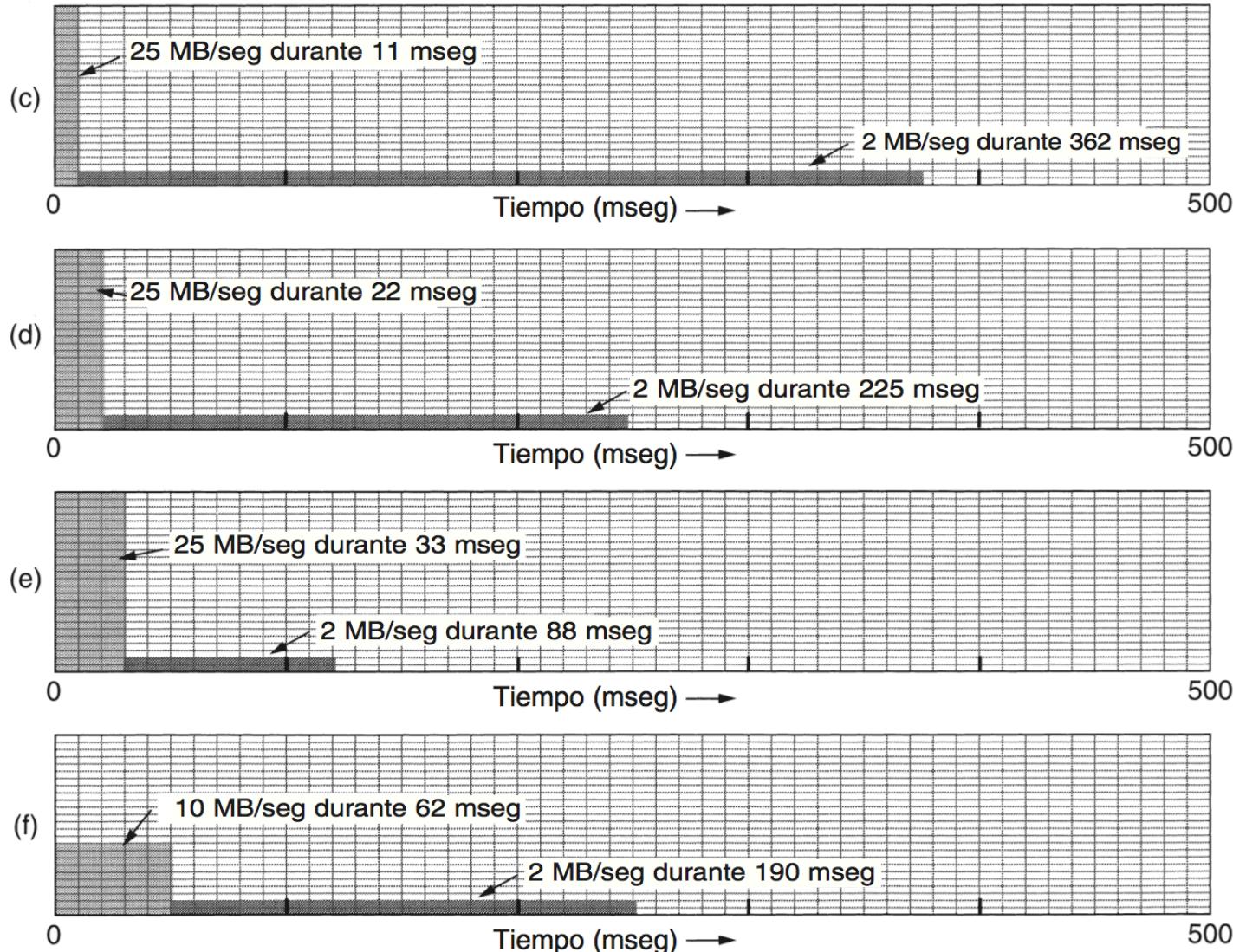


Figura 5-32. (a) Una cubeta con goteo, llena de agua. (b) Cubeta con goteo, llena de paquetes.

Token bucket

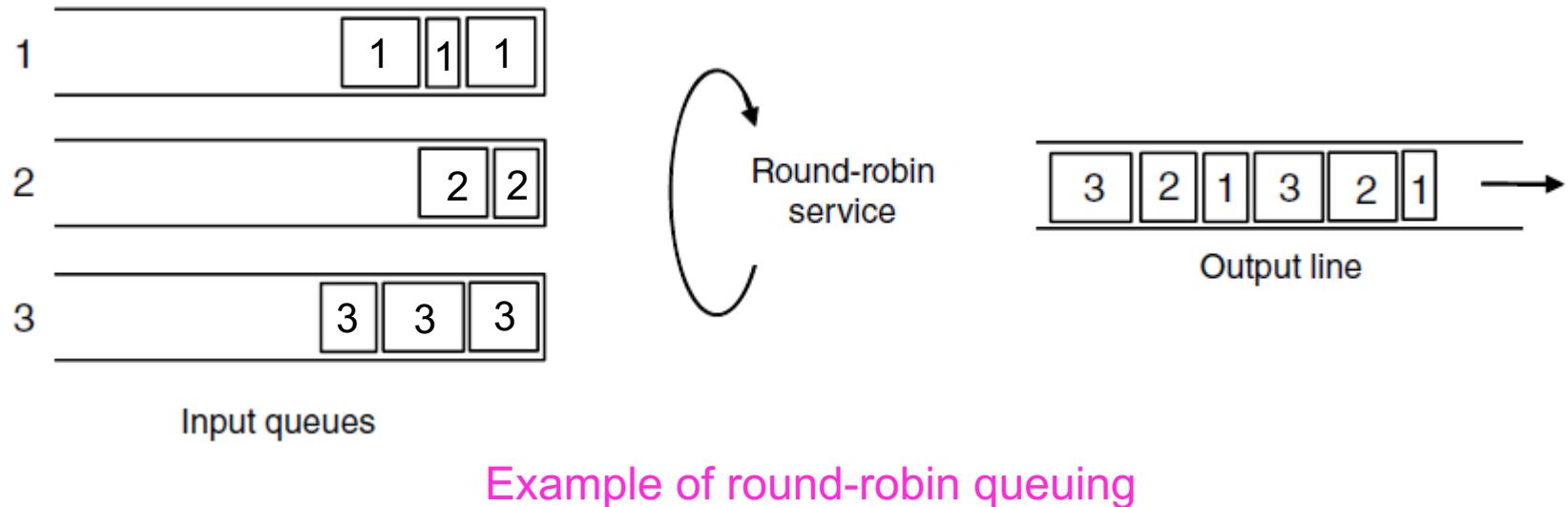


Traffic Shaping (Leaky Bucket)



Packet Scheduling (1)

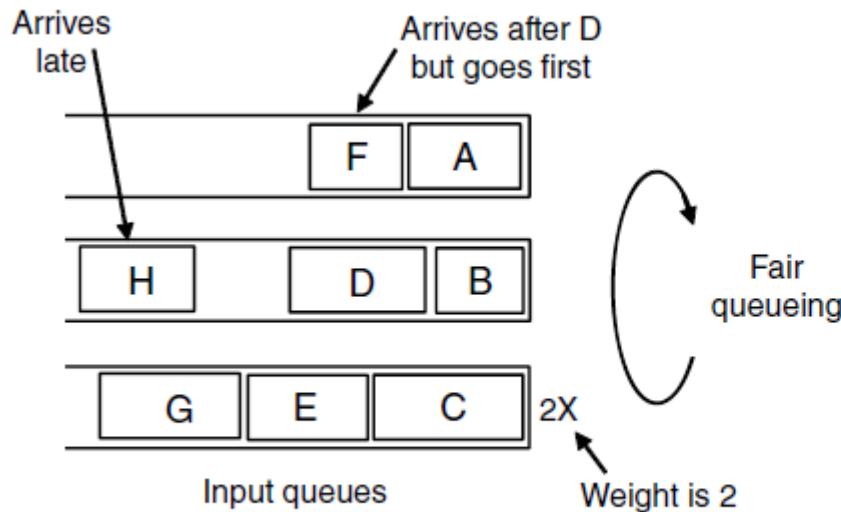
Packet scheduling divides router/link resources among traffic flows with alternatives to FIFO (First In First Out)



Packet Scheduling (2)

Fair Queueing approximates bit-level fairness with different packet sizes; weights change target levels

- Result is WFQ (Weighted Fair Queueing)



Packet	Arrival time	Length	Finish time	Output order
A	0	8	8	1
B	5	6	11	3
C	5	10	10	2
D	8	9	20	7
E	8	8	14	4
F	10	6	16	5
G	11	10	19	6
H	20	8	28	8

$$F_i = \max(A_i, F_{i-1}) + L_i/W$$

Finish virtual times determine transmission order

máximo tiempo de arribo y tiempo anterior

Admission Control (1)

Admission control takes a traffic flow specification and decides whether the network can carry it

- Sets up packet scheduling to meet QoS

Parameter	Unit
Token bucket rate	Bytes/sec
Token bucket size	Bytes
Peak data rate	Bytes/sec
Minimum packet size	Bytes
Maximum packet size	Bytes

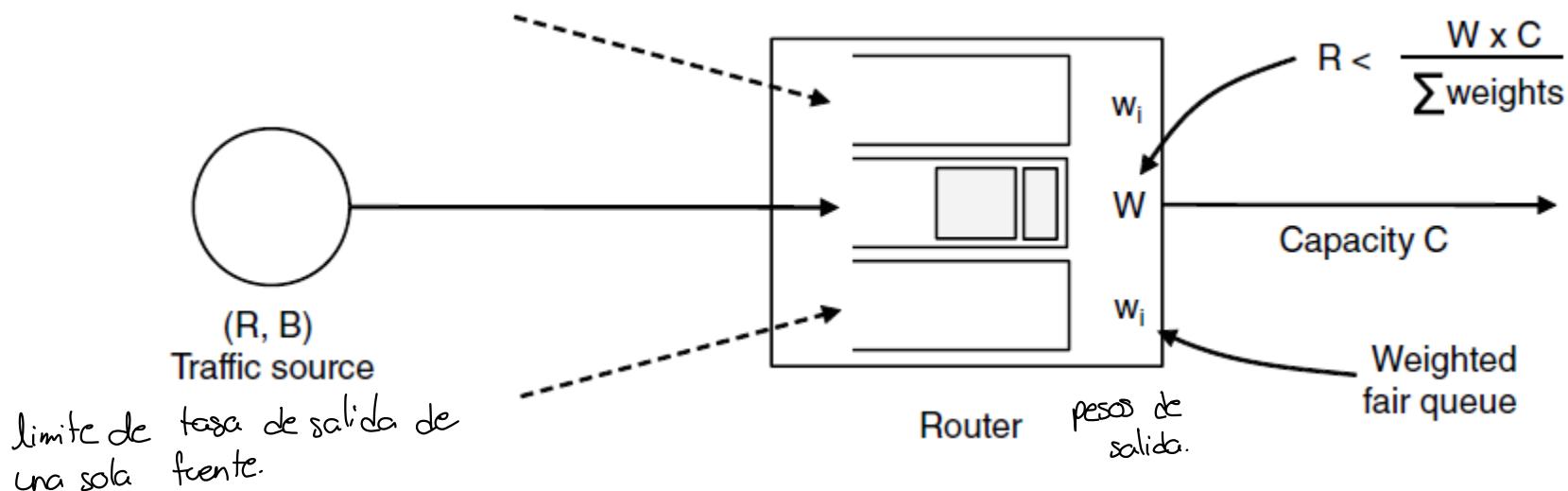
Example flow specification

Admission Control (2)

Cota máxima.

Construction to guarantee bandwidth B and delay D:

- Shape traffic source to a (R, B) token bucket
- Run WFQ with weight W / all weights $> R/\text{capacity}$
- Holds for all traffic patterns, all topologies



Integrated Services (1)

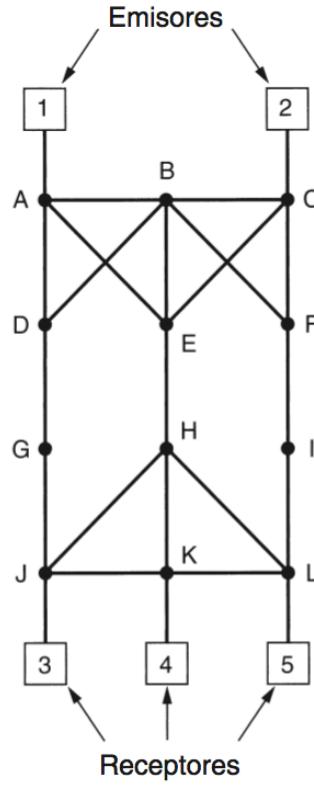
Design with QoS for each flow; handles multicast traffic.

Admission with RSVP (Resource reSerVation Protocol):

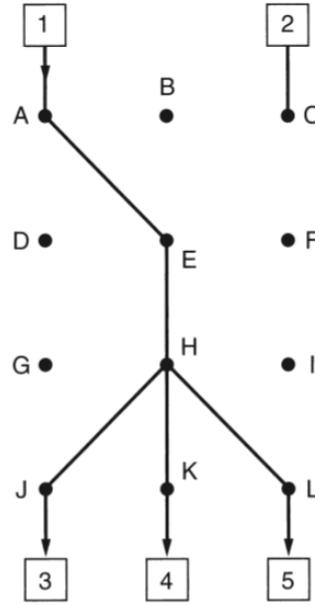
- Receiver sends a request back to the sender
- Each router along the way reserves resources
- Routers merge multiple requests for same flow
- Entire path is set up, or reservation not made

Difusión a gran número de usuarios

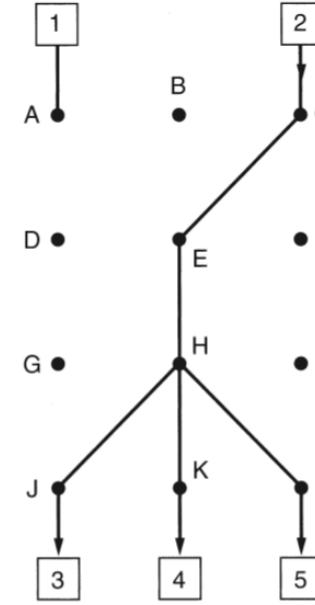
Integrated services. Multicast (Multidifusión)



(a)



(b)

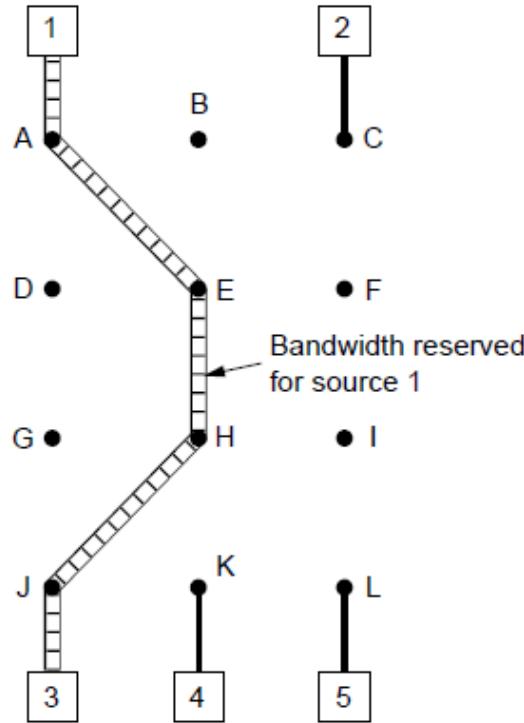


(c)

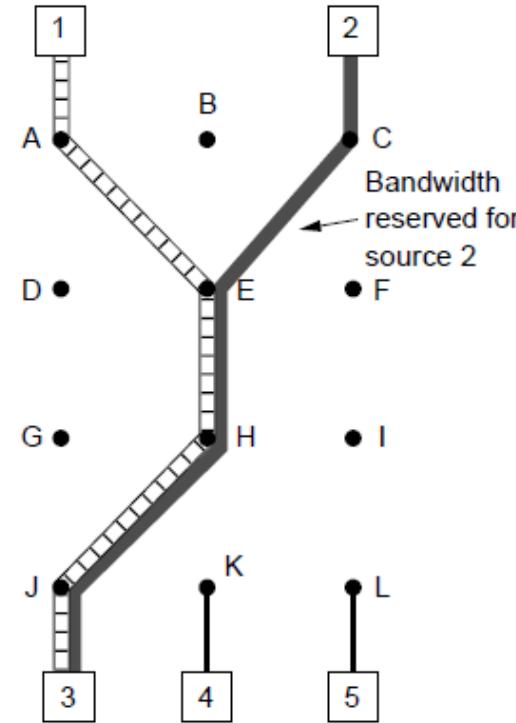
Figura 5-37. (a) Red. (b) Árbol de expansión de multidifusión para el *host* 1. (c) Árbol de expansión de multidifusión para el *host* 2.

Integrated Services (2)

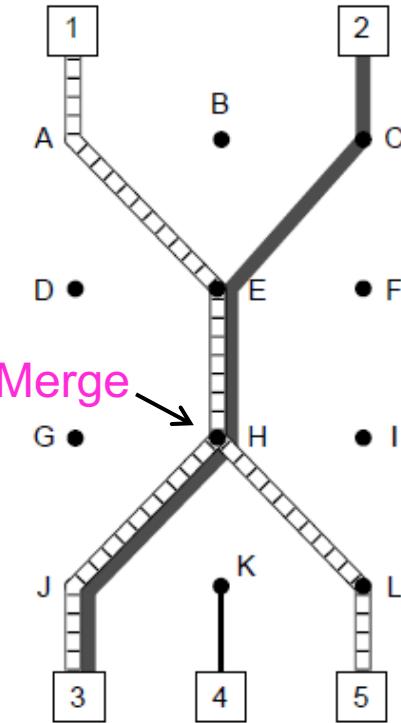
Reserva recursos de memoria y banda ancha.



R3 reserves flow
from S1



R3 reserves flow
from S2



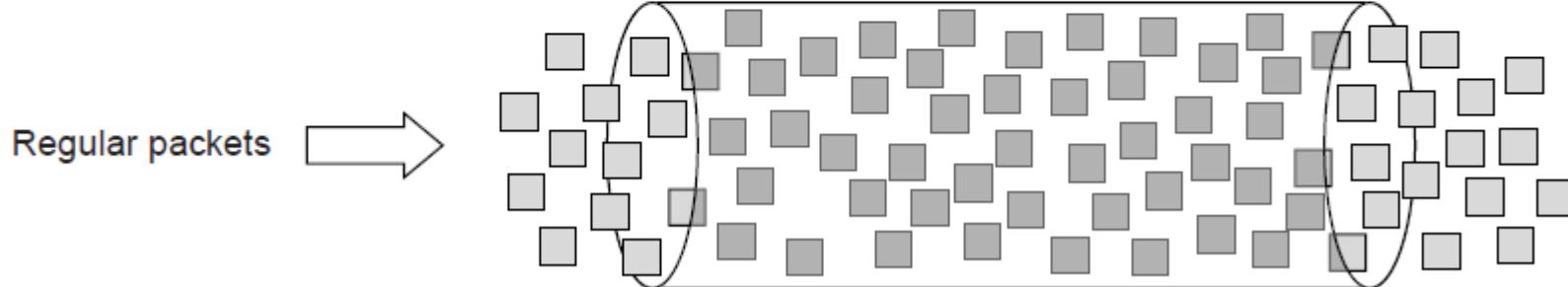
R5 reserves flow from S1;
merged with R3 at H

Differentiated Services (1)

Vídeo conferencia, difusión de películas. Red. Haciendo diferenciación de clases para servicios con calidad distinta. Capacidad de hacer selecciones de diferenciación de tráfico.
Redirigir banda ancha.

Design with classes of QoS; customers buy what they want

- Expedited class is sent in preference to regular class
- Less expedited traffic but better quality for applications

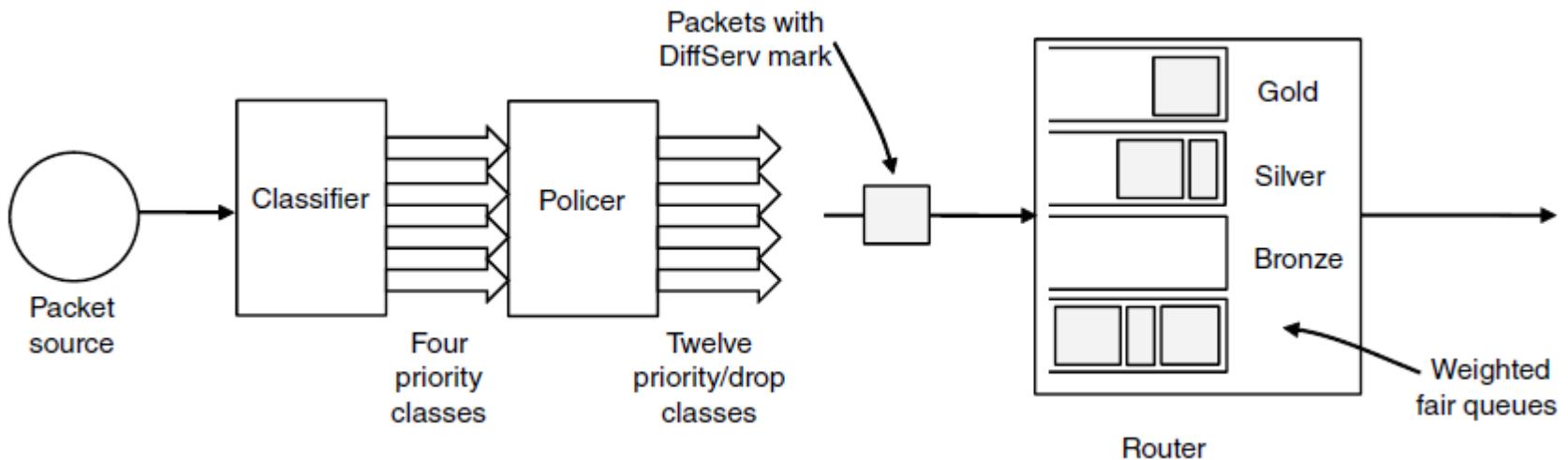


Differentiated Services (2)

Redes privadas que no utilizan el internet. Para dar la calidad del servicio. Optimización de la red.
Intercambian información en diferentes nodos
Depende de maestría de la red

Implementation of DiffServ:

- Customers mark desired class on packet
- ISP shapes traffic to ensure markings are paid for
- Routers use WFQ to give different service levels



Internetworking

Interc Conexión de redes. Protocolos circulando en cada parte de la red.
Estación base se comunica con otras hasta el destino final

Internetworking joins multiple, different networks into a single larger network

- How networks differ »
- How networks can be connected »
- Tunneling »
- Internetwork routing »
- Packet fragmentation »

How Networks Differ

Redes pueden ser diferentes

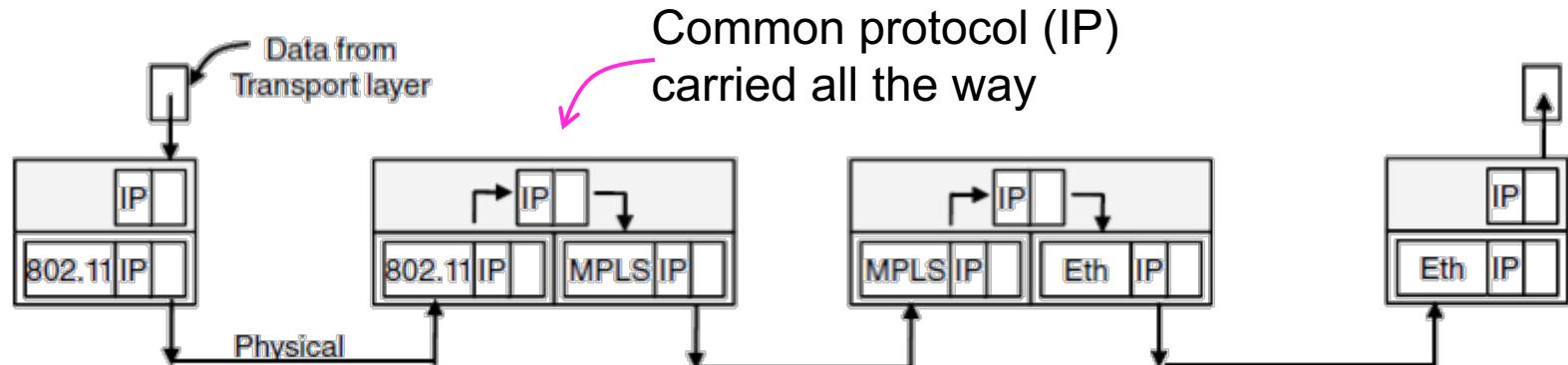
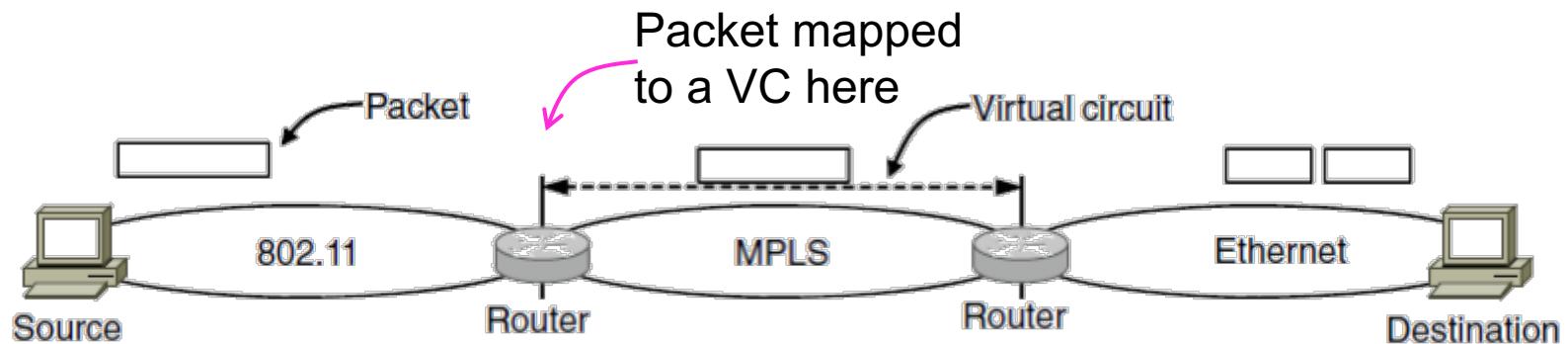
Differences can be large; complicates internetworking

Item	Some Possibilities
Service offered	Connectionless versus connection oriented
Addressing	Different sizes, flat or hierarchical
Broadcasting	Present or absent (also multicast)
Packet size	Every network has its own maximum
Ordering	Ordered and unordered delivery
Quality of service	Present or absent; many different kinds
Reliability	Different levels of loss
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, packet, byte, or not at all

How Networks Can Be Connected

No necesitamos abrir el paquete.

Internetworking based on a common network layer – IP

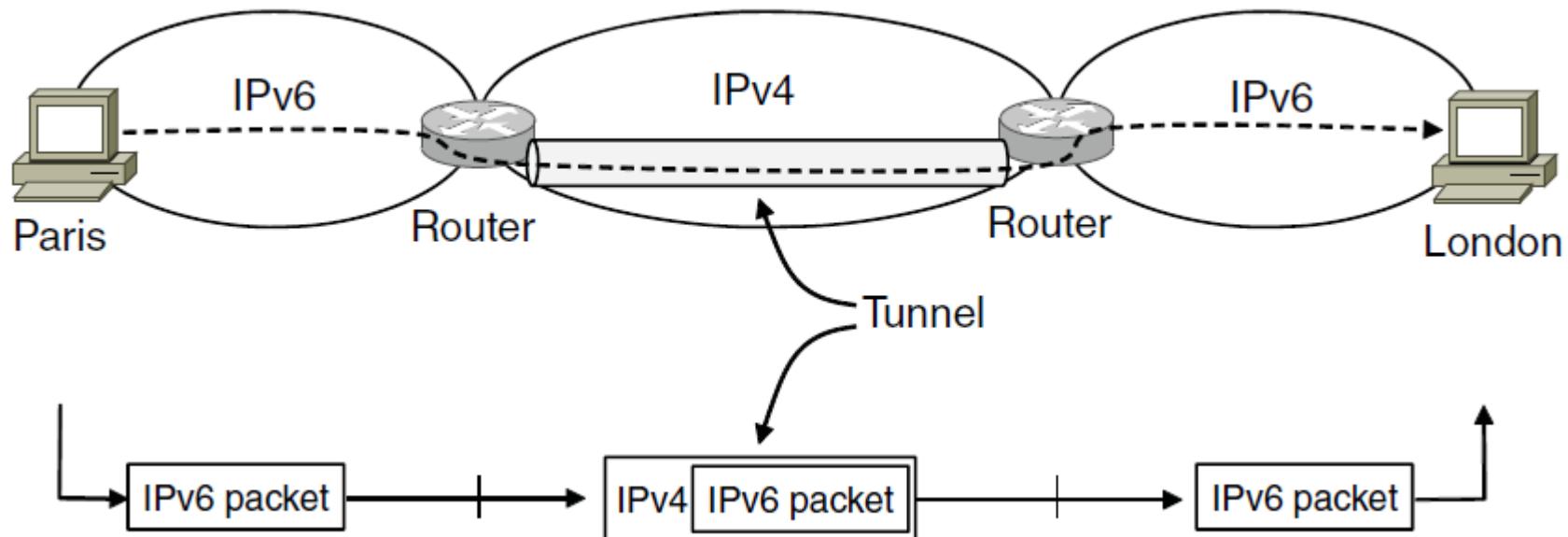


Tunneling (1)

2 tipos de redes en extremos mientras que la de en medio se comporta como transporte.

Connects two networks through a middle one

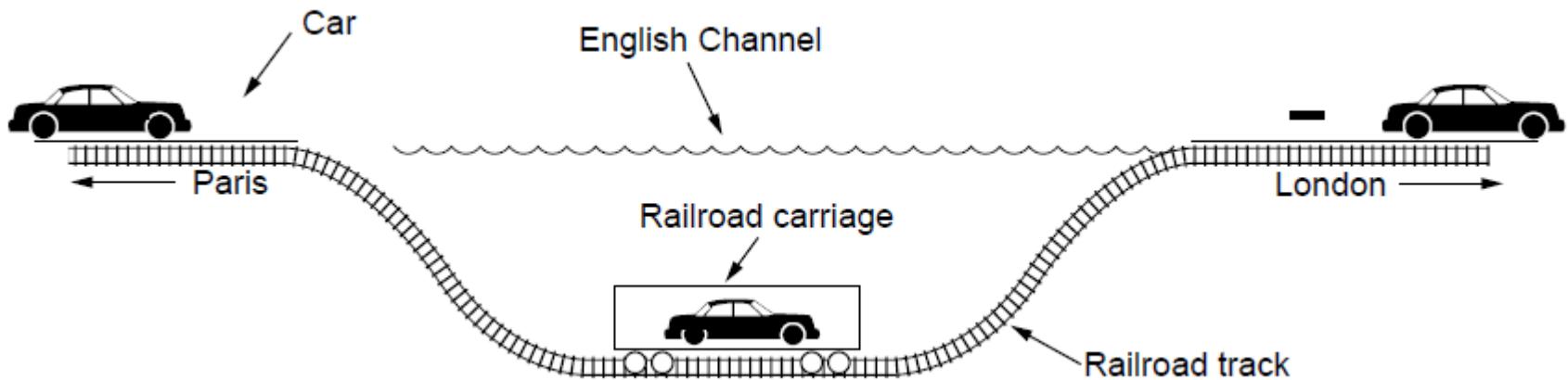
- Packets are encapsulated over the middle



Tunneling (2)

Tunneling analogy:

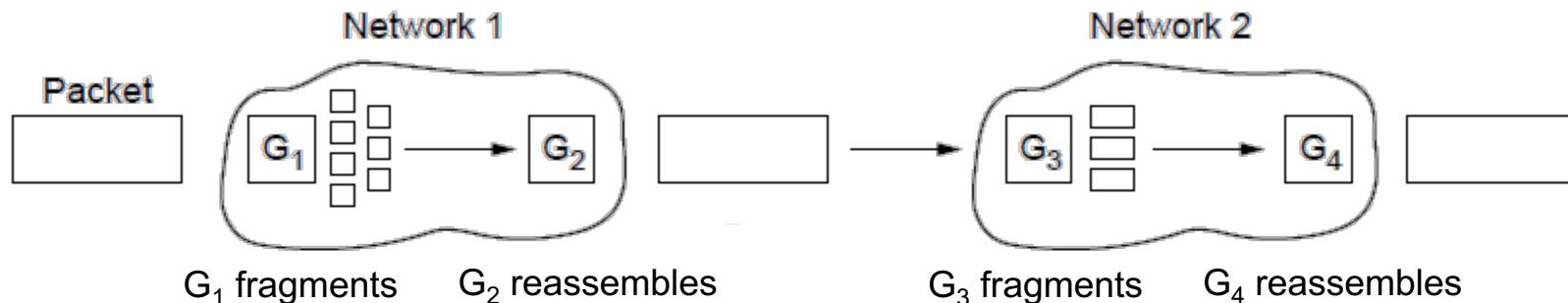
- tunnel is a link; packet can only enter/exit at ends



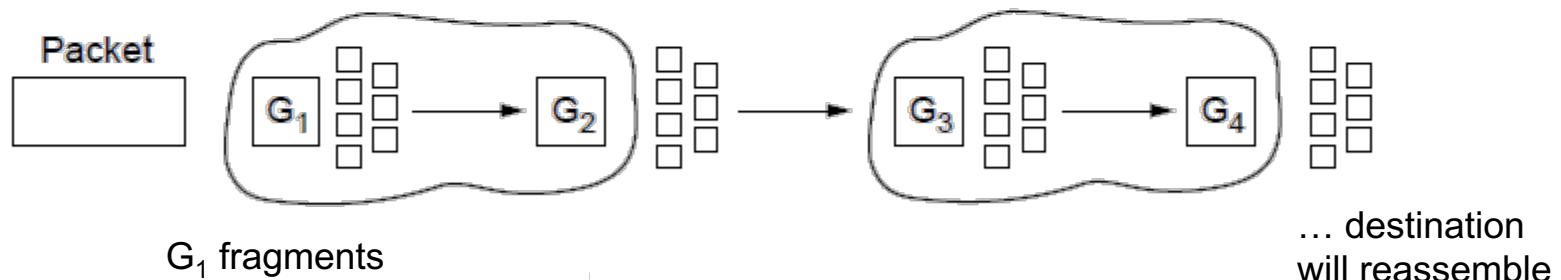
Packet Fragmentation (1)

Networks have different packet size limits for many reasons

- Large packets sent with fragmentation & reassembly



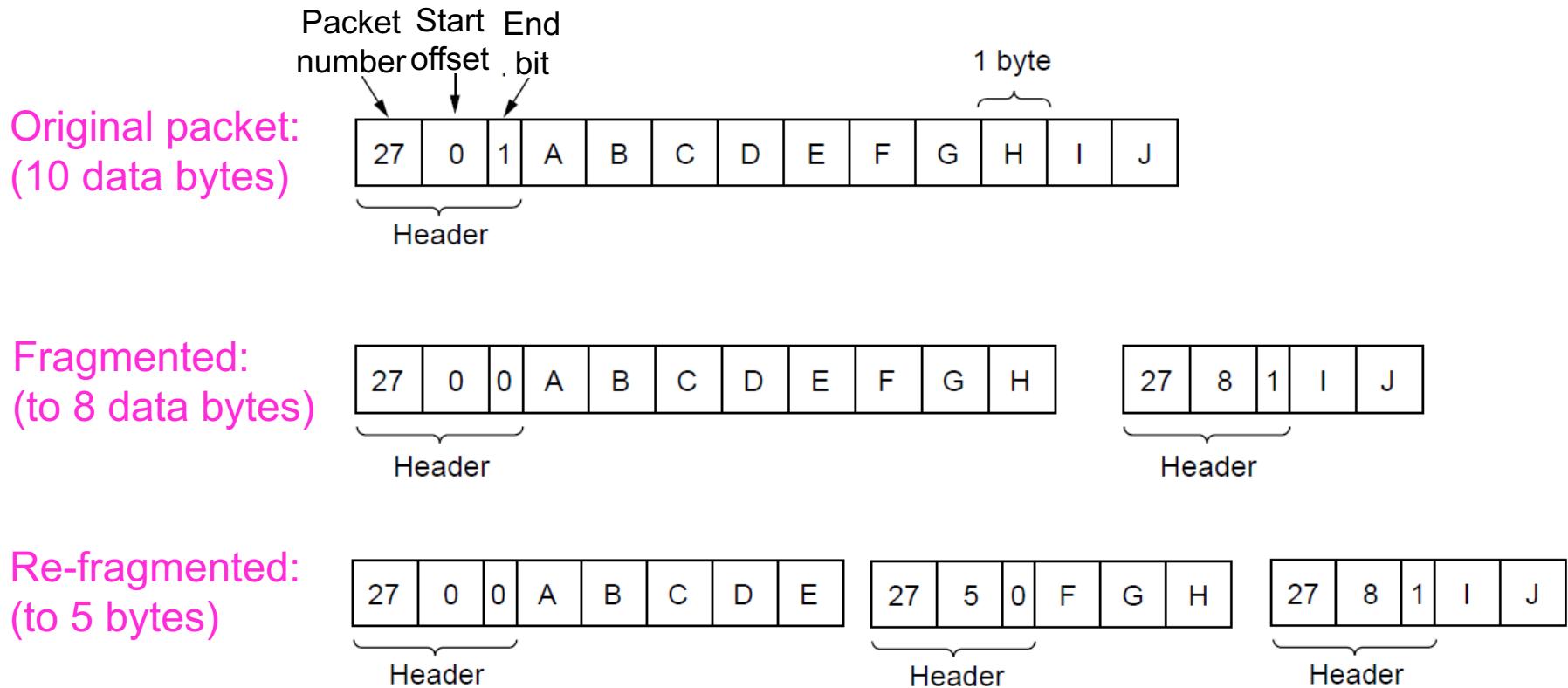
Transparent – packets fragmented / reassembled in each network



Non-transparent – fragments are reassembled at destination

Packet Fragmentation (2)

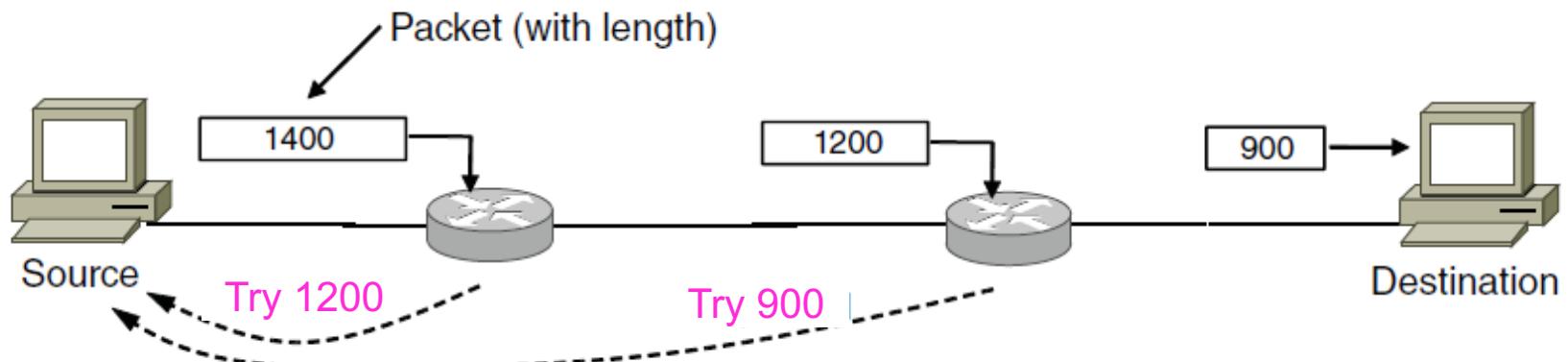
Example of IP-style fragmentation:



Packet Fragmentation (3)

Path MTU Discovery avoids network fragmentation

- Routers return MTU (Max. Transmission Unit) to source and discard large packets



Network Layer in the Internet (1)

- IP Version 4 »
- IP Addresses »
- IP Version 6 »
- Internet Control Protocols »
- Label Switching and MPLS »
- OSPF—An Interior Gateway Routing Protocol »
- BGP—The Exterior Gateway Routing Protocol »
- Internet Multicasting »
- Mobile IP »

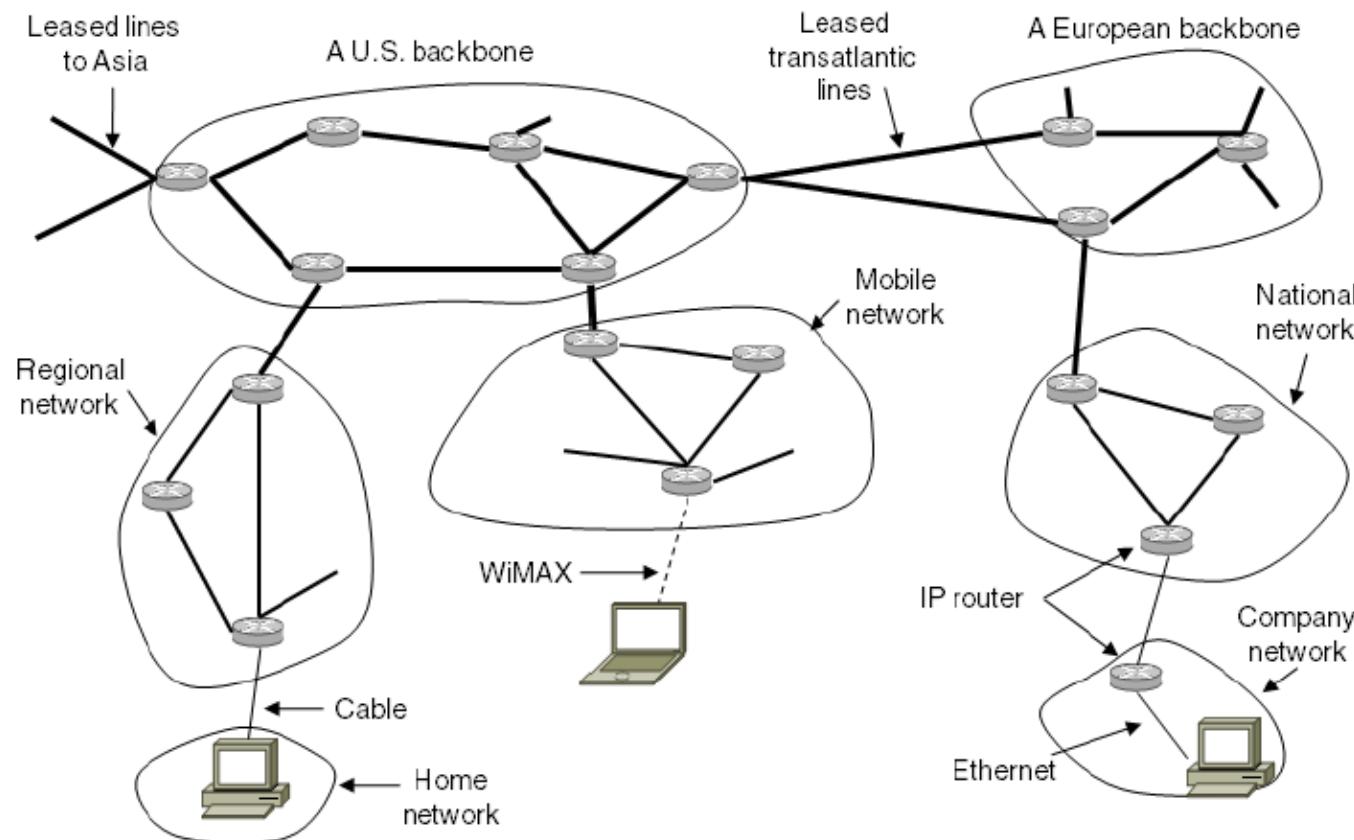
Network Layer in the Internet (2)

IP has been shaped by guiding principles:

- Make sure it works
- Keep it simple
- Make clear choices
- Exploit modularity
- Expect heterogeneity
- Avoid static options and parameters
- Look for good design (not perfect)
- Strict sending, tolerant receiving
- Think about scalability
- Consider performance and cost

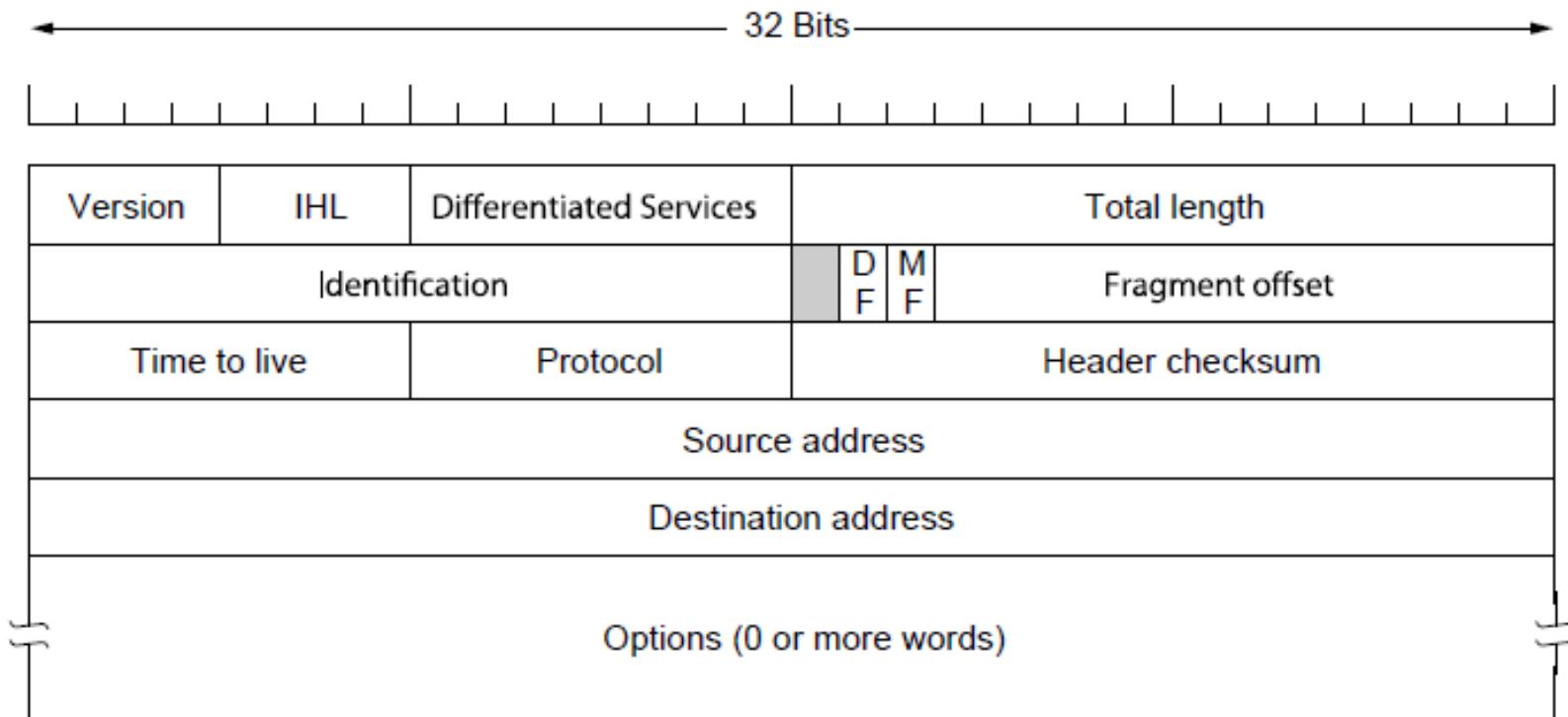
Network Layer in the Internet (3)

Internet is an interconnected collection of many networks that is held together by the IP protocol



IP Version 4 Protocol (1)

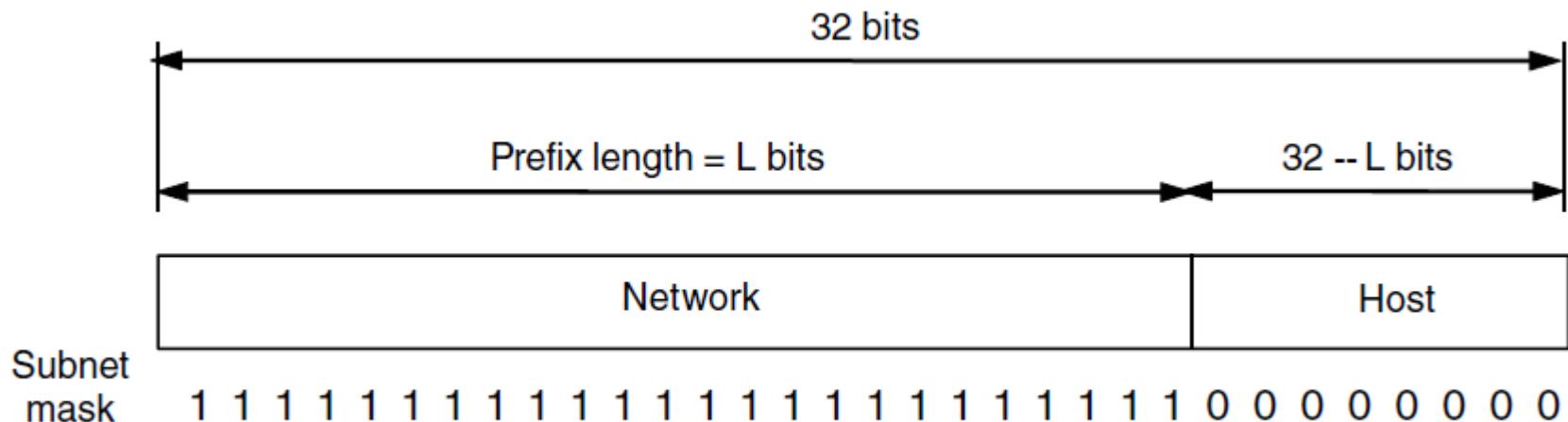
IPv4 (Internet Protocol) header is carried on all packets and has fields for the key parts of the protocol:



IP Addresses (1) – Prefixes

Addresses are allocated in blocks called prefixes

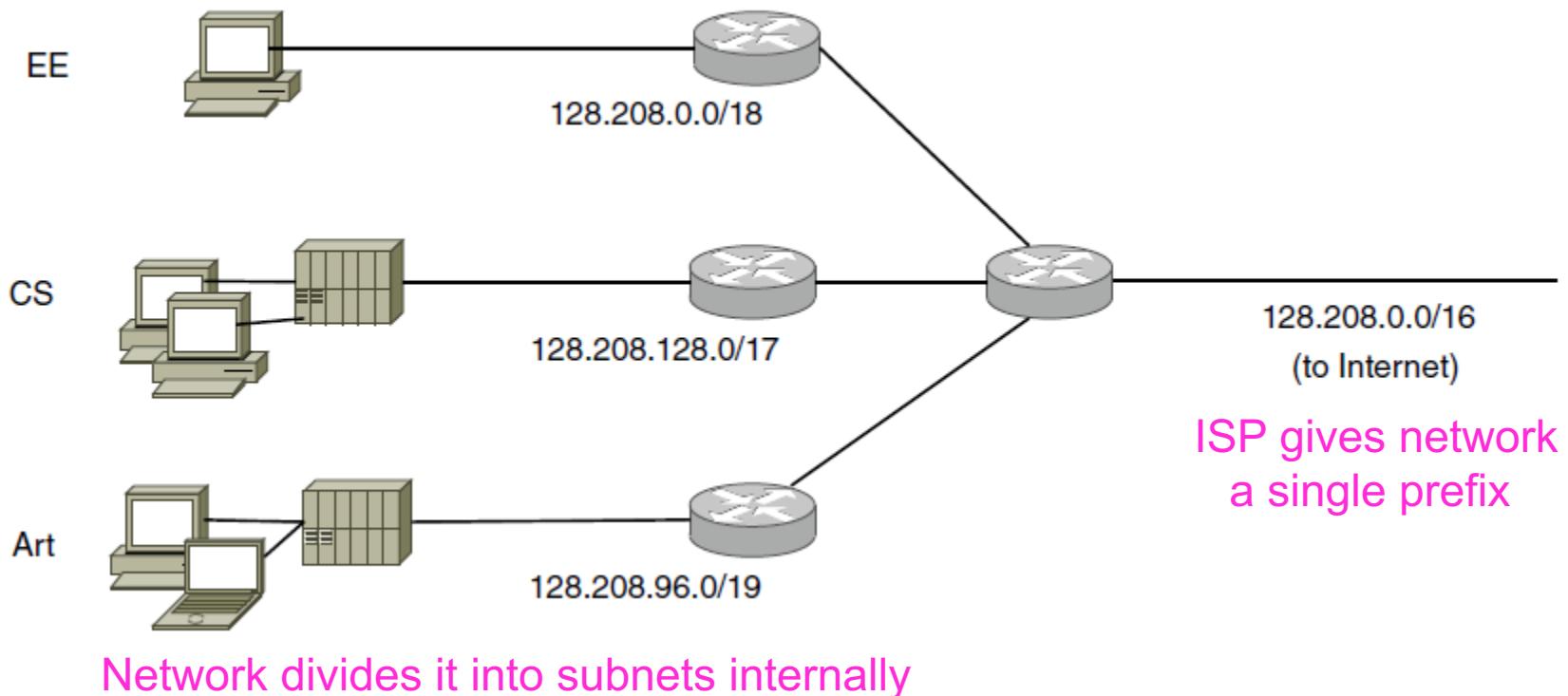
- Prefix is determined by the network portion
- AddressMask
- Written address/length, e.g., 18.0.31.0/24



IP Addresses (2) – Subnets

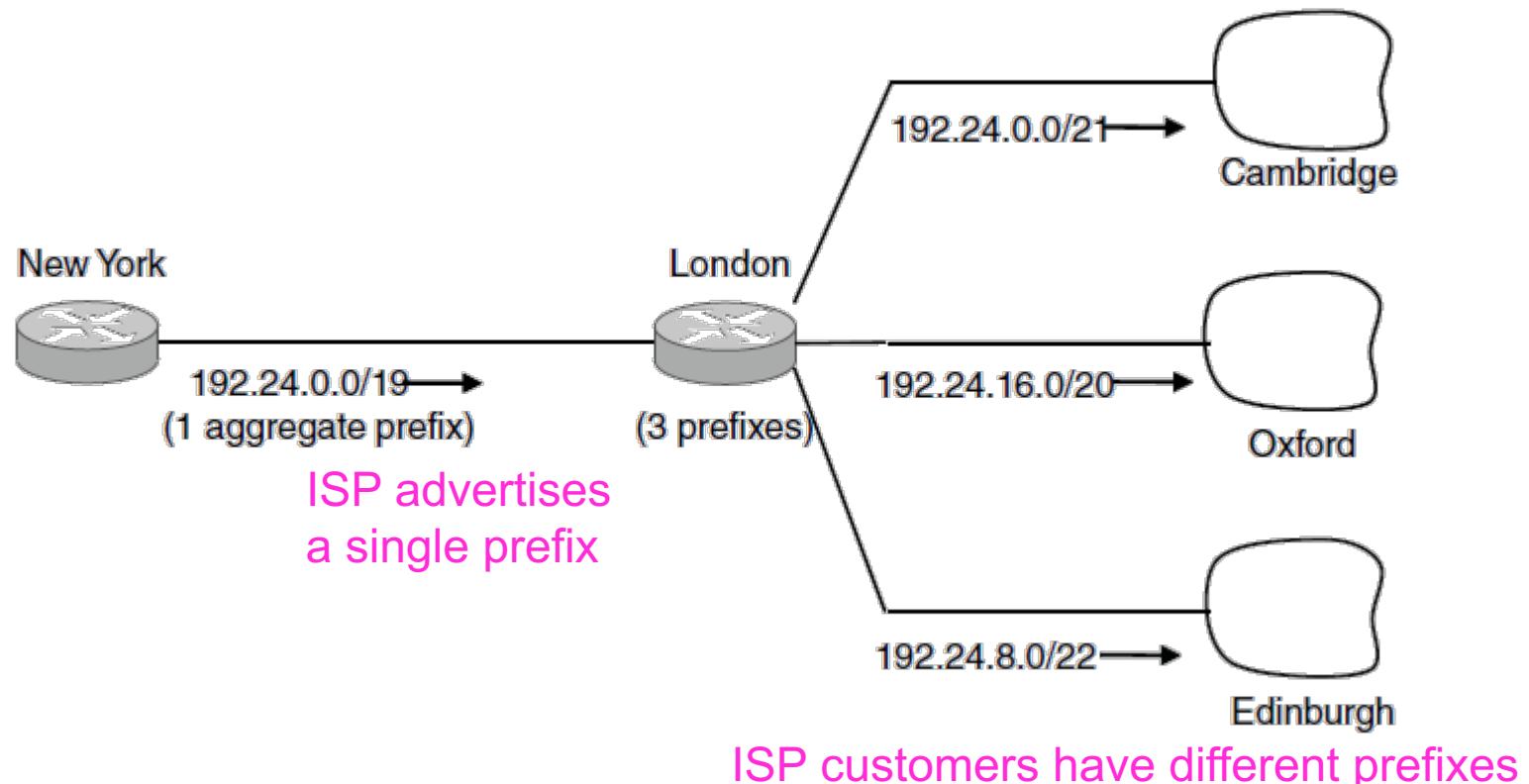
Subnetting splits up IP prefix to help with management

- Looks like a single prefix outside the network



IP Addresses (3) – Aggregation

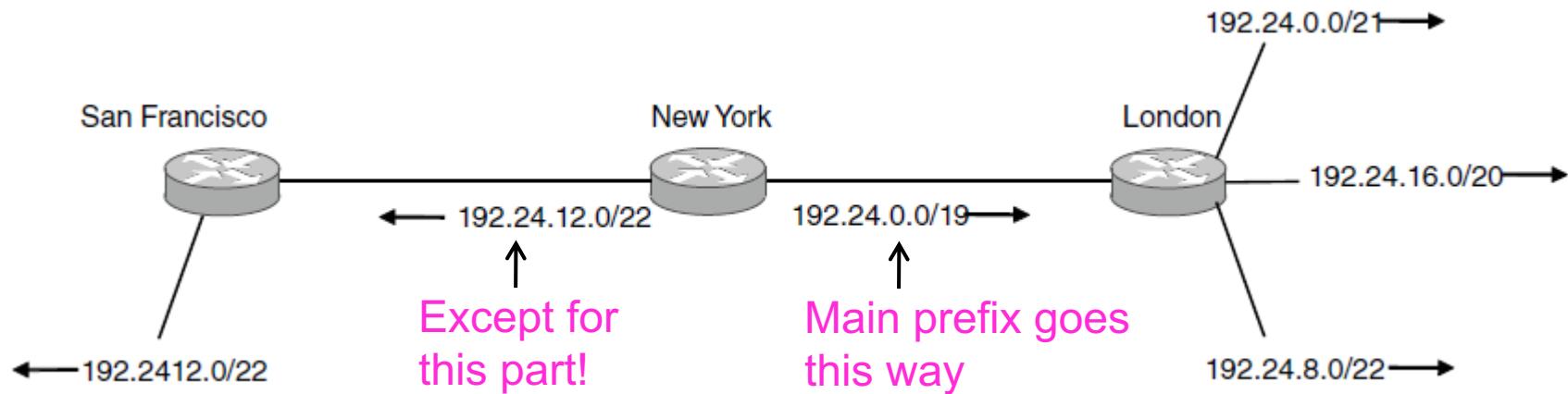
Aggregation joins multiple IP prefixes into a single larger prefix to reduce routing table size



IP Addresses (4) – Longest Matching Prefix

Packets are forwarded to the entry with the longest matching prefix or smallest address block

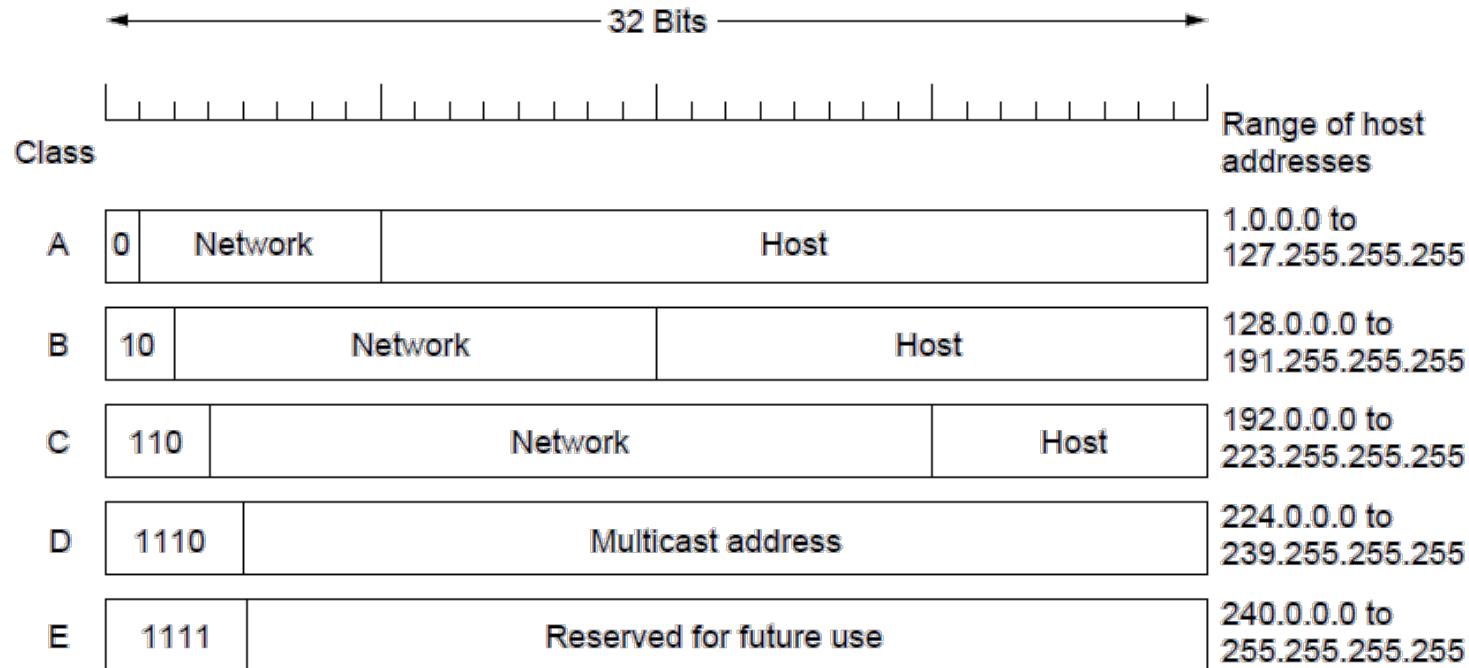
- Complicates forwarding but adds flexibility



IP Addresses (5) – Classful Addressing

Old addresses came in blocks of fixed size (A, B, C)

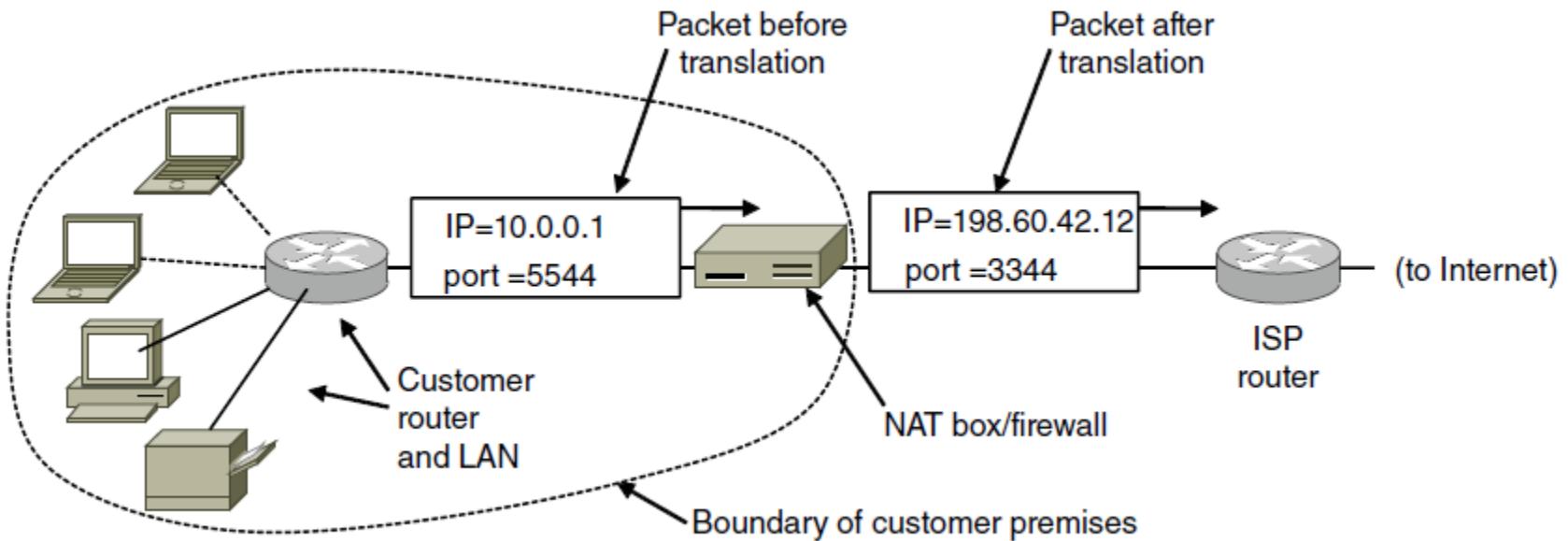
- Carries size as part of address, but lacks flexibility
- Called classful (vs. classless) addressing



IP Addresses (6) – NAT

NAT (Network Address Translation) box maps one external IP address to many internal IP addresses

- Uses TCP/UDP port to tell connections apart
- Violates layering; very common in homes, etc.



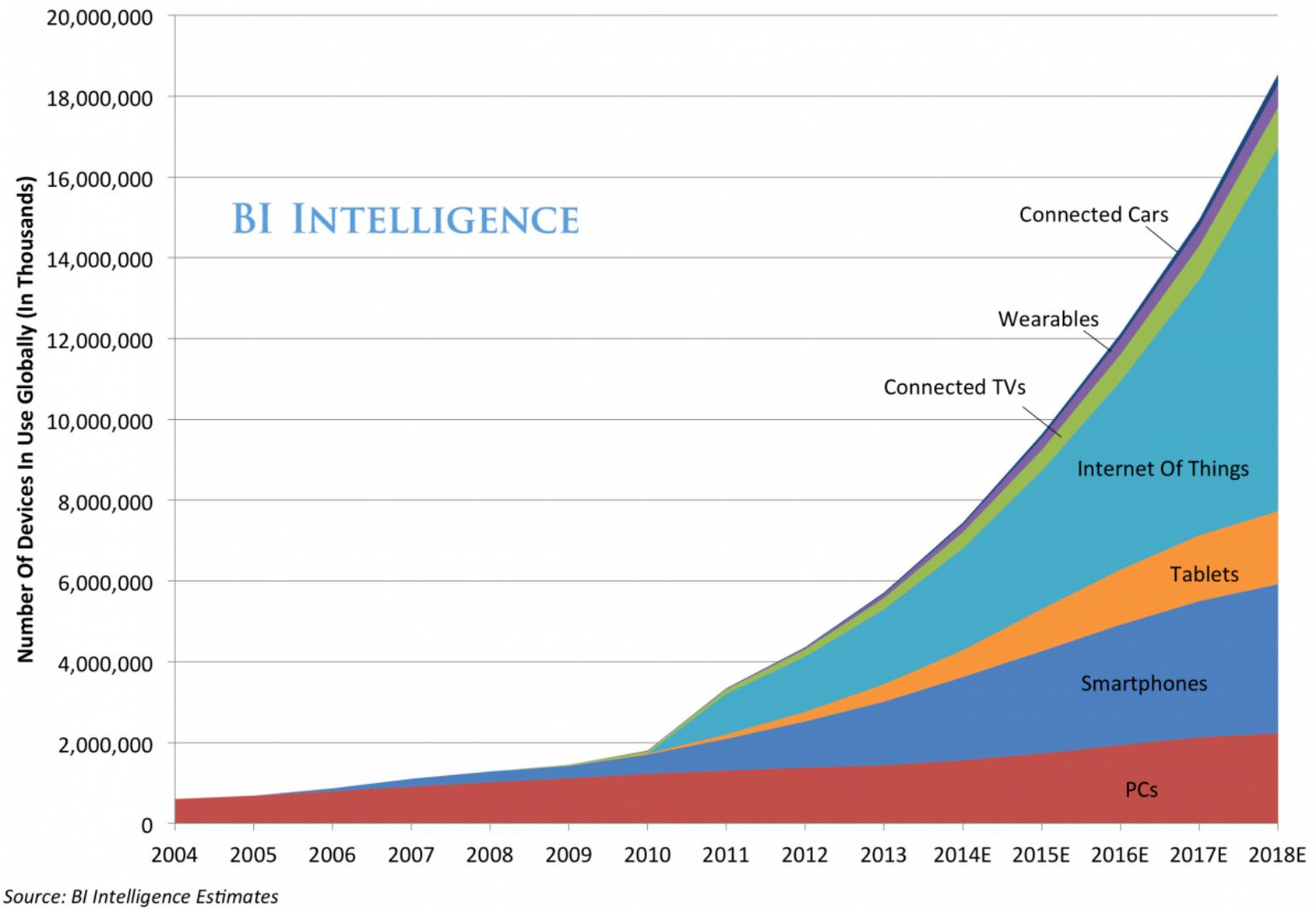
IP Version 6 (1)

Major upgrade in the 1990s due to impending address exhaustion, with various other goals:

- Support billions of hosts
- Reduce routing table size
- Simplify protocol
- Better security
- Attention to type of service
- Aid multicasting
- Roaming host without changing address
- Allow future protocol evolution
- Permit coexistence of old, new protocols, ...

Deployment has been slow & painful, but may pick up pace now that addresses are all but exhausted

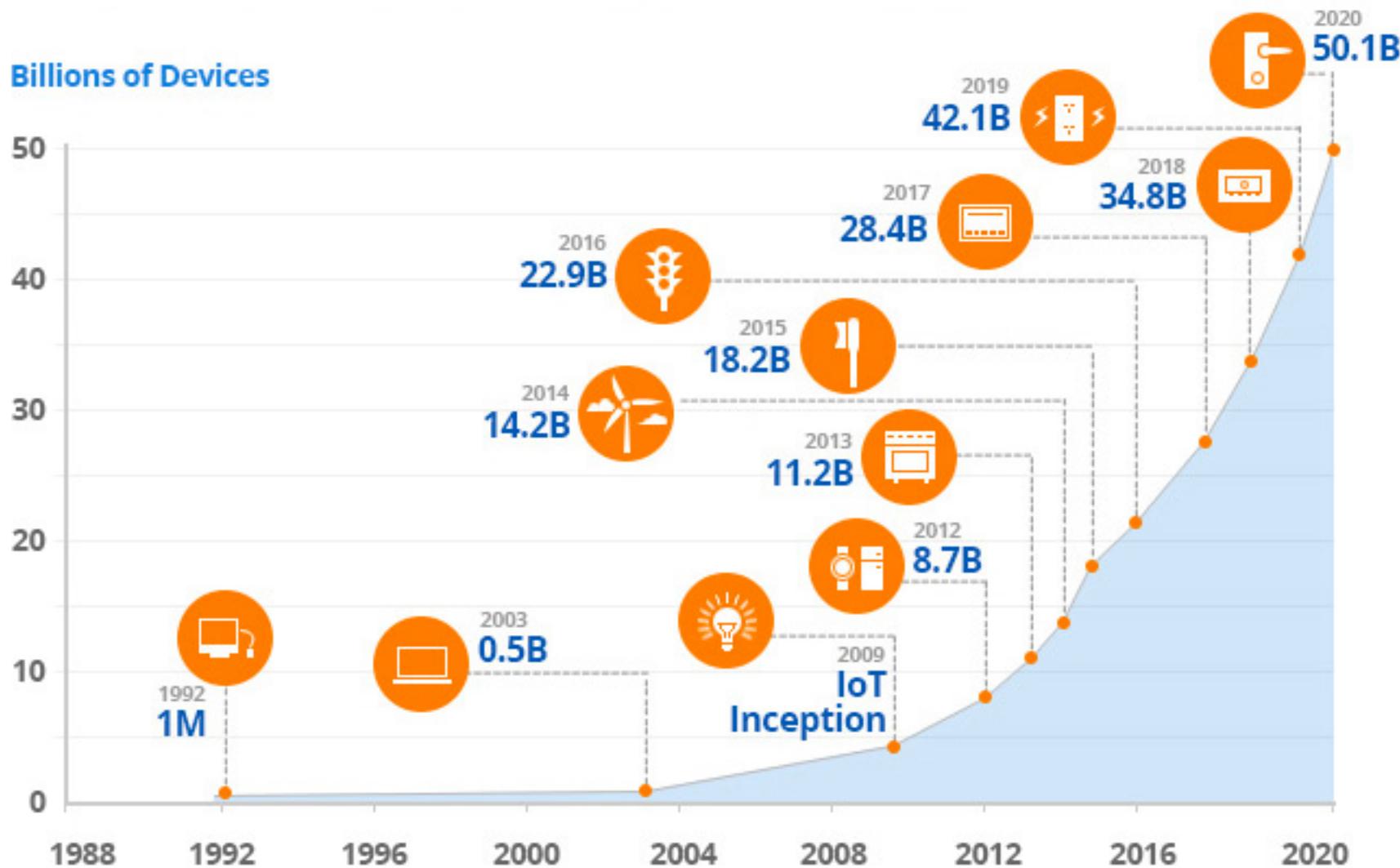
The Internet Of Everything



Growth in the internet of things

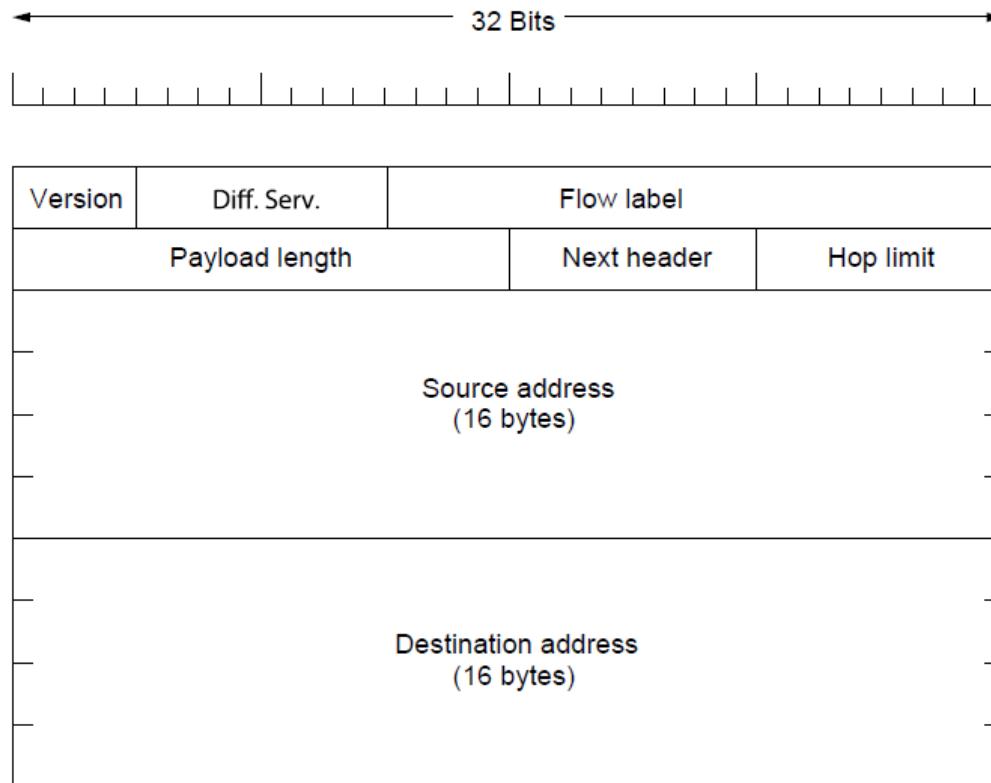
The number of connected devices will exceed 50 billion by 2020

Billions of Devices



IP Version 6 (2)

IPv6 protocol header has much longer addresses (128 vs. 32 bits) and is simpler (by using extension headers)



IP Version 6 (3)

IPv6 extension headers handles other functionality

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

Internet Control Protocols (1)

IP works with the help of several control protocols:

- ICMP is a companion to IP that returns error info
 - Required, and used in many ways, e.g., for traceroute
- ARP finds Ethernet address of a local IP address
 - Glue that is needed to send any IP packets
 - Host queries an address and the owner replies
- DHCP assigns a local IP address to a host
 - Gets host started by automatically configuring it
 - Host sends request to server, which grants a lease

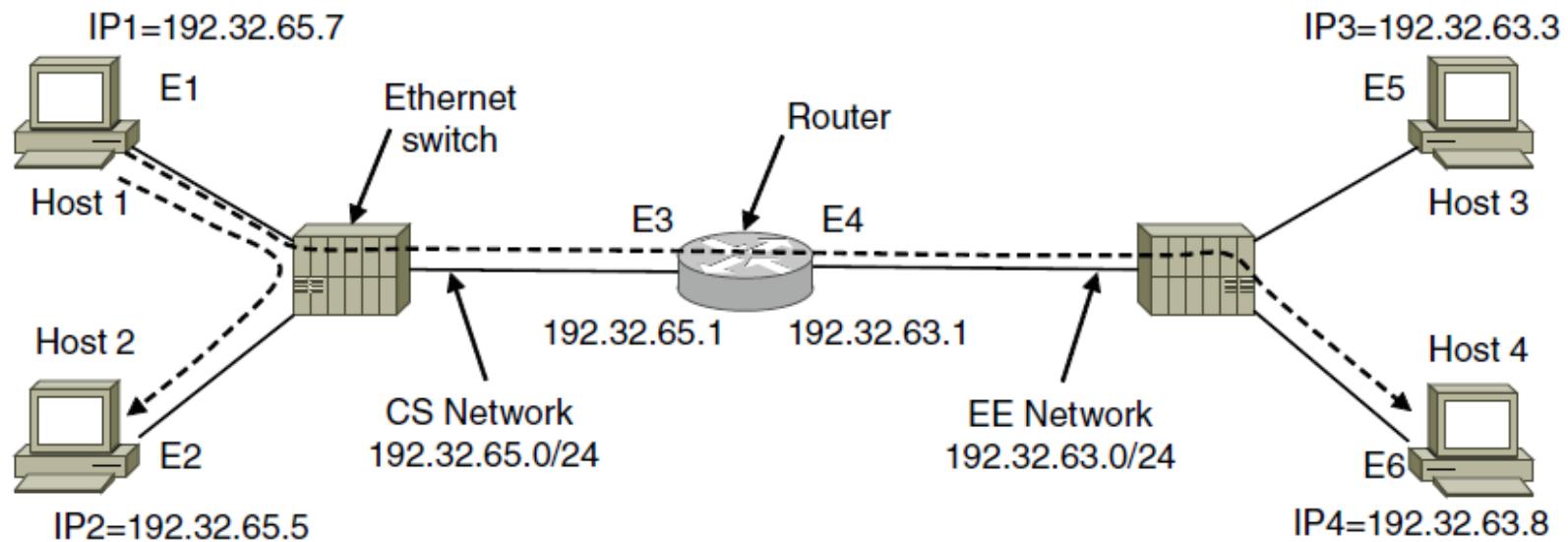
Internet Control Protocols (2)

Main ICMP (Internet Control Message Protocol) types:

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo and Echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with timestamp
Router advertisement/solicitation	Find a nearby router

Internet Control Protocols (3)

ARP (Address Resolution Protocol) lets nodes find target Ethernet addresses [pink] from their IP addresses

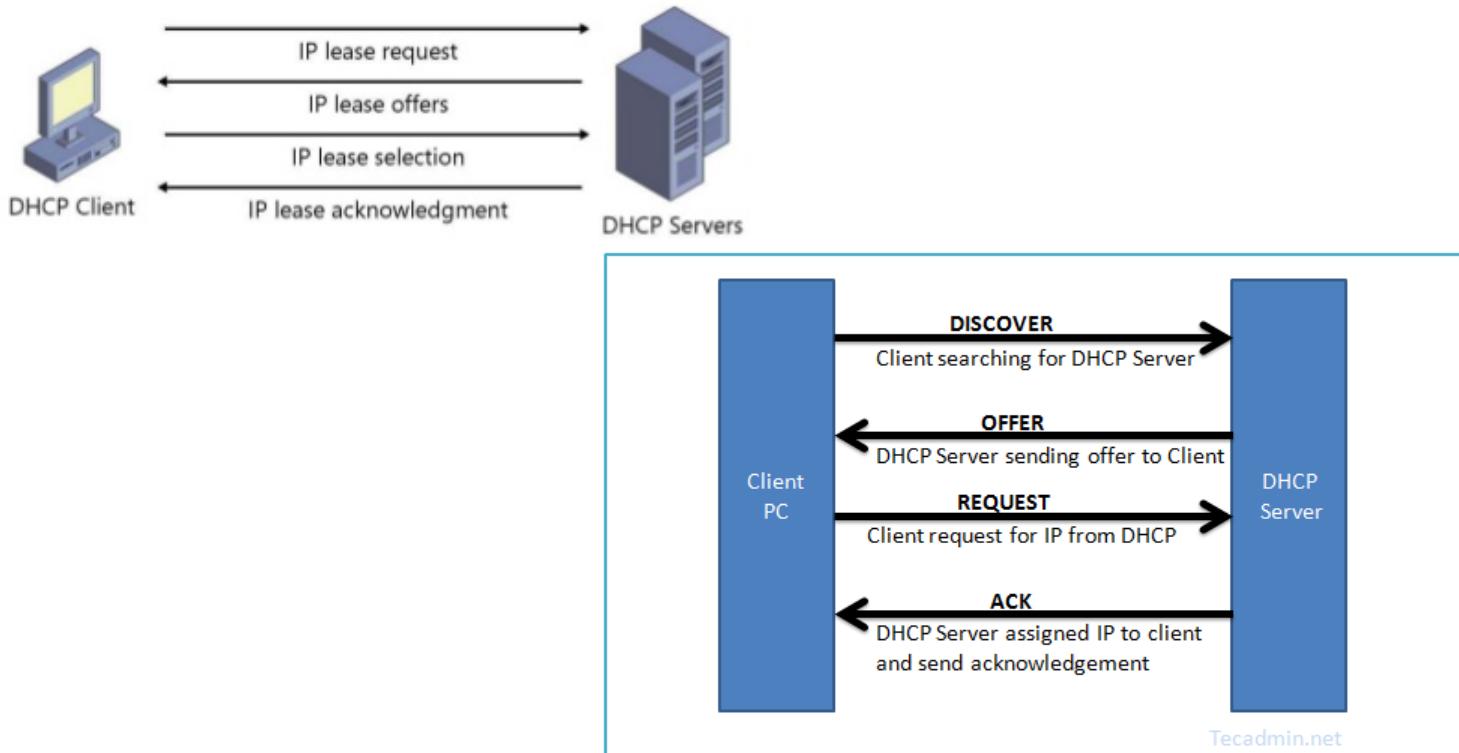


Frame	Source IP	Source Eth.	Destination IP	Destination Eth.
Host 1 to 2, on CS net	IP1	E1	IP2	E2
Host 1 to 4, on CS net	IP1	E1	IP4	E3
Host 1 to 4, on EE net	IP1	E4	IP4	E6

DHCP Server DHCP Client

The DHCP server provides the client with the following configuration information:

- IP address
- Subnet mask
- Default gateway



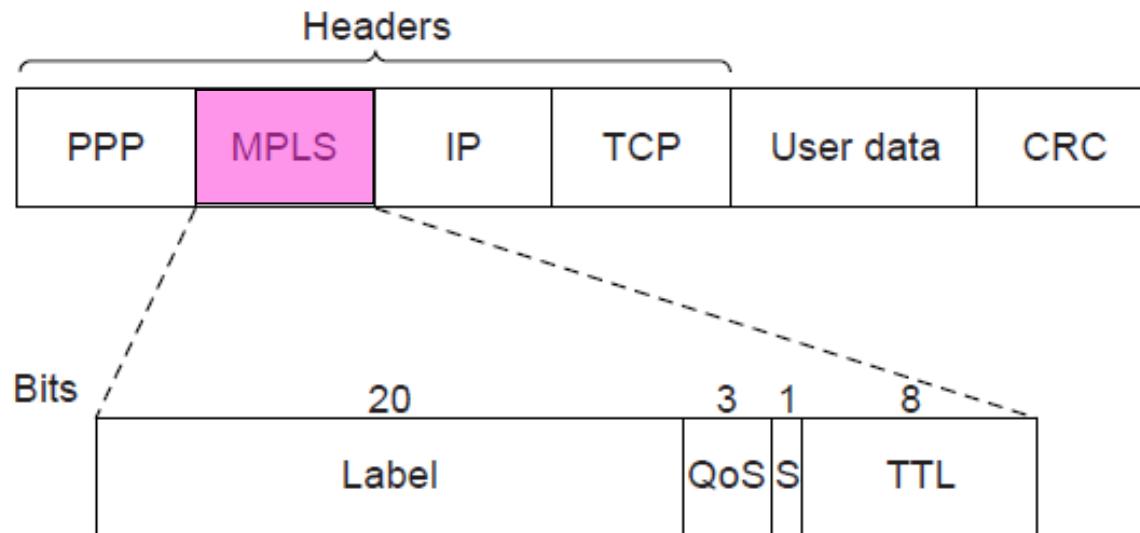


DIR-655 //	SETUP	ADVANCED	TOOLS	STATUS	HELP																																																																																		
INTERNET WIRELESS SETTINGS NETWORK SETTINGS USB SETTINGS	<div style="border: 1px solid orange; padding: 5px;"> <p>NETWORK SETTINGS</p> <p>Use this section to configure the internal network settings of your router and also to configure the built-in DHCP Server to assign IP addresses to the computers on your network. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.</p> <p><input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/></p> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>ROUTER SETTINGS</p> <p>Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.</p> <table border="0"> <tr> <td>Router IP Address :</td> <td><input type="text" value="192.168.0.1"/></td> </tr> <tr> <td>Subnet Mask :</td> <td><input type="text" value="255.255.255.0"/></td> </tr> <tr> <td>Device Name :</td> <td><input type="text" value="dlinkrouter"/></td> </tr> <tr> <td>Local Domain Name :</td> <td><input type="text"/></td> </tr> <tr> <td>Enable DNS Relay :</td> <td><input checked="" type="checkbox"/></td> </tr> </table> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>DHCP SERVER SETTINGS</p> <p>Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.</p> <table border="0"> <tr> <td>Enable DHCP Server :</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>DHCP IP Address Range :</td> <td><input type="text" value="192.168.0.100"/> to <input type="text" value="192.168.0.199"/></td> </tr> <tr> <td>DHCP Lease Time :</td> <td><input type="text" value="10080"/> (minutes)</td> </tr> <tr> <td>Always broadcast :</td> <td><input checked="" type="checkbox"/> (compatibility for some DHCP Clients)</td> </tr> <tr> <td>NetBIOS announcement :</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Learn NetBIOS from WAN :</td> <td><input type="checkbox"/></td> </tr> <tr> <td>NetBIOS Scope :</td> <td><input type="text"/> (optional)</td> </tr> <tr> <td>NetBIOS node type :</td> <td> <input type="radio"/> Broadcast only (use when no WINS servers configured) <input type="radio"/> Point-to-Point (no broadcast) <input checked="" type="radio"/> Mixed-mode (Broadcast then Point-to-Point) <input type="radio"/> Hybrid (Point-to-Point then Broadcast) </td> </tr> <tr> <td>Primary WINS IP Address :</td> <td><input type="text"/></td> </tr> <tr> <td>Secondary WINS IP Address :</td> <td><input type="text"/></td> </tr> </table> </div> <div style="border: 2px solid red; padding: 5px; margin-top: 10px;"> <p>ADD DHCP RESERVATION</p> <table border="0"> <tr> <td>Enable :</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Computer Name :</td> <td><input type="text"/> << <input type="button" value="Computer Name"/></td> </tr> <tr> <td>IP Address :</td> <td><input type="text"/></td> </tr> <tr> <td>MAC Address :</td> <td><input type="text"/></td> </tr> <tr> <td colspan="2"><input type="button" value="Copy Your PC's MAC Address"/></td> </tr> <tr> <td><input type="button" value="Save"/></td> <td><input type="button" value="Clear"/></td> </tr> </table> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>DHCP RESERVATIONS LIST :</p> <table border="1"> <thead> <tr> <th>Enable</th> <th>Host Name</th> <th>MAC Address</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NUMBER OF DYNAMIC DHCP CLIENTS : 4</p> <table border="1"> <thead> <tr> <th>Hardware Address</th> <th>Assigned IP</th> <th>Hostname</th> <th>Expires</th> </tr> </thead> <tbody> <tr> <td>48:5b:39:d9:05:b8</td> <td>192.168.0.100</td> <td>[REDACTED]</td> <td>Fri Jun 4 12:15:54 2010 Revoke Reserve</td> </tr> <tr> <td>00:22:fb:afa4:76</td> <td>192.168.0.102</td> <td>[REDACTED]</td> <td>Fri Jun 4 11:00:53 2010 Revoke Reserve</td> </tr> <tr> <td>f0:1c:13:64:88:99</td> <td>192.168.0.105</td> <td>[REDACTED]</td> <td>Thu Jun 3 23:08:00 2010 Revoke Reserve</td> </tr> <tr> <td>f0:4f:7c:8b:fb:c2</td> <td>192.168.0.106</td> <td>[REDACTED]</td> <td>Fri Jun 4 11:31:47 2010 Revoke Reserve</td> </tr> </tbody> </table> </div>					Router IP Address :	<input type="text" value="192.168.0.1"/>	Subnet Mask :	<input type="text" value="255.255.255.0"/>	Device Name :	<input type="text" value="dlinkrouter"/>	Local Domain Name :	<input type="text"/>	Enable DNS Relay :	<input checked="" type="checkbox"/>	Enable DHCP Server :	<input checked="" type="checkbox"/>	DHCP IP Address Range :	<input type="text" value="192.168.0.100"/> to <input type="text" value="192.168.0.199"/>	DHCP Lease Time :	<input type="text" value="10080"/> (minutes)	Always broadcast :	<input checked="" type="checkbox"/> (compatibility for some DHCP Clients)	NetBIOS announcement :	<input type="checkbox"/>	Learn NetBIOS from WAN :	<input type="checkbox"/>	NetBIOS Scope :	<input type="text"/> (optional)	NetBIOS node type :	<input type="radio"/> Broadcast only (use when no WINS servers configured) <input type="radio"/> Point-to-Point (no broadcast) <input checked="" type="radio"/> Mixed-mode (Broadcast then Point-to-Point) <input type="radio"/> Hybrid (Point-to-Point then Broadcast)	Primary WINS IP Address :	<input type="text"/>	Secondary WINS IP Address :	<input type="text"/>	Enable :	<input type="checkbox"/>	Computer Name :	<input type="text"/> << <input type="button" value="Computer Name"/>	IP Address :	<input type="text"/>	MAC Address :	<input type="text"/>	<input type="button" value="Copy Your PC's MAC Address"/>		<input type="button" value="Save"/>	<input type="button" value="Clear"/>	Enable	Host Name	MAC Address	IP Address	<input type="checkbox"/>				Hardware Address	Assigned IP	Hostname	Expires	48:5b:39:d9:05:b8	192.168.0.100	[REDACTED]	Fri Jun 4 12:15:54 2010 Revoke Reserve	00:22:fb:afa4:76	192.168.0.102	[REDACTED]	Fri Jun 4 11:00:53 2010 Revoke Reserve	f0:1c:13:64:88:99	192.168.0.105	[REDACTED]	Thu Jun 3 23:08:00 2010 Revoke Reserve	f0:4f:7c:8b:fb:c2	192.168.0.106	[REDACTED]	Fri Jun 4 11:31:47 2010 Revoke Reserve												
Router IP Address :	<input type="text" value="192.168.0.1"/>																																																																																						
Subnet Mask :	<input type="text" value="255.255.255.0"/>																																																																																						
Device Name :	<input type="text" value="dlinkrouter"/>																																																																																						
Local Domain Name :	<input type="text"/>																																																																																						
Enable DNS Relay :	<input checked="" type="checkbox"/>																																																																																						
Enable DHCP Server :	<input checked="" type="checkbox"/>																																																																																						
DHCP IP Address Range :	<input type="text" value="192.168.0.100"/> to <input type="text" value="192.168.0.199"/>																																																																																						
DHCP Lease Time :	<input type="text" value="10080"/> (minutes)																																																																																						
Always broadcast :	<input checked="" type="checkbox"/> (compatibility for some DHCP Clients)																																																																																						
NetBIOS announcement :	<input type="checkbox"/>																																																																																						
Learn NetBIOS from WAN :	<input type="checkbox"/>																																																																																						
NetBIOS Scope :	<input type="text"/> (optional)																																																																																						
NetBIOS node type :	<input type="radio"/> Broadcast only (use when no WINS servers configured) <input type="radio"/> Point-to-Point (no broadcast) <input checked="" type="radio"/> Mixed-mode (Broadcast then Point-to-Point) <input type="radio"/> Hybrid (Point-to-Point then Broadcast)																																																																																						
Primary WINS IP Address :	<input type="text"/>																																																																																						
Secondary WINS IP Address :	<input type="text"/>																																																																																						
Enable :	<input type="checkbox"/>																																																																																						
Computer Name :	<input type="text"/> << <input type="button" value="Computer Name"/>																																																																																						
IP Address :	<input type="text"/>																																																																																						
MAC Address :	<input type="text"/>																																																																																						
<input type="button" value="Copy Your PC's MAC Address"/>																																																																																							
<input type="button" value="Save"/>	<input type="button" value="Clear"/>																																																																																						
Enable	Host Name	MAC Address	IP Address																																																																																				
<input type="checkbox"/>																																																																																							
<input type="checkbox"/>																																																																																							
<input type="checkbox"/>																																																																																							
<input type="checkbox"/>																																																																																							
Hardware Address	Assigned IP	Hostname	Expires																																																																																				
48:5b:39:d9:05:b8	192.168.0.100	[REDACTED]	Fri Jun 4 12:15:54 2010 Revoke Reserve																																																																																				
00:22:fb:afa4:76	192.168.0.102	[REDACTED]	Fri Jun 4 11:00:53 2010 Revoke Reserve																																																																																				
f0:1c:13:64:88:99	192.168.0.105	[REDACTED]	Thu Jun 3 23:08:00 2010 Revoke Reserve																																																																																				
f0:4f:7c:8b:fb:c2	192.168.0.106	[REDACTED]	Fri Jun 4 11:31:47 2010 Revoke Reserve																																																																																				

Label Switching and MPLS (1)

MPLS (Multi-Protocol Label Switching) sends packets along established paths; ISPs can use for QoS

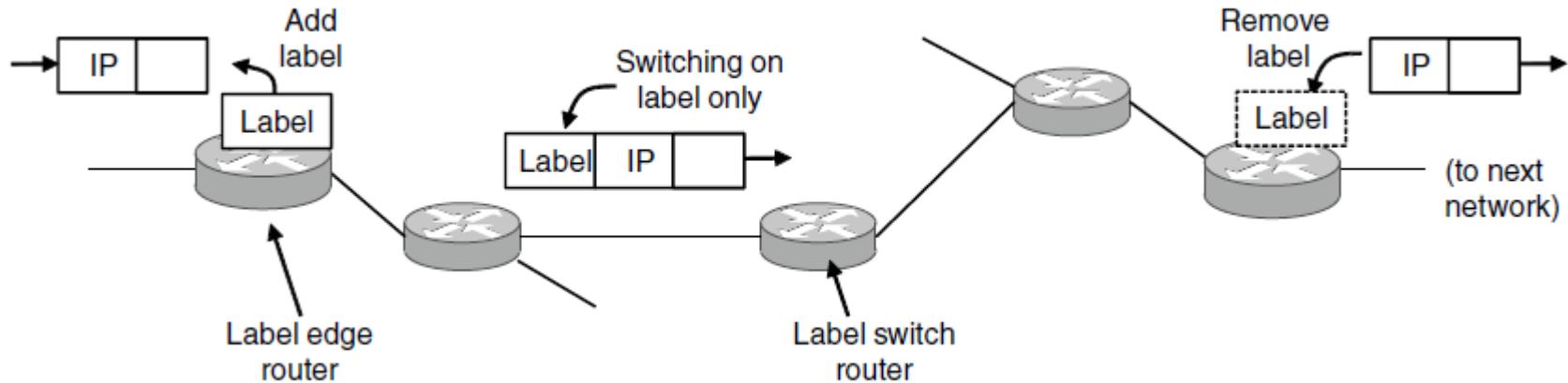
- Path indicated with label below the IP layer



Label Switching and MPLS (2)

Label added based on IP address on entering an MPLS network (e.g., ISP) and removed when leaving it

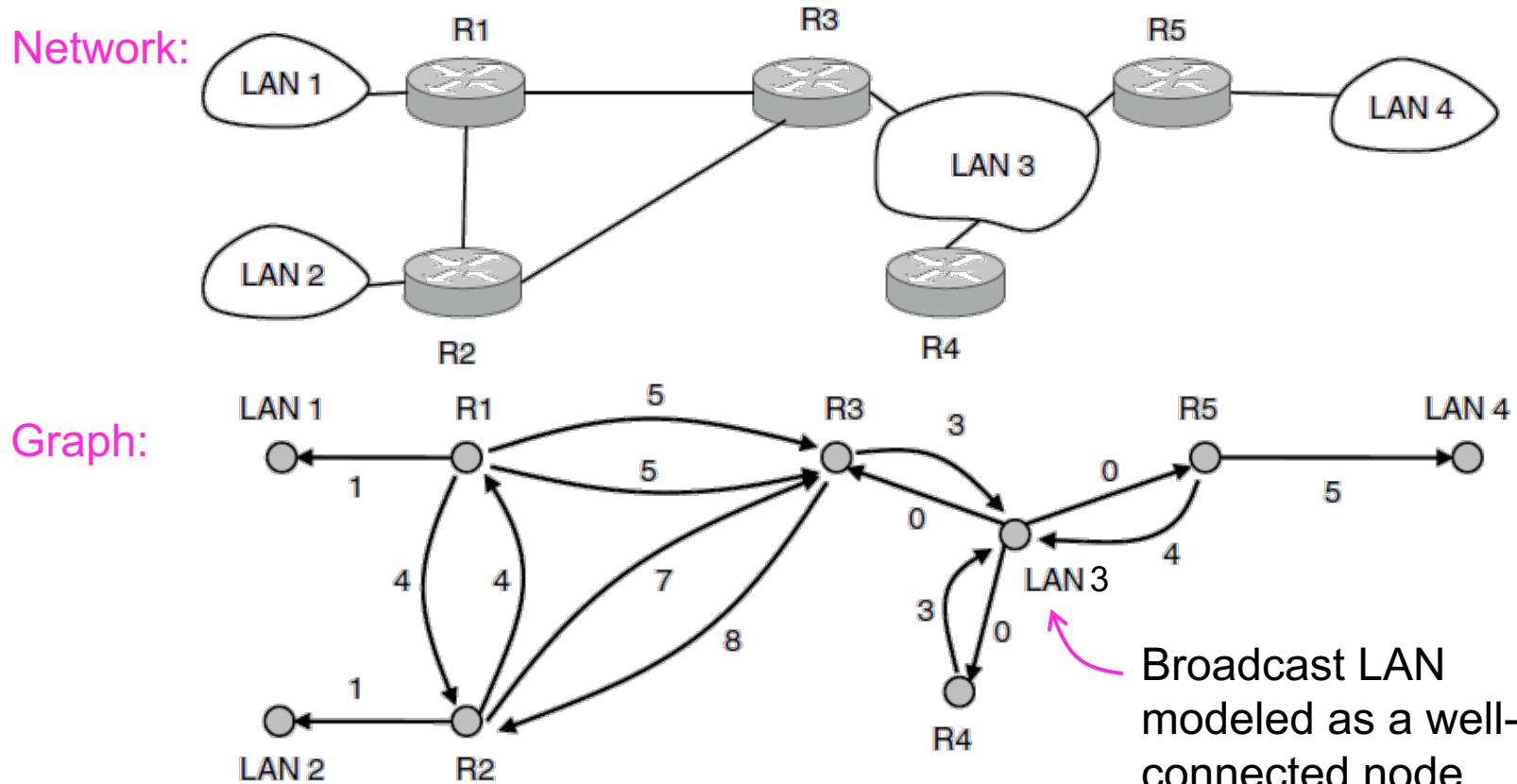
- Forwarding only uses label inside MPLS network



OSPF(open shortest path first)— Interior Gateway Protocol (1)

OSPF computes routes for a single network (e.g., ISP)

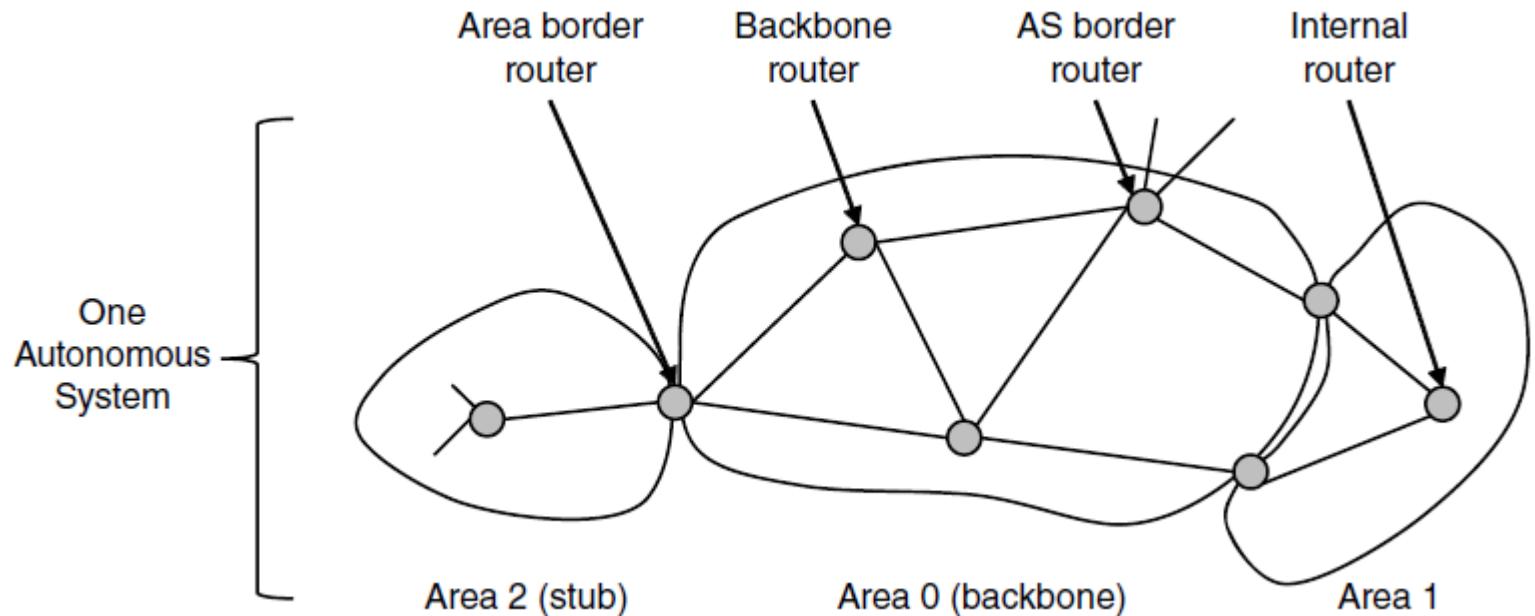
- Models network as a graph of weighted edges



OSPF— Interior Gateway Protocol (2)

OSPF divides one large network (Autonomous System) into areas connected to a backbone area

- Helps to scale; summaries go over area borders



OSPF— Interior Gateway Protocol (3)

OSPF (Open Shortest Path First) is link-state routing:

- Uses messages below to reliably flood topology
- Then runs Dijkstra to compute routes

Message type	Description
Hello	Used to discover who the neighbors are
Link state update	Provides the sender's costs to its neighbors
Link state ack	Acknowledges link state update
Database description	Announces which updates the sender has
Link state request	Requests information from the partner

BGP— Exterior Routing Protocol (1)

BGP (Border Gateway Protocol) computes routes across interconnected, autonomous networks

- Key role is to respect networks' policy constraints

Example policy constraints:

- No commercial traffic for educational network
- Never put Iraq on route starting at Pentagon
- Choose cheaper network
- Choose better performing network
- Don't go from Apple to Google to Apple

Internet Exchange Points



TeleGeography Internet Exchange Map

The Internet Exchange Map is a free resource from TeleGeography. Data contained in this map was compiled by TeleGeography and is updated on a regular basis.

To learn more about TeleGeography or this map, please visit www.telegeography.com.



Sponsored by Telx

Feedback [Twitter](#) [Facebook](#) [GitHub](#)

Q Search

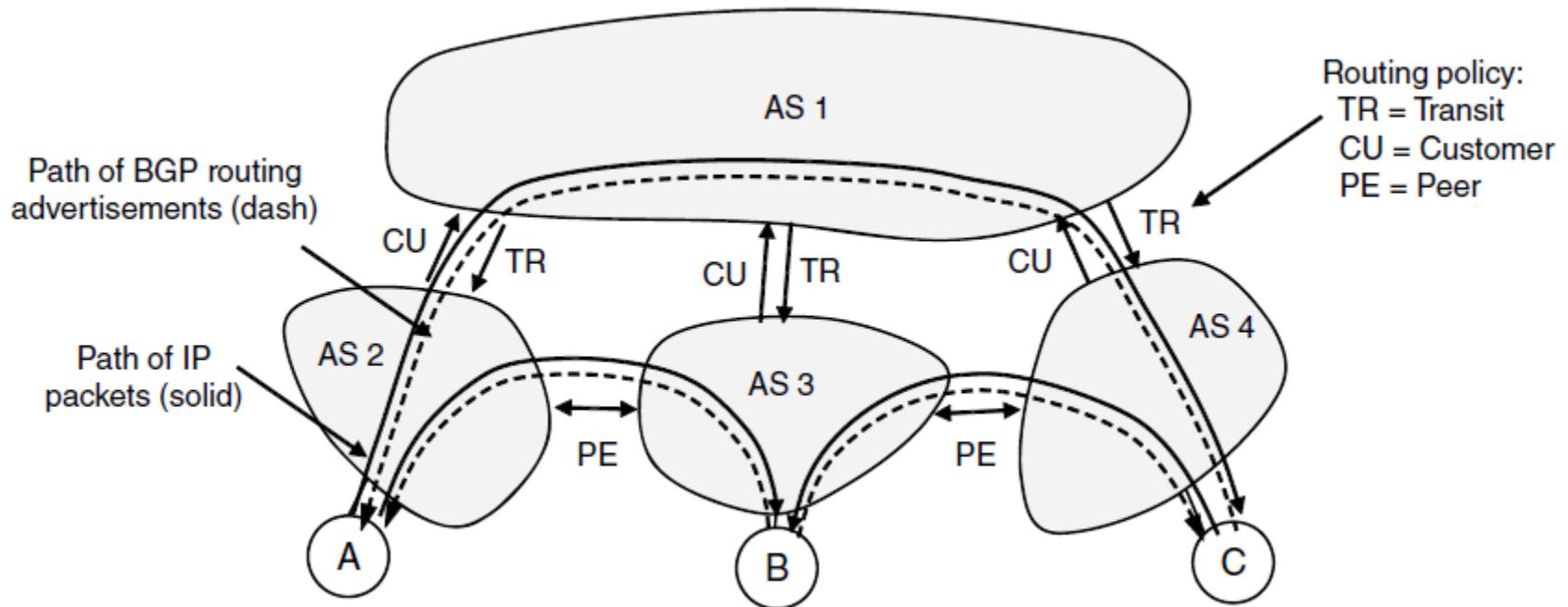
Internet Exchanges

- 6NGIX (Seoul, Korea, Rep.)
- AAIX (Klagenfurt, Austria)
- ADN-IX (Valence, France)
- AIXP (Arusha, Tanzania)
- AIXP (Port-au-Prince, Haiti)
- ALB-IX (Tirane, Albania)
- AMPATH (Miami, United States)
- AMS-IX (Amsterdam, Netherlands)
- AMS-IX Bay Area (San Francisco, United States)
- AMS-IX Caribbean (Willemstad, Netherlands Antilles)
- AMS-IX Chicago (Chicago, United States)
- AMS-IX Hong Kong (Hong Kong, China)
- AMS-IX New York (New York, United States)
- ANG-IXP (Luanda, Angola)
- Angonix (Luanda, Angola)
- APE (Auckland, New Zealand)

BGP— Exterior Routing Protocol (2)

Common policy distinction is transit vs. peering:

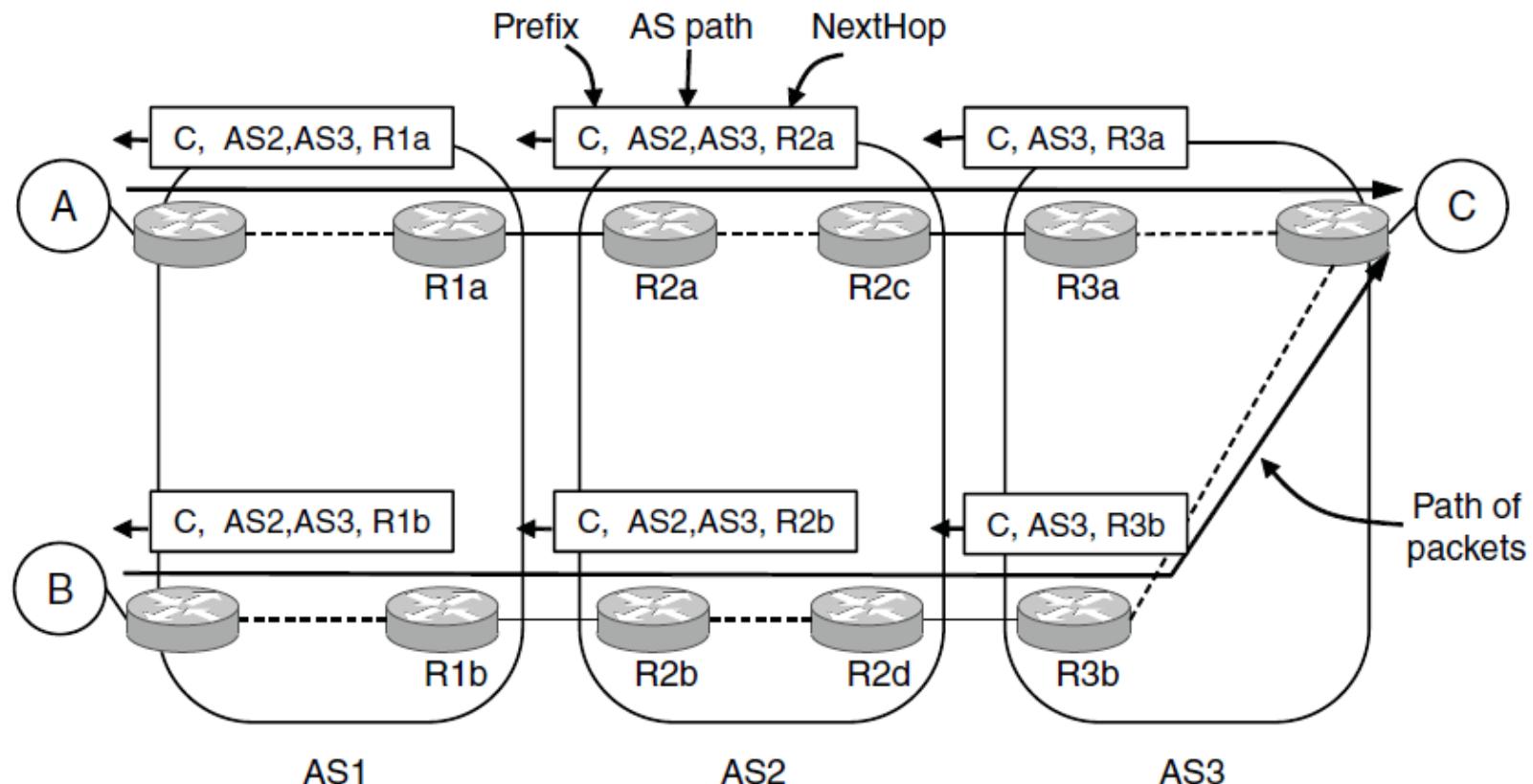
- Transit carries traffic for pay; peers for mutual benefit
- AS1 carries AS2↔AS4 (Transit) but not AS3 (Peer)



BGP— Exterior Routing Protocol (3)

BGP propagates messages along policy-compliant routes

- Message has prefix, AS path (to detect loops) and next-hop IP (to send over the local network)



Internet Multicasting

Groups have a reserved IP address range (class D)

- Membership in a group handled by IGMP (Internet Group Management Protocol) that runs at routers

Routes computed by protocols such as PIM:

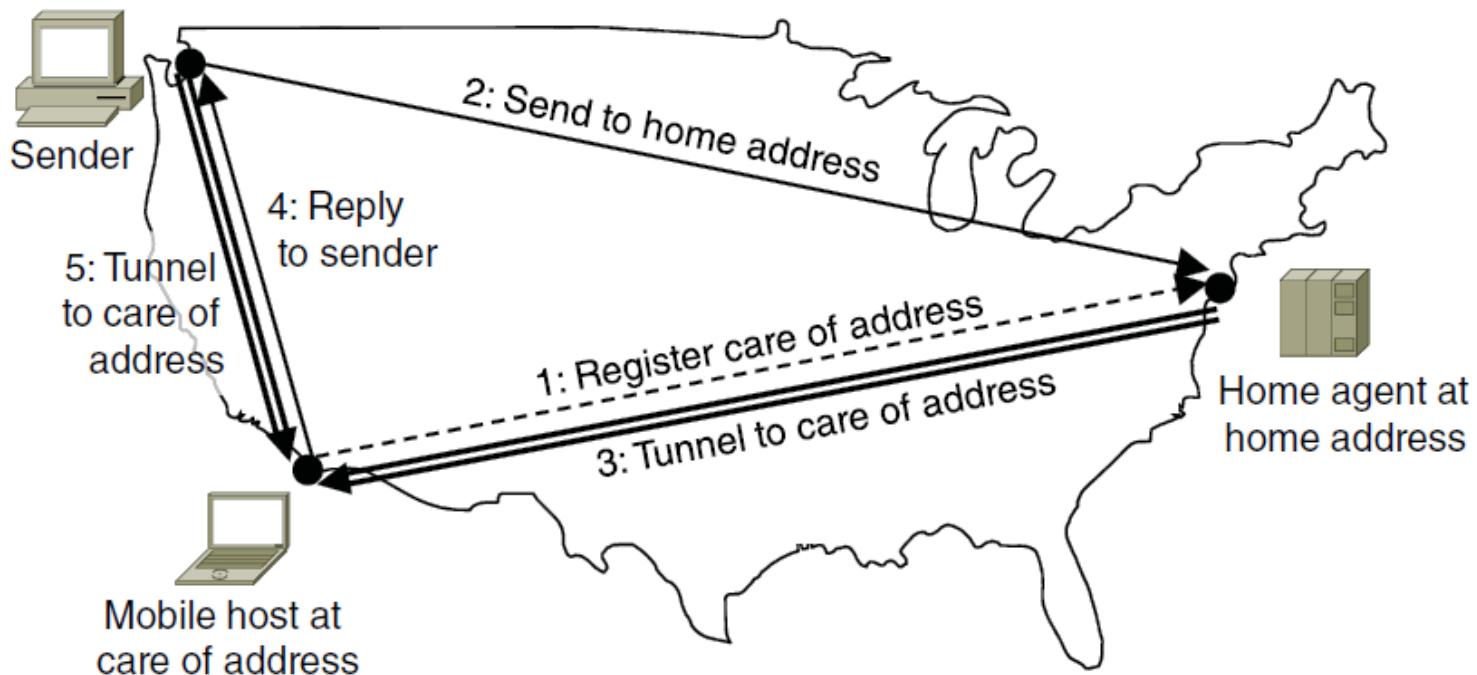
- Dense mode uses RPF with pruning
- Sparse mode uses core-based trees

IP multicasting is not widely used except within a single network, e.g., datacenter, cable TV network.

Mobile IP

Mobile hosts can be reached at fixed IP via a home agent

- Home agent tunnels packets to reach the mobile host; reply can optimize path for subsequent packets
- No changes to routers or fixed hosts



End

Chapter 5