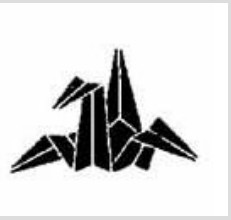
Tecnologías de Redes
“Redes de Área Local”

www.shellsec.net

Xavier Vila i Espinosa

Ing. Técnico en Telecomunicaciones – Esp. Telemática



ÍNDICE DE LA SESIÓN

OBJETIVOS DE LA SESIÓN

- Introducción a los conceptos básicos de redes de área local, así como los estándares más utilizados actualmente:

Ethernet

Fast-Ethernet

Gigabit-Ethernet.

- Descripción de los distintos elementos de interconexión a nivel de enlace, así como las diferentes técnicas de conmutación.

PROGRAMA DE LA SESIÓN

1.- Redes de Área Local.
   - Definición y características
   - Modelo OSI de ISO
   - Medios de Transmisión
   - Topología

2.- Redes Ethernet
   - Ethernet
   - Fast-Ethernet
   - Gigabit-Ethernet

3.- Elementos de interconexión de nivel de enlace
   - Bridges
   - Switches
   - LAN switching

4.- Casos prácticos

1. Redes de Área Local

Definición y características

Por qué necesitamos redes LAN:

- Desarrollo de la informática personal
- Organización distribuida
- Organización en grupos de trabajo
- Programas y datos compartidos
- Recursos compartidos
- Agilización de Comunicación: Correo electrónico, transferencias de ficheros y documentos
- Racionalización del cableado

1. Redes de Área Local

Definición y características

Tecnologías para el transporte de información

Conmutación de circuitos

- RTC, RDSI (XDSI, ISDN) (nivel físico)

Conmutación de paquetes

- Orientado a conexión (circuitos virtuales)

  X.25, Frame Relay, ATM

- No orientado a conexión (datagrama)

  Ethernet, WLAN, (nivel 2)

  IP (nivel 3)

1. Redes de Área Local

Definición y características

Un Sistema de comunicación que proporciona interconexión a una variedad de dispositivos en una área restringida (recinto, edificio, campus) y que no utiliza medios de telecomunicación externos

1. Redes de Área Local

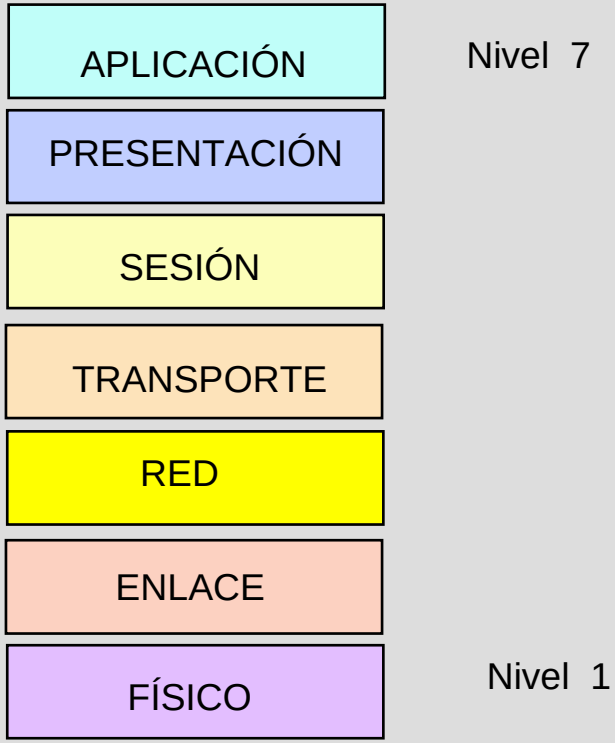
Definición y características

- **Propiedad:** Utilización de medios privados de comunicación.
- **Alcance:** Desde metros hasta pocos kilómetros.
- **Velocidad:** Alta en comparación con las de WAN.
- **Conectividad:** Permiten conexión de igual a igual.
- **Interconexión:** Ofrecen posibilidad de conexión con otras LANs.

1. Redes de Área Local

Modelo OSI de ISO

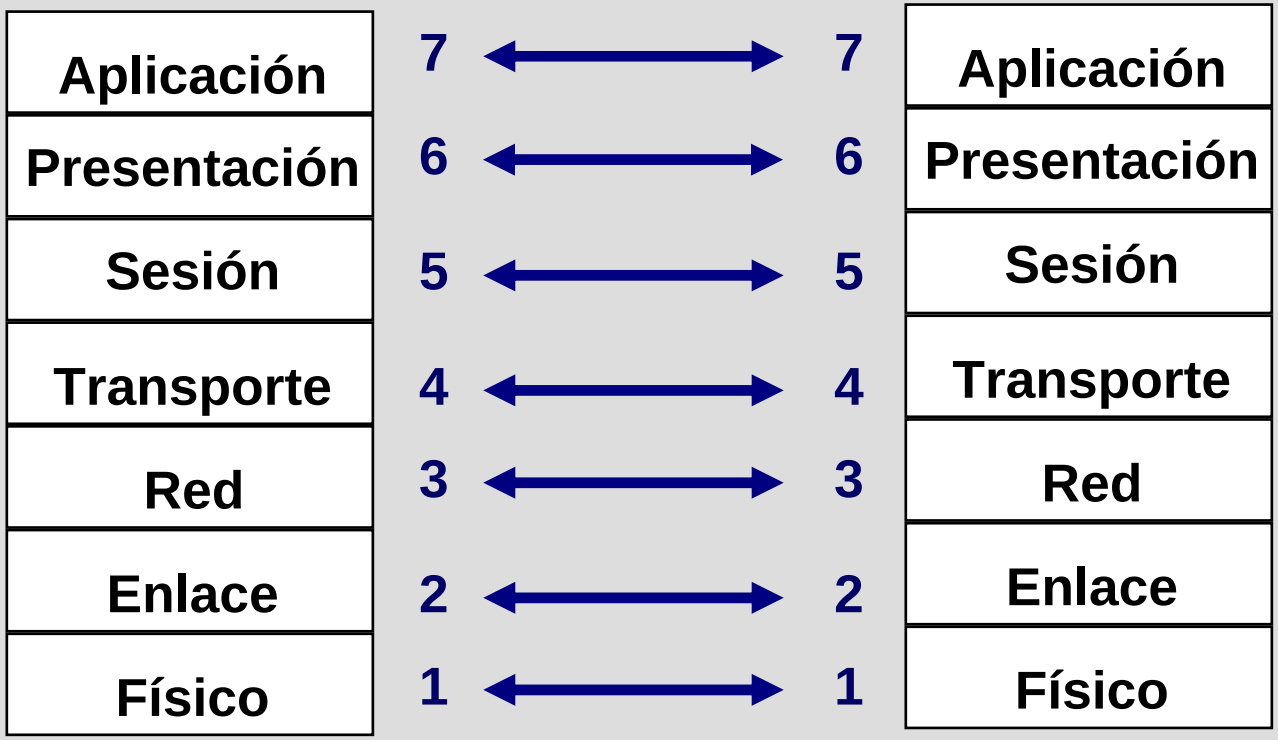
OSI: Open Systems Interconnection



1. Redes de Área Local

Modelo OSI de ISO

OSI: Open Systems Interconnection



1. Redes de Área Local

Modelo OSI de ISO

OSI: Open Systems Interconnection

Nivel de Aplicación:

- Interficie entre las aplicaciones y el usuario con la arquitectura de comunicaciones.
- Proporciona servicios de comunicaciones básicos para:
  - Acceso a sistemas de ficheros remotos NFS, RFS.
  - Ejecución remota de trabajos Telnet, RPC.
  - Gestión de terminales virtuales VT.
  - Servicios de mensajería MHS, X.400, SMTP.
  - Servicios de directorios remotos DNS, X.500.
  - Servicios para gestión de redes, SNMP.

1. Redes de Área Local

Modelo OSI de ISO

OSI: Open Systems Interconnection

- ③ **Nivel de Presentación:**
  - **Normas de sintaxis para la transmisión, estructuración y visualización de los datos.**
  - **Permite la transmisión en diferentes formatos en una misma sesión.**
  - **Realización de las conversiones entre códigos de transmisión diferentes (por ejemplo ASCII-EBCEDIC).**
  - **Emuladores de terminal para PCs.**

1. Redes de Área Local

Modelo OSI de ISO

OSI: Open Systems Interconnection

- ③ **Nivel de Sesión:**
  - **Establecer, mantener y finalizar sesiones concurrentes contra uno o más sistemas remotos de forma transparente.**
  - **NetBIOS.**

1. Redes de Área Local

Modelo OSI de ISO

OSI: Open Systems Interconnection

- ③ **Nivel de Transporte:**
  - **Establecer, mantener y finalizar conexiones simultáneas a una o más redes de forma concurrente y transparente.**
  - **Comunicación “extremo a extremo”.**
  - **Garantiza la fiabilidad en el envío de información a través de la red.**
  - **Nivel de transición.**
  - **TCP, UDP.**

1. Redes de Área Local

Modelo OSI de ISO

OSI: Open Systems Interconnection

- **Nivel de red:**
  - **Servicios de encaminamiento y direccionamiento de mensajes.**
  - **Independencia del enlace utilizado.**
  - **IP, IPX.**

1. Redes de Área Local

Modelo OSI de ISO

OSI: Open Systems Interconnection

- ③ **Nivel de Enlace:**
  - **Controla el acceso al medio físico.**
  - **Proporciona los elementos necesarios para conectar entidades de nivel de red a través de un enlace de datos.**
  - **Garantiza una transferencia fiable entre nodos colaterales del enlace.**
  - **Fragmentación y secuenciación de la información en tramas.**
  - **BSC, SDLC, HDLC, HDLC/LAPB, LAP-D.**
  - **En redes de área local se divide en dos : LLC (Logical Link Control) y MAC (Medium Access Control).**
  - **Normas IEEE 802.X.**

1. Redes de Área Local

Modelo OSI de ISO

OSI: Open Systems Interconnection

- **Nivel Físico:**
  - **Define las características de conexión de los equipos al medio en términos eléctricos y mecánicos.**
  - **Permite la transmisión transparente del flujo de bits entre entidades de nivel de enlace a través de conexiones físicas.**
  - **Normas RS-232C, RS-422, V.24, V.35, G.703, X.21, 10BaseT, 100BaseTX, ...**

1. Redes de Área Local

Medios de transmisión

El medio físico nos condiciona la red?

- **Ancho de Banda**
- **Longitud**
- **Fiabilidad en la transferencia**
- **Seguridad**
- **Facilidad de instalación**
- **Coste**

1. Redes de Área Local

Medios de transmisión

Par Trenzado

Tipos:

- **UTP (Unshielded Twisted Pair)**
  - **Bajo Coste**
  - **Fácil instalación**
  - **Se utiliza para telefonía y datos**
  - **Suele ser de 4 pares**
- **STP (Shielded Twister Pair)**
  - **Para distancias grandes**
  - **Entornos ruidosos**

1. Redes de Área Local

Medios de transmisión

Par Trenzado

Características:

- Soportan grandes velocidades.
- Impedancia:
  - **de 120 a 150 Ohms per STP**
  - **de 100 Ohms per UTP**
- Categorías de UTP:
  - **Categoría 3**
  - **Categoría 5, 5e (enhanced)**
- Conectores RJ45

1. Redes de Área Local

Medios de transmisión

Cable Coaxial

Tipos:

- **10BASE5 (Cable coaxial [illegible]ueso)**
  - **Impe[illegible]de 50**
  - **Velocid[illegible]**
  - **Longitud r[illegible]l segmento 0,5 Km**
- **10BASE[illegible]delgado)**
  - **[illegible]a de 50**
  - **Velocidad de 10 Mbps**
  - **Longitud máxima de 185 m**

1. Redes de Área Local

Medios de transmisión

Fibra Óptica

Tipos:

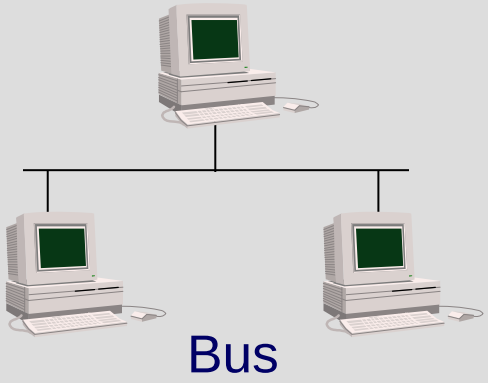
- **Multimodo (Normalmente Color naranja)**
  - **Bajo Coste de los Transceptores**
  - **Utiliza diodos LED**
  - **Distancias pequeñas (<1500m)**
- **Monomodo (Normalmente Color Amarillo)**
  - **Para distancias grandes (Varios Km)**
  - **Utiliza emisor Láser**
  - **Alto coste de los transceptores**
- **Connectores: ST, SC**

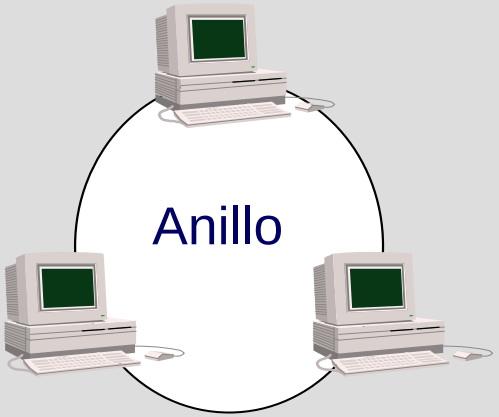
1. Redes de Área Local: Topología

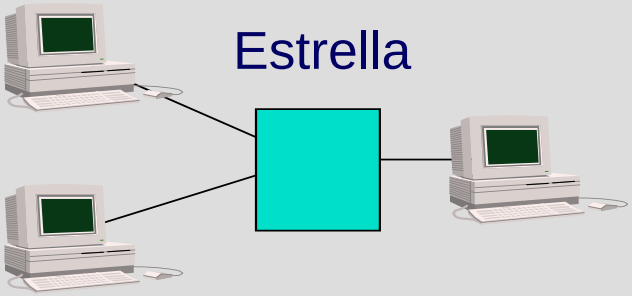
La topología define la distribución?

- **Complejidad de la instalación y mantenimiento**
- **Vulnerabilidad a fallos o averías**
- **Gestión del medio**
- **Facilidad de localización de averías**
- **Capacidad de expansión y reconfiguración**
- **Coste**

1. Redes de Área Local: Topología







Tecnología de Redes de Comunicaciones

2. Redes Ethernet

2. Redes Ethernet:

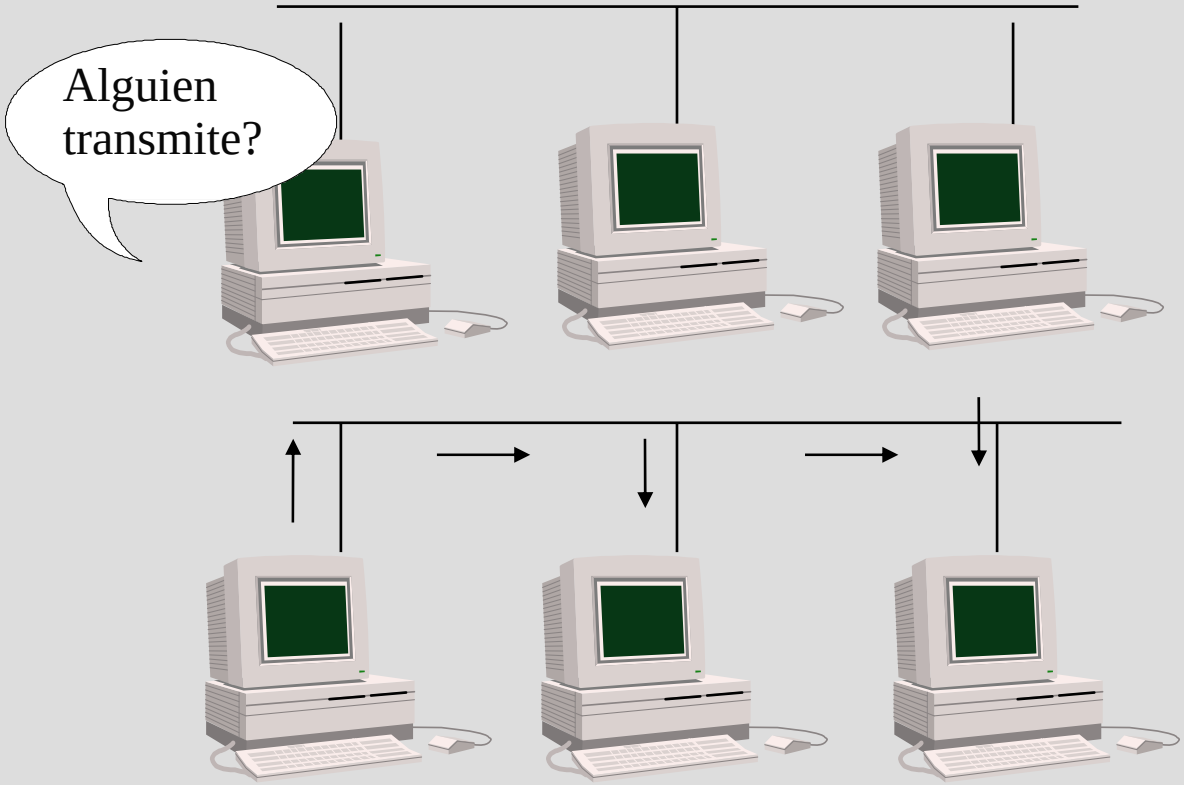
Ethernet

- Diseñada por Xerox en el año 1970
- Puesta en el mercado en el año 1980
- Mejorada en el año 1985 (Ethernet II)
- Normalizada por el IEEE como 802.3
- Dos versiones:
  - Ethernet II
  - IEEE 802.3
- En breve la norma IEEE 802.3 incluirá también la versión Ethernet II

2. Redes Ethernet: Ethernet

CSMA/CD

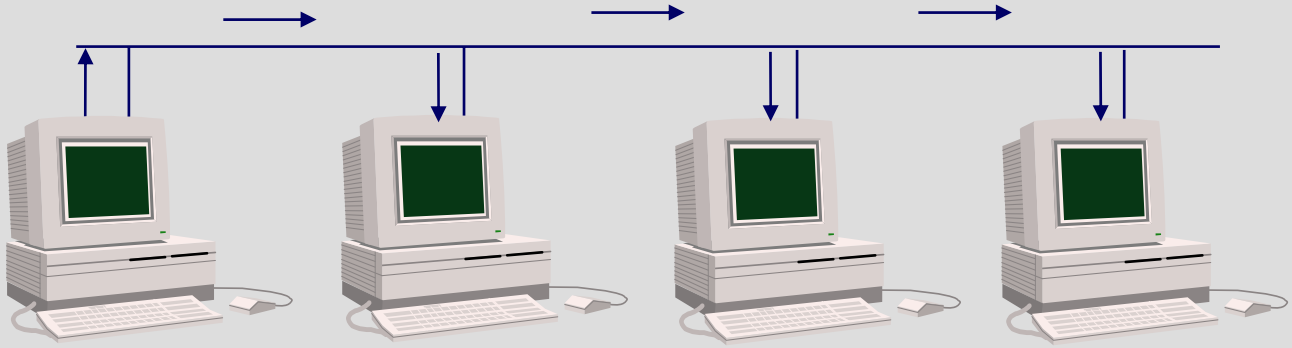
CSMA/CD : Carrier Sense Multiple Access with Collision Detection



Las estaciones escuchan el medio antes de transmitir, para ver si está ocupado

2. Redes Ethernet: Ethernet

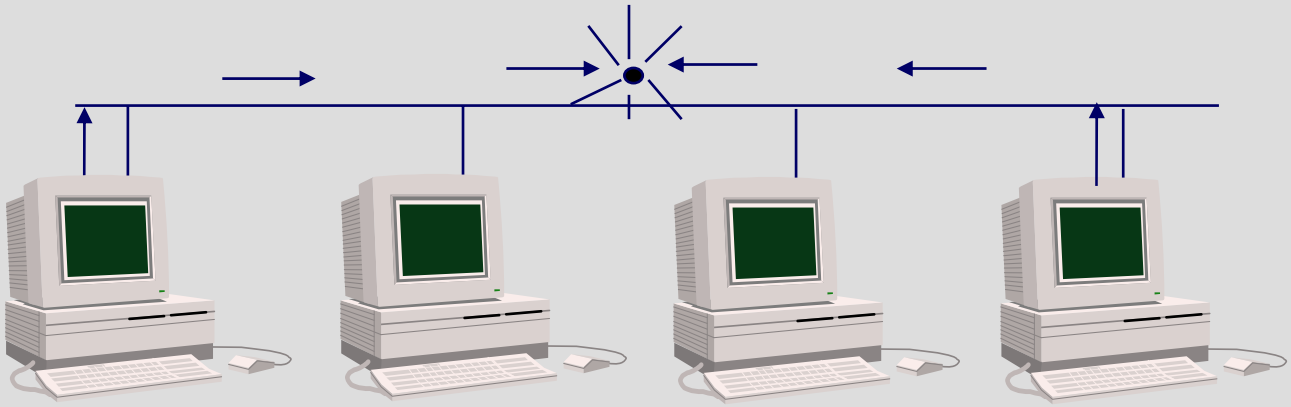
CSMA/CD



Una vez que se inicia la transmisión, todas las estaciones “escuchan” las tramas enviadas por las otras estaciones

2. Redes Ethernet: Ethernet

CSMA/CD



Cuando dos estaciones transmiten a la vez se produce una colisión.

Las estaciones transmisoras detectan la colisión

Esperan un tiempo aleatorio (entre 10 y 90 micro segundos) antes de transmitir otra vez

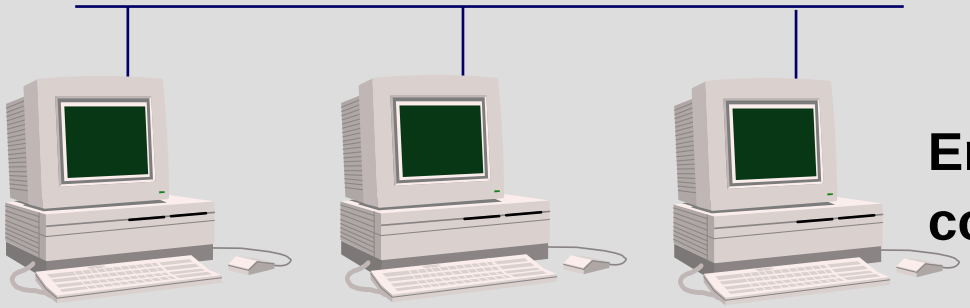
2. Redes Ethernet: Ethernet

Ethernet

- 10base5 (thicknet)
- 10base2 (thinnet)
- 10baseT
- 10baseFL
- ...

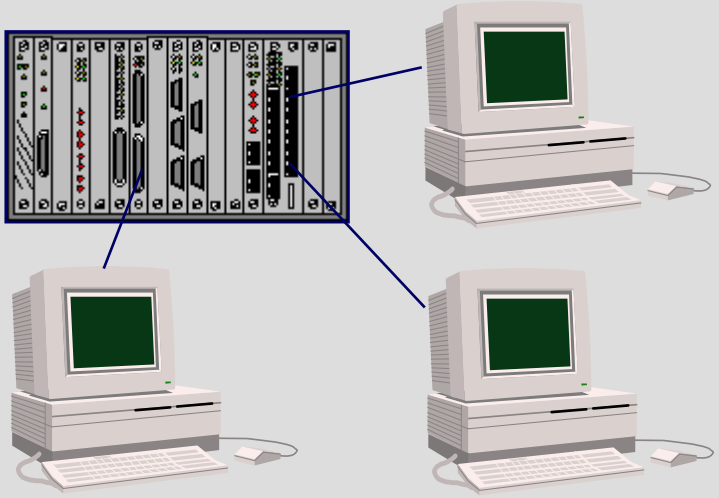
2. Redes Ethernet: Ethernet

TOPOLOGIA ETHERNET



En Bus, utilizando coaxial

En Estrella, utilizando Hubs o Commutadores



2. Redes Ethernet: Ethernet

ESTRUCTURA DE LA TRAMA (Ethernet II)

Preámbulo: 10101010 (7 bytes) 10101011 (1 byte)

Destino: **Dirección MAC destino. 6 bytes.**

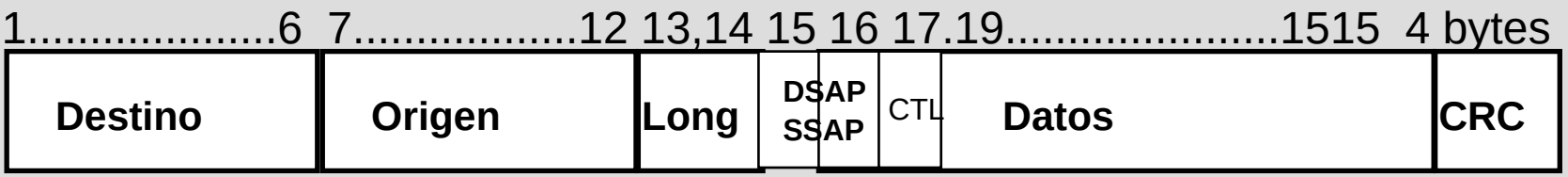
Origen: **Dirección MAC origen. 6 bytes.**

Tipo: **Tipo de protocolo encapsulado en el campo de datos: IP, ARP, DECnet, Xerox NS, AppleTalk, etc...). 2 bytes.**

CRC: **Código de Redundancia Cíclico. 4 bytes**

2. Redes Ethernet: Ethernet

ESTRUCTURA DE LA TRAMA (802.3)



Destino: Dirección MAC destino. 6 bytes.

Origen: Dirección MAC origen. 6 bytes.

Long.: Longitud de la trama (< 1514). 2 bytes

DSAP/SSAP: Equivalente al campo "Tipo" en l' Ethernet II. 2 bytes.

CTL: Control. 2 bytes

CRC: Código de Redundancia Cíclico.

2. Redes Ethernet: Ethernet

CÓMO DIFERENCIAR EL TIPO DE TRAMA

- **IEEE 802.3**
  - **Los valores del campo “Longitud” toman valores de 1500 (0x05DC) como máximo.**
- **Ethernet II**
  - **Los valores del campo “Tipo” toman valores superiores a 1500. Ej:**

08-00	**IP**	**08-06**	**ARP**
80-35	**RARP**	**81-37**	**NOVELL**

2. Redes Ethernet: Ethernet

DIRECCIONES MAC

- **Constan de 48 bits (6 bytes)**
- **Los 3 primeros bytes especifican el fabricante, y son asignados por el IEEE.**
- **Se suelen expresar en formato hexadecimal, separando los bytes por guión o dos puntos.**

- Ejemplo de direcciones de algunos fabricantes:

00-00-0C-XX-XX-XX	**CISCO**
00-20-08-XX-XX-XX	**FORE Systems**
08-00-20-XX-XX-XX	**Sun**
09-00-09-XX-XX-XX	**Hewlett-Packard**
08-00-5A-XX-XX-XX	**IBM**

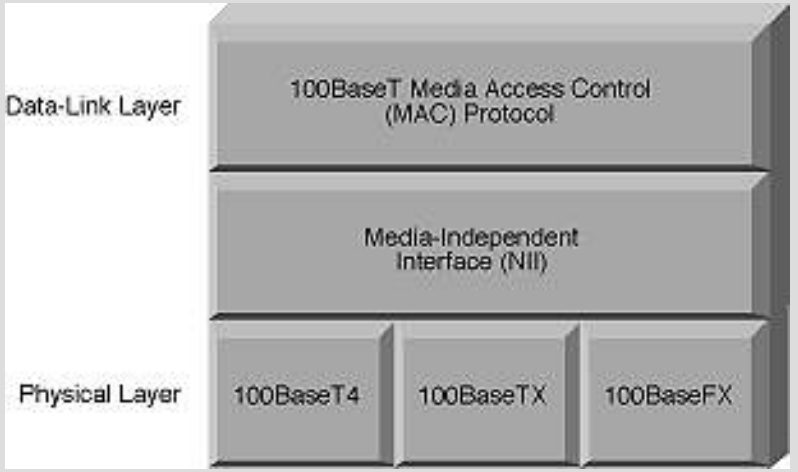
2. Redes Ethernet: Fast Ethernet

Fast Ethernet

- 100 Mbps
- Coste reducido
- Preserva el nivel MAC, simplifica la interoperación con les redes existentes
- Fácil Coexistencia con les redes ya existentes

2. Redes Ethernet: Fast Ethernet

Physical Layer



- **100BaseTX:**
  - **UTP, Categoría 5**
  - **Utiliza dos pares**
- **100BaseT4:**
  - **Para instalaciones con UTP Cat. 3 y 4**
  - **Utiliza los 4 pares**
- **100BaseFX :**
  - **Fibra Multimodo**
  - **Fibra Monomodo**

2. Redes Ethernet: Fast Ethernet

ESTÁNDARD	TIPO DE CABLE	MODO	PARES	DISTANCIA (m)
10BaseT	Cat. 3, 4 y 5	Half dúplex	2	100
100Base-Tx	Cat. 5	Half Dúplex Full Dúplex	2	100
100Base-T4	Cat. 3	Half Dúplex	4	100
100Base-Fx	Monomodo	Half Dúplex Full Dúplex	1	412 (Half Dúplex) 2000 (Full Dúplex)
100Base-Fx	Multimodo	Half Dúplex Full Dúplex	1	10km

2. Redes Ethernet: Fast Ethernet

Full-Duplex

- Permite 100Mbps en cada dirección
- No hay colisiones.
- Incrementa la máxima distancia a 2 Km.
- Sólo máquinas conectadas a un switch pueden trabajar a full duplex.

Auto-Negotiation

- Autonegociación 10/100
- Autonegociación Full/Half

2. Redes Ethernet: Fast Ethernet

Agregación de Enlaces

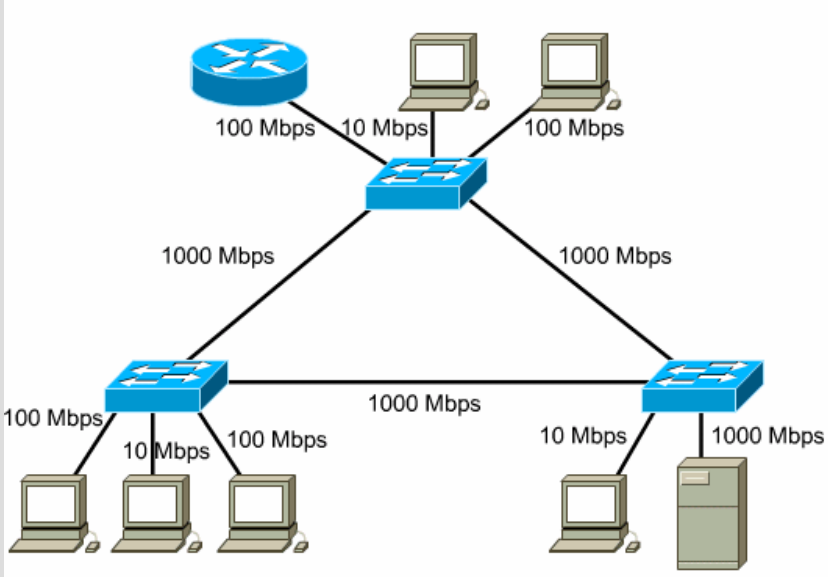
- **Posibilidad de “agregar” varios puertos de 100Mbps como un único flujo de datos entre dos conmutadores.**

- **Permite obtener un *backbone* de mayor velocidad sin tener que adquirir puertos a 1Gbps.**

2. Redes Ethernet: Gigabit Ethernet

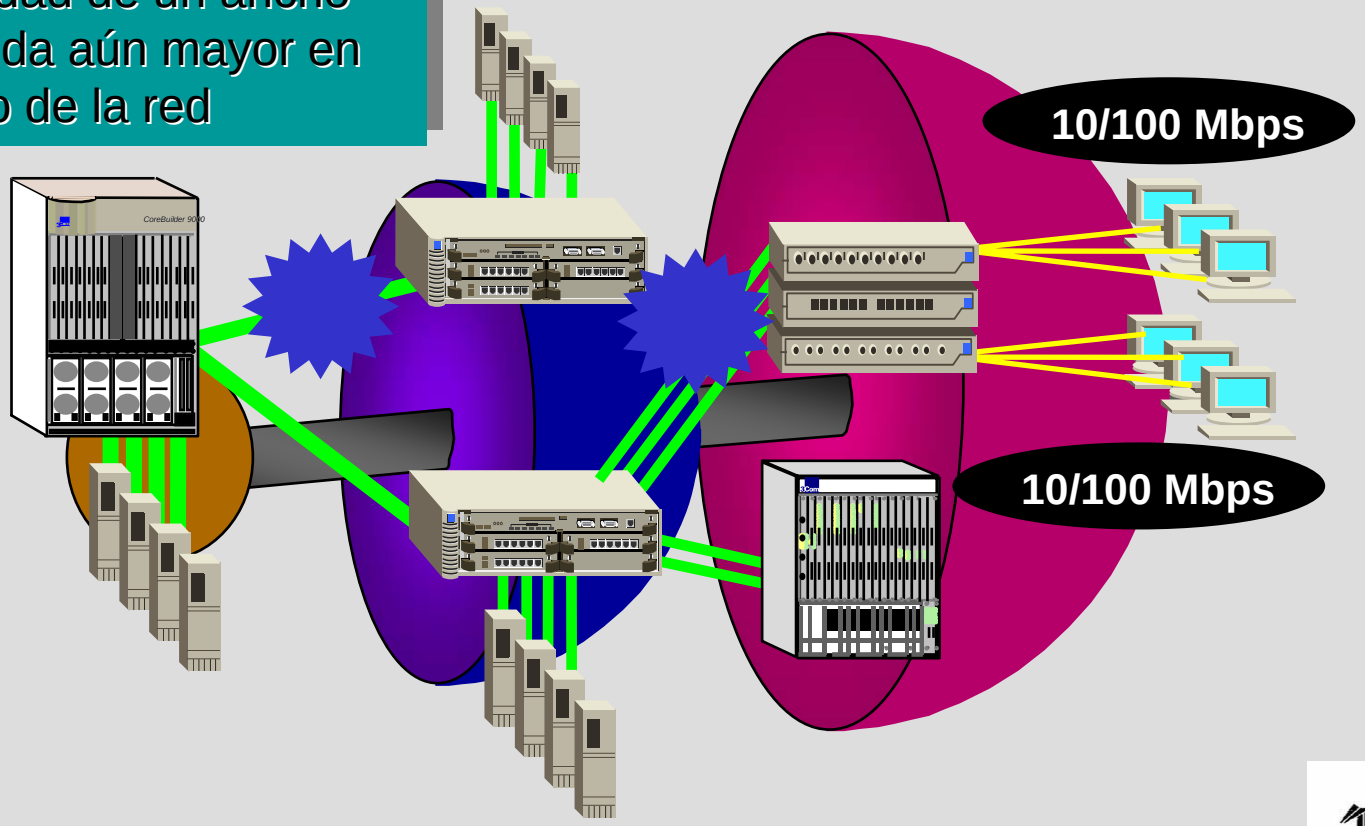
Gigabit Ethernet

- Standard aprobado en el año 1998, IEEE-802.3z
- Conserva el nivel MAC de Ethernet
- La capa física utiliza tecnología Fiber Channel.
- Inicialmente, tecnología de backbone

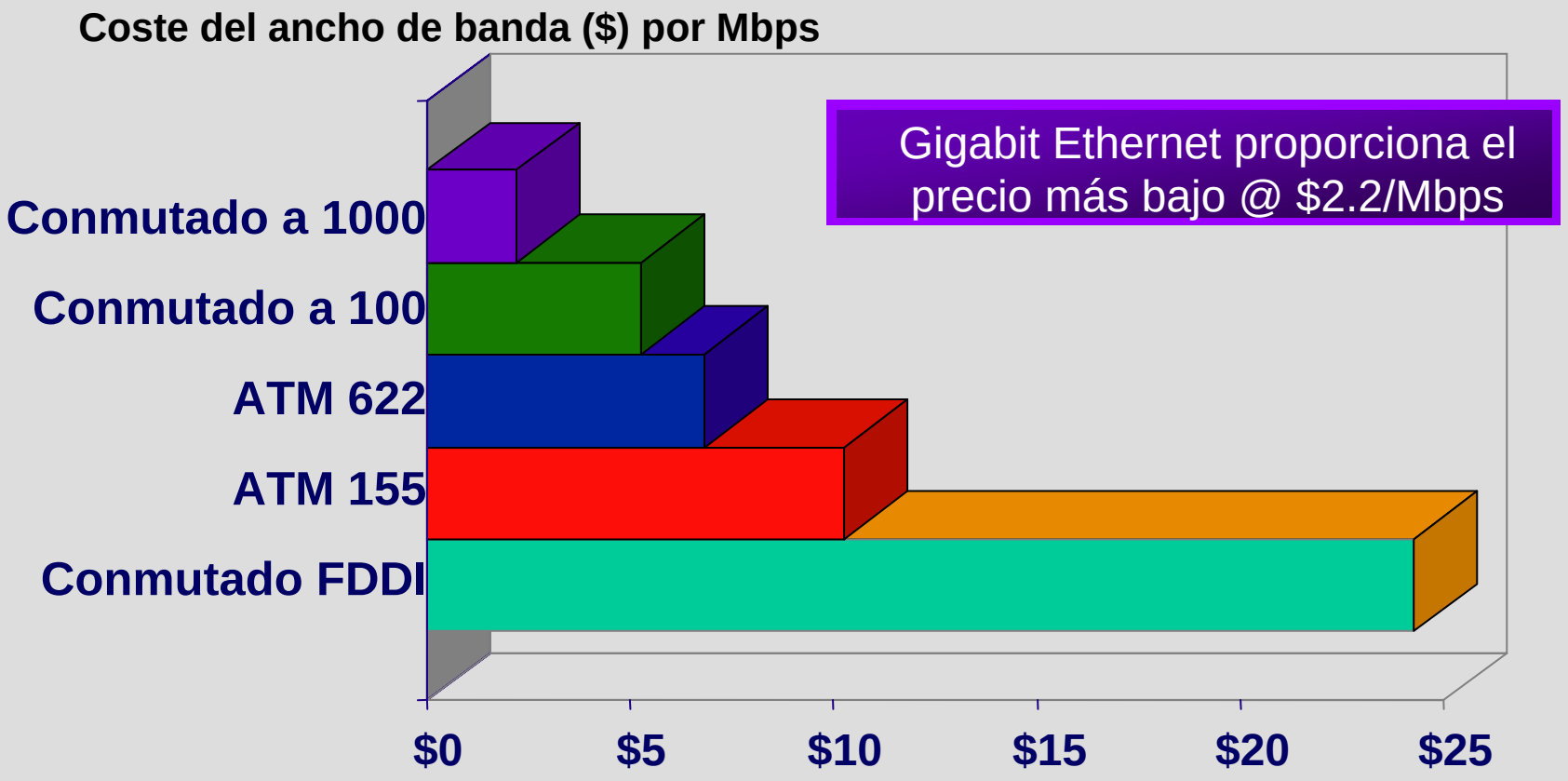


2. Redes Ethernet: Gigabit Ethernet

El aumento de ancho de banda en el extremo de la red (NICs) provoca la necesidad de un ancho de banda aún mayor en el resto de la red



2. Redes Ethernet: Gigabit Ethernet



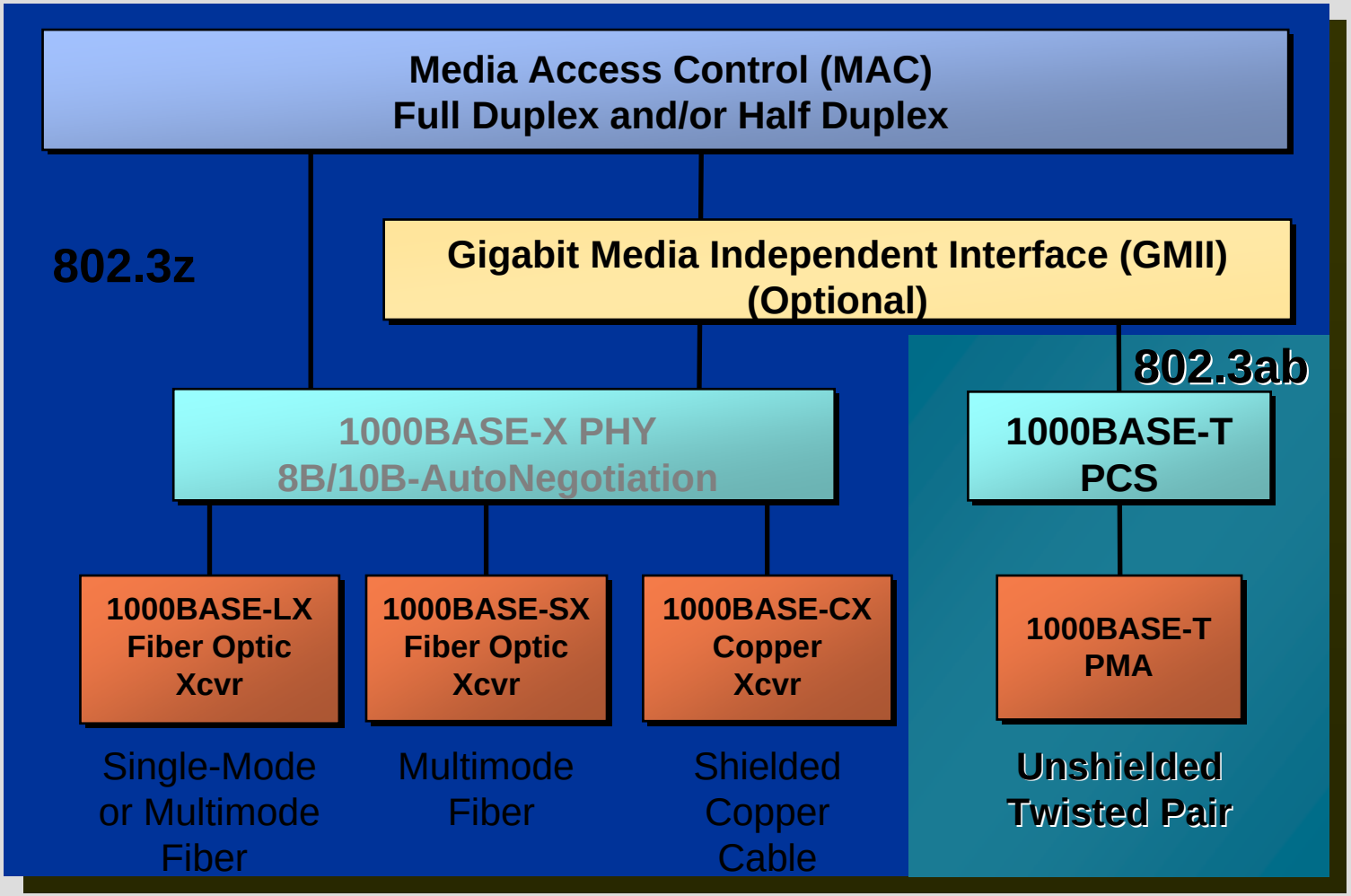
Source: Dell'Oro Group, CY1997

2. Redes Ethernet: Gigabit Ethernet

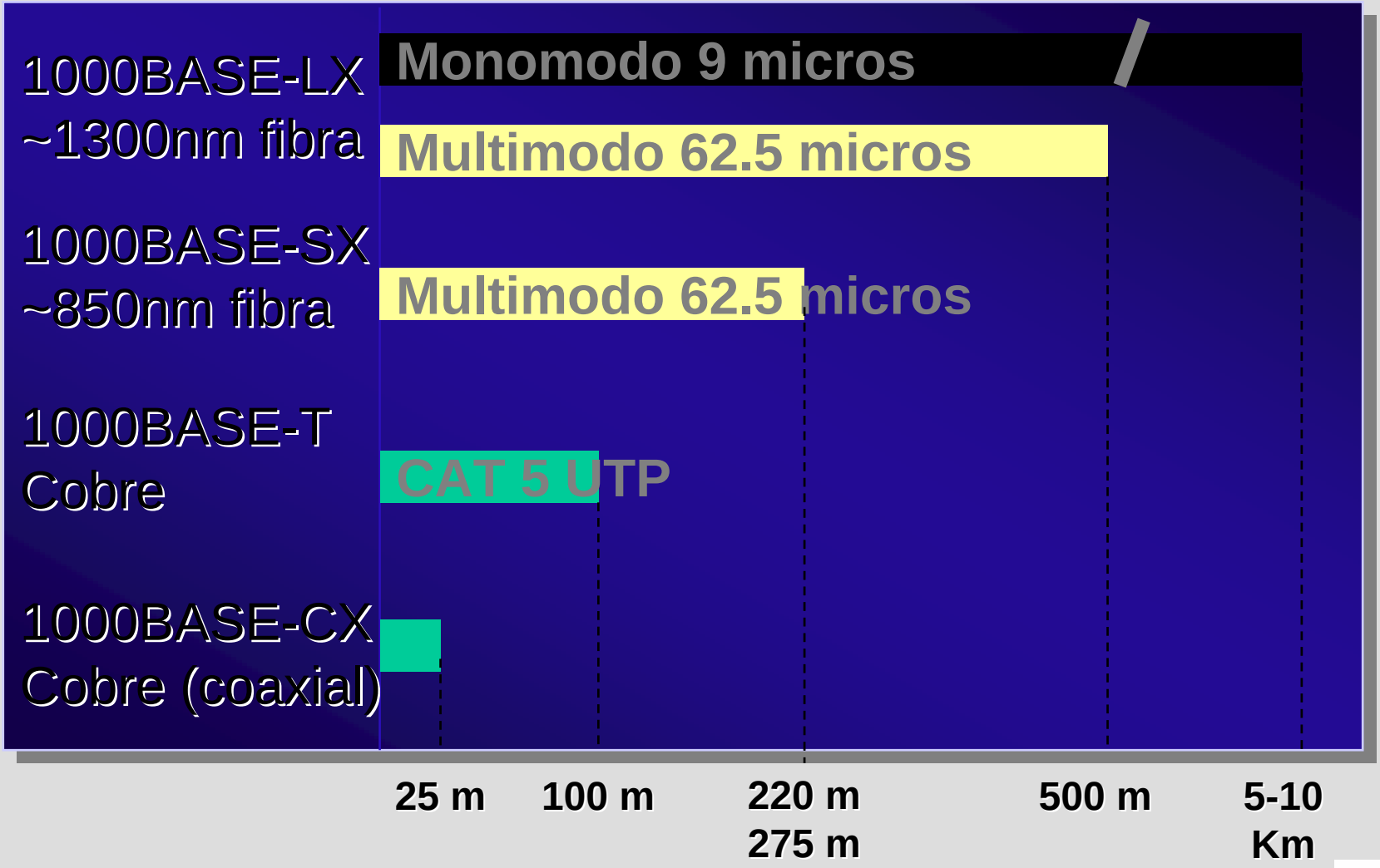
Nivel Físico

- **1000BaseX**
  - **1000BaseSX: Multimodo, entre 300 y 500m**
  - **1000BaseLX: Monomodo, entre 550m y 3000m**
  - **1000BaseCX: para cable twinax**
- **1000BaseT:**
  - **Sobre UTP, distancia max 100m, utiliza 4 pares**

2. Redes Ethernet: Gigabit Ethernet



2. Redes Ethernet: Gigabit Ethernet



2. Redes Ethernet: Gigabit Ethernet

Nivel de MAC

- En entornos Full-Duplex en los que no se utiliza CSMA/CD:
  - Mismo formato de trama que Ethernet

- En entornos Half-duplex en los que se requiere detección de colisiones (CSMA/CD):
  - Carrier Extension
  - Packet Bursting

2. Redes Ethernet: Gigabit Ethernet

Carrier Extension

- Cómo detectar una colisión a 1Gbps ?
- Aprovechamos poco el ancho de banda.

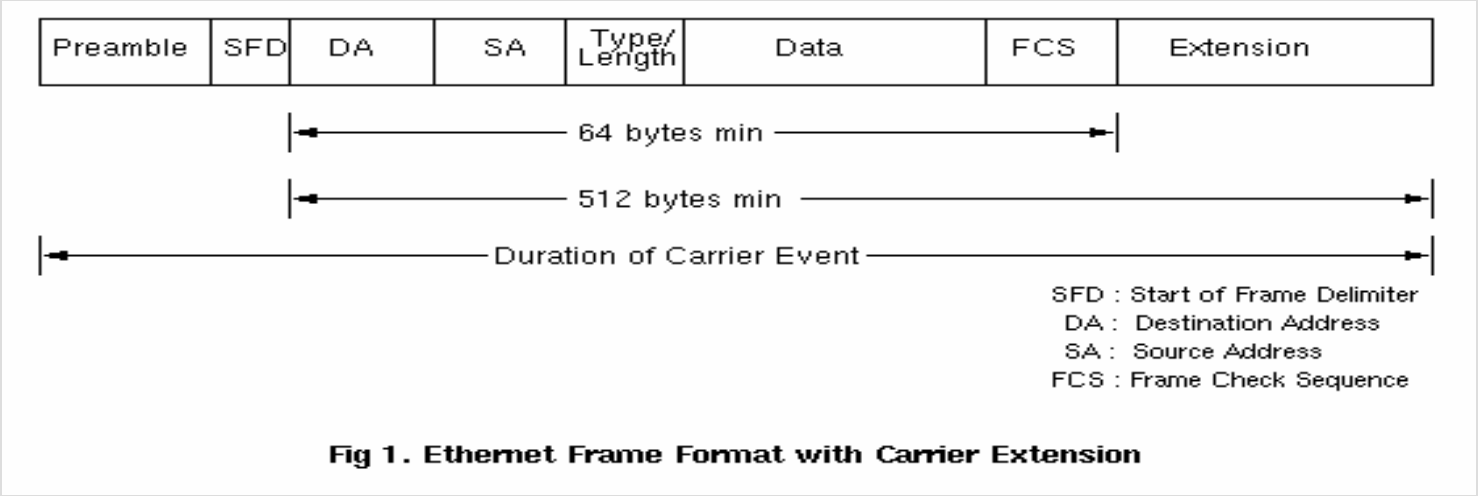
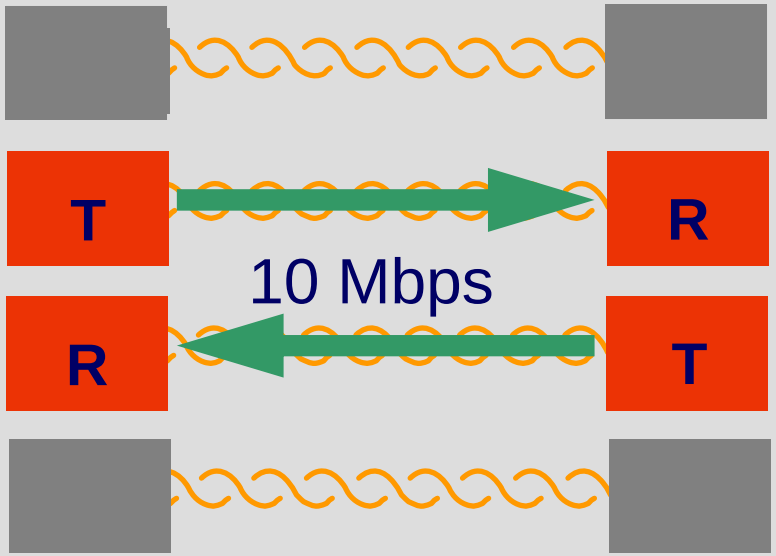


Fig 1. Ethernet Frame Format with Carrier Extension

2. Redes Ethernet: Gigabit Ethernet

10 / 100 en Cat-5



Gigabit en Cat-5

Requiere la cancelación de eco en cada par

2. Redes Ethernet: Gigabit Ethernet

Packet Bursting

- Cómo podemos mejorar el carrier extension

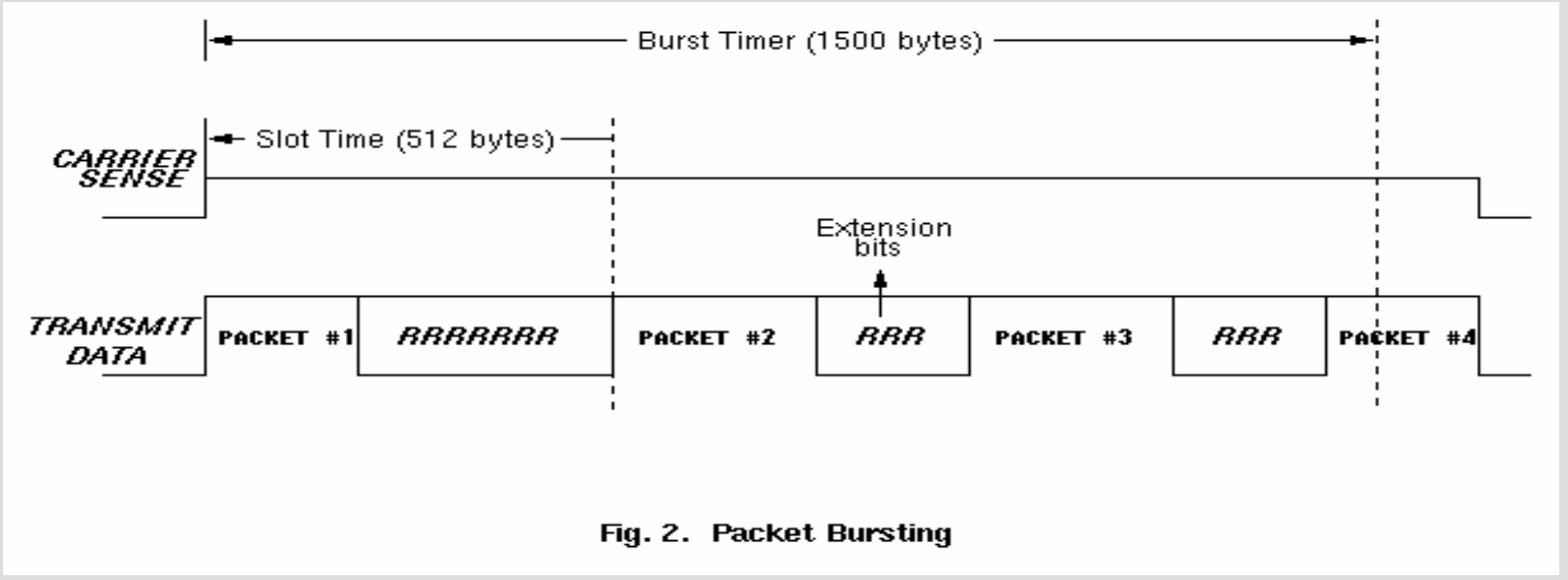


Fig. 2. Packet Bursting

2. Redes Ethernet: Gigabit Ethernet

Ejemplo

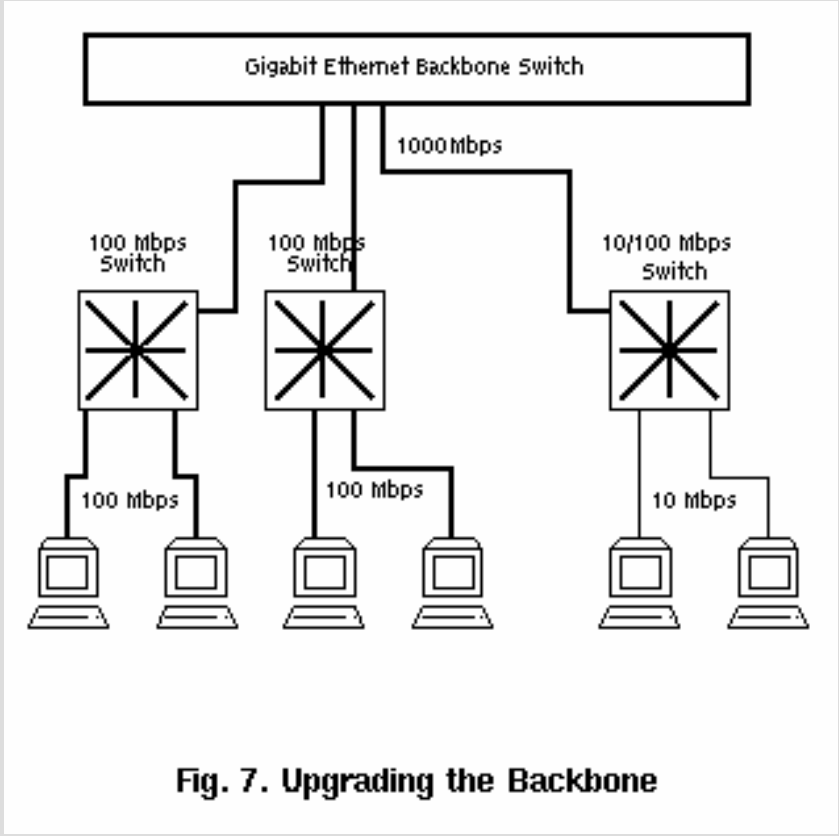


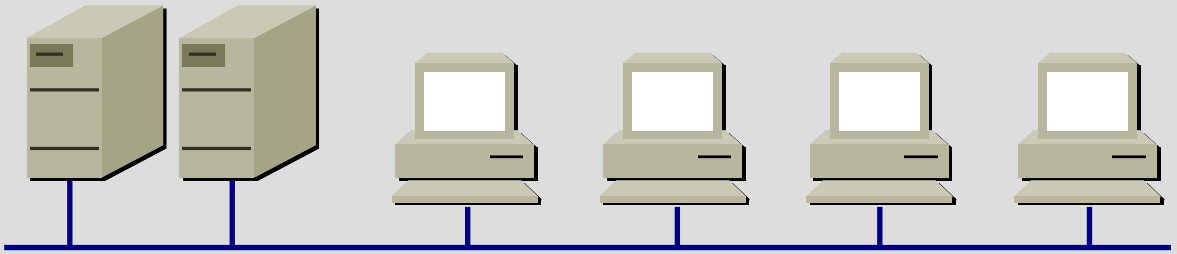
Fig. 7. Upgrading the Backbone

Tecnología de Redes de Comunicaciones

3. Elementos de interconexión de nivel de enlace

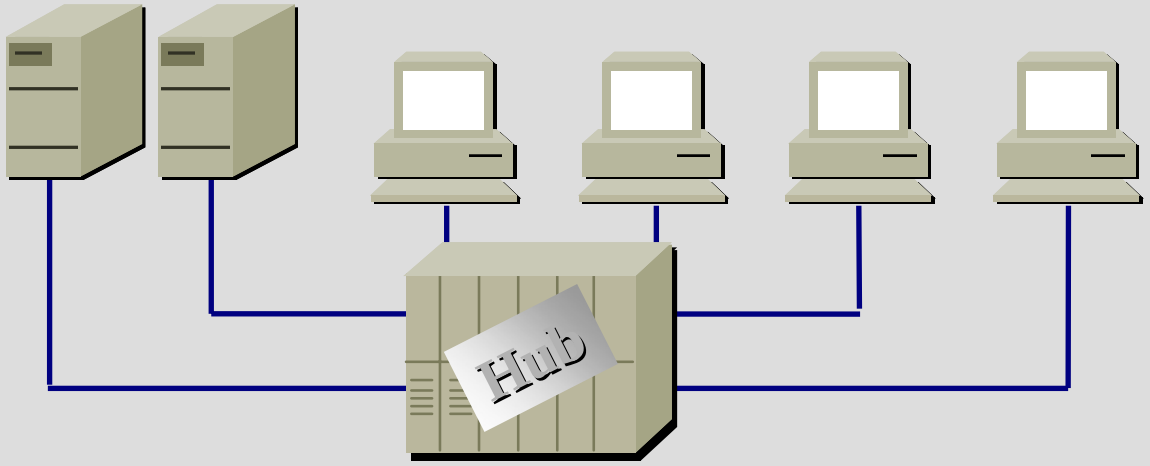
3. Interconexión a nivel 2: Redes compartidas

- Se comparte el ancho de banda entre todas las estaciones.
- Sólo puede transmitir una estación en un momento dado
- Las colisiones (en el caso de ethernet) se “ven” en toda la red.



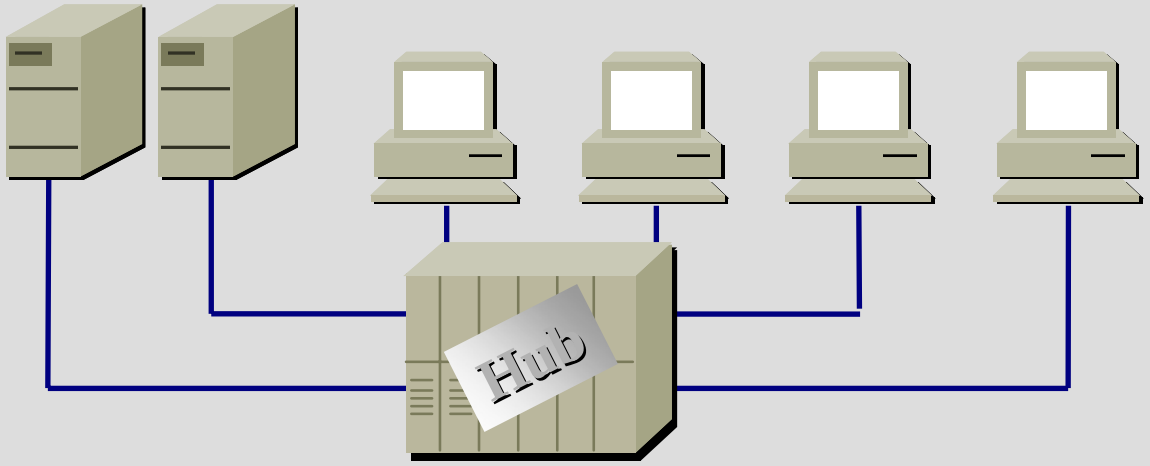
3. Interconexión a nivel 2: Redes compartidas

- **Existen las mismas limitaciones con Hubs y con segmentos físicos.**



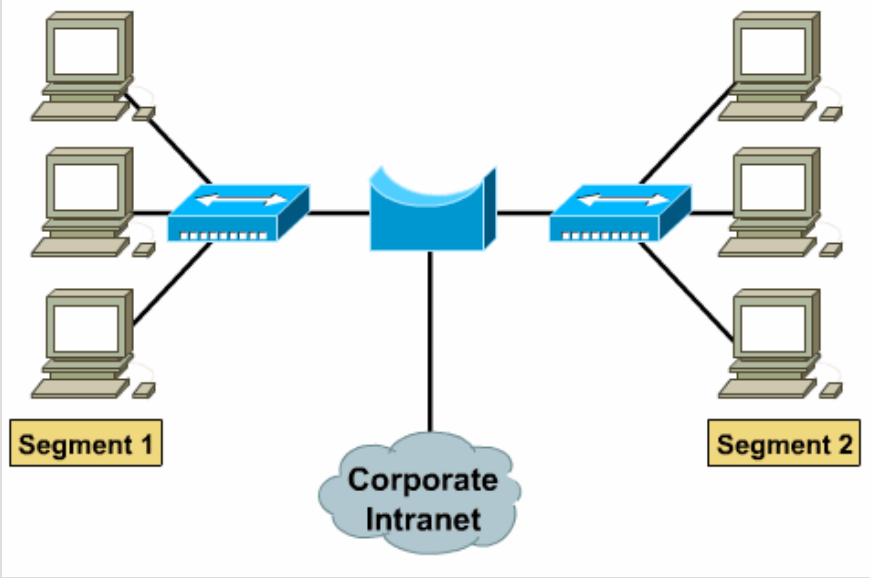
3. Interconexión a nivel 2: Redes compartidas

- **No es idóneo para topologías multi-servidor**
- **Sólo puede acceder a un servidor en un instante determinado.**



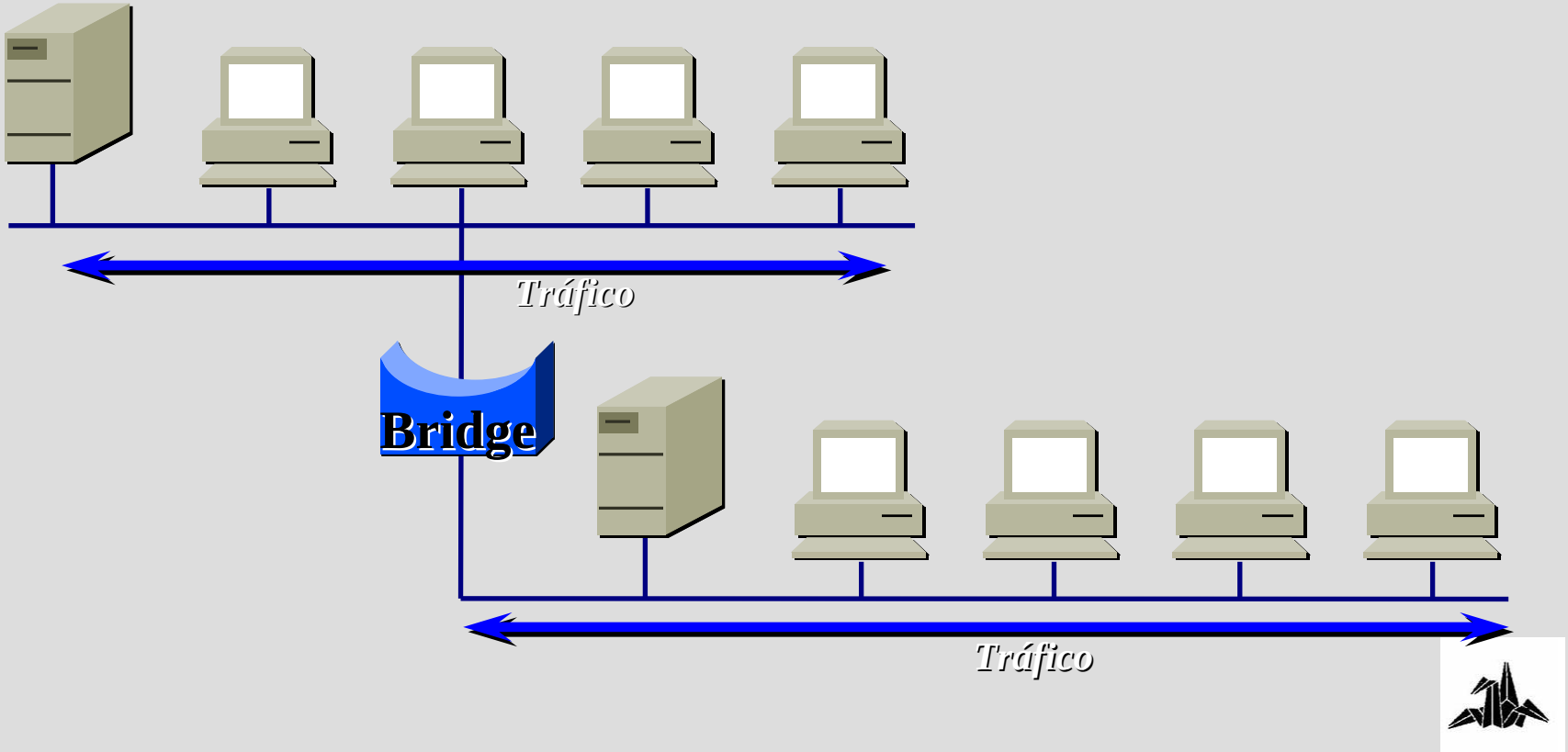
3. Interconexión: Mejoras en la red compartida

- **Red Compartida**
  - **Todas las estaciones forman parte del mismo dominio de colisión**
- **Red Segmentada (Bridging)**
  - **Dominios de colisiones separados**
  - **Mayor ancho de banda agregado**



3. Interconexión: Redes segmentadas

- Hay dos tráficos simultáneo, uno en cada segmento
- Útil en entornos de diferentes grupos de trabajo



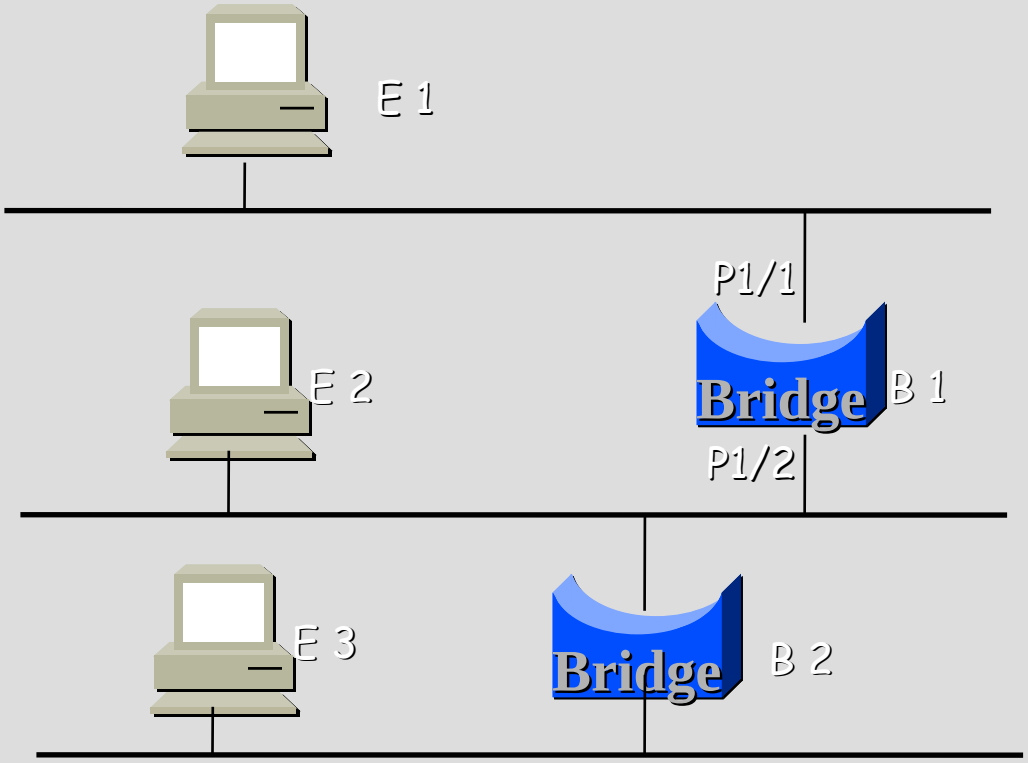
3. Interconexión: Bridges

- Realizan su función a nivel 2
- Analizan el tráfico entrante
- Filtran los paquetes según la información de nivel de enlace.
- Se utilizan básicamente cuatro algoritmos:
  - Transparent bridge
  - Translating bridge
  - Source route bridge
  - Encapsulating bridge

3. Bridges: Bridges transparentes

- Los bridges aprenden las MAC que hay en cada segmento.
- Propagan sólo el tráfico que tiene que pasar .
- Mantienen una tabla de direcciones.
- No puede haber bucles en la topología lógica:
  - Spanning Tree

3. Bridges: Bridges transparentes



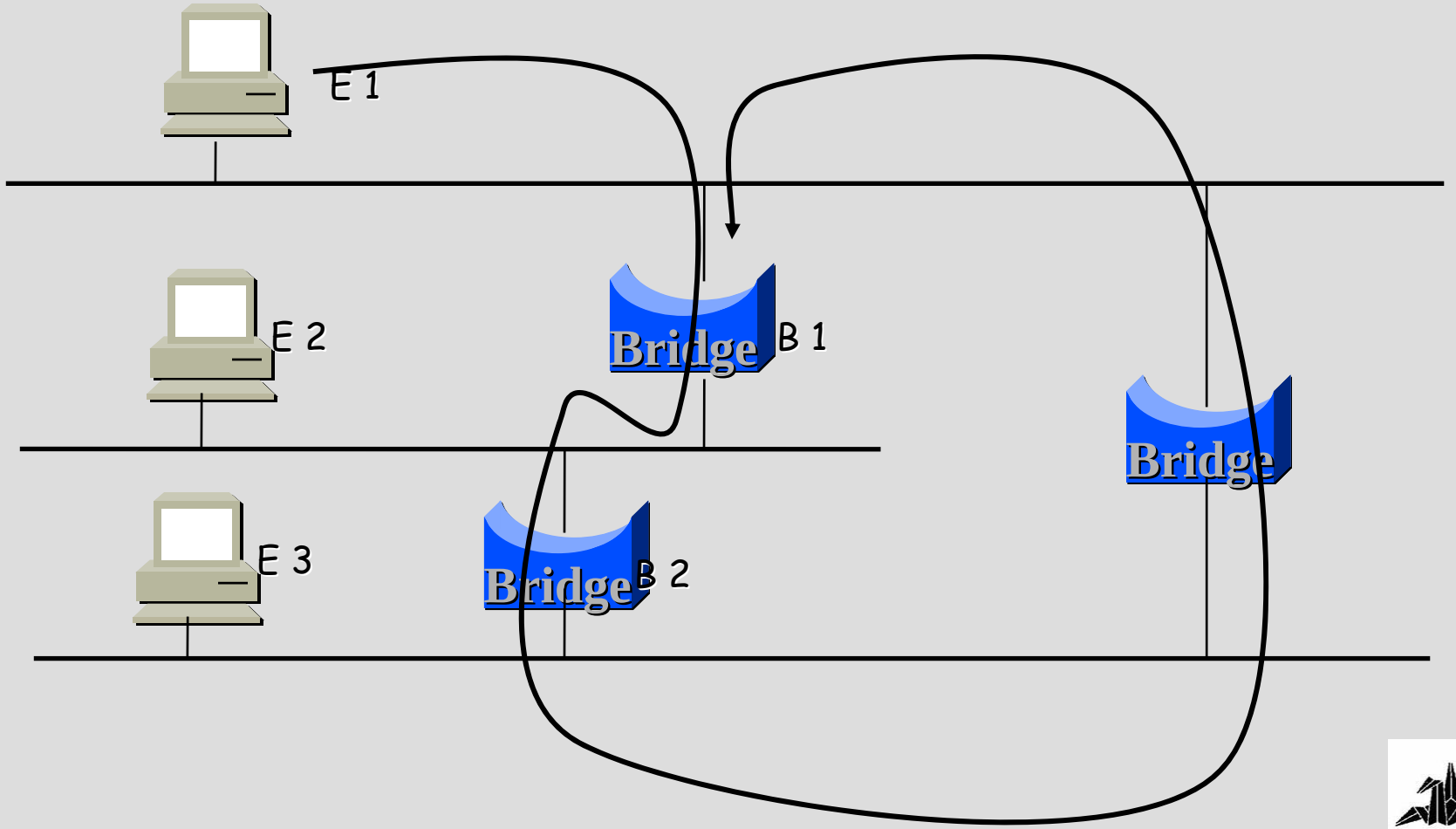
	P1/1	P1/2
E1 –> E2	E1	E2
E3 –> E1	- E1	E2 E3

3. Bridges: Spanning Tree

- **En una topología de Bridge Transparentes no pueden existir bucles.**
- **Los bridges crean un esquema lógico (árbol de expansión)**
- **Spanning tree es un algoritmo para prevenir bucles**
- **Permite tener enlaces de backup.**

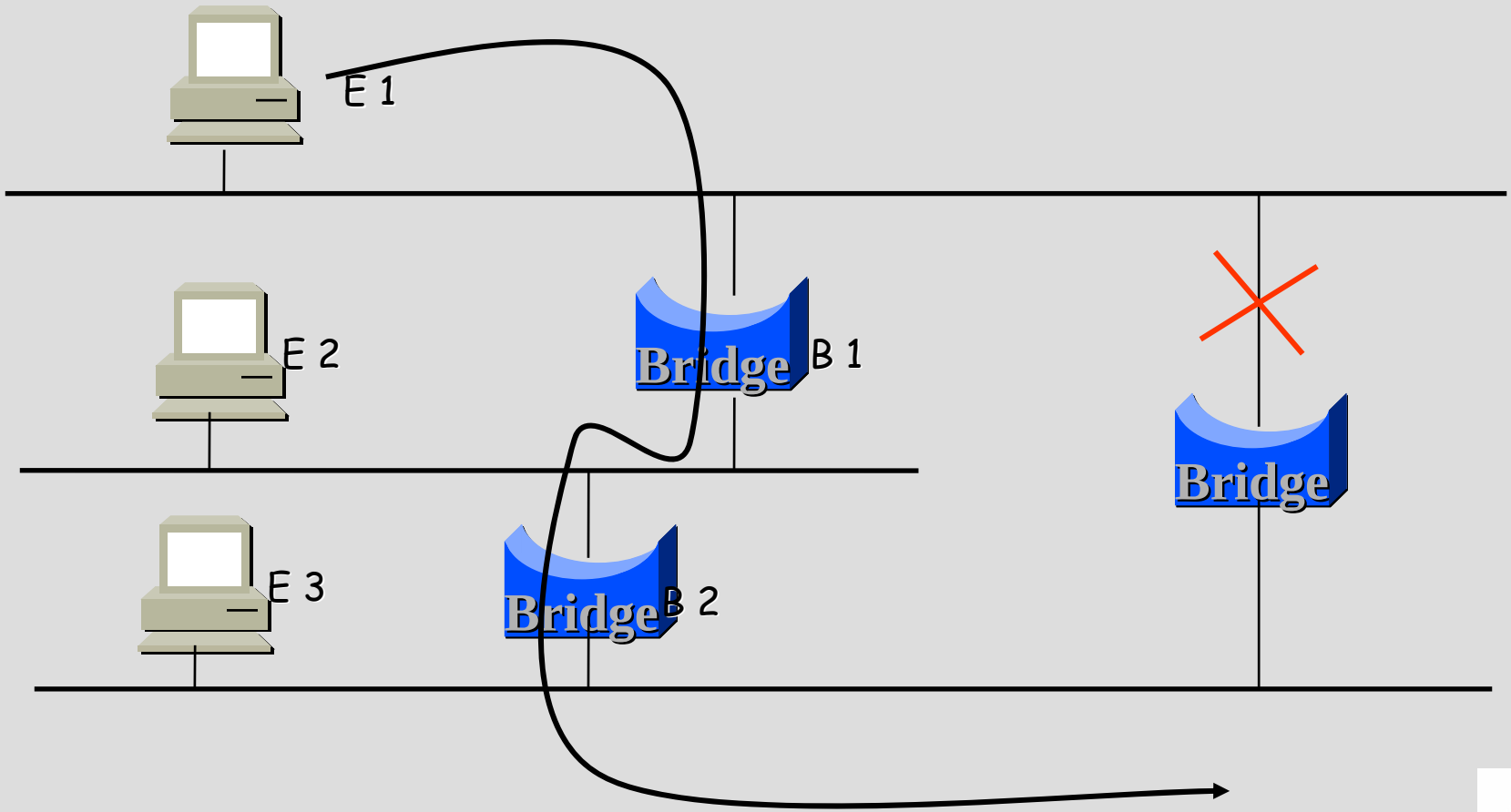
3. Bridges: Spanning Tree

- Red física con bucles



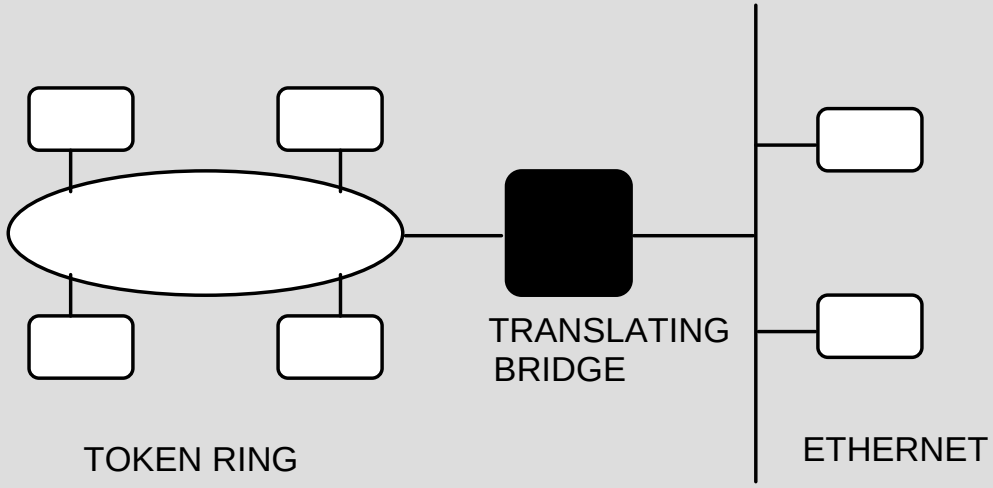
3. Bridges: Spanning Tree

- Red lógica



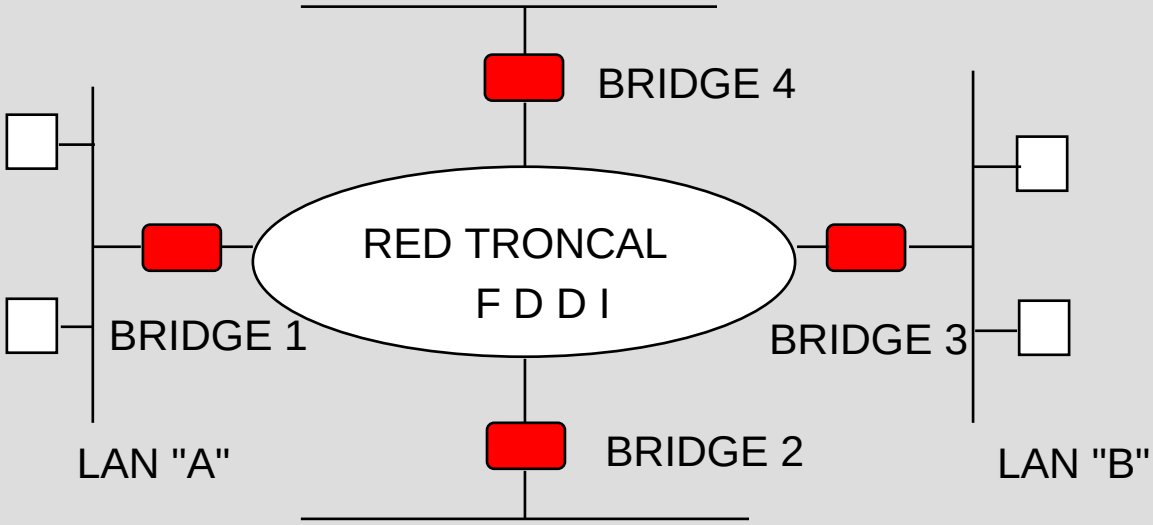
3. Bridges: Translating bridges

• **Proporcionan interconexión entre LANs con diferentes niveles físico y de enlace. Son bridges transparentes especializados:**



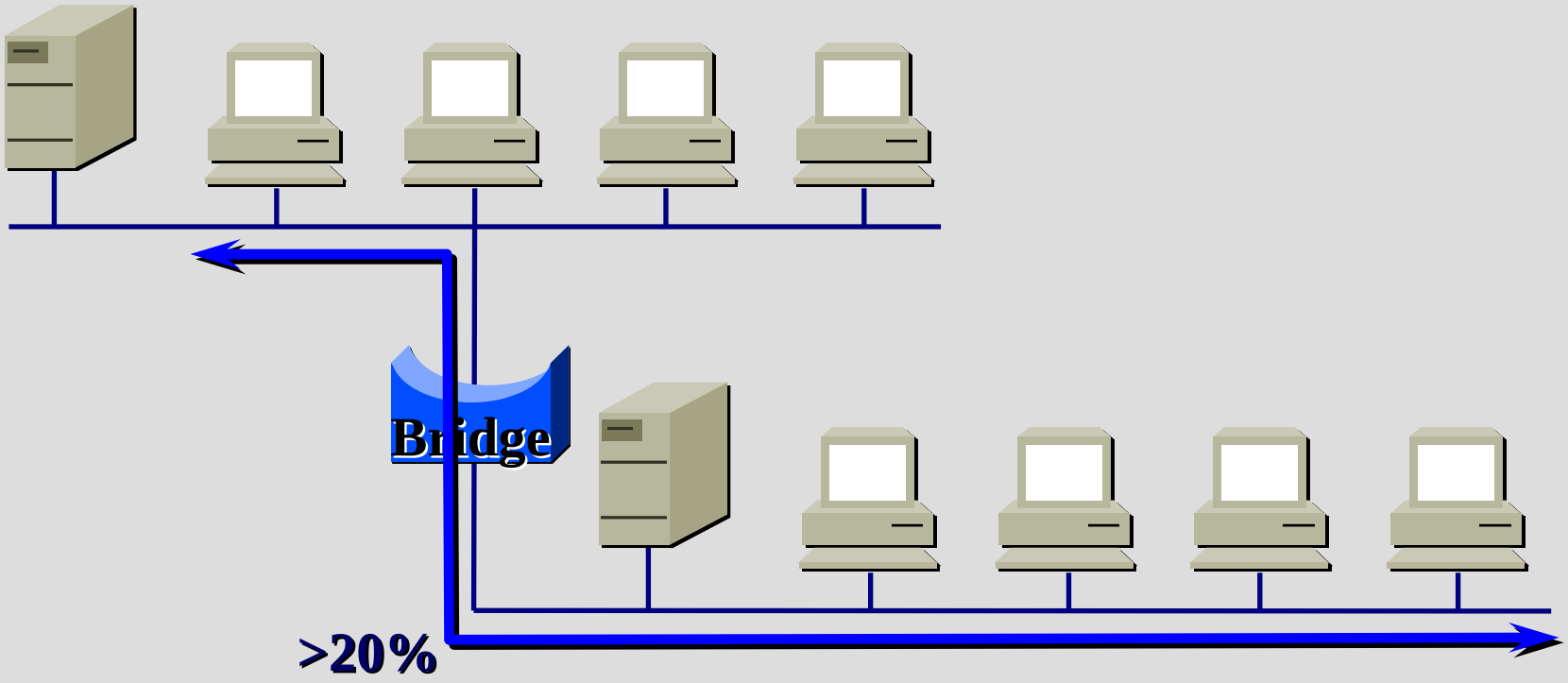
3. Bridges: Bridges encapsuladores

- Se asocian con redes troncales (backbone).
- Pone los mensajes en un "sobre", para su transmisión a través de la red troncal.



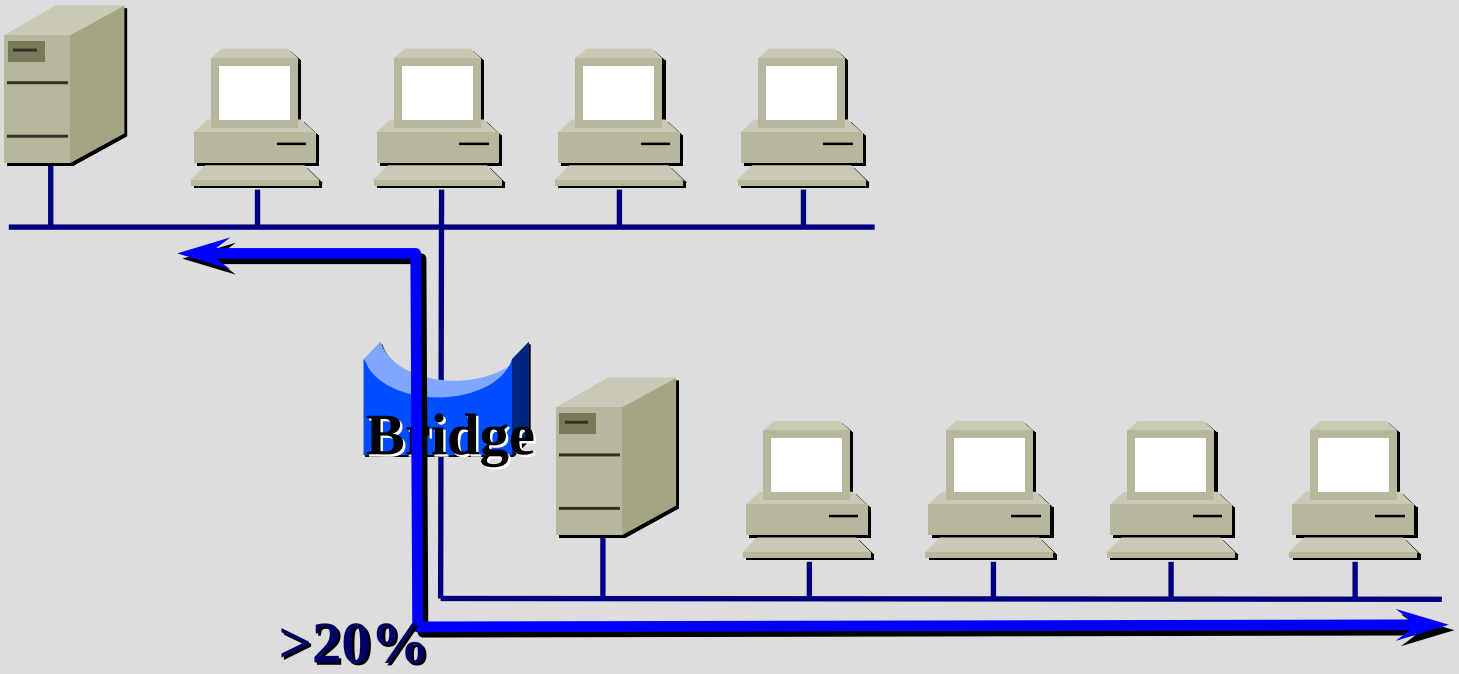
3. Bridges: Redes segmentadas

- Si el tráfico inter-segmento es superior al 20%, debemos plantearnos de nuevo la solución de segmentación.



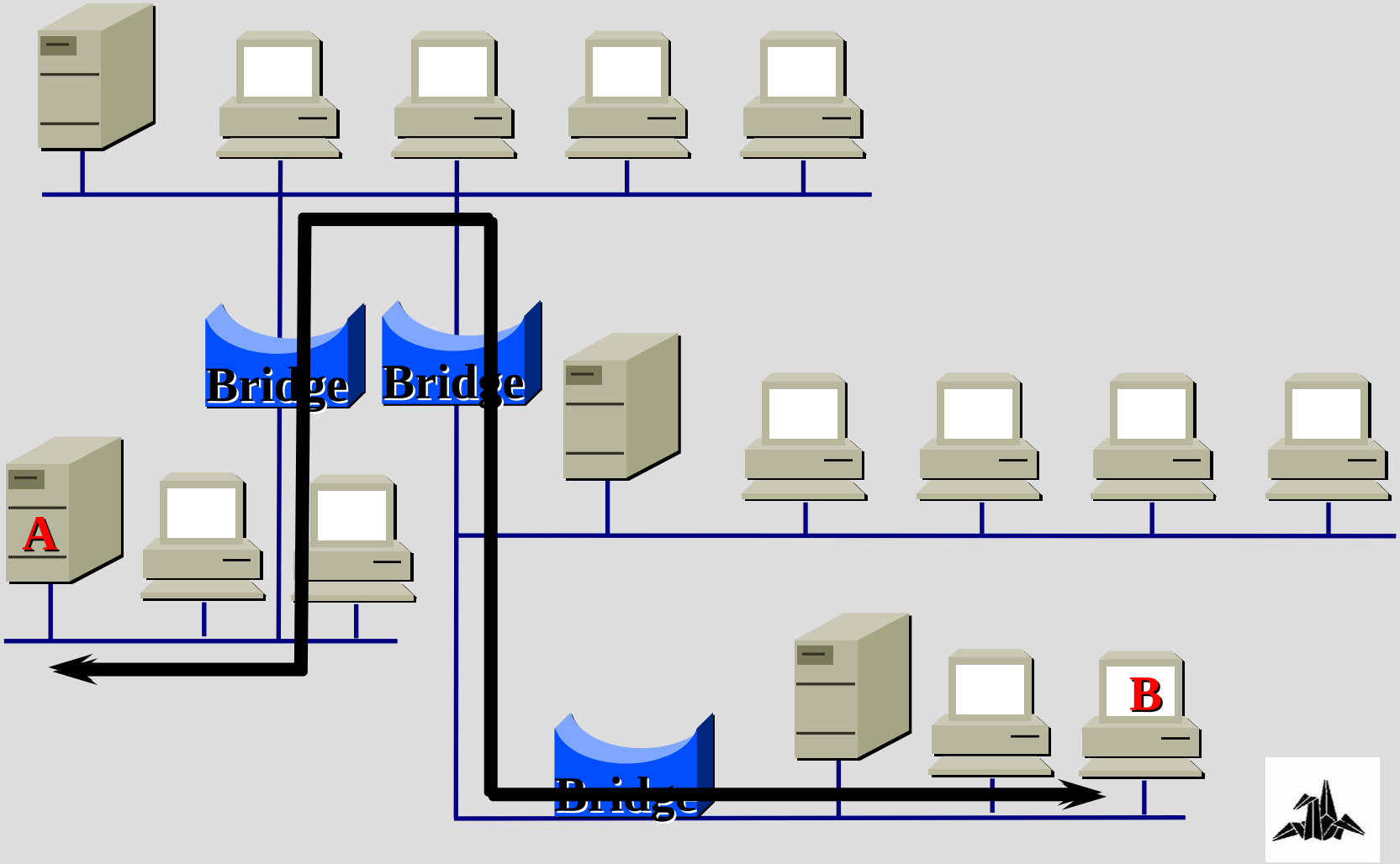
3. Bridges: Redes segmentadas

- El gran problema es el “tráfico transeunte” que atraviesa diferentes segmentos.
- La situación puede empeorar en entornos con mucha segmentación.



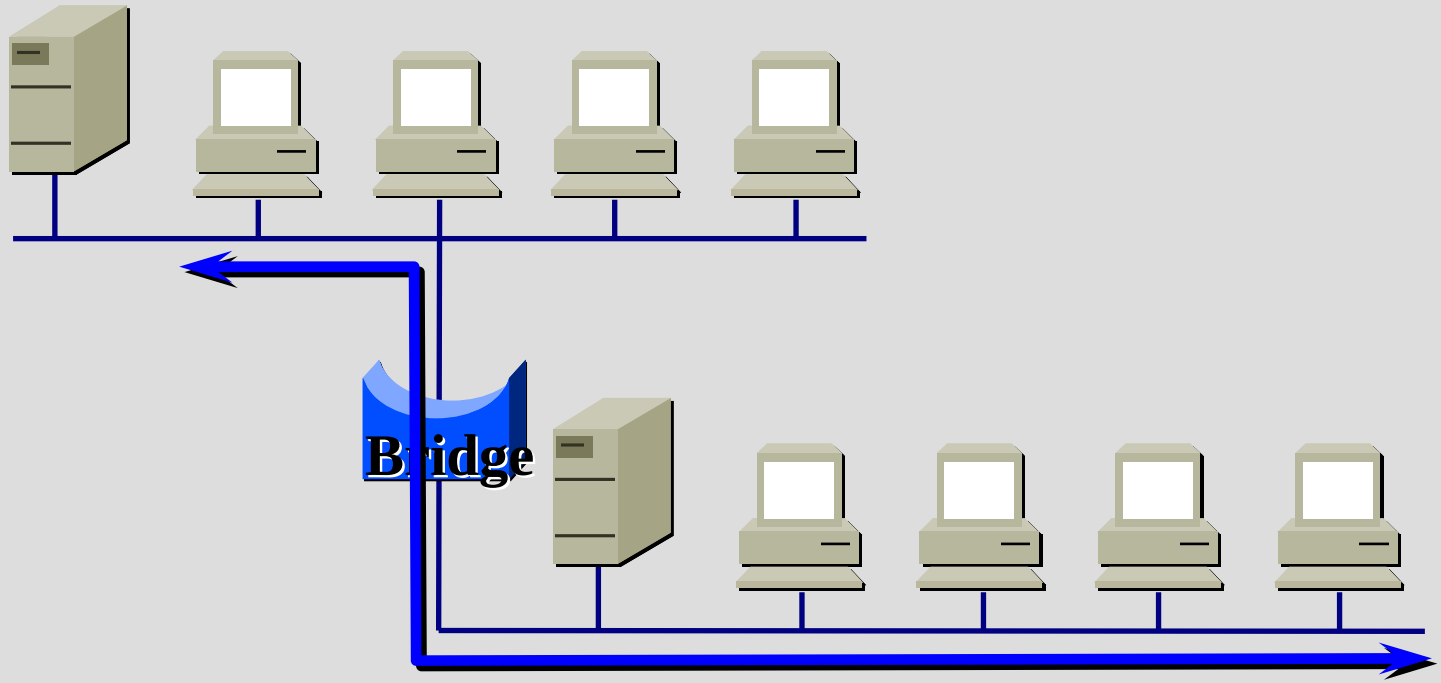
3. Bridges

- El tráfico entre A y B ocupa TODOS los segmentos



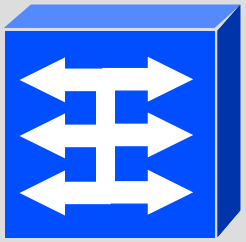
3. Bridges

- **Soluciones.**
  - **Replantear la distribución de los clientes y servidores**
  - **Segmentar más (posible empeoramiento del rendimiento).**
- **Switching Ethernet**



3. Switching: Introducción

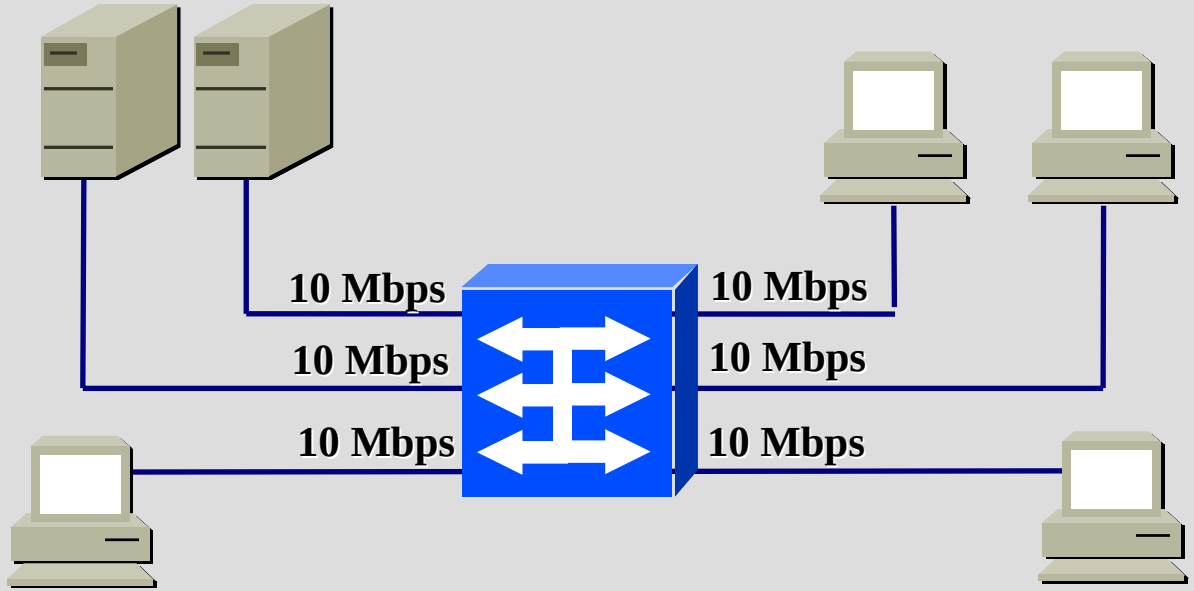
- **Funcionamento**
  - Funciona a nivel 2, como los bridges.
  - Menor latencia
  - Mayor número de interfaces



- **Objectivos LAN switching**
  - Proporcionar TODO el ancho de banda de la LAN a una estación o grupo de estaciones
  - Evitar el tráfico “transeúnte”
  - Disminuir las colisiones
  - Aumentar el ancho de banda agregado
  - Disminuir el número de colisiones

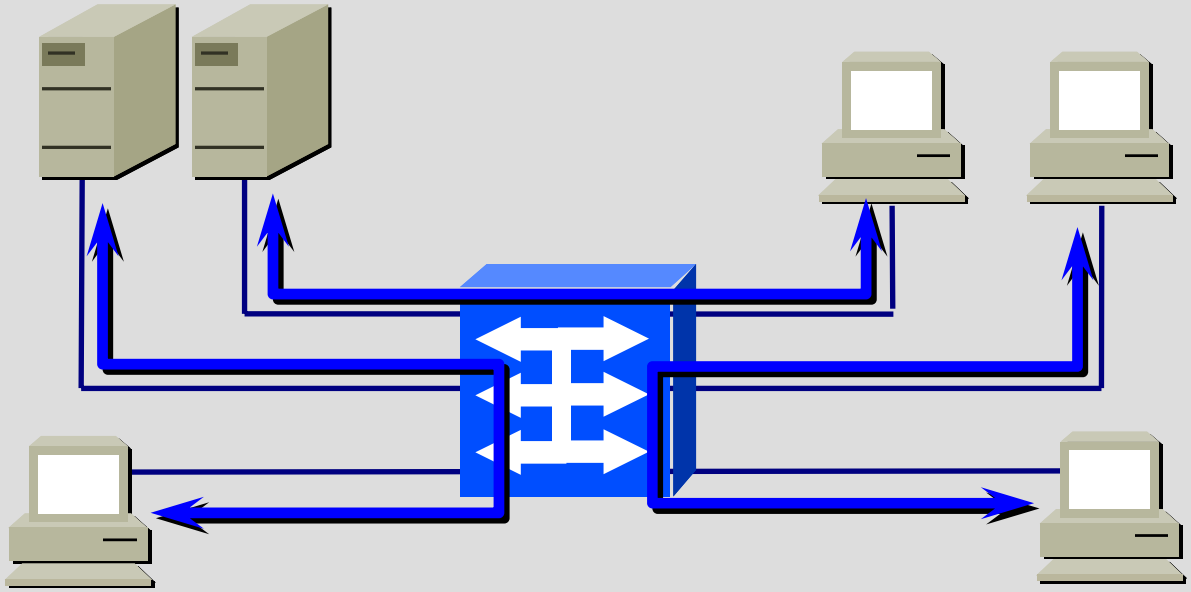
3. Switching: Ancho de banda dedicado

- **Proporciona TODO el ancho de banda de la LAN a una estación o grupo de estaciones.**
  - **Gracias a los mecanismos de commutación del equipo.**



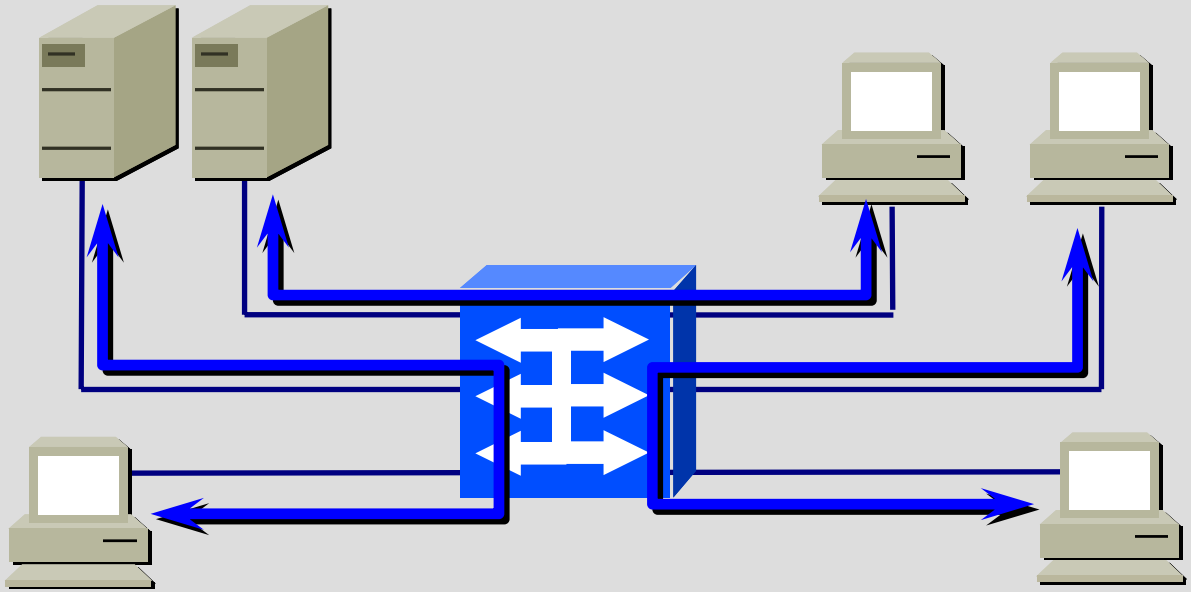
3. Switching: Más ancho de banda agregado

- El commutador permite comunicaciones simultáneas entre diferentes estaciones de trabajo.
  - En el ejemplo, el ancho de banda agregado es de 10 X 3 = 30 Mbps.



3. Switching: Optimización ancho de banda

- Evita el tráfico “transeúnte”
  - El tráfico se dirige DIRECTAMENTE a la estación destino.



3. Switching: Técnicas de Switching

Existen dos técnicas de conmutación:

- **Store & Forward**
- **Cut Through**
  - **Fast Forward switching**
  - **Fragment-Free switching**

3. Switching: Store & Forward

- Cada trama entrante se almacena en un buffer.
- Una vez almacenada, se analiza completamente toda la trama.
- Permite comprobar errores.
- Latencia mayor con paquetes grandes.
- Detección de errores mayor, puesto que se analiza toda la trama.

3. Switching: Cut Through

- También conocido como “on the fly”
- Se omite el paso por un buffer.
- A partir de la cabecera de la trama se toma la decisión de forwarding.
- Se conmuta la trama antes de recibir toda la trama.
- Problema: en caso de error, se transmite
- Menor latencia que en *Store & Forward*.
- Menor control de errores.

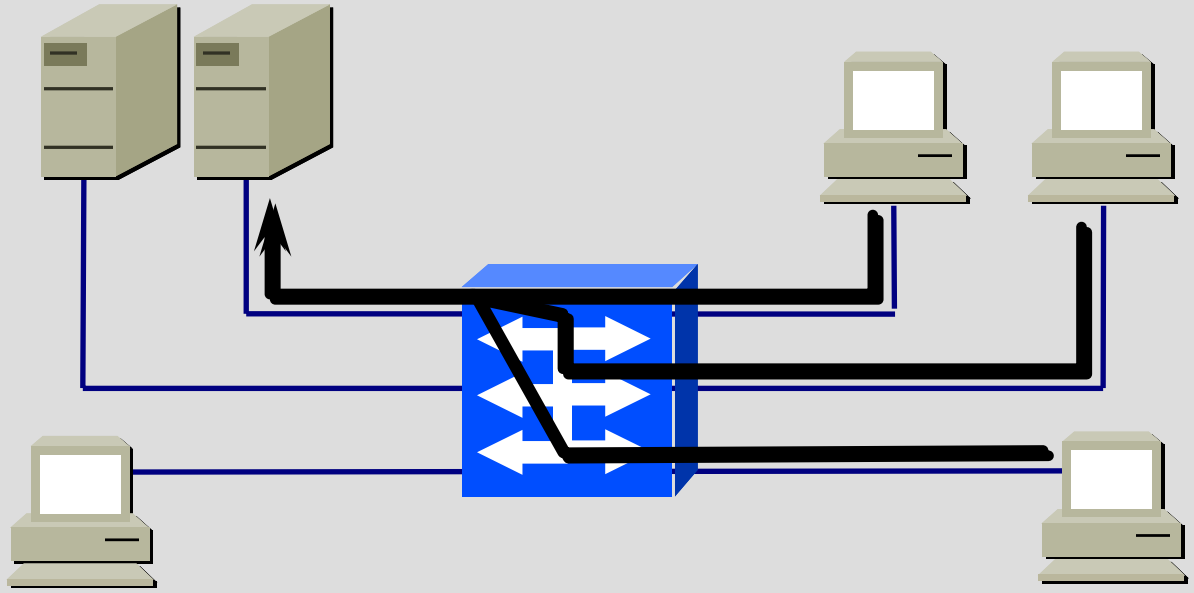
3. Switching: Cut Through

Tipos de conmutación *Cut Through*:

- **Fast Forward:**
  - **Conmuta la trama al leer la dirección MAC destino**
  - **Mínimo control**
  - **Mínima latencia**
- **Fragment-Free:**
  - **Filtra fragmentos de colisión**
  - **Filtra paquetes menores de 64 bytes**

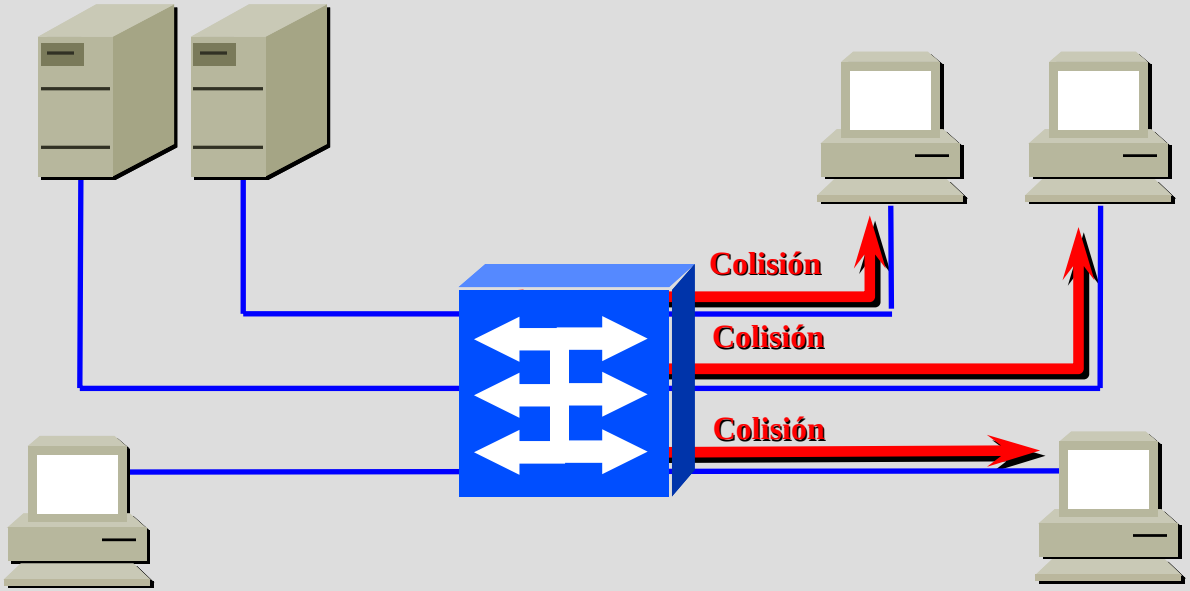
3. Switching: Mecanismos de congestión

- Si muchas estaciones se dirigen simultáneamente al mismo servidor, se pueden producir situaciones de congestión.



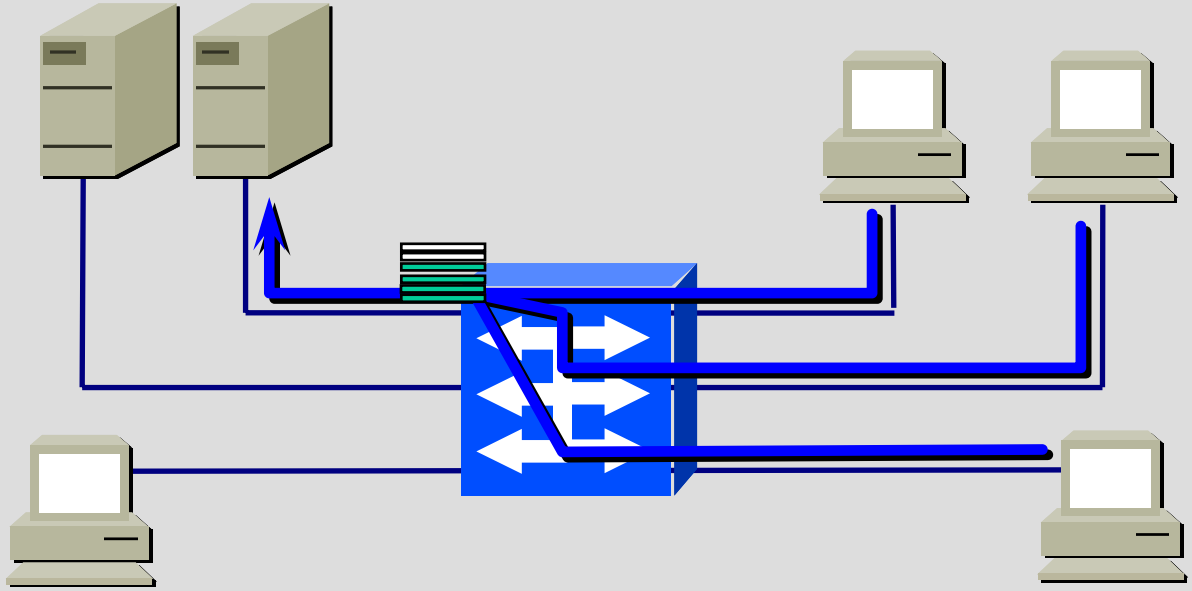
3. Switching: Backpressure

- En situaciones de congestión el switch genera colisiones.
  - De esta manera las estacions generadoras del tráfico dejarán de enviar información.



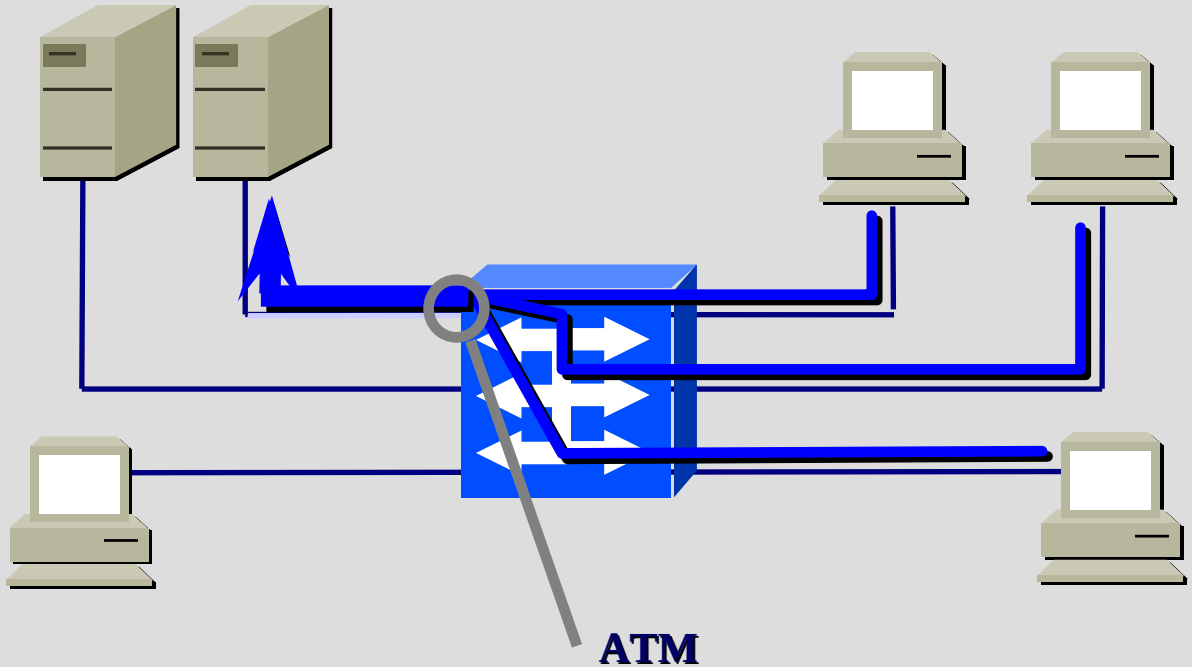
3. Switching: Buffers internos

- **El tráfico al cual no se le puede dar salida se almacena en un buffer.**
  - **Las situaciones de congestión suelen ser puntuales.**
  - **Los buffers actúan como "un colchón" absorbiendo estos "picos" de tráfico.**



3. Switching: Interfaces de alta velocidad

- Mayor ancho de banda en los servidores.
  - La suma de los tráficos entrantes es muy improbable que sature la interface del servidor.



ATM
Fast Ethernet
Ethernet Full Duplex

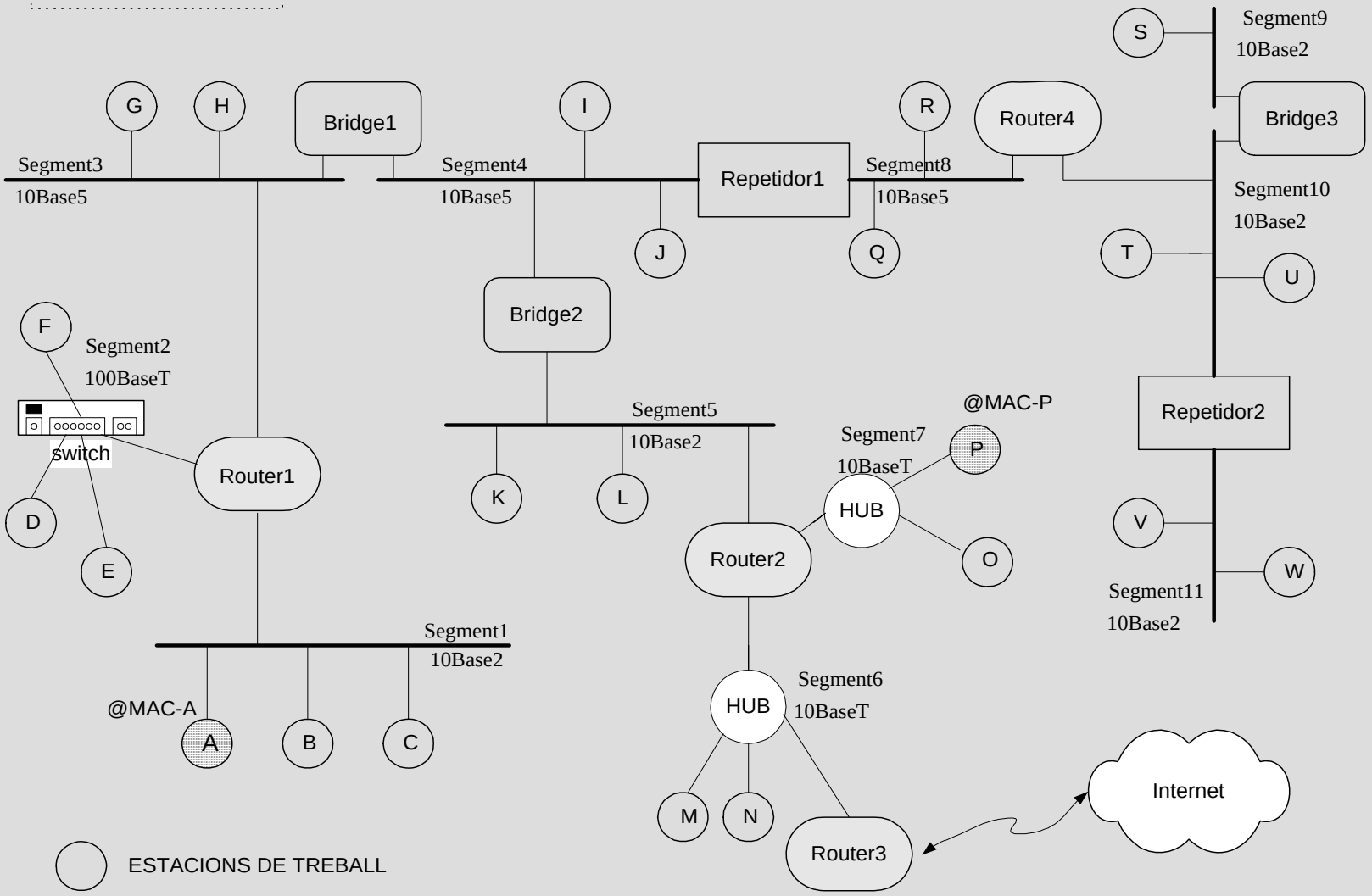
Tecnología de Redes de Comunicaciones

4. Casos prácticos

4. Caso práctico 1

③ ¿ Cuántos dominios de colisión hay en este escenario?

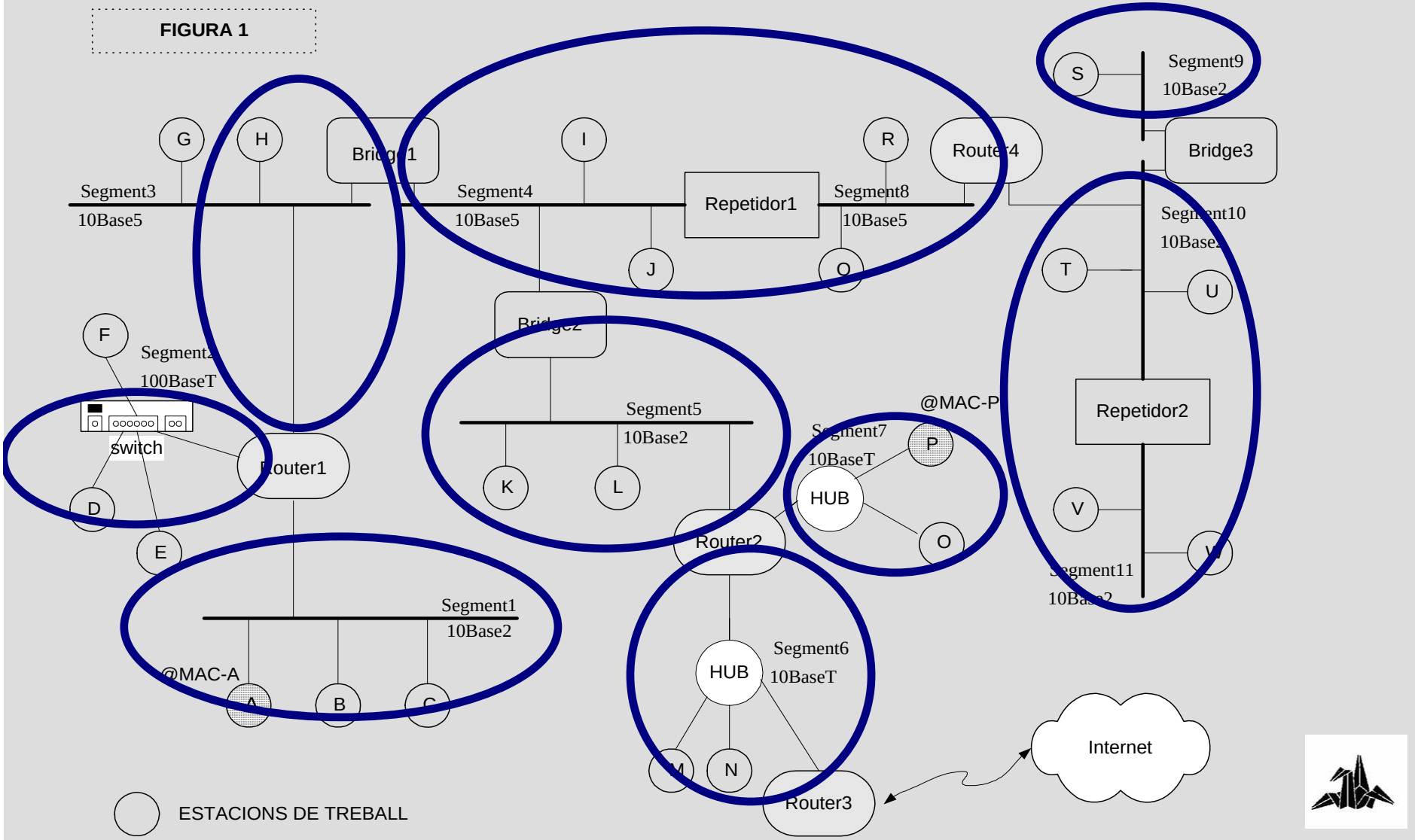
FIGURA 1



4. Caso práctico 1

③ Dominios de colisión:

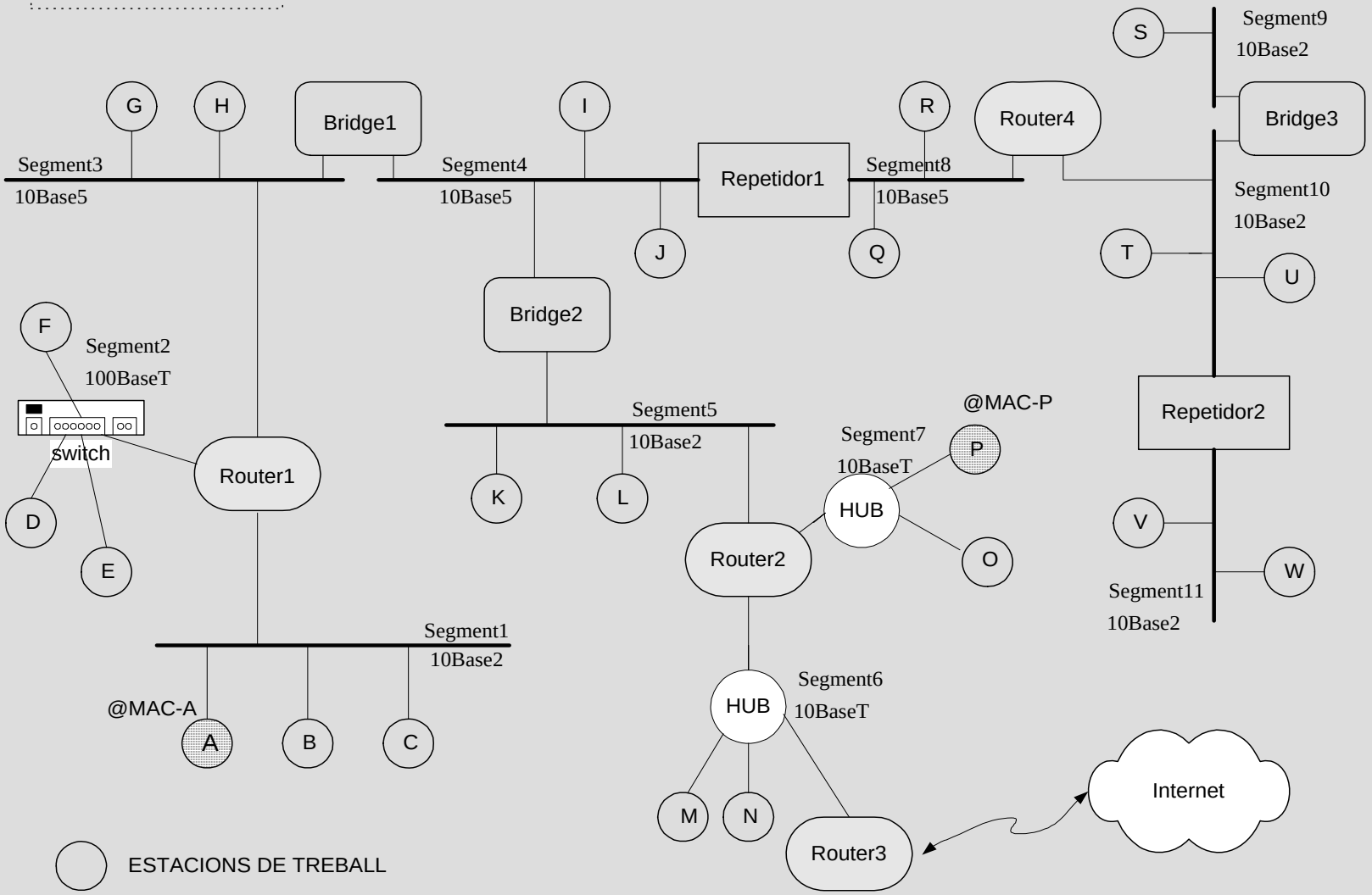
FIGURA 1



4. Caso práctico 1

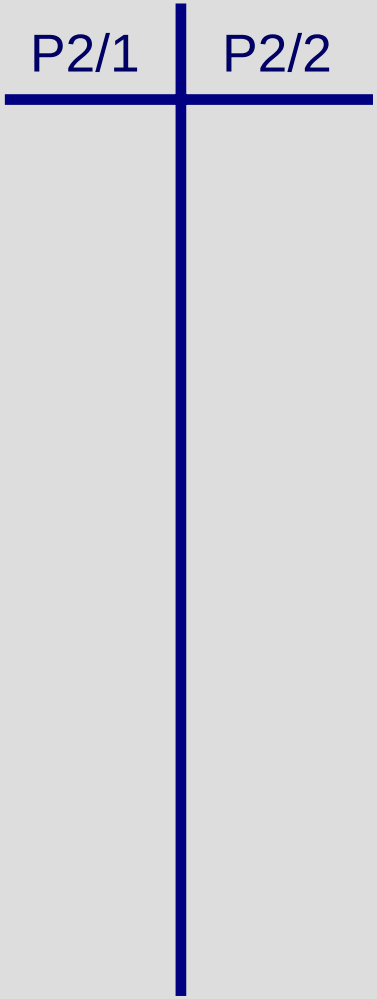
③ ¿Tabla de direcciones del Bridge 2?

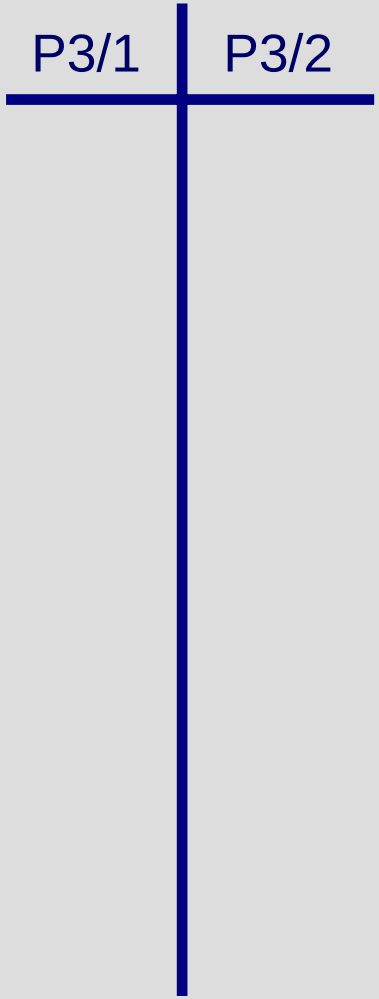
FIGURA 1



4. Caso práctico 1

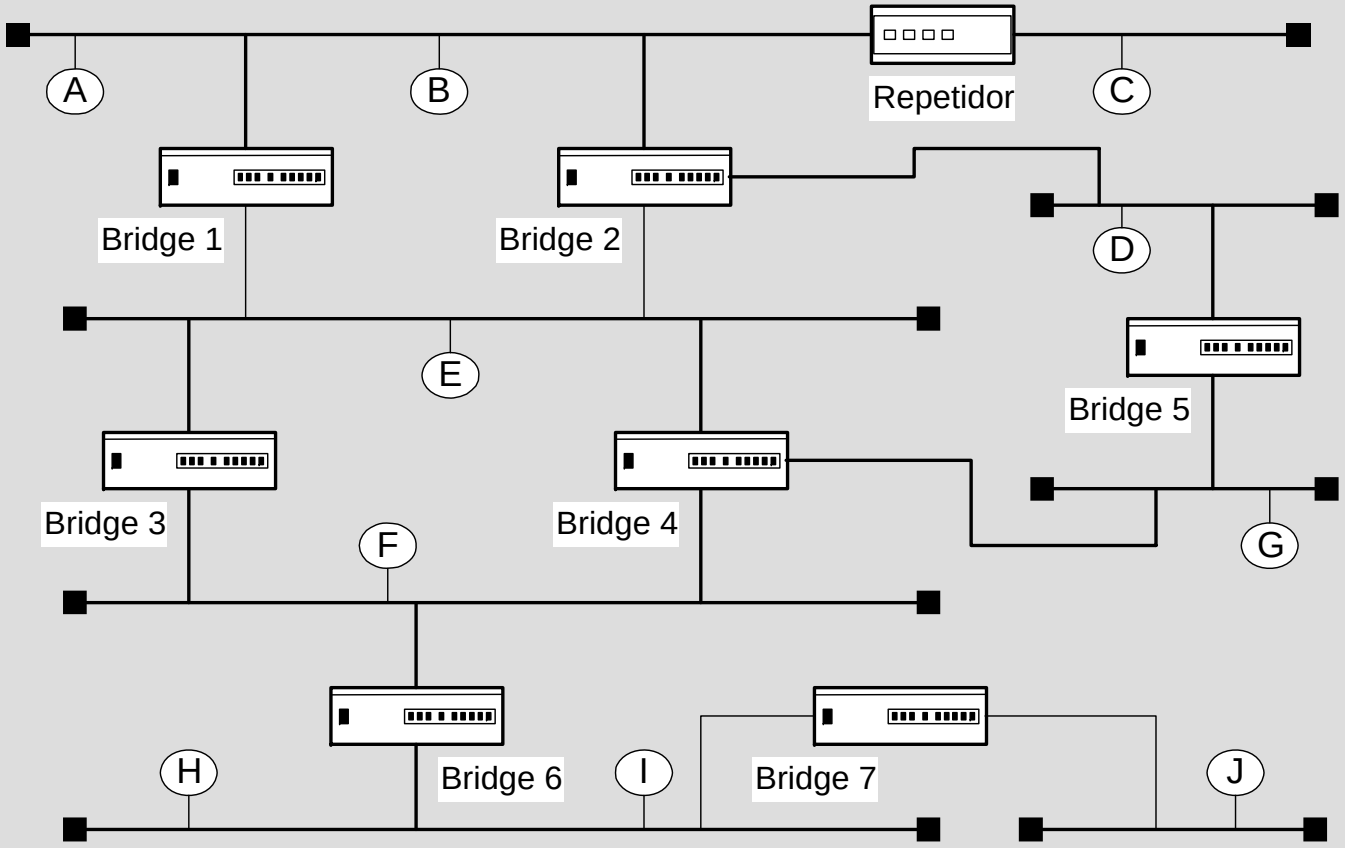
- ¿Tabla de direcciones del Bridge 2?
- ¿Y del Bridge 3?





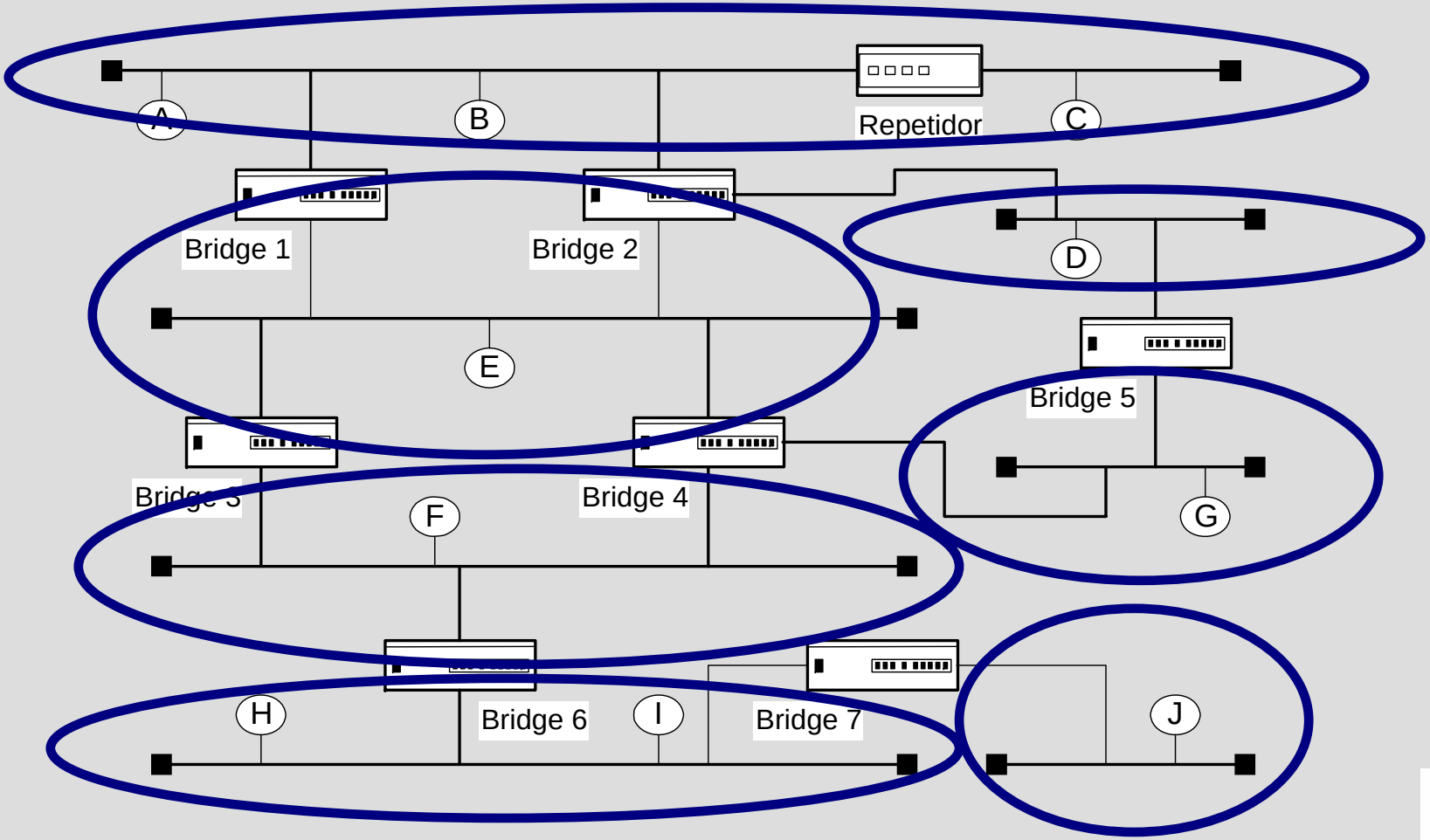
4. Caso práctico 2

- ¿ Cuántos dominios de colisión hay en este escenario?



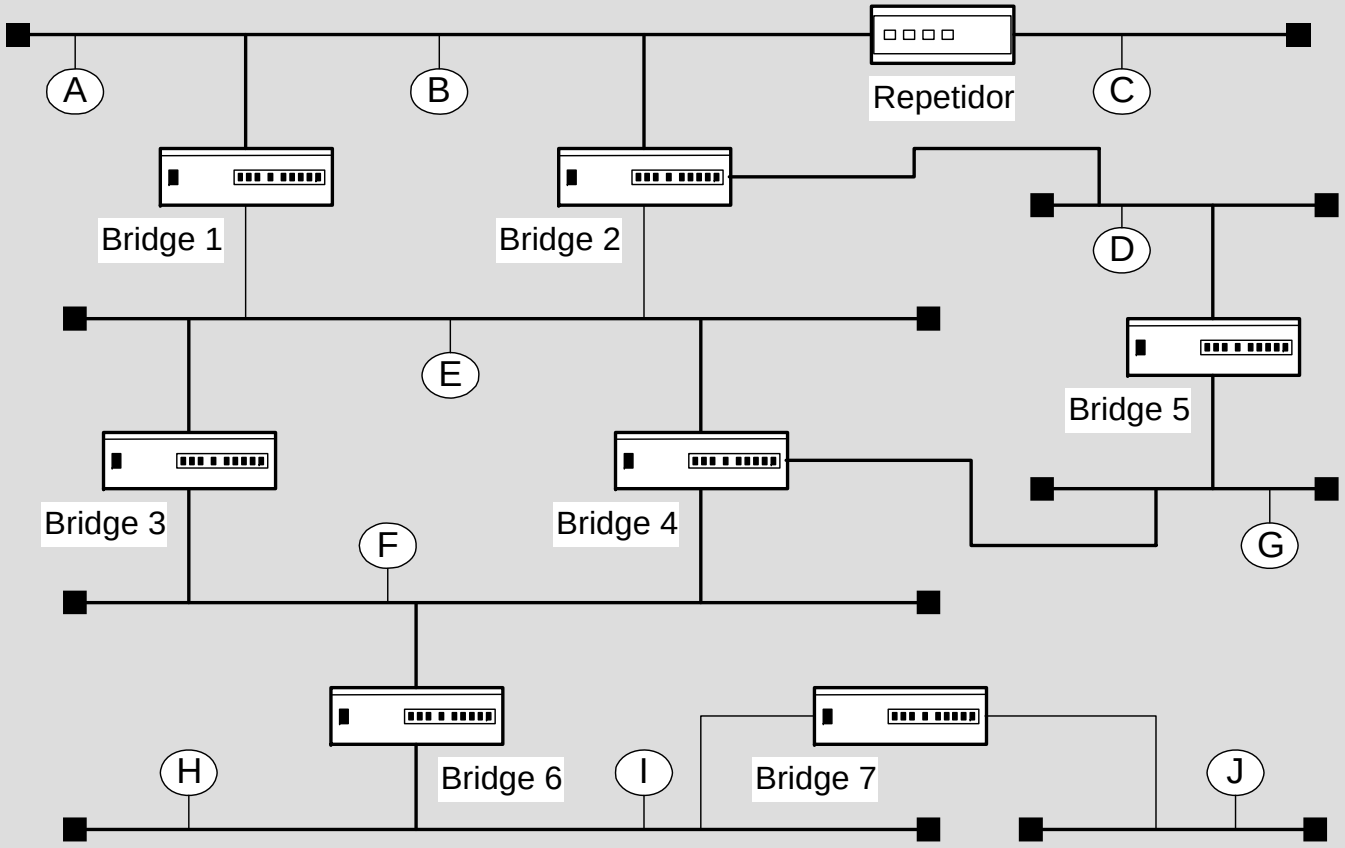
4. Caso práctico 2

- **Dominios de colisión:**



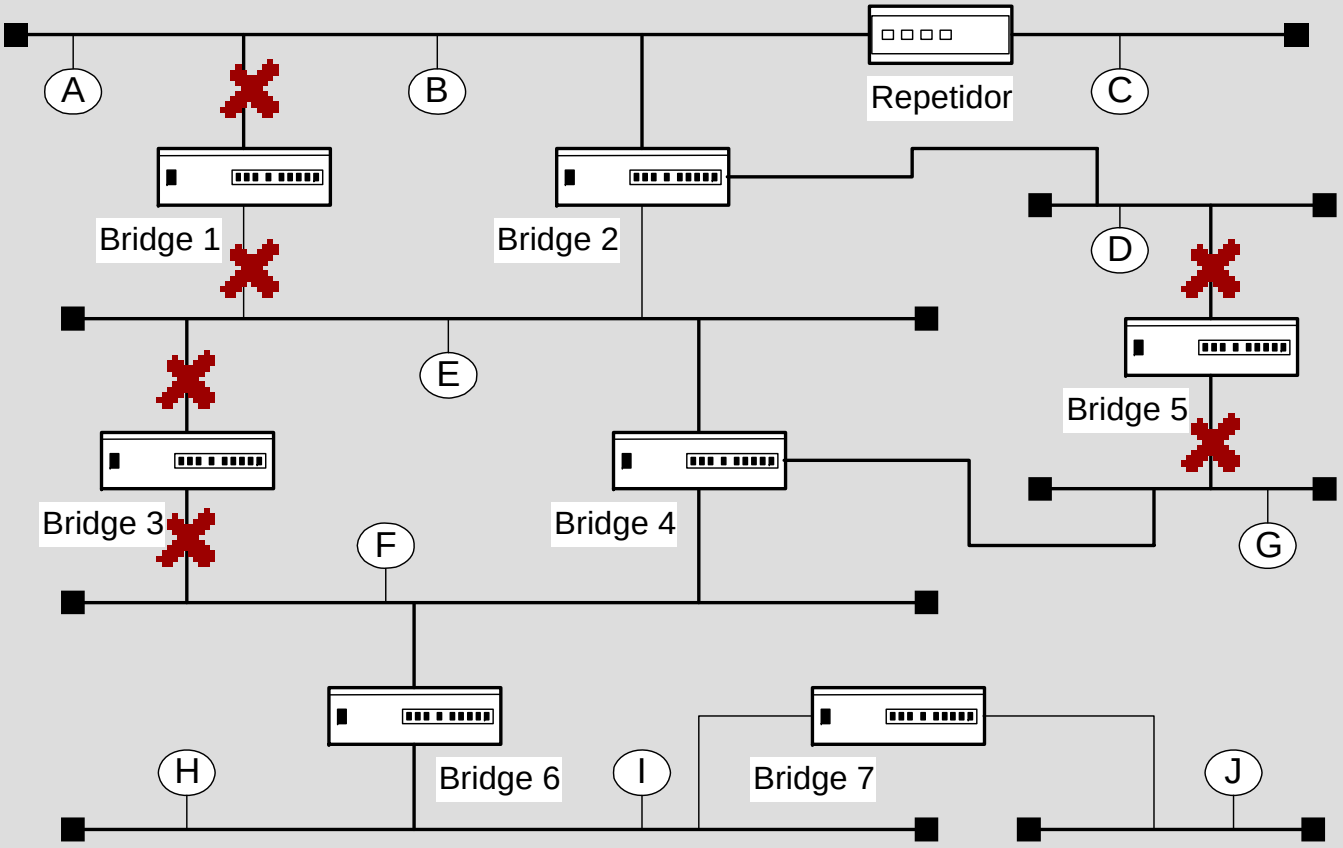
4. Caso práctico 2

- ¿Tabla de direcciones del bridge 6?



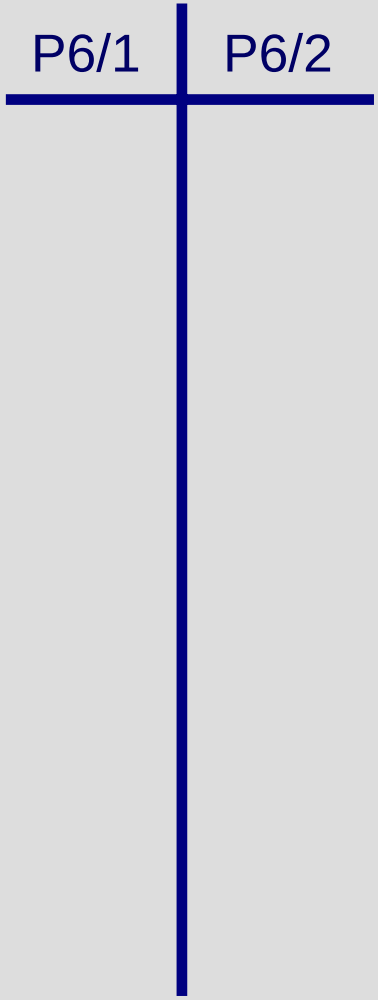
4. Caso práctico 2

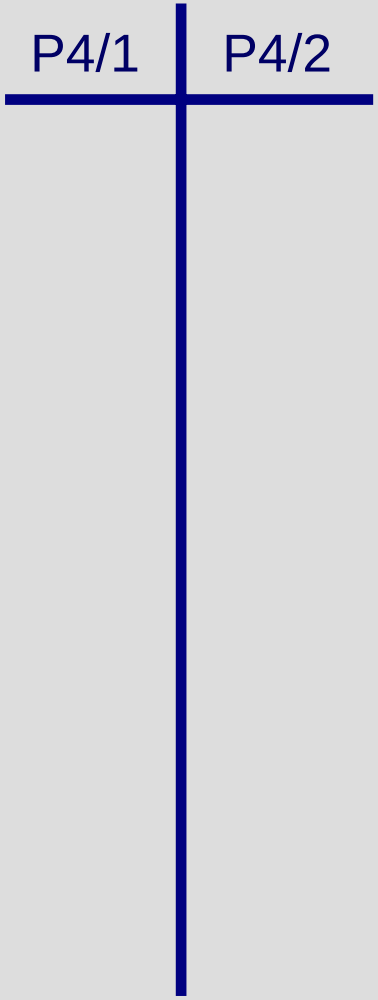
- ¿Tabla de direcciones del bridge 6?
  - Spanning Tree necesario!



4. Caso práctico 2

- ¿Tabla de direcciones del Bridge 6?
- ¿Y del Bridge 4?





FIN DE LA SESIÓN

Gracias por su atención!

Tecnologías de Redes
“Entorno TCP/IP”

www.shellsec.net

Xavier Vila i Espinosa

Ing. Técnico en Telecomunicaciones – Esp. Telemática

ÍNDICE DE LA SESIÓN

OBJETIVOS DE LA SESIÓN

- **Introducción a los conceptos referentes a la arquitectura de comunicaciones TCP/IP, así como el análisis y funcionamiento de la capa de red de esta arquitectura.**
- **Estudio de distintos protocolos de nivel de red:**
  - **IP**
  - **ICMP**
  - **ARP**
- **Descripción de los elementos de interconexión a nivel de red.**

PROGRAMA DE LA SESIÓN

- 1.- Entorno TCP/IP.
  - Definición y características
  - Modelo de referencia OSI – TCP/IP
  - Estructura de los datos
- 2.- Nivel IP
  - Direccionamiento IP
  - Protocolo IP y cabecera
  - Subnetting
  - Direccionamiento IP: Problemas y soluciones
  - CIDR
  - VLSM
  - IPv6
- 3.- Protocolos de nivel de red
  - ARP
  - ICMP
- 4.- Elementos de interconexión de nivel de enlace
  - Routers
  - Switching y Routing
- 5.- Casos prácticos

Tecnología de Redes de Comunicaciones

Entorno TCP / IP

1. Entorno TCP / IP

- **Paquete de protocolos de comunicación de datos formado por un conjunto de más de 100 protocolos**

- **Los dos protocolos más importantes de este paquete le dan el nombre**

TCP	Transmission Control protocol
IP	Internet protocol

1. Entorno TCP / IP

- **1969: DARPA (Defense Advanced Research Project Agency) crea la red experimental ARPANET**
- **1975:**
  - **ARPANET se convierte en una red operativa**
  - **Es administrada por la DCA (Defense Communications Agency)**
  - **Interconecta un gran número de bases militares, oficinas gubernamentales, universidades y centros de investigación**

1. Entorno TCP / IP

- **1983:**
  - **TCP/IP se adopta como Military Standard (MIL STD)**
  - **Para implantar TCP/IP fácilmente en ARPANET, DARPA fundó BBN para desarrollar TCP/IP en entorno UNIX de Berkeley**
  - **ARPANET se divide en:**
    - **MILNET**
    - **ARPANET**
  - **Se añade a la red la NSF y algunas universidades**
  - **Internet = MILNET + ARPANET + NFSnet + LAN's + ….**
- **1989:**
  - **CERN desarrolla el lenguaje de hipertexto HTML y el protocolo HTTP: nace la World Wide Web**
- **1990: desaparece ARPANET**
- **Hoy Internet engloba redes de ámbito mundial**

1. Entorno TCP / IP

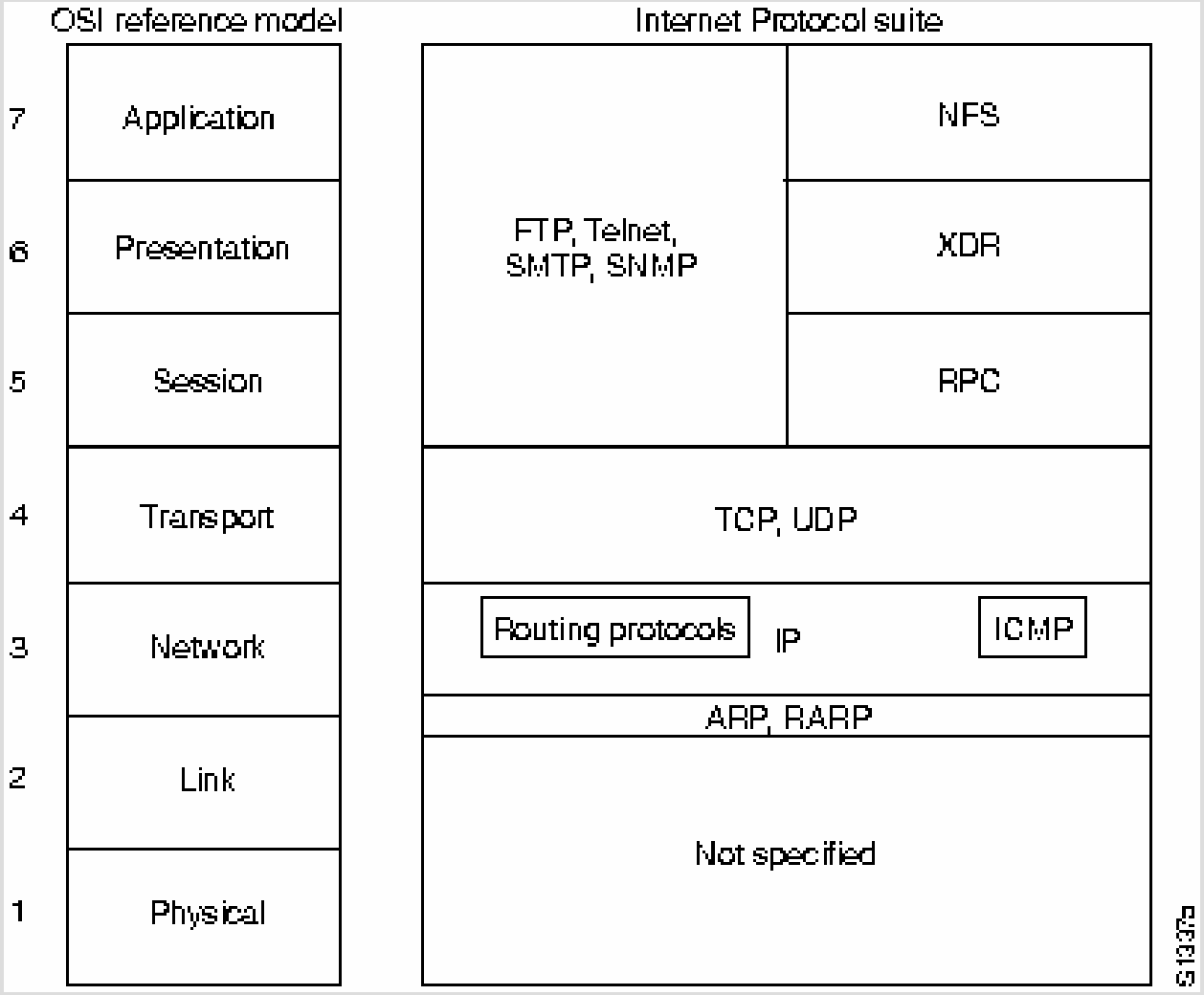
- **TCP/IP satisface en el momento adecuado la necesidad de comunicaciones de datos a nivel mundial debido a que:**
- **Son protocolos estándares abiertos**
  - **Ampliamente difundidos.**
  - **Independientes de sistemas operativos.**
  - **Independientes de la arquitectura de red: X.25, Ethernet, Token Ring, RTC, punto a punto, etc.**

1. Entorno TCP / IP

- **Dispone de un esquema de direccionamiento que permite asignar una dirección única a cualquier dispositivo en un entorno de redes intercomunicadas a nivel mundial.**
- **Dispone de protocolos de alto nivel para servicios de usuarios ampliamente implantados.**

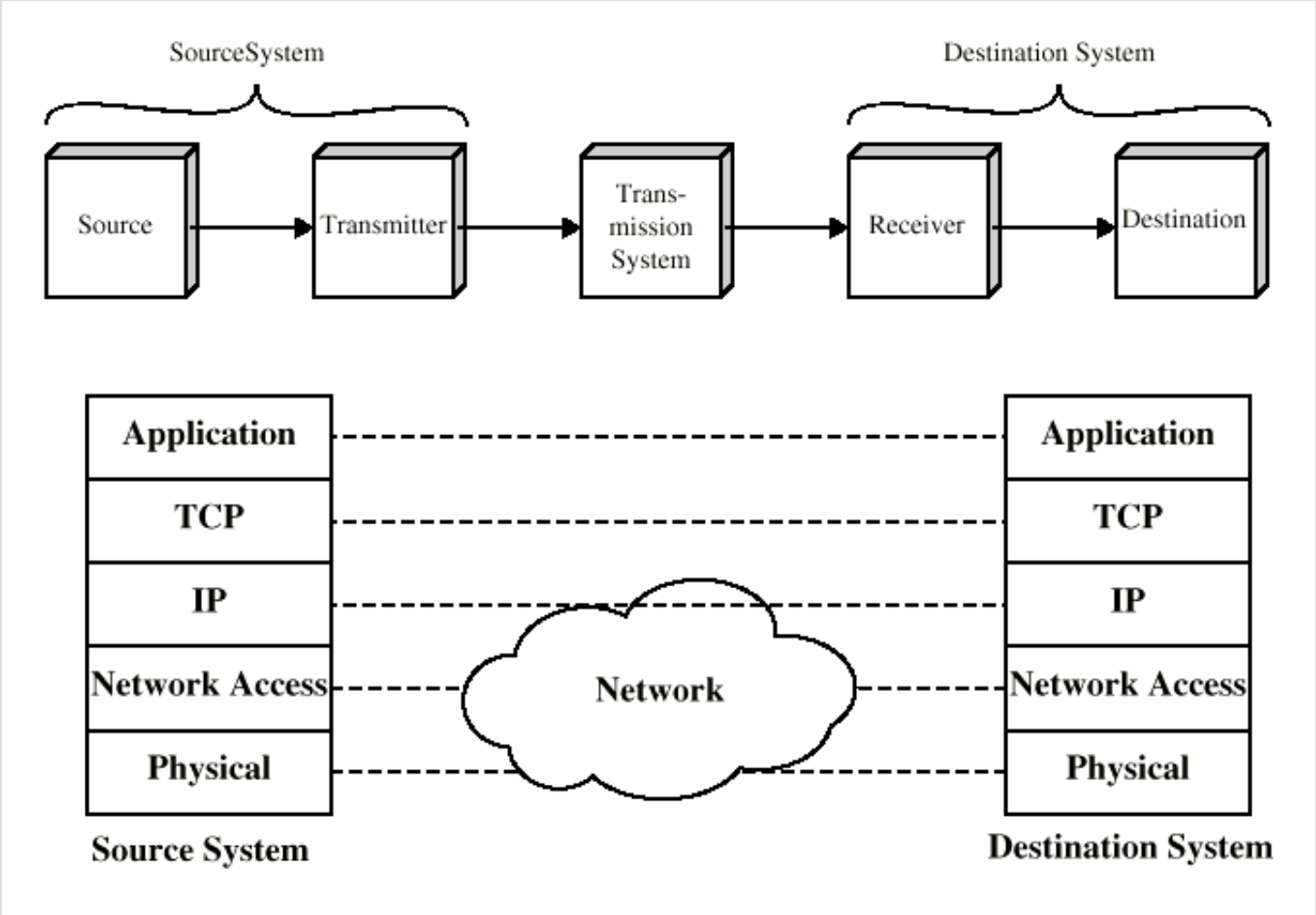
1. Entorno TCP / IP

Modelo de referencia OSI – TCP/IP



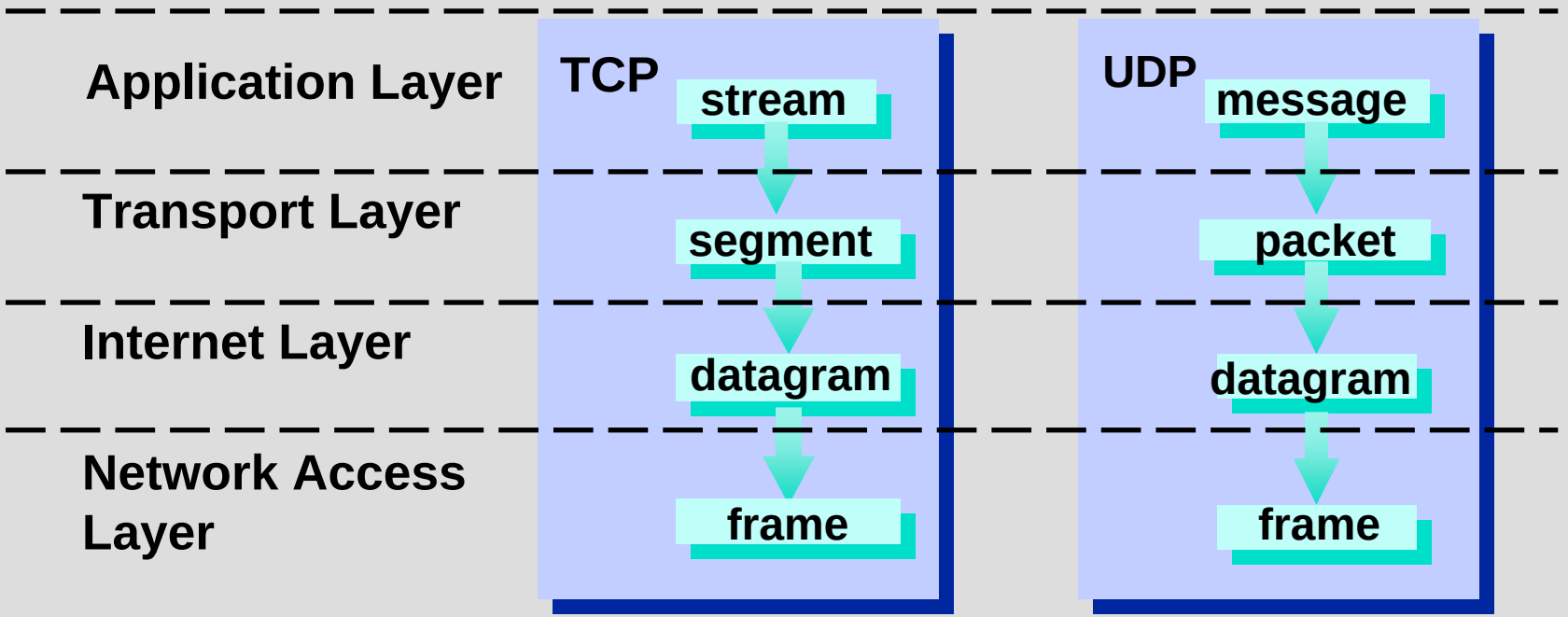
1. Entorno TCP / IP

Modelo de referencia OSI – TCP/IP



1. Entorno TCP / IP

Estructura de los datos



Tecnología de Redes de Comunicaciones

Nivel IP

2. Nivel IP

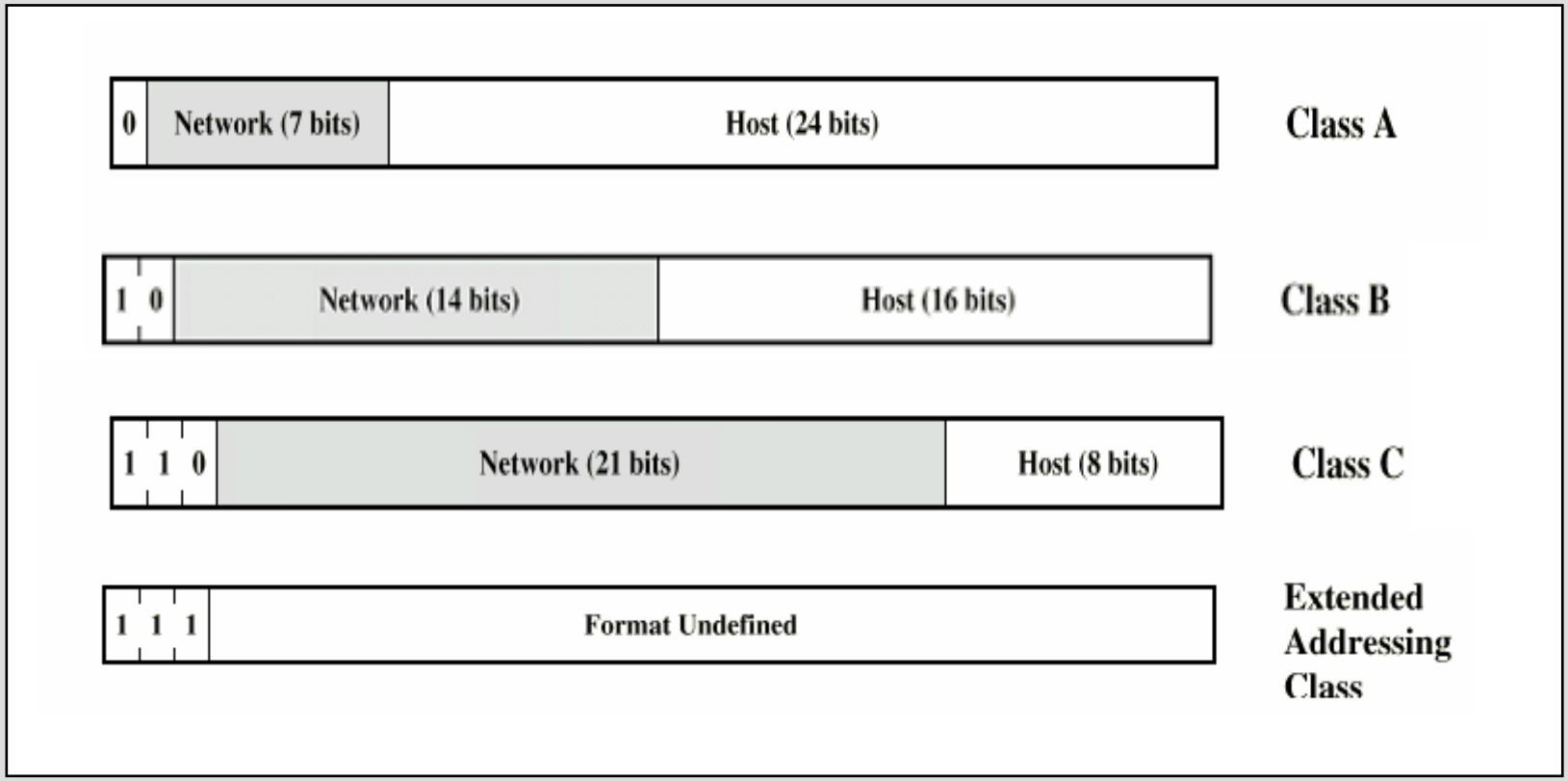
Direcciones IP (Classful addressing)

- **Se aplican a interfícies de red.**
- **Campo de 32 bit formado por:**
  - **Identificador de red.**
  - **Identificador de host.**
- **Clases de Direcciones:**

	Primeros bits	Ident. red	Ident. host	Primer byte
A	0	7 bits	24 bits	menor que 128
B	10	14 bits	16 bits	128 - 191
C	110	21 bits	8 bits	192 - 223
D	111	Identifica un conjunto de hosts que comparten un protocolo		

2. Nivel IP

Direcciones IP



2. Nivel IP

Direcciones IP

- **Direcciones reservadas = Direcciones privadas**
  - **10.0.0.0 hasta 10.255.255.255**
  - **172.16.0.0 hasta 172.31.255.255**
  - **192.168.0.0 hasta 192.168.255.255**
- **Para uso privado**
- **Para acceder a Internet, es necesaria la traducción de direcciones : NAT (*Network Address Translation)***
- **Seguridad**

2. Nivel IP

Direcciones IP

- **Otras direcciones reservadas**
  - **Identificador de red** **0**
  - **Identificador de red** **127.0.0.0**
    - **loopback address** **127.0.0.1**
    - **Permite direccionar un host local como si fuera remoto**
  - **Identificador de host** **0**
    - **Ej: 26.0.0.0** **Identifica la red 26 (clase A)**
  - **Identificador de broadcast** **255**
    - **Ej: 128.66.255.255** **dirección broadcast en la red 128.66.0.0**

2. Nivel IP

Protocolo IP

- **RFC 791 *Internet Protocol***
  - **Datagrama: Unidad básica de transmisión en las redes Internet.**
  - **Esquema de direccionamiento**
  - **Encaminamiento de datagramas a hosts remotos.**
  - **Fragmentación y reensamblaje de datagramas.**
- **IP es un protocolo no orientado a conexión**
- **Funciones realizadas en protocolos de nivel superior:**
  - **Establecimiento de conexión para aplicaciones que requieren servicios orientados a conexión.**
  - **Detección y recuperación de errores.**

2. Nivel IP

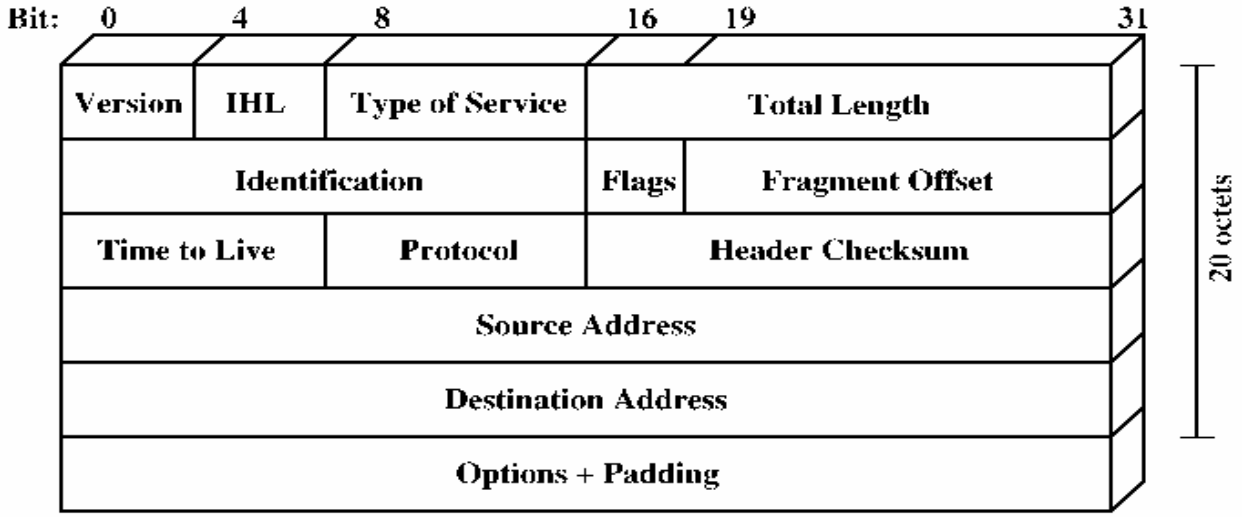
Protocolo IP

- **Datagrama IP**

2. Nivel IP

Protocolo IP

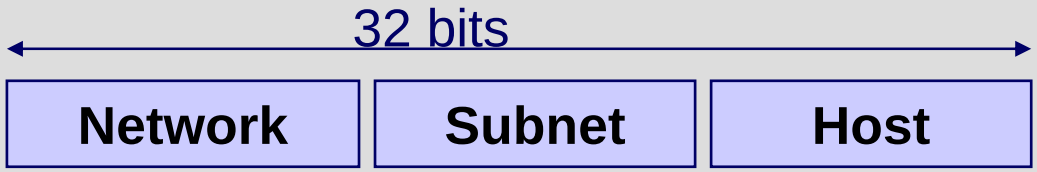
- **Cabecera IP**



2. Nivel IP

Subnetting

- **Problema: Espacio de direcciones poco aprovechado.**
- **Solución:**
  - **Dividir grandes redes en redes más pequeñas.**
  - **Crear otra sección en la dirección IP: subred.**
- **Máscara de subred**
  - **Permite diferenciar la dirección de la red y subred respecto a la dirección del host**



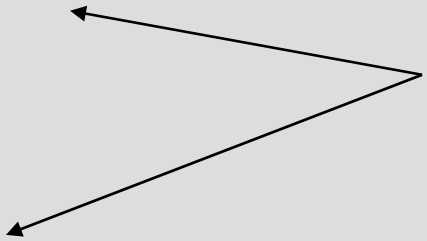
Netmask: 1 1 1 1 ……1 1 1 0 0 0 …....0 0

2. Nivel IP

Subnetting

- **Máscaras por defecto en clases IP**
  - **Clase A: 255.0.0.0 (8 bits)**
  - **Clase B: 255.255.0.0 (16 bits)**
  - **Clase C: 255.255.255.0 (24 bits)**

- **Ejemplo:**
  - **172.16.5.20 / 255.255.0.0**
    - **Red: 172.16.0.0**
    - **Host: 5.20**
  - **10.1.14.100 / 255.0.0.0**
    - **Red: 10.0.0.0**
    - **Host: 1.14.100**



2. Nivel IP

Subnetting: Ejemplos

- **Dirección IP:** **172.24.100.45**
- **Máscara de subred:** **255.255.255.224**

Decimal	172	24	100	45
Binario	10101100	00011000	01100100	00101101
Decimal	255	255	255	224
Binario	11111111	11111111	11111111	11100000

Subred

2. Nivel IP

Subnetting: Ejemplos

- **Dirección IP: 164.35.0.0**
- **Con 3 bits de subred א $2^3 - 2$ = 6 subredes**
- **Máscara: 255.255.224.0**
- **Hosts por subred א $2^{13} - 2$**

10100100.00100011.0000 0000.0	164.35.0.0
10100100.00100011.0010 0000.0	164.35.32.0
10100100.00100011.0100 0000.0	164.35.64.0
10100100.00100011.0110 0000.0	164.35.96.0
10100100.00100011.1000 0000.0	164.35.128.0
10100100.00100011.1010 0000.0	164.35.160.0
10100100.00100011.1100 0000.0	164.35.192.0
10100100.00100011.1110 0000.0	164.35.224.0

2. Nivel IP

Subnetting: Ejemplos

- **¿Cuántos bits se utilizan para subredes en una dirección de Clase B con una máscara de 255.255.240.0 ?**

- **¿Cuántas redes útiles se pueden conseguir en el caso anterior?**

- **¿Cuál será la dirección de la subred n. 6 si la dirección de clase B es 132.80.0.0?**

2. Nivel IP

Direccionamiento IP: Problemas

- **Asignación ineficiente de direcciones**
  - **Desperdicio de muchas direcciones**
    - **Clase A: 16.777.214 hosts / red**
    - **Clase B: 65.534 hosts / red**
    - **Clase C: 254 hosts / red**
- **Gran crecimiento de Internet**
- **Direcciones casi agotadas**
- **Gran tamaño de las tablas de encaminamiento de los routers**

2. Nivel IP

Direccionamiento IP: Soluciones

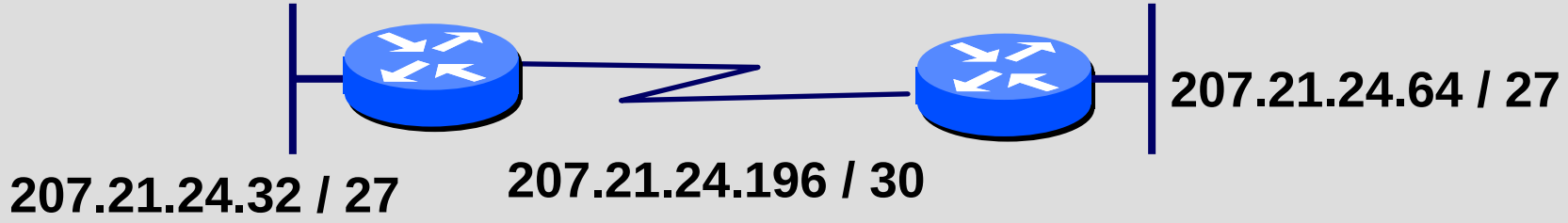
- Classless Interdomain Routing (CIDR)
- Route aggreggation
- Variable-length Subnet Masks (VLSM)
- Direccionamiento privado
- IPv6

2. Nivel IP

Variable Length Subnet Masks (VLSM)

- Permite la existencia de diferentes máscaras de subred en un mismo espacio de direcciones.
- Uso más eficiente del direccionamiento.

- Ej: enlaces punto a punto solo necesitan dos direcciones ⁎ Máscara 255.255.255.252



2. Nivel IP

Classless InterDomain Routing (CIDR)

- No se tienen en cuenta las clases de direcciones IP
- Imprescindible la utilización de máscaras
  - Distinción de red / host
- Permite la agregación de rutas = Supernetting
  - Bloques contiguos de direcciones

- Ejemplo: Uso de 220.220.1.0 a 220.220.255.0
  - Resumen de rutas: 220.220.0.0 / 16

2. Nivel IP

Classless InterDomain Routing (CIDR): Ejemplo

- **Una empresa necesita direcciones para 400 hosts**
  - **Solución A: pedir una clase B**
    - **Clase B ⇒ 65.534 hosts !!!!**
  - **Solución B: pedir dos clases C**
    - **Clase C ⇒ 254 hosts …… 254 x 2 = 508 hosts**

Red	1r. Byte	2o. Byte	3r. Byte	4o. Byte
207.21.54.0	11001111	00010101	00110110	00000000
207.21.55.0	11001111	00010101	00110111	00000000

  - **Resumen de rutas:**
    - **207.21.54.0 / 23**

2. Nivel IP

IPv6

- Nueva versión de IP.
- Direcciones de 128 bits.
- Distintas cabeceras
- Incorpora
  - Autenticación
  - Seguridad

CABECERA IPv6
CABECERA DE OPCIONES SALTO A SALTO
CABECERA DE ENCAMINAMIENTO
CABECERA DE FRAGMENTACIÓN
CABECERA DE AUTENTIFICACIÓN
CABECERA DE SEGURIDAD DE CONTENIDO
CABECERA DE OPCIONES DE DESTINO
CABECERA TCP
DATOS

2. Nivel IP

IPv6

VERSIÓN	PRIORIDAD	ETIQUETA DE FLUJO	
LONGITUD CARGA ÚTIL		PROXIMA CABECERA	LÍMITE DE SALTOS
DIRECCION ORIGEN (128 BITS)			
DIRECCION DESTINO (128 BITS)			

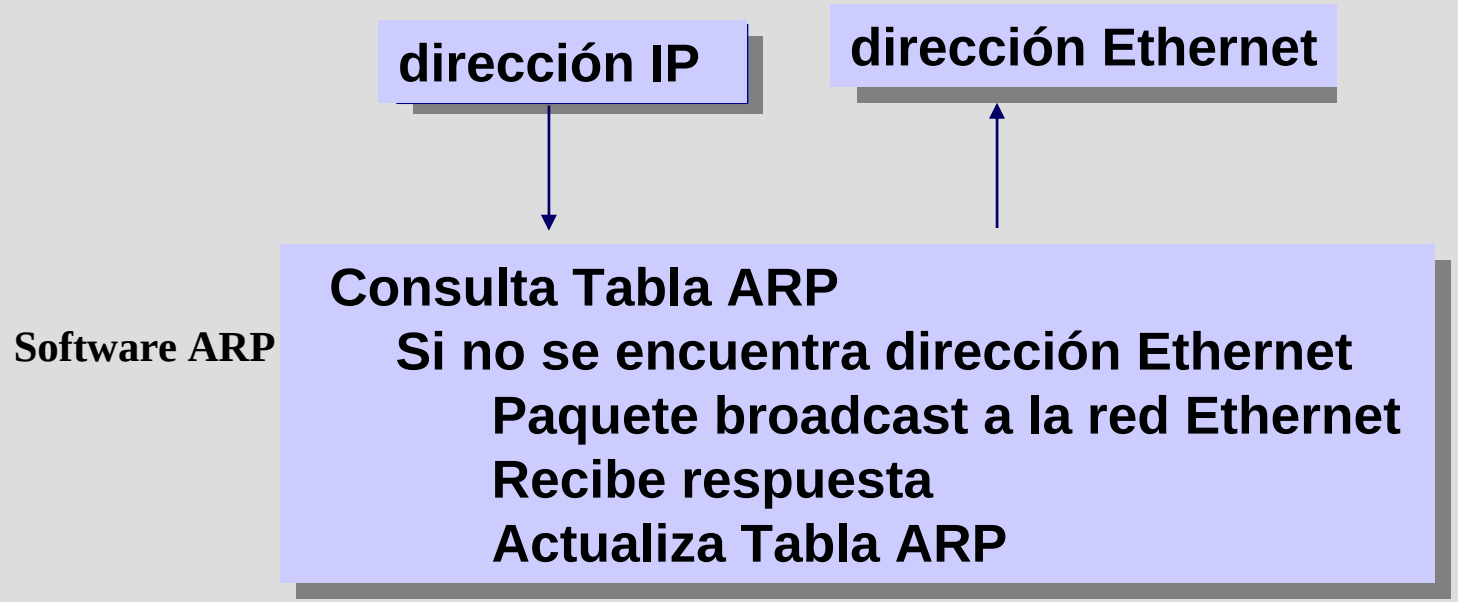
Tecnología de Redes de Comunicaciones

Protocolos de nivel de red

3. Protocolos a nivel de red

Address Resolution Protocol (ARP)

- RFC 826
- El software ARP mantiene dinámicamente la Tabla ARP para asociar direcciones IP con direcciones Ethernet



3. Protocolos a nivel de red

Internet Control Message Protocol (ICMP)

- RFC 792 ICMP
- Mensajes de control, errores, información.
- Control de Flujo:
  - ICMP Source Quench Message
  - De host de destino o gateway intermedio a host de origen.
- Detección de destinos inalcanzables:
  - Destination Unreachable Message
  - Desde un gateway a host origen si el destino inalcanzable es una red o un host.
  - Desde host de destino si el destino inalcanzable es un puerto.

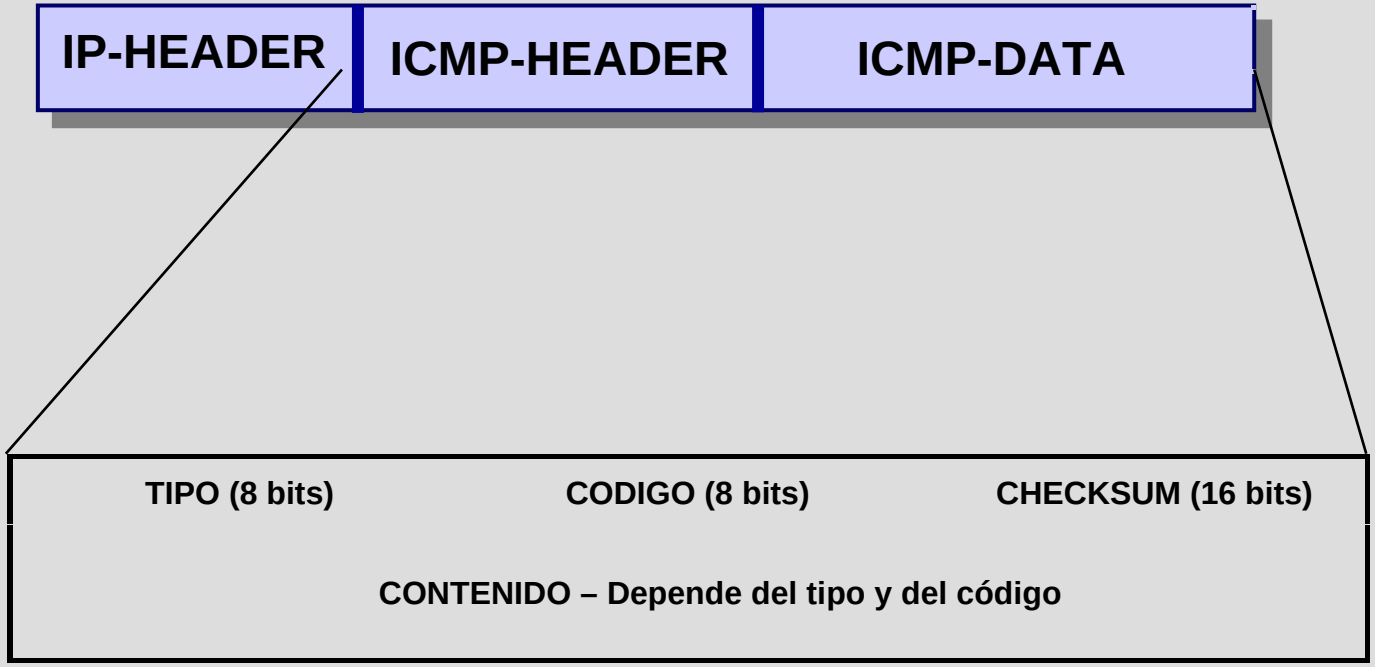
3. Protocolos a nivel de red

Internet Control Message Protocol (ICMP)

- **Redireccionamiento de rutas:**
  - **ICMP Redirect Message**
    - **Desde un gateway a un host en la misma red. Debe haber más de un gateway conectados a la misma red.**
- **Prueba de host remoto :**
  - **ICMP Echo Message**
  - **El comando ping de Unix utiliza este mensaje.**

3. Protocolos a nivel de red

Internet Control Message Protocol (ICMP)



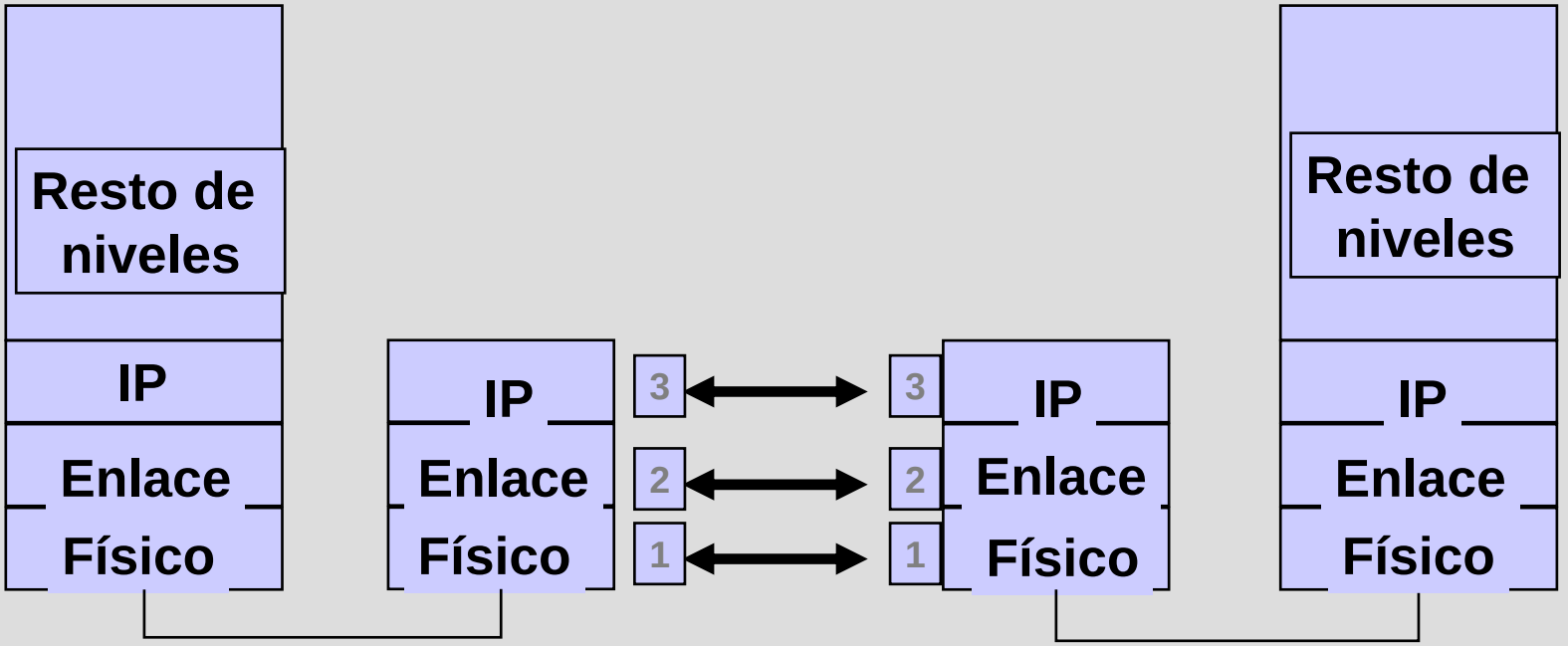
Tecnología de Redes de Comunicaciones

Elementos de Interconexión a nivel de red

4. Elementos de interconexión a Nivel 3

Routing IP

- Interconexión de redes a nivel 3



4. Elementos de interconexión a Nivel 3

Routers

- **Proporcionan servicios de conexión a nivel de red (Nivel 3 de OSI).**
- **Las redes interconectadas pueden tener diferentes niveles de enlace y físico.**
- **El router selecciona activamente la ruta entre origen y destino, según criterios como coste, retardo, congestión o distancia.**

4. Elementos de interconexión a Nivel 3

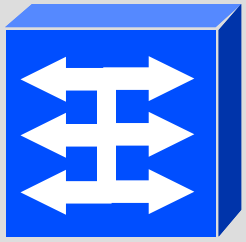
Routers

- Funciones de los routers
  - Interconectar dos o más redes
  - Separar redes
  - Encaminar la información
  - Trabaja a nivel 3
- Los routers tienen N IP’s y N direcciones MAC

4. Elementos de interconexión a Nivel 3

¿Pueden coexistir Switches y Routers?

- **Switch**
  - **Trabaja a nivel 2**
  - **Latencia muy baja**
  - **Interconexión de estaciones o segmentos**
- **Router**
  - **Trabaja a nivel 3**
  - **Latencia más alta**
  - **Interconexión de Redes**

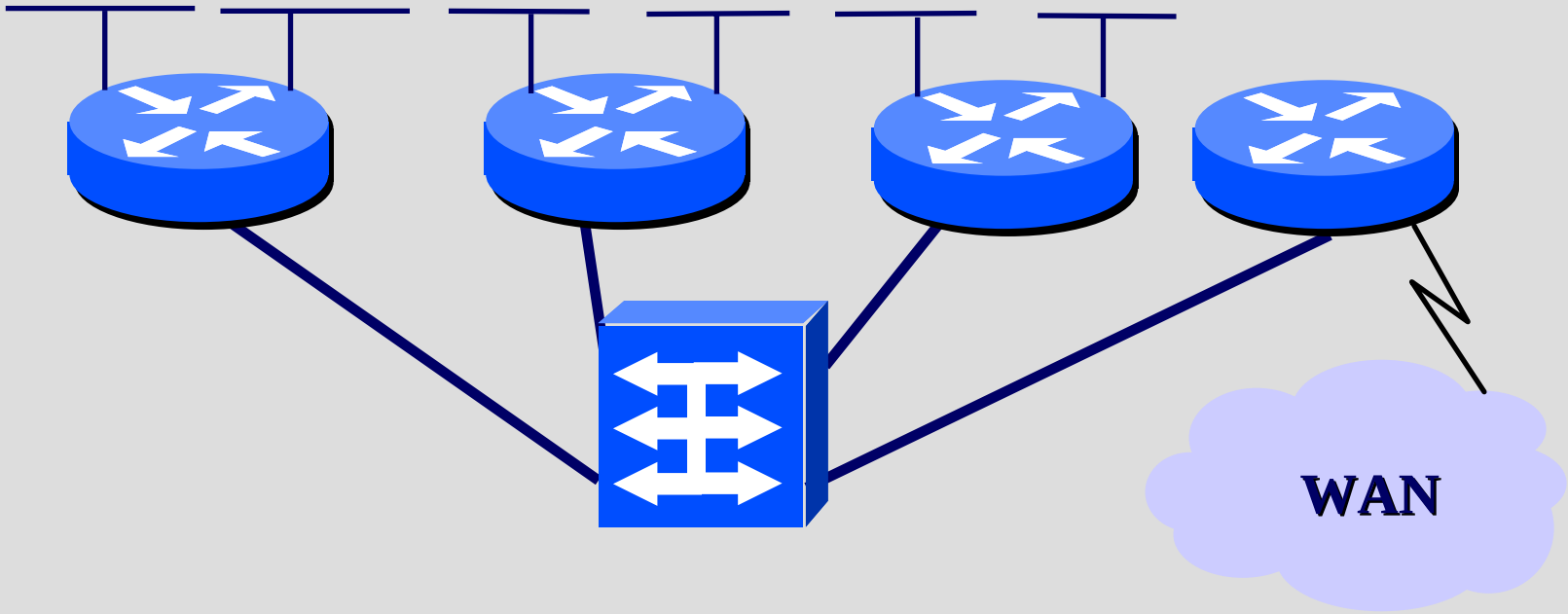


Pueden coexistir perfectamente

4. Elementos de interconexión a Nivel 3

Switch como Backbone de Router

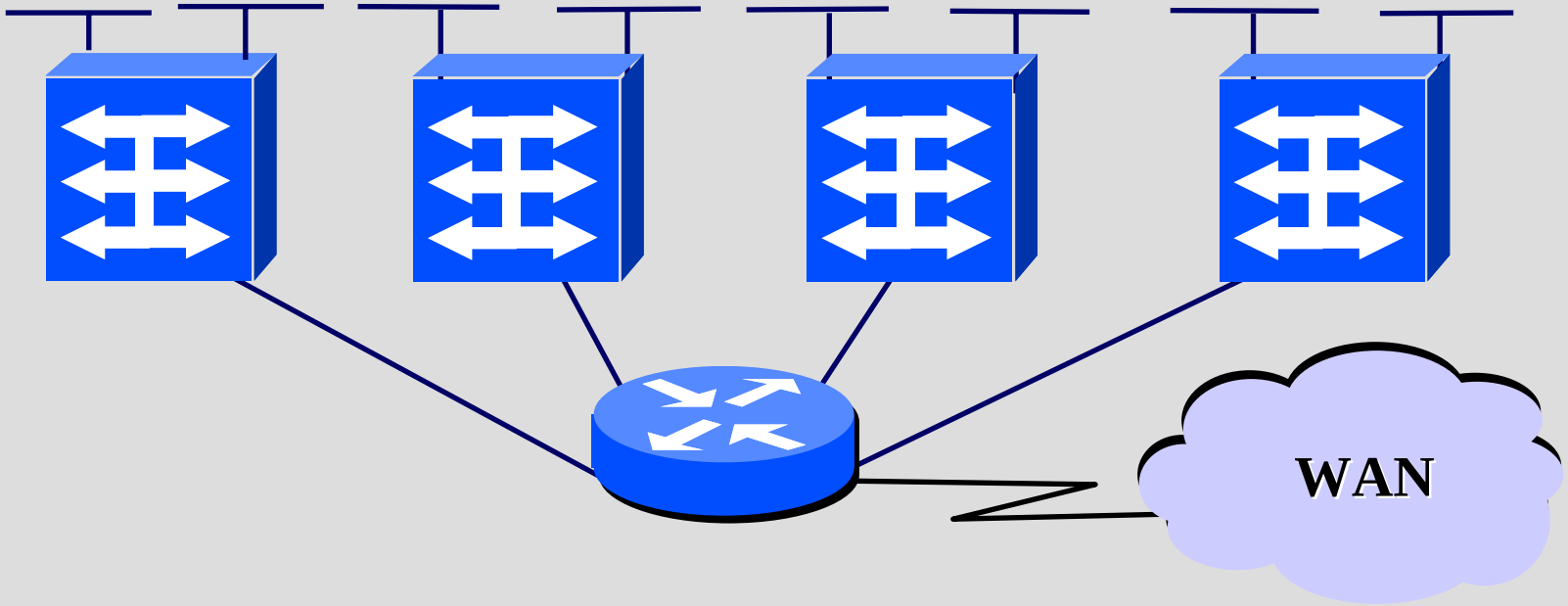
- El switch permite conectar varios routers entre ellos.



4. Elementos de interconexión a Nivel 3

Router como Backbone de Switch

- El router permite unir los switches entre sí.
- Cada switch implementa una red distinta.



Tecnología de Redes de Comunicaciones

Casos prácticos

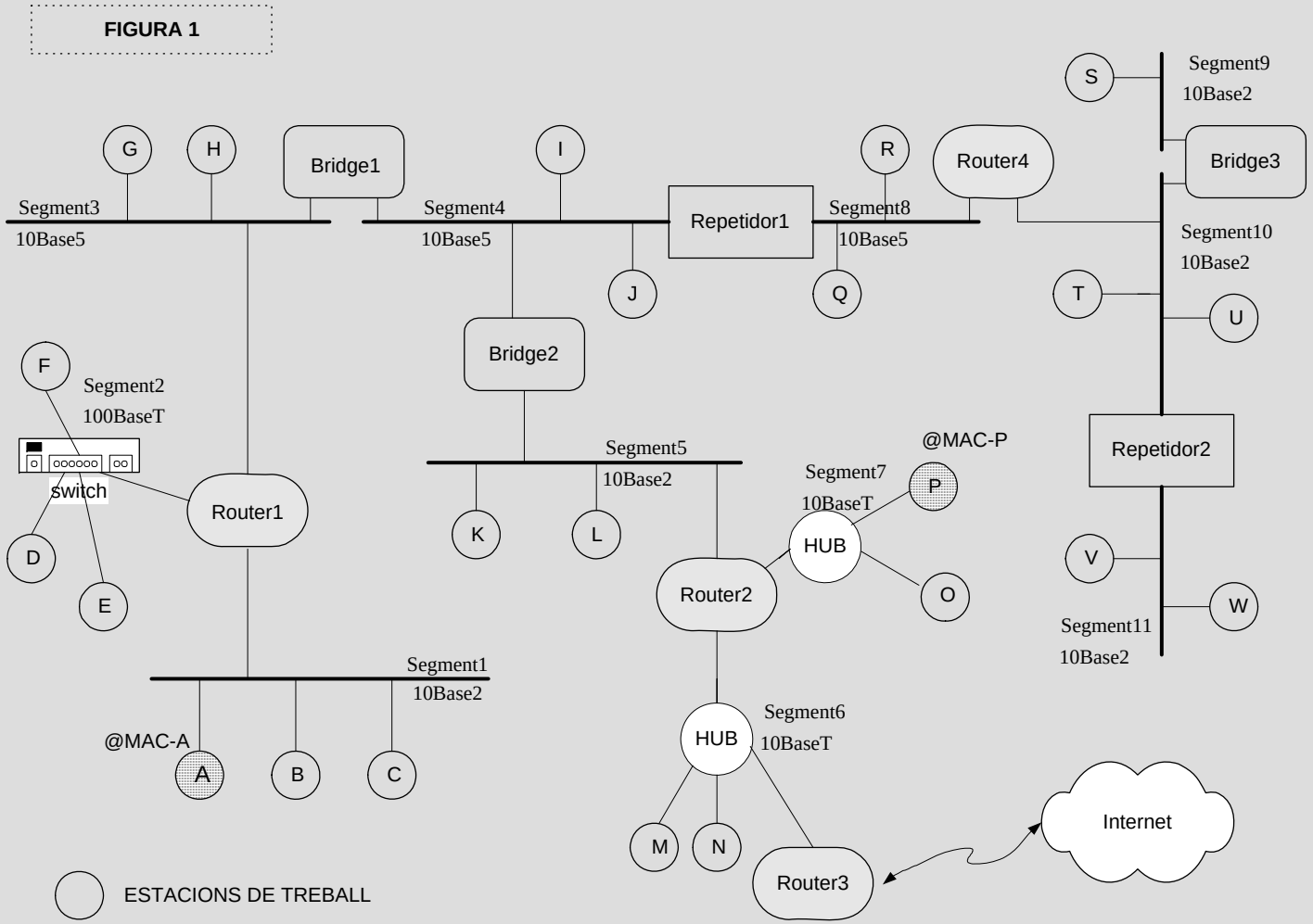
5. Casos prácticos

Caso práctico 1

- ¿Cuántas subredes hay en el siguiente escenario?
- ¿Cuántos bits se necesitan para dimensionar las distintas subredes?
- ¿Qué direcciones de subred y netmask asignarías a cada red, si se dispone para todo nuestro sistema de
  - dirección 132.23.240.0
  - netmask 255.255.240.0 ?

5. Casos prácticos

Caso práctico 1



5. Casos prácticos

Caso práctico 1

¿Cuántas subredes hay en este escenario? 6

FIGURA 1

5. Casos prácticos

Caso práctico 1

- **Cuántos bits se necesitan para dimensionar las distintas subredes?**
  - **Hay 6 subredes א mínimo, 3 bits**
  - **La dirección IP disponible es : 132.23.240.0**
  - **La netmask disponible es: 255.255.240.0**

    1 1 1 1 0 0 0 0

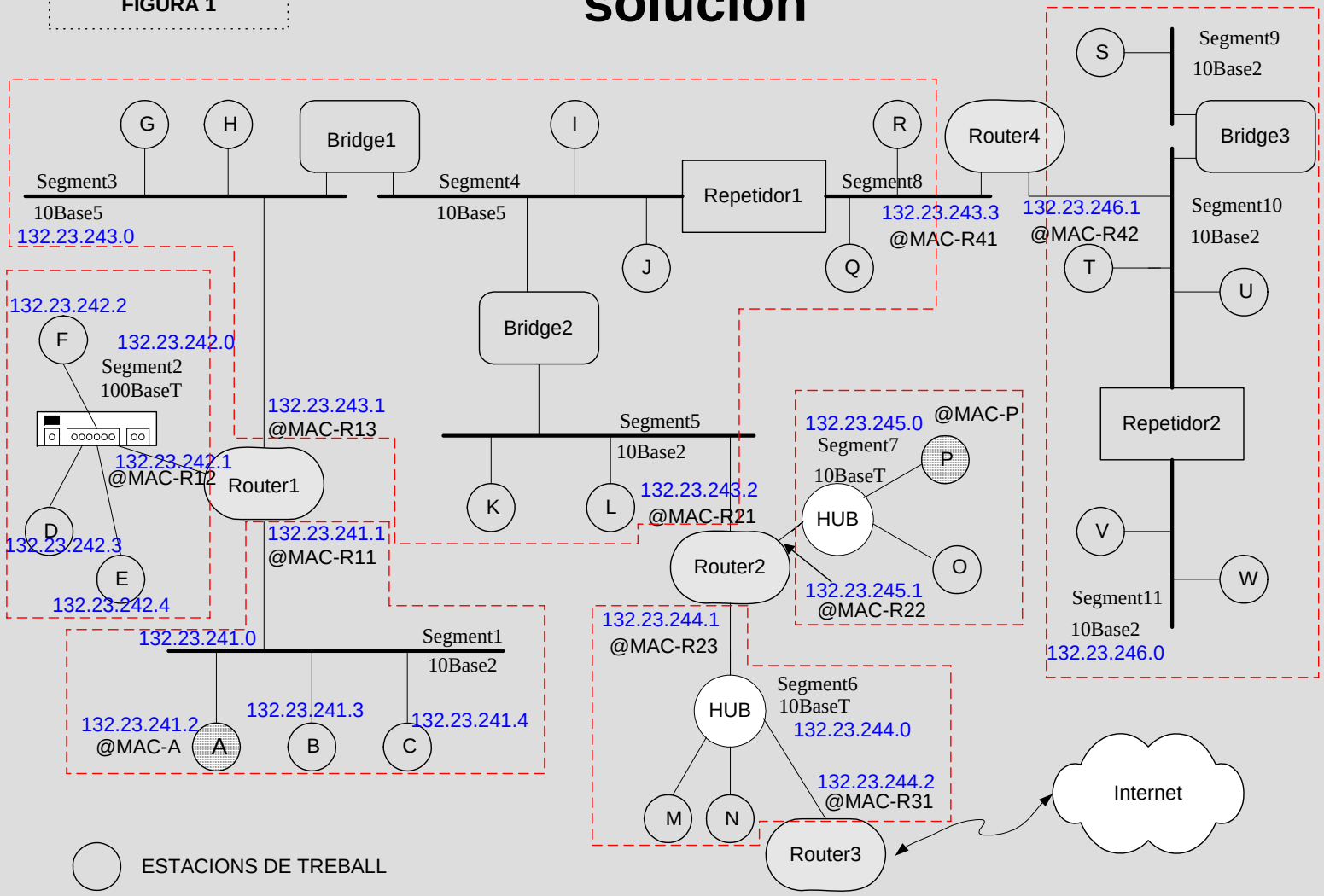
  - **Podemos usar los 4 bits restantes del 3r. Byte de la netmask para las subredes.**
  - **Así daremos las distintas direcciones a las redes.**
  -
  - **1ª: @IP 132.23.241.0 netmask 255.255.255.0**
  - **2ª: @IP 132.23.242.0 netmask 255.255.255.0**
  - **3ª: @IP 132.23.243.0 netmask 255.255.255.0**
  - **4ª: @IP 132.23.244.0 netmask 255.255.255.0**
  - **5ª: @IP 132.23.245.0 netmask 255.255.255.0**
  - **6ª: @IP 132.23.246.0 netmask 255.255.255.0**

5. Casos prácticos

Caso práctico 1

Direccionamiento: posible solución

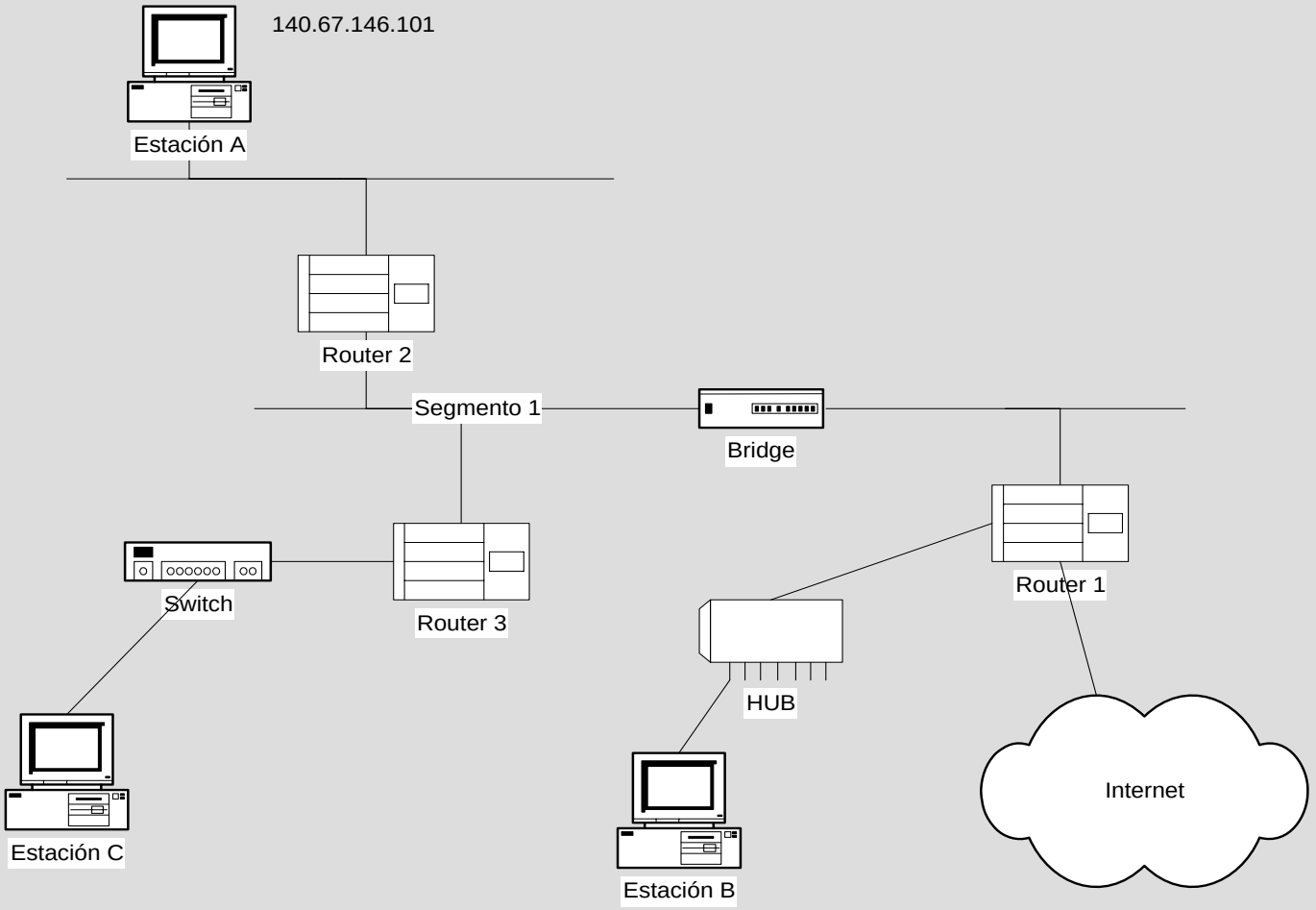
FIGURA 1



5. Casos prácticos

Caso práctico 2: Escenario

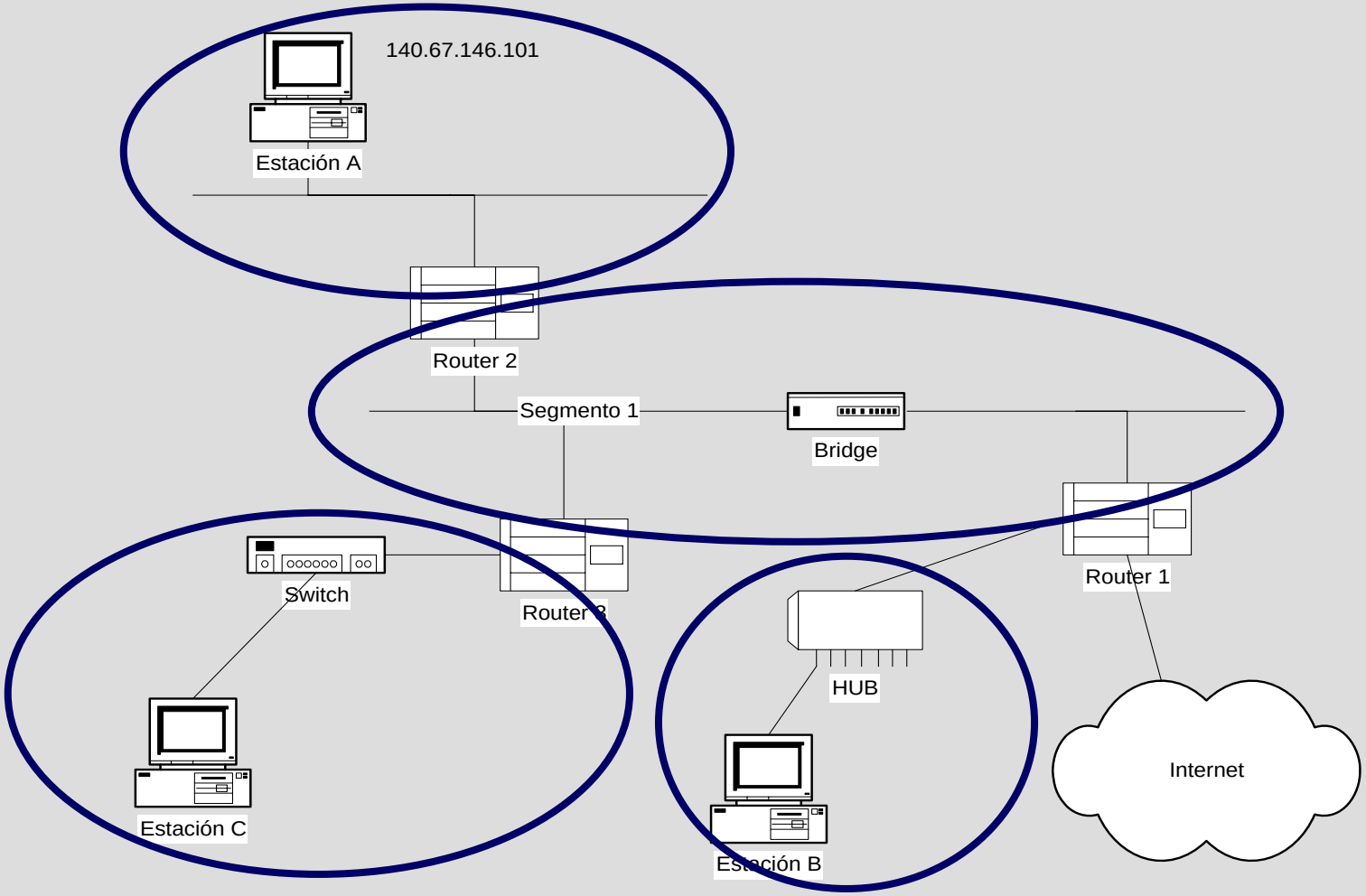
- ¿Cuántas redes podemos encontrar?



5. Casos prácticos

Caso práctico 2: Solución

Número de redes:



5. Casos prácticos

Caso práctico 2: Pregunta

- **Dada la siguiente dirección**
  - **IP 140.67.144.0**
  - **netmask 255.255.240.0**
- **Para todo el sistema, se pide asignar convenientemente direcciones IP y netmask a cada subred, sabiendo que en cada subred habrá entre 200 y 300 hosts, y que la estación A ya tiene una dirección IP asignada.**

5. Casos prácticos

Caso práctico 2: Solución

- En cada subred puede haber entre 200 y 300 host. Por ello, con un byte (8 bits) no hay suficiente ($2^8 = 256$). Es necesario usar 9 bits.
- La máscara 255.255.240.0 (255.255.11110000.00000000) permite jugar con los últimos 12 bits de la dirección IP. Por lo tanto, como necesitamos 9 para cada host, únicamente podemos usar 3 para identificar las subredes.
- La netmask será:
  - 255.255.11111110.00000000 => 255.255.254.0
- La dirección de todo el sistema será:
  - 140.67.144.0 => 140.67.10010000.00000000
- Las direcciones de subred serán:
  - 140.67.10010010.00000000 => 140.67.146.0 / 23
  - 140.67.10010100.00000000 => 140.67.148.0 / 23
  - 140.67.10010110.00000000 => 140.67.150.0 / 23
  - 140.67.10011000.00000000 => 140.67.152.0 / 23

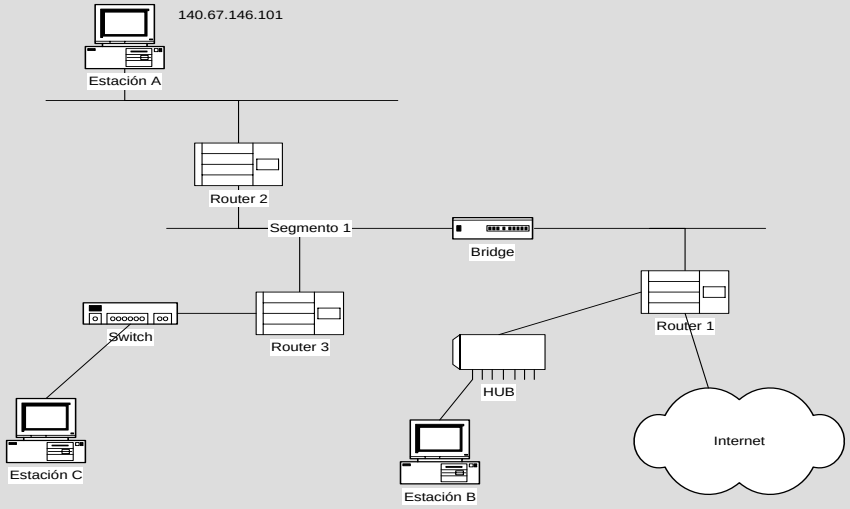
5. Casos prácticos

Caso práctico 2: Enunciado

③ **En el segmento 1 capturamos con un *sniffer* la siguiente trama, de la cual solo se muestran, en el orden correcto, algunos de los campos:**

00789F E3E445	00789F E36792	0800	...	140.67.146.101	140.67.160.102	... SYN ...

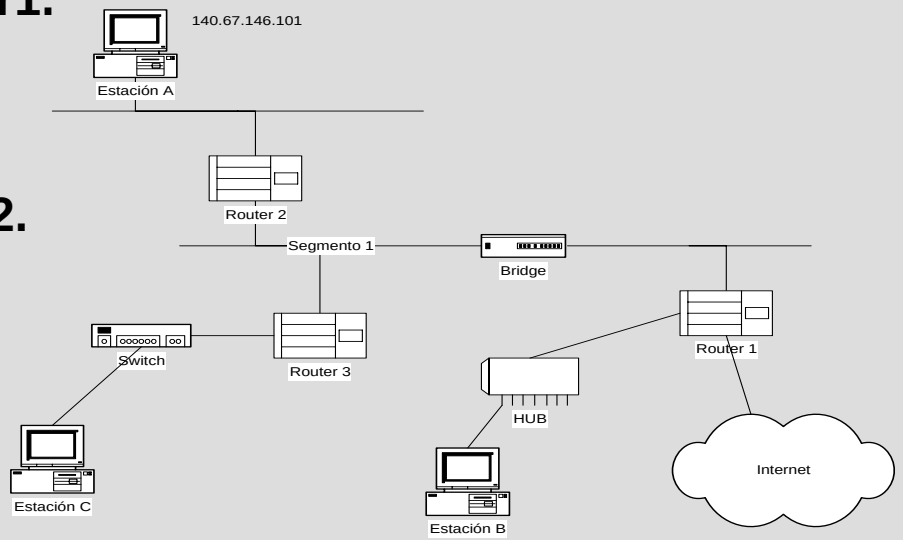
¿A quién corresponden cada una de las direcciones que aparecen en la trama?



5. Casos prácticos

Caso práctico 2: Solución

- Las direcciones de la trama:
- 00 78 9F E3 E4 45:
  - Dirección MAC DESTINO
  - MAC del puerto superior del router1.
- 00 78 9F E3 67 92:
  - Dirección MAC ORIGEN
  - MAC del puerto inferior del router2.
- 140.67.146.101:
  - Dirección IP ORIGEN
  - IP de la estación A
- 140.67.160.102:
  - Dirección IP de la estación destino. Se puede observar que no está en nuestra red, aplicando la netmask.



00789F E3E445	00789F E36792	0800	...	140.67.146.101	140.67.160.102	...

5. Casos prácticos

Caso práctico 3: Escenario

- **“LASALIAN CLOTHES” es una red de tiendas de ropa con tiendas en distitos países. En este momento se dispone de 6 tiendas. Se plantea la conexión de las tiendas con un almacén central para aumentar la productividad del negocio. Las tiendas se conectarán formando una red IP con distintos routers:**
  - **Un router en el almacén central tendrá 7 interfícies IP**
  - **Cada tienda tendrá un encaminador con 2 interfícies IP**
  - **Habrá una red IP entre el router del almacén central y cada tienda (total: 6 redes de conexión)**
  - **Cada tienda tendrá una red Ethernet interna (IP) para conectar los PCs.**
  - **El almacén central tendrá una red Ethernet interna (IP) para conectar los PCs y los servidores corporativos. También habrá otro router con una conexión a Internet.**

5. Casos prácticos

Caso práctico 3: Escenario

- **¿Cuál es la topología de la red propuesta?**
- **Es necesario asignar direcciones a cada una de las 6 redes de conexión (redes entre el router central y el router de cada tienda) y a las interfícies IP directamente conectadas en los router implicados, siguiendo los criterios:**
  - **Las direcciones IP a utilizar son: 192.168.x.0**
  - **La máscara de red a utilizar es: 255.255.255.0**
  - **La primera dirección IP utilizable por red se asigna al router central**
  - **La segunda dirección IP utilizable por red se asigna al router de la tienda**
- **Es necesario asignar direcciones IP a cada una de las 6 redes IP (Ethernet) de las tiendas y a la red Ethernet del almacén central sabiendo que se dispone de la dirección 17.96.0.0 con netmask 255.224.0.0 para todo el sistema.**

FIN DE LA SESIÓN

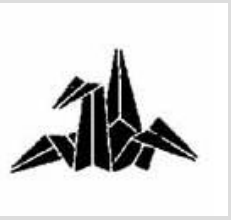
Gracias por su atención!

Tecnologías de Redes
“Redes de Área Local”

www.shellsec.net

Xavier Vila i Espinosa

Ing. Técnico en Telecomunicaciones – Esp. Telemática



ÍNDICE DE LA SESIÓN

- 0. Objetivos.
- 1. Routing IP
- 2. Protocolos de encaminamiento
- 3. Nivel de Transporte
- 4. Casos prácticos

OBJETIVOS DE LA SESIÓN

- **Introducción a los conceptos referentes al encaminamiento de la información en el nivel de red**
- **Estudio de distintos protocolos de encaminamiento:**
  - **RIP**
  - **IGRP**
  - **OSPF**
- **Descripción de las funciones del nivel de transporte y de sus protocolos:**
  - **TCP**
  - **UDP**

PROGRAMA DE LA SESIÓN

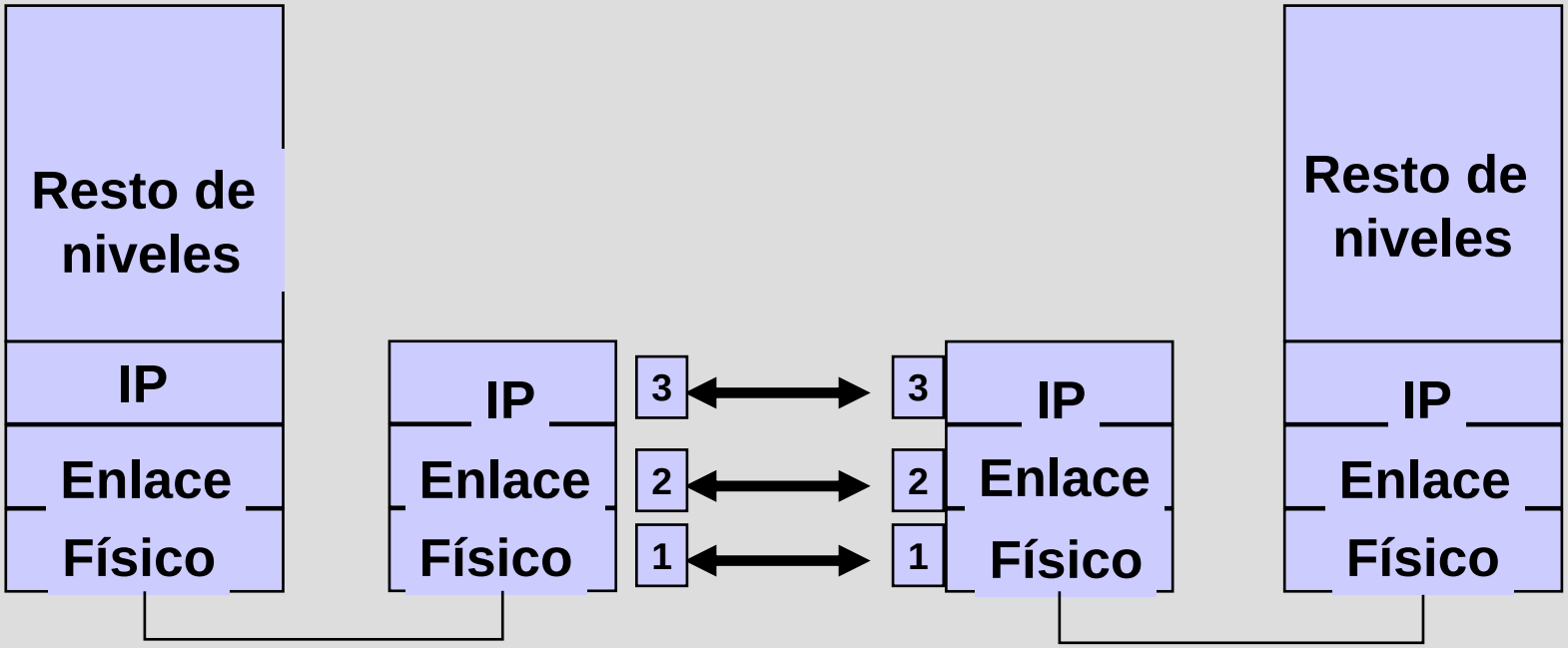
- 1.- Routing IP
  - Definición y características
  - Decisiones de encaminamiento
  - Tablas de encaminamiento
- 2.- Protocolos de encaminamiento
  - Direccionamiento IP
  - Protocolos estáticos
  - Protocolos dinámicos
  - Protocolos distance-vector
  - Protocolos link-state
  - Interior Gateway Protocols
  - Exterior Gateway Protocols
- 3.- Nivel de Transporte
  - Funciones del nivel de Transporte
  - TCP
  - UDP
- 5.- Casos prácticos

Tecnología de Redes de Comunicaciones

1. Routing IP

1. Routing IP

- Interconexión de redes a nivel 3



1. Routing IP

Routers

- Proporcionan servicios de conexión a nivel de red (Nivel 3 de OSI).
- Las redes interconectadas pueden tener diferentes niveles de enlace y físico.
- El router selecciona activamente la ruta entre origen y destino, según criterios como coste, retardo, congestión o distancia.

1. Routing IP

- **Encaminamiento**
  - **Proceso orientado a red**
- **Decisiones de encaminamiento en hosts**
- **Decisiones de encaminamiento en routers**

1. Routing IP

Decisiones de encaminamiento

- **Decisiones de encaminamiento en hosts:**
  - **Si el host de destino está en la propia red, los datos se direccionan directamente al host.**
  - **Si el host destino está en otra red, los datos se envían al router local.**
- **Decisiones de encaminamiento en routers:**
  - **Si el host de destino está en la propia red, los datos se direccionan directamente al host.**
  - **Si el host de destino está en otra red, los datos se envían a otro router local.**

1. Routing IP

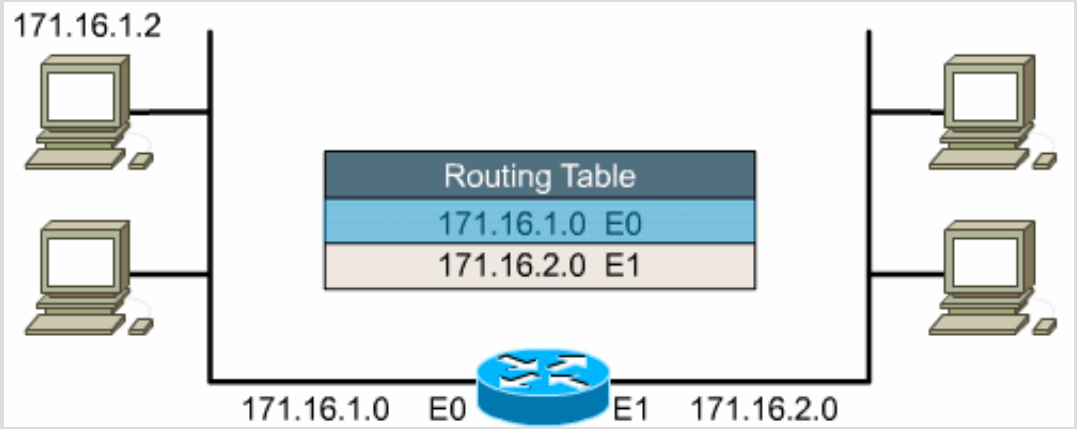
Decisiones de encaminamiento

- El router evalúa las rutas disponibles hacia el destino
- El router escoge la mejor ruta
- Necesita la información de la topología de red
  - Configurada por el administrador de red
  - Recogida mediante procesos dinámicos
- La información se almacena en la tabla de encaminamiento

1. Routing IP

Routing Table

- Información sobre las mejores rutas
- Relación entre redes, interfaces de salida y siguiente salto
- El router utiliza la @IP de red destino

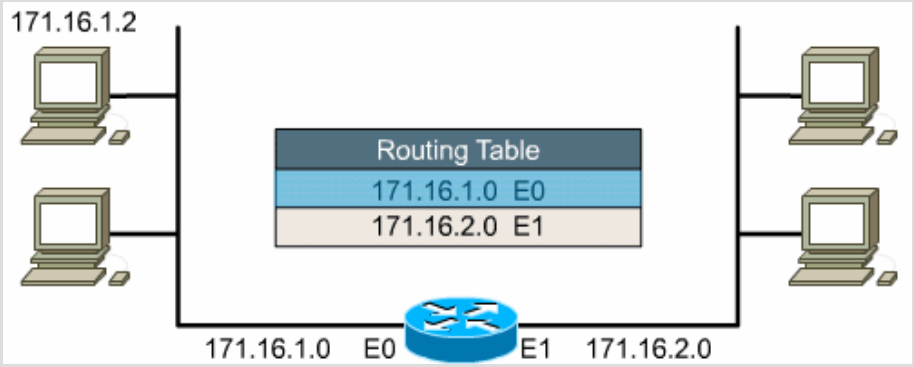


1. Routing IP

Decisiones de encaminamiento

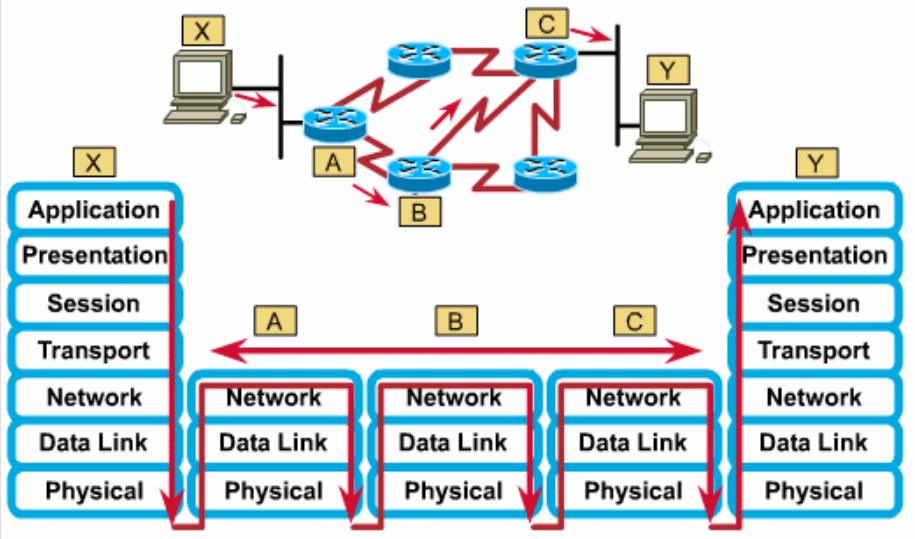
- **Las decisiones de encaminamiento sólo tienen en cuenta el identificador de red de la dirección IP.**
- **A partir del identificador de la red de destino se obtienen de la Tabla de Encaminamiento una dirección de interfaz de red.**

@IP destino	171.16.1.2
	AND
Máscara de red	255.255.255.0
@IP de red destino	171.16.1.0



1. Routing IP

- Host envía un paquete a un host de otra red:
  - Host envía la trama al router de salida (Router A)
  - Router A:
    - Analiza la @IP destino
    - Busca la @IP de red destino en su tabla de routing
    - Encapsula el datagrama en la trama de N2
    - Envía la trama por la interfície de salida
  - Mismo proceso por cada router por donde pasa el datagrama.

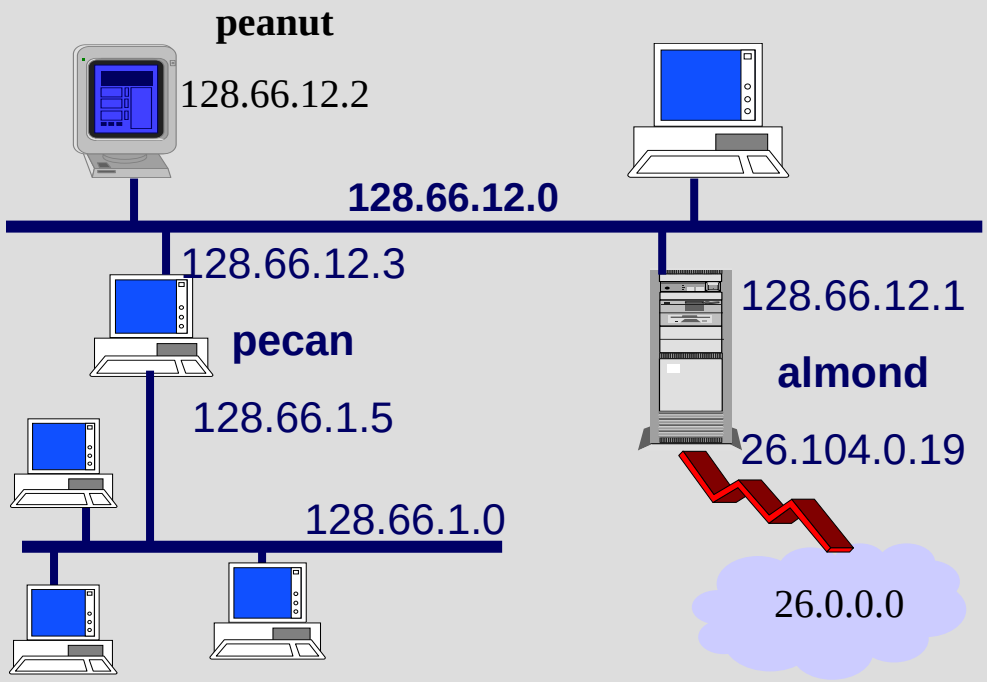


1. Routing IP

Tabla de direcciones de un host

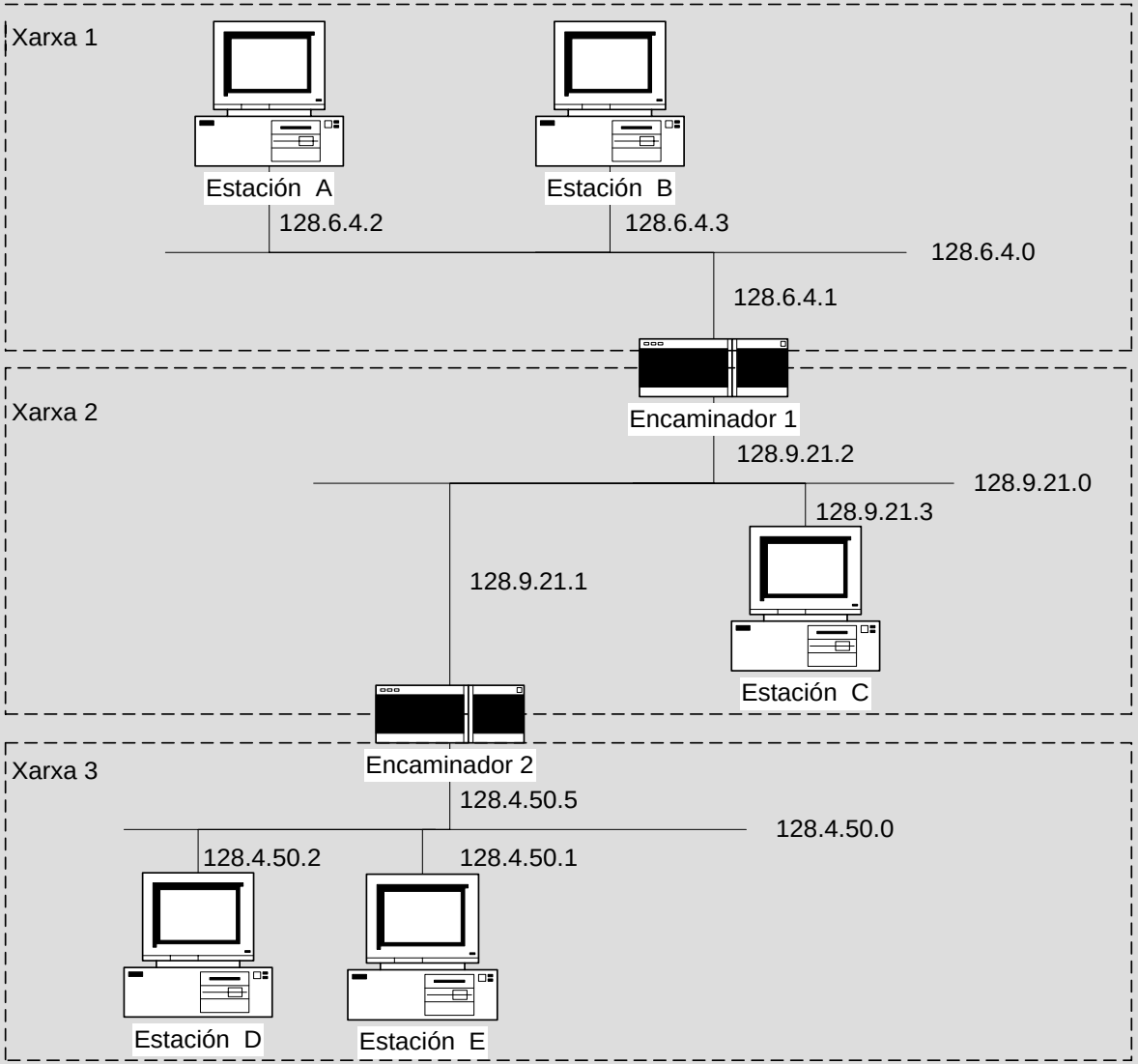
peanut % netstat -nr
routing tables

DESTINATION	GATEWAY
127.0.0.1	127.0.0.1
default	128.66.12.1
128.66.12.0	128.66.12.2
128.66.1.0	128.66.12.3



1. Routing IP

Tabla de direcciones de un router



③ **Router 1**

Network	Gateway
128.6.4.0	128.6.4.1
128.9.21.0	128.9.21.2
128.4.50.0	128.9.21.1

Tecnología de Redes de Comunicaciones

2. Protocolos de encaminamiento

2. Protocolos de encaminamiento

- **Protocolos de routing**
  - **Estáticos / Dinámicos**
  - **Distance-vector / Link-state**
  - **Intra-Domain / Inter-Domain**

2. Protocolos de encaminamiento

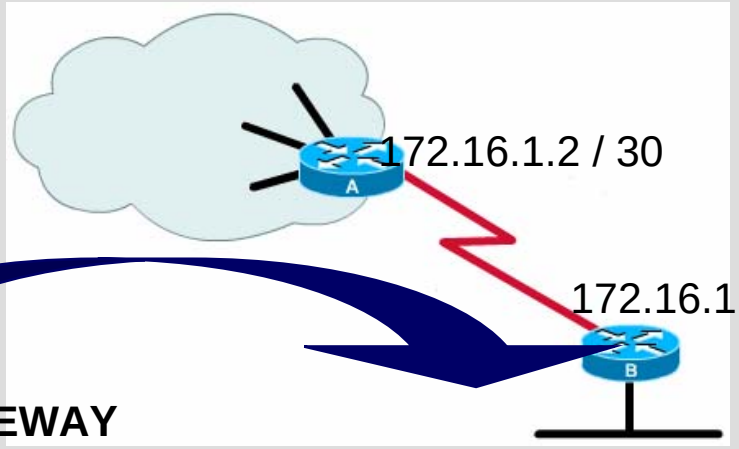
Protocolos estáticos

- El administrador define manualmente la rutas
- Ventajas:
  - Baja sobrecarga del procesador
  - No utilización de ancho de banda (no hay *updates*)
  - Operación segura
    - No se reciben actualizaciones
    - No se envían actualizaciones
  - Comportamiento más predecible
- Inconvenientes:
  - Mantenimiento de la configuración muy alto
  - No se adapta a los cambios en la red

2. Protocolos de encaminamiento

Protocolos estáticos

- **Utilidades:**
  - **El encaminamiento dinámico puede revelar aspectos de redes que, por seguridad, no se desearían propagar.**
  - **Útil en redes accesibles por una sola ruta**
    - **Disminuye la sobrecarga del encaminamiento dinámico**



Ruta por defecto:

NETWORK	MASK	GATEWAY
0.0.0.0	0.0.0.0	172.16.1.2

2. Protocolos de encaminamiento

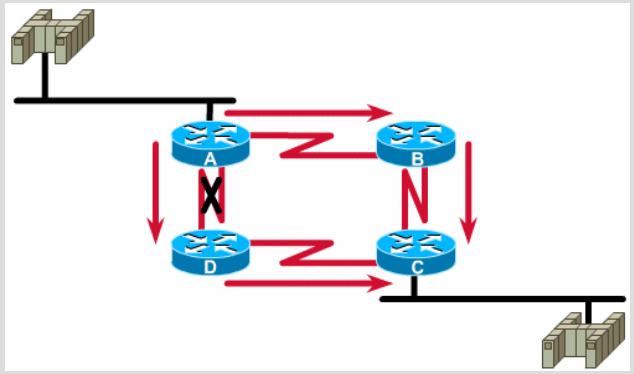
Protocolos dinámicos

- **Los routers aprenden las rutas a partir de:**
  - **Intercambio de información entre ellos**
  - **Aplicación de las reglas del protocolo de routing**
- **Ventajas:**
  - **Capacidad de adaptación a los cambios en la red**
  - **Mantenimiento de la configuración muy bajo**
- **Inconvenientes:**
  - **Mayor sobrecarga del procesador**
  - **Mayor utilización del ancho de banda**
- **Ejemplos: RIP, OSPF, IGRP, EIGRP, BGP,…**

2. Protocolos de encaminamiento

Protocolos dinámicos

- **Ejemplo:**
  - **A siempre transmite información a C pasando por B**
    - **Si tenemos una ruta estática configurada, si el enlace entre A y D cae, A y C no se podrán comunicar**
  - **El encaminamiento dinámico proporcionará más flexibilidad:**
    - **Si el enlace entre A y D cae, A encaminará los datos por B.**
    - **Cuando el enlace entre A y D se restablezca, podrán cambiar las tablas de encaminamiento otra vez.**



2. Protocolos de encaminamiento

Protocolos dinámicos

- **El éxito del encaminamiento depende:**
  - **Mantenimiento de las tablas de routing**
  - **Distribución de la información de encaminamiento (*updates)* entre los routers**

- **Será necesario fijar:**
  - **Cómo enviar las actualizaciones**
  - **Qué información viaja en las actualizaciones**
  - **Cuándo se envían las actualizaciones**
  - **Quiénes recibirán las actualizaciones**

2. Protocolos de encaminamiento

Protocolos dinámicos

- Los routers escogen la ‘mejor’ ruta.
- ¿Qué significa ‘mejor’?
- Métrica
  - Ancho de banda
  - Retardo
  - Carga
  - Fiabilidad
  - Número de saltos
  - Coste
  - …

2. Protocolos de encaminamiento

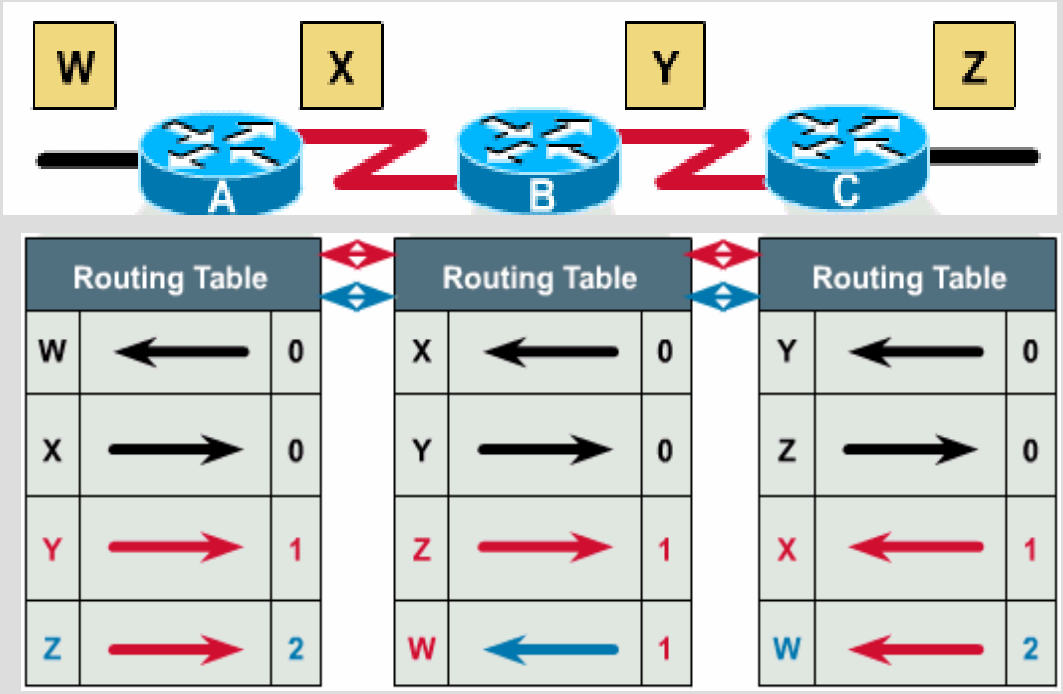
Protocolos Distance-Vector

- **Determina la dirección y distancia a cualquier enlace.**
- **Los routers se intercambian sus tablas de encaminamiento completas**
- **Son intercambios periódicos**
- **Proceso:**
  - **Cada router vecino:**
    - **Recibe un *update***
    - **Examina el *update* y compara la información con la que tiene actualmente en su tabla de encaminamiento**
    - **Añade a su tabla las rutas a nuevas redes o rutas con mejores métricas**
    - **Transmite su tabla de encaminamiento actualizada**

2. Protocolos de encaminamiento

Protocolos Distance-Vector

- Cada router acumula distancias de red y pasa la información a sus vecinos
- Ej:



2. Protocolos de encaminamiento

Protocolos Distance-Vector

- **Ventajas:**
  - **Configuración relativamente fácil**
  - **Necesitan menos recursos de memoria y procesador**
- **Inconvenientes:**
  - **No son buenos para redes grandes**
  - **Tiempo de convergencia grande**
  - **El router no conoce la topología exacta de la red**
  - **Envío periódico de *updates*, aunque no haya cambios en la red.**
    - **RIP cada 30 segundos**
    - **IGRP cada 90 segundos**

2. Protocolos de encaminamiento

Protocolos Link-state

- También se llaman *shortest path first*
- Recrean la topología exacta de las redes
  - Conocimiento sobre los routers distantes
  - Información de cómo están interconectados
- Es necesario:
  - Anuncios de los estados de las rutas (LSAs)
  - Base de datos de la topología
  - El algoritmo de cálculo de rutas
  - La tabla de encaminamiento
- Intercambio de LSAs sólo si hay cambios en la red
- Ejemplo: OSPF

2. Protocolos de encaminamiento

Protocolos Link-state

- **Ventajas:**
  - **Se envían updates (LSAs) cuando hay cambios**
  - **Son updates parciales**
  - **Updates א son multicast, no broadcast**
  - **Tiempo de convergencia menor**
  - **Los routers disponen de la topología de la red**
- **Inconvenientes:**
  - **Mayores requerimientos de memoria**
  - **Mayores requerimientos de capacidad de proceso**
  - **Requerimiento grande de ancho de banda en el estado inicial**

2. Protocolos de encaminamiento

Interior Routing Protocols

- **Protocolos utilizados dentro de un sistema autónomo.**
- **Ejemplos:**
  - **RIP, IGRP, OSPF, EIGRP**
- **Sistema autónomo:**
  - **Conjunto de Routers gestionado por uno o más administradores**
  - **Presenta una vista de encaminamiento consistente hacia el mundo exterior**
  - **Network Information Center (NIC) asigna un único número de sistema autónomo (AS)**
  - **Ejemplo: una empresa, una universidad,…**

2. Protocolos de encaminamiento

Exterior Routing Protocols

- **Protocolos de encaminamiento utilizados entre sistemas autónomos**
- **Se suelen usar para intercambiar información:**
  - **entre ISPs**
  - **entre un usuario y su ISP**
- **Ejemplo: BGP (*Border Gateway Protocol*)**

2. Protocolos de encaminamiento

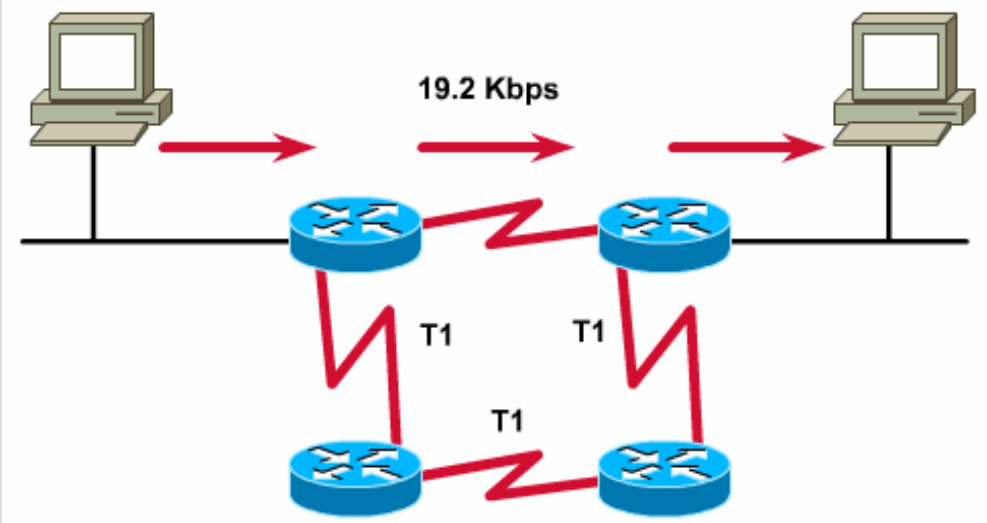
RIP

- **RIP (Routing Information Protocol)**
  - **Tipo de protocolo**
    - **Dinámico**
    - **Intra-domain**
    - **Distance-vector**
  - **Métrica ≡ nº de saltos**
  - **Número máximo de saltos = 16**
  - **Routing updates א broadcast cada 30 segundos**
  - **Encapsulado dentro de UDP**
  - **Basado en el algoritmo de Bellman-Ford**

2. Protocolos de encaminamiento

RIP

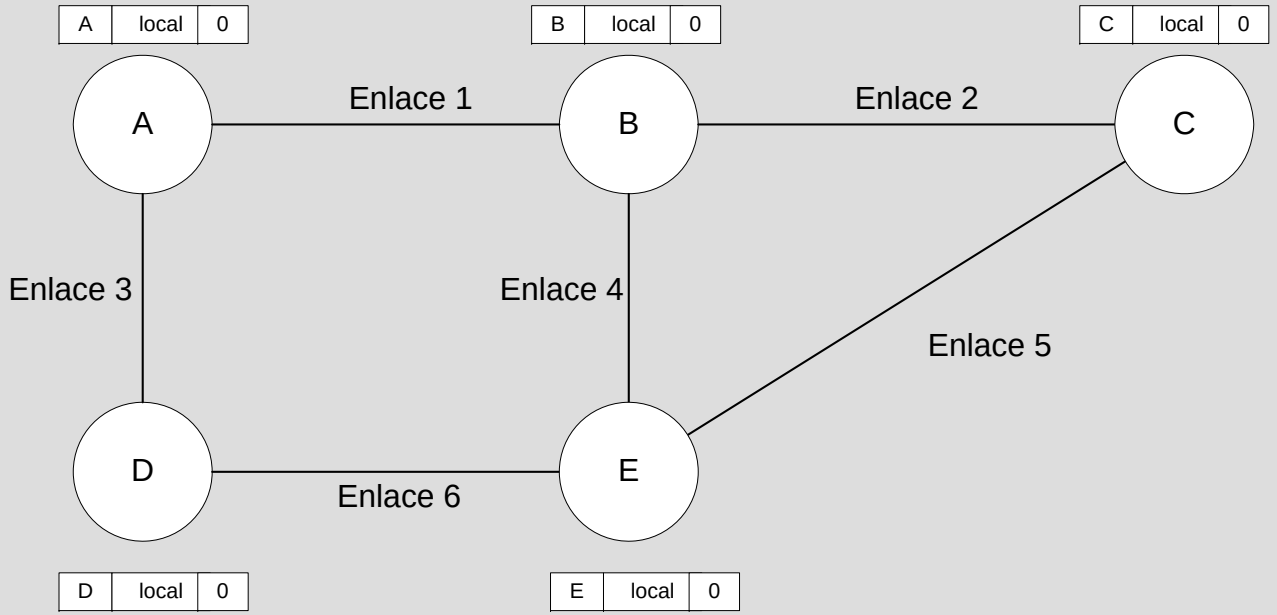
- **RIPv1: no transmite la información de *subnetting* en los *updates***
- **RIPv2: permite CIDR y VLSM**
- **Mejor camino ≠ el camino más corto**



2. Protocolos de encaminamiento

RIP: Ejemplo

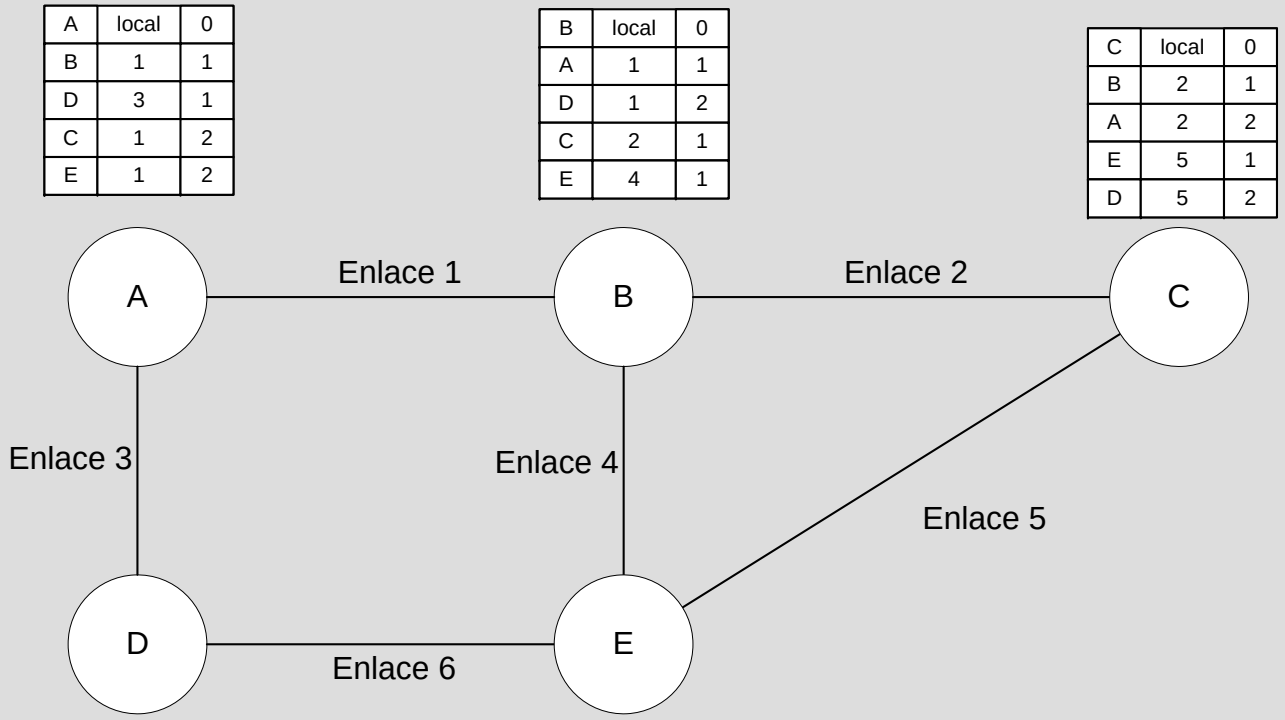
③ **Estado de las tablas de routing antes de iniciar RIP**



2. Protocolos de encaminamiento

RIP: Ejemplo

③ **Estado de las tablas de routing después de la convergencia**



A	local	0
B	1	1
D	3	1
C	1	2
E	1	2

B	local	0
A	1	1
D	1	2
C	2	1
E	4	1

C	local	0
B	2	1
A	2	2
E	5	1
D	5	2

D	local	0
A	3	1
B	3	2
E	6	1
C	6	2

E	local	0
B	4	1
A	4	2
D	6	1
C	5	1

2. Protocolos de encaminamiento

IGRP

- **IGRP (*Interior Gateway Routing Protocol*)**
  - **Tipo de protocolo:**
    - **Dinámico**
    - **Intra-domain**
    - **Distance-vector**
  - **Métrica אcombinación de:**
    - **Ancho de banda**
    - **Retardo**
    - **Carga**
    - **Fiabilidad**
  - **Protocolo de Cisco**
  - **Routing updates א broadcast cada 90 segundos**
  - **No transmite la información de *subnetting* en los *updates***

2. Protocolos de encaminamiento

OSPF

- **OSPF (Open Shortest Path First)**
  - **Tipo de protocolo**
    - **Dinámico**
    - **Intra-domain**
    - **Link-State**
  - **Métrica variable**
    - **Long. Trama, retardo, coste económico, etc...**
  - **Encapsulado dentro de IP**

2. Protocolos de encaminamiento

OSPF

- **Operación de OSPF:**
  - **Establecimiento de las adyacencias de routers**
  - **Elección de:**
    - **DR (Designated Router) א 2 funciones:**
      - **Adyacente a todos los otros routers de la red**
      - **Portavoz de la red**
    - **BDR (Backup Designated Router)**
  - **Descubrimiento de las rutas**
  - **Cálculo y selección de rutas**
  - **Mantenimiento de la información de encaminamiento**

2. Protocolos de encaminamiento

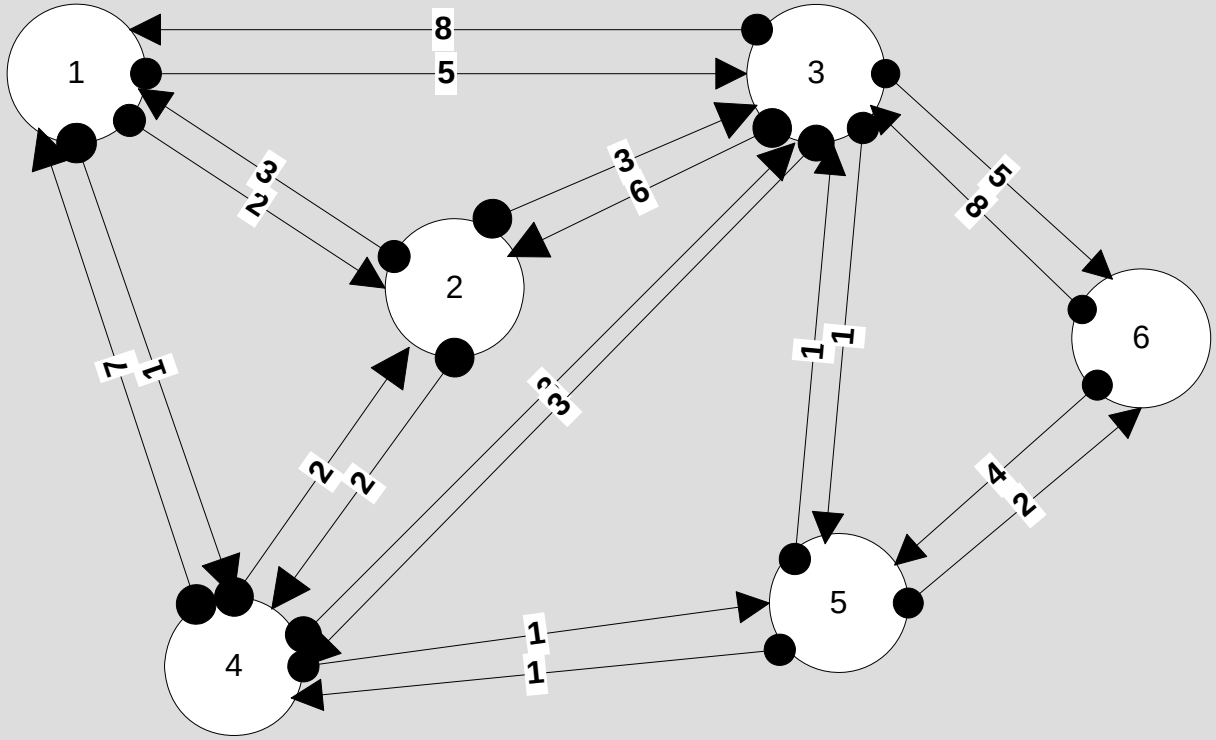
OSPF

- **OSPF (Open Shortest Path First)**
  - **Basado en el algoritmo de Dijkstra**
  - **Puede calcular distintas rutas en función del tipo de servicio IP**
  - **Puede hacer “load balancing”**
  - **Utiliza dos tablas:**
    - **Estado de los enlaces**
    - **Estado de los routers**

2. Protocolos de encaminamiento

OSPF

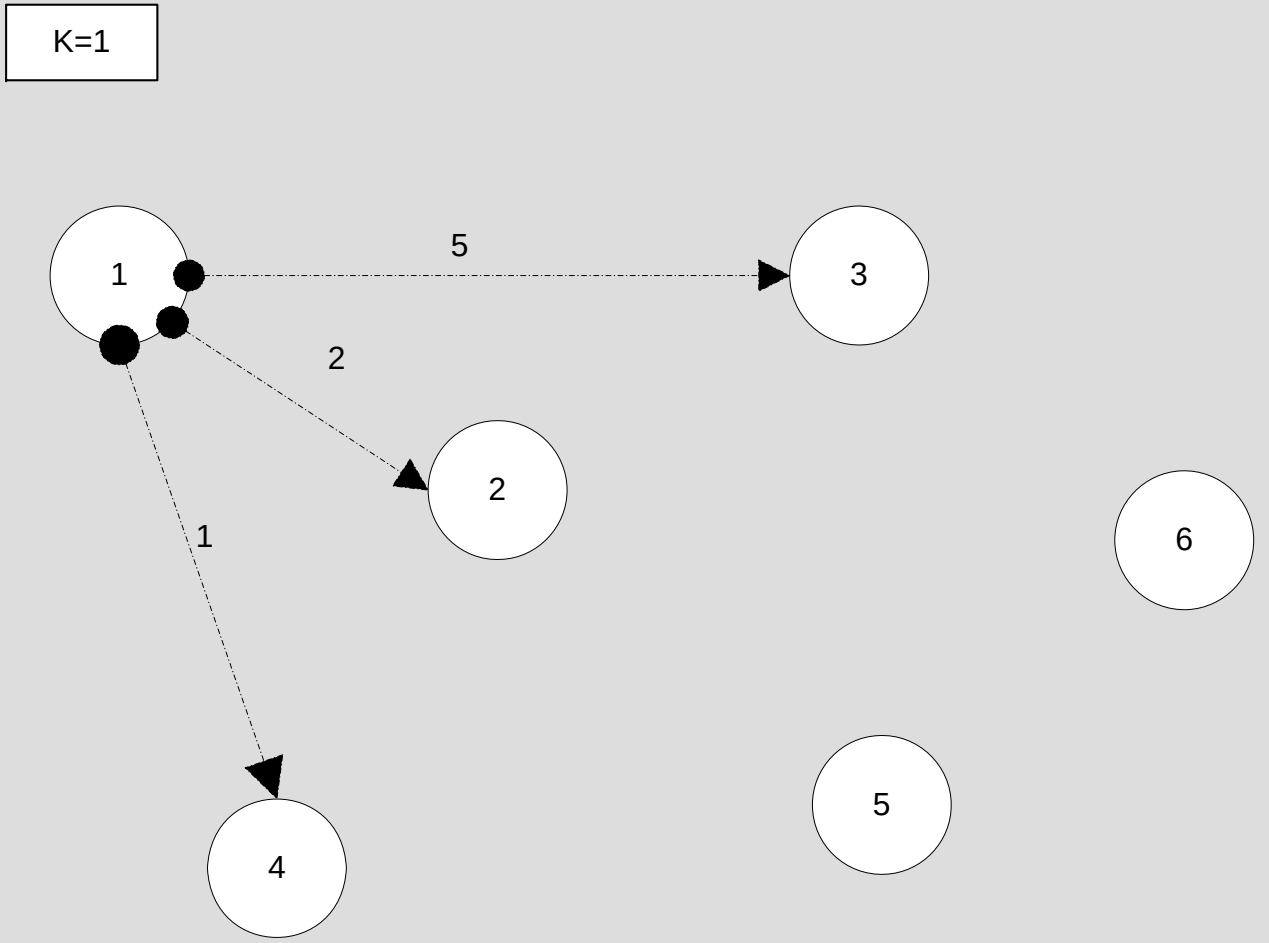
- Coste de los enlaces
- Cálculo desde el router 1



2. Protocolos de encaminamiento

OSPF: Ejemplo

- Caminos con coste menor desde el router 1

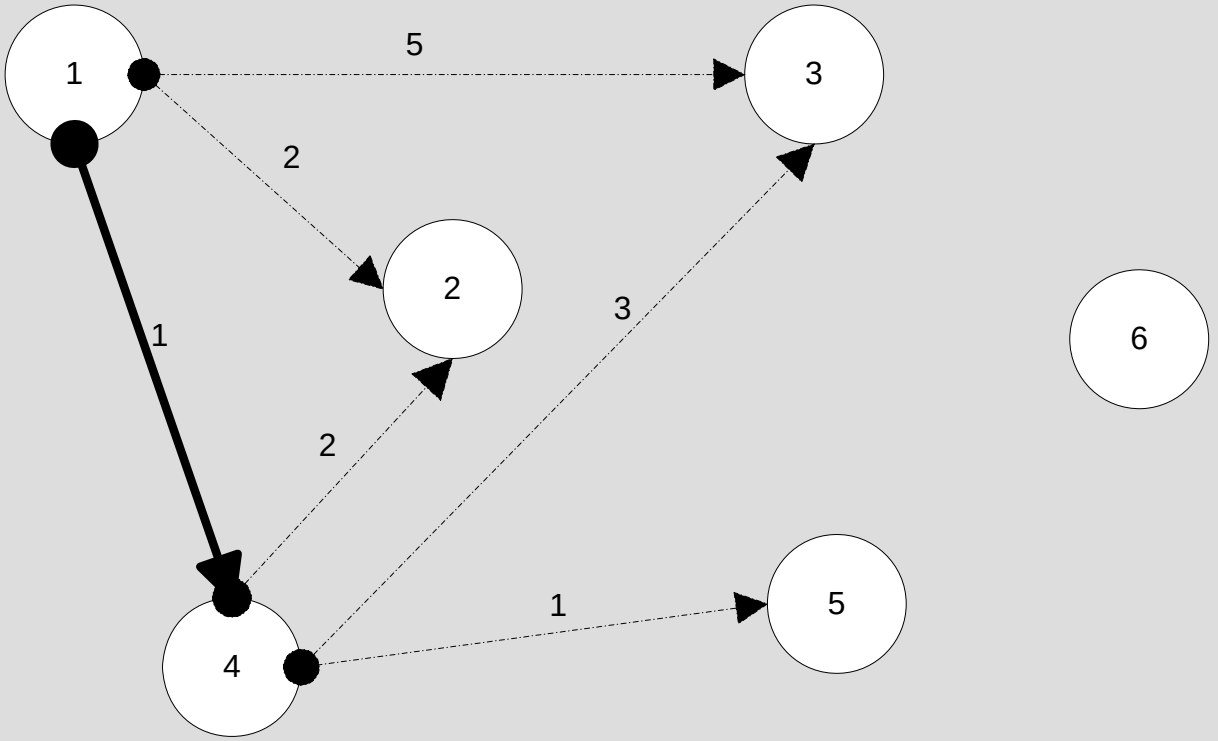


2. Protocolos de encaminamiento

OSPF: Ejemplo

- Caminos con coste menor desde el router 1
  - Se ha visitado el router 4

K=2



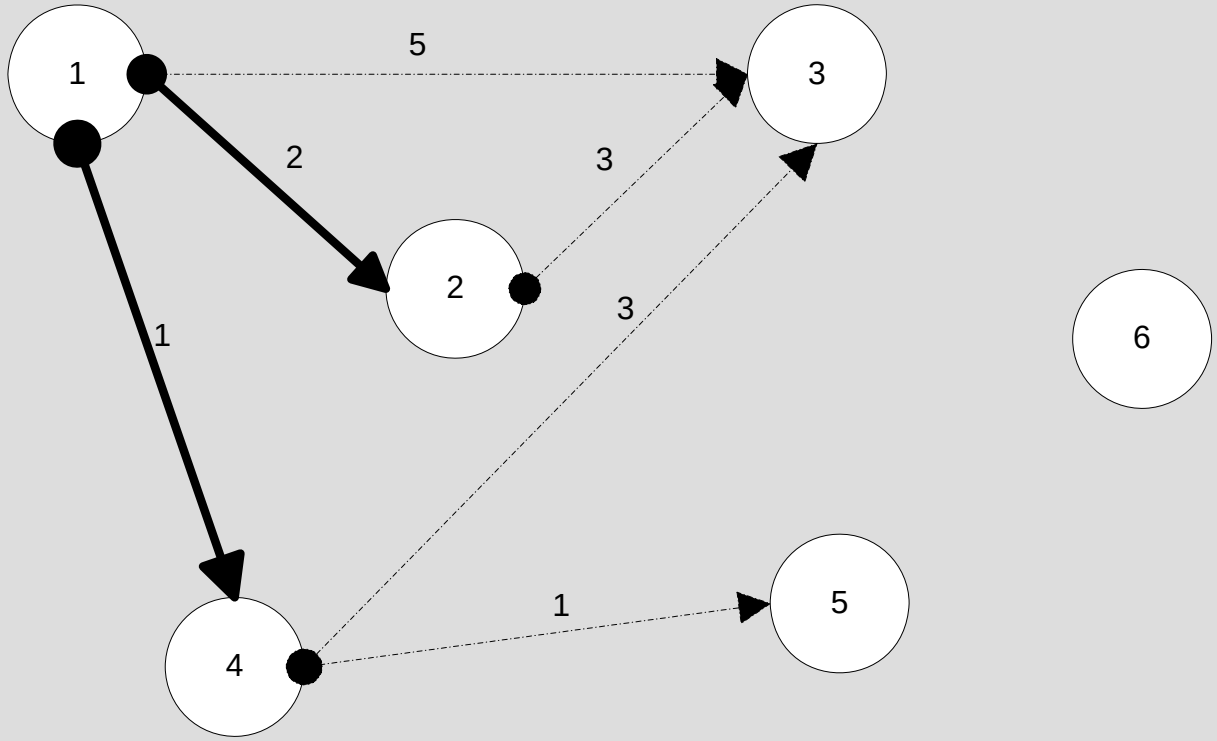
2. Protocolos de encaminamiento

OSPF: Ejemplo

- Caminos con coste menor desde el router 1

K=3

- Se han visitado los routers 4, 2



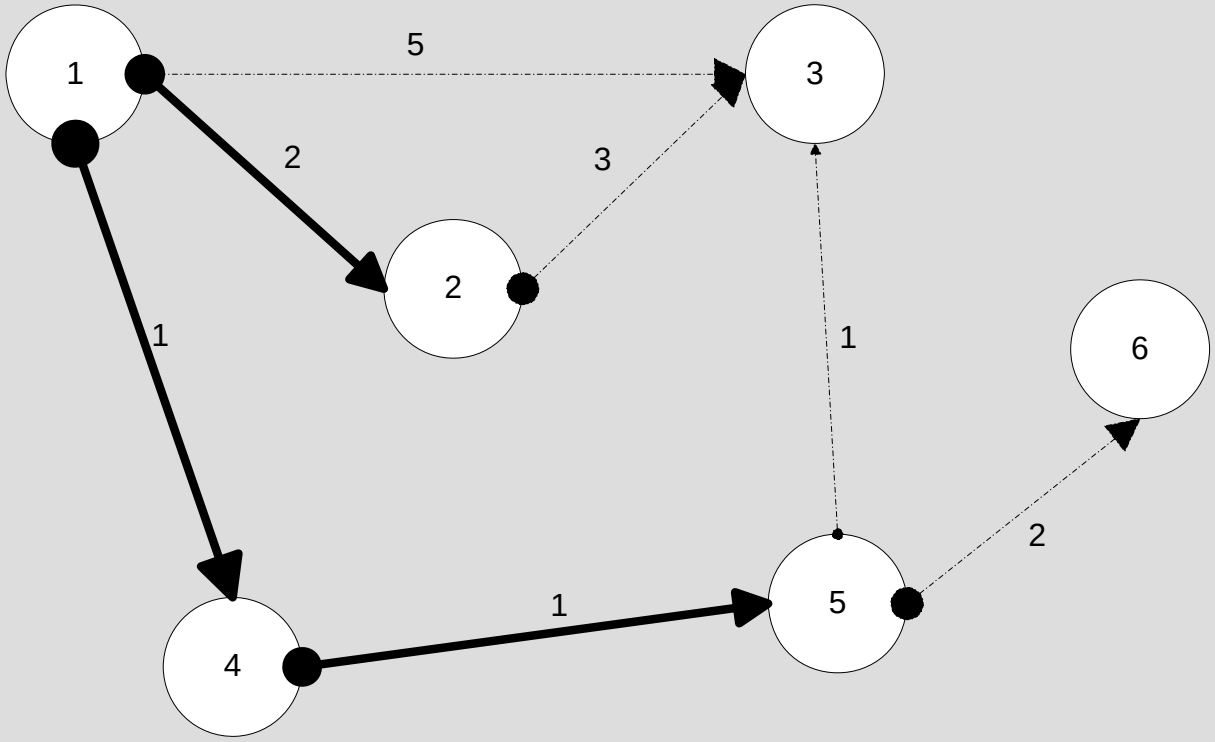
2. Protocolos de encaminamiento

OSPF: Ejemplo

- Caminos con coste menor desde el router 1

K=4

- Se han visitado los routers 4, 2, 5



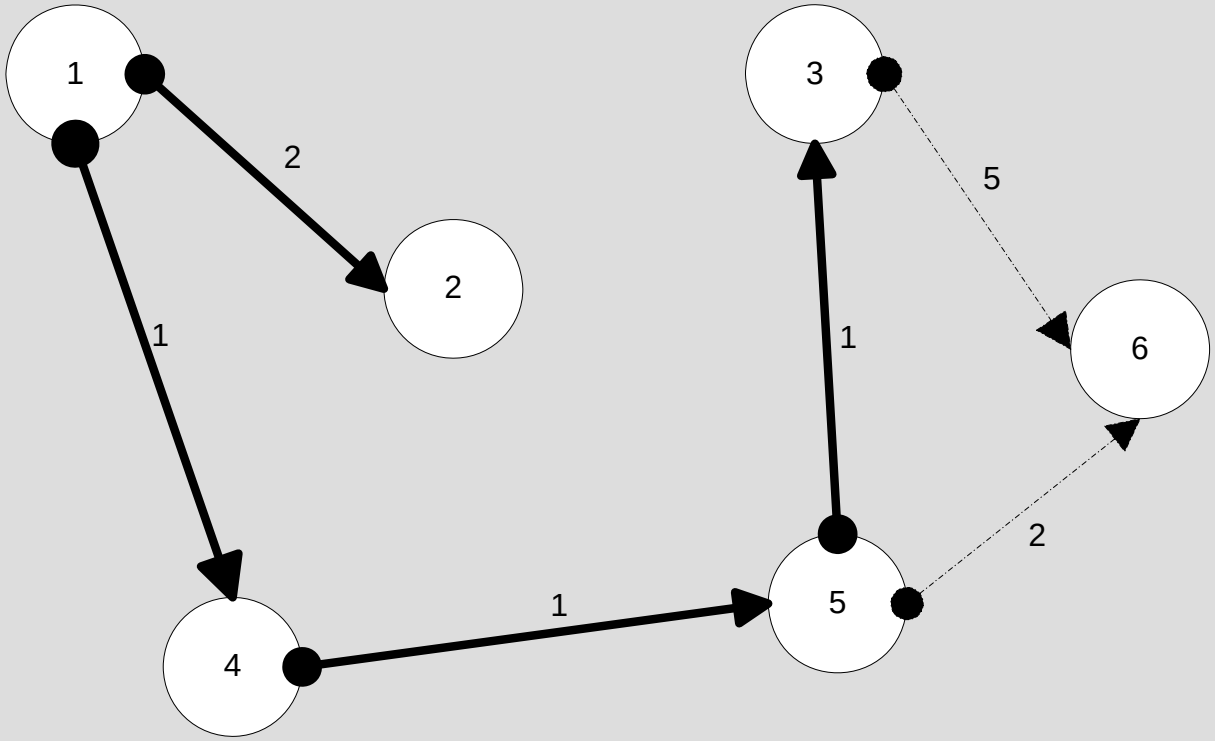
2. Protocolos de encaminamiento

OSPF: Ejemplo

- Caminos con coste menor desde el router 1

K=5

- Se han visitado los routers 4, 2, 5, 3



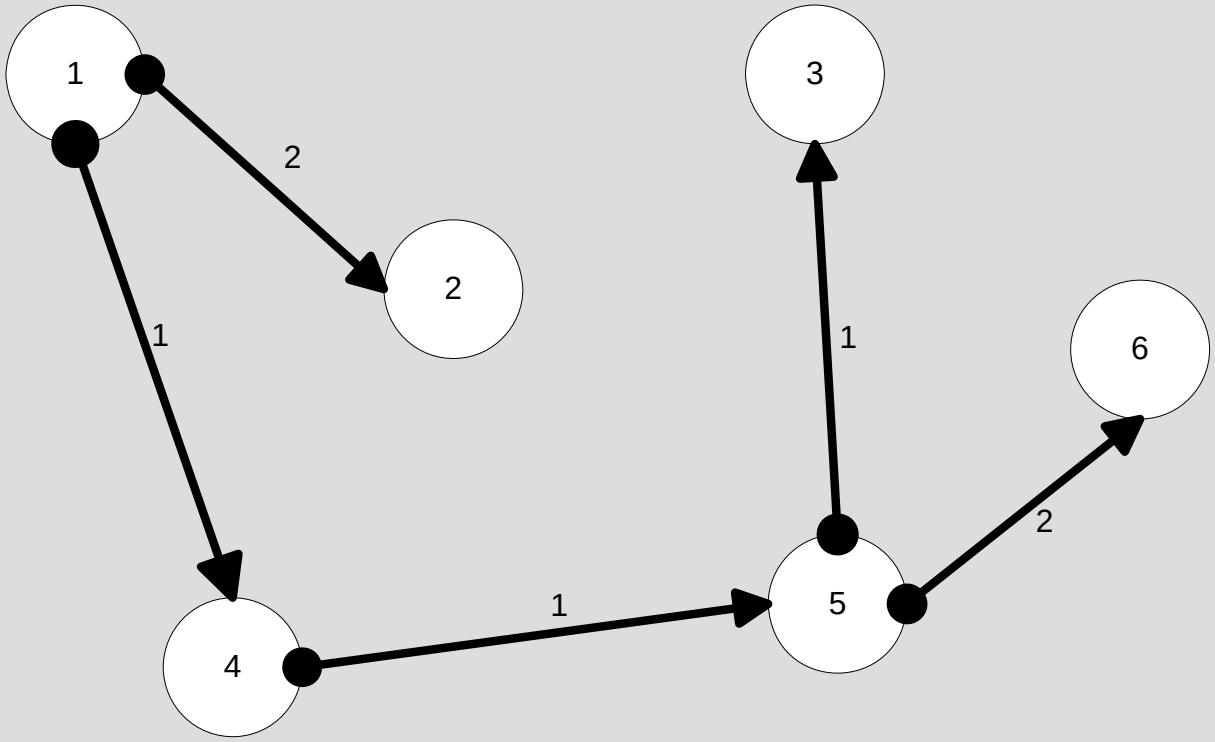
2. Protocolos de encaminamiento

OSPF: Ejemplo

- Caminos con coste menor desde el router 1

K=6

- Árbol de rutas



Tecnología de Redes de Comunicaciones

3. Nivel de Transporte

3. Nivel de Transporte

Funciones

- Define la conectividad extremo a extremo entre las aplicaciones de host
- Segmenta los datos de aplicación
- Establece operaciones extremo a extremo
- Envía los segmentos desde host origen hasta host destino
- Asegura la fiabilidad de los datos
- Proporciona control de flujo
  - Reconocimiento de los segmentos en destino
  - Retransmisión de los segmentos no reconocidos
  - Ordenación de la secuencia de segmentos
  - Control de congestión
- Protocolos: TCP y UDP

3. Nivel de Transporte

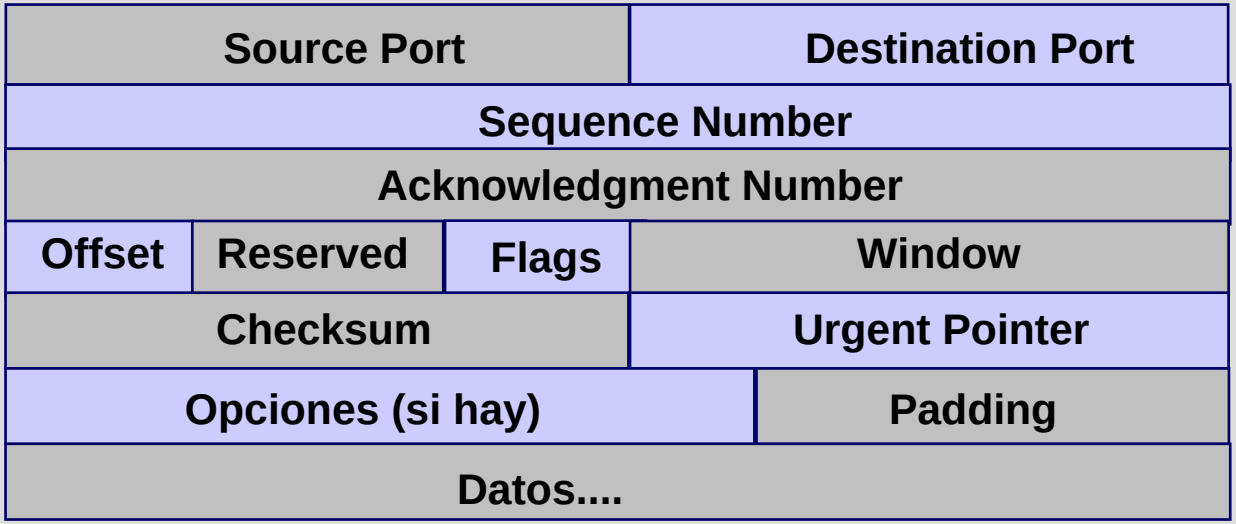
TCP

- **TCP (*Transmission Control Protocol*)**
  - **Protocolo orientado a conexión**
    - **Establecimiento de la conexión**
    - **Transmisión de datos**
    - **Finalización de la conexión**
  - **Protocolo confiable**
  - **Divide los mensajes de salida en segmentos**
  - **Reensambla los mensajes en el destino**
  - **Reenvía los segmentos no recibidos**
  - **Proporciona control de flujo**

3. Nivel de Transporte

TCP

- **Formato del segmento TCP**



3. Nivel de Transporte

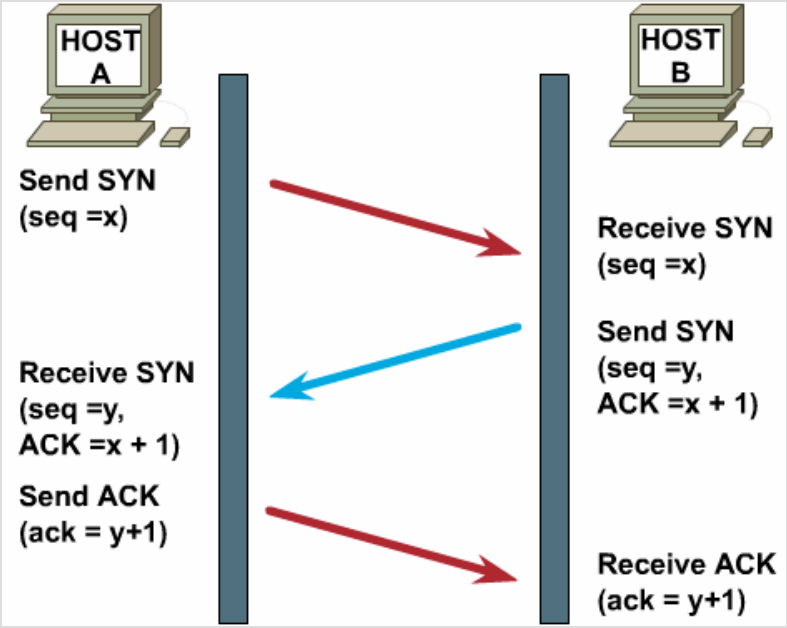
TCP: Números de puerto

- **Números de puerto**
  - Permiten mantener distintas conversaciones a la vez
  - Indican el protocolo de aplicación que está utilizando el nivel de transporte
  - Rangos de puertos:
    - 0 – 255 : para aplicaciones públicas
    - 256-1023 : para aplicaciones de empresas
    - >1023 : sin regulación
  - Ejemplos:
    - 21: FTP
    - 23: Telnet
    - 25: SMTP
    - 69: TFTP
    - 80: HTTP

3. Nivel de Transporte

TCP: Establecimiento de la conexión

- **Establecimiento de la conexión**
  - **Se reservan los recursos para la conexión**
  - **Three-way hand-shake**
  - **Intercambio de números de secuencia א Flag SYN**



3. Nivel de Transporte

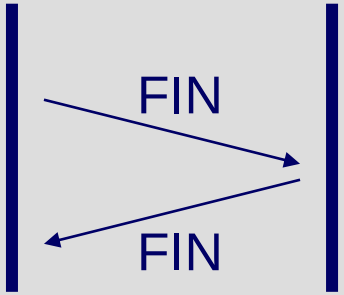
TCP: Transmisión de datos

- **Hay constancia de la entrega correcta de datos en el extremo receptor:**
  - **Flag ACK:**
    - **Segmento recibido correctamente implica una respuesta afirmativa.**
- **Hay control de flujo**
  - **Campo *Window*:**
    - **Bytes que el receptor está dispuesto a aceptar sin esperar confirmación**

3. Nivel de Transporte

TCP: Finalización de la conexión

- **Finalización de la conexión:**
  - **Flag FIN:**
    - **Se activa cuando se quiere finalizar una conexión**
  - **Se liberan los recursos reservados para la conexión**



3. Nivel de Transporte

UDP

- **UDP (*User Datagram Protocol*)**
  - **Protocolo no orientado a conexión**
  - **Protocolo no confiable**
  - **Transmite mensajes ≡ datagramas de usuario**
  - **No controla errores en los datos**
  - **No reensambla mensajes de entrada**
  - **No hay constancia de la entrega correcta de datos en el extremo receptor**
  - **No realiza control de flujo**
  - **Adecuado en aplicaciones en las que los datos a transmitir son pequeños:**
    - **Ej: Aplicaciones “query-response”**

3. Nivel de Transporte

UDP

- **Formato del mensaje UDP**
  - **Las direcciones corresponden a puertos que identifican procesos de aplicación**
  - **Bajo overhead**
  - **Protocolos que utilizan UDP:**
    - **TFTP, SNMP, DHCP, DNS**

Source Port	Destination Port
Length	Checksum
datos..	

Tecnología de Redes de Comunicaciones

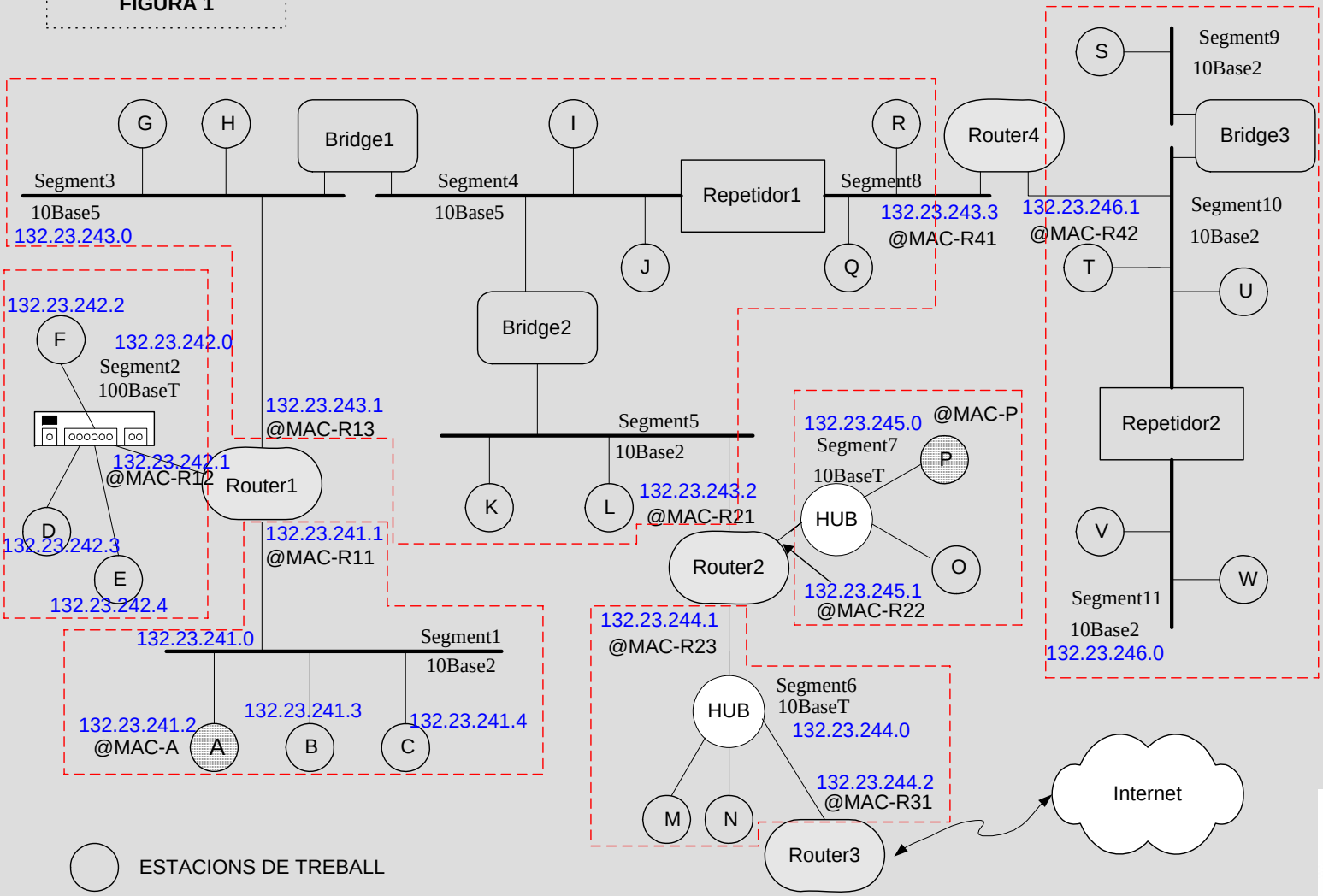
4. Casos prácticos

4. Casos prácticos

Caso práctico 1

③ ¿Tabla de routing del Router 2?

FIGURA 1



4. Casos prácticos

Caso práctico 1

- ¿Tabla de routing del Router 2?

Destino	Next Gateway / Port

4. Casos prácticos

Caso práctico 1

③ **¿Tabla de routing del Router 2?**

Destino	Next Gateway / Port
132.23.241.0	132.23.243.1
132.23.242.0	132.23.243.1
132.23.243.0	132.23.243.2
132.23.244.0	132.23.244.1
132.23.245.0	132.23.245.1
132.23.246.0	132.23.243.3
Default	132.23.244.2

4. Casos prácticos

Caso práctico 2

- **Conocemos las tablas de routing de 2 routers de una empresa y la tabla de direcciones entera del único bridge que hay.**
- **¿Cuál será la topología lógica de la red?**

Router 1		
DESTINATION	GATEWAY	INTERFACE
192.192.192.0	192.192.192.1	@MAC1
198.20.12.0	198.20.12.5	@MAC2
195.30.40.0	195.30.40.2	@MAC3
200.100.30.0	195.30.40.1	
200.100.31.0	195.30.40.1	
200.100.32.0	195.30.40.1	
Default	195.30.40.3	

4. Casos prácticos

Caso práctico 2

Router 2		
DESTINATION	GATEWAY	INTERFACE
192.192.192.0	192.192.40.2	
198.20.12.0	192.192.40.2	
195.30.40.0	195.30.40.1	@MAC7
200.100.30.0	195.30.30.1	@MAC4
200.100.31.0	195.30.31.1	@MAC5
200.100.32.0	195.30.32.7	@MAC6
Default	195.30.40.3	

Bridge	
PUERTO	@MAC
A	@MAC3
B	@MAC7
B	@MAC12

4. Casos prácticos

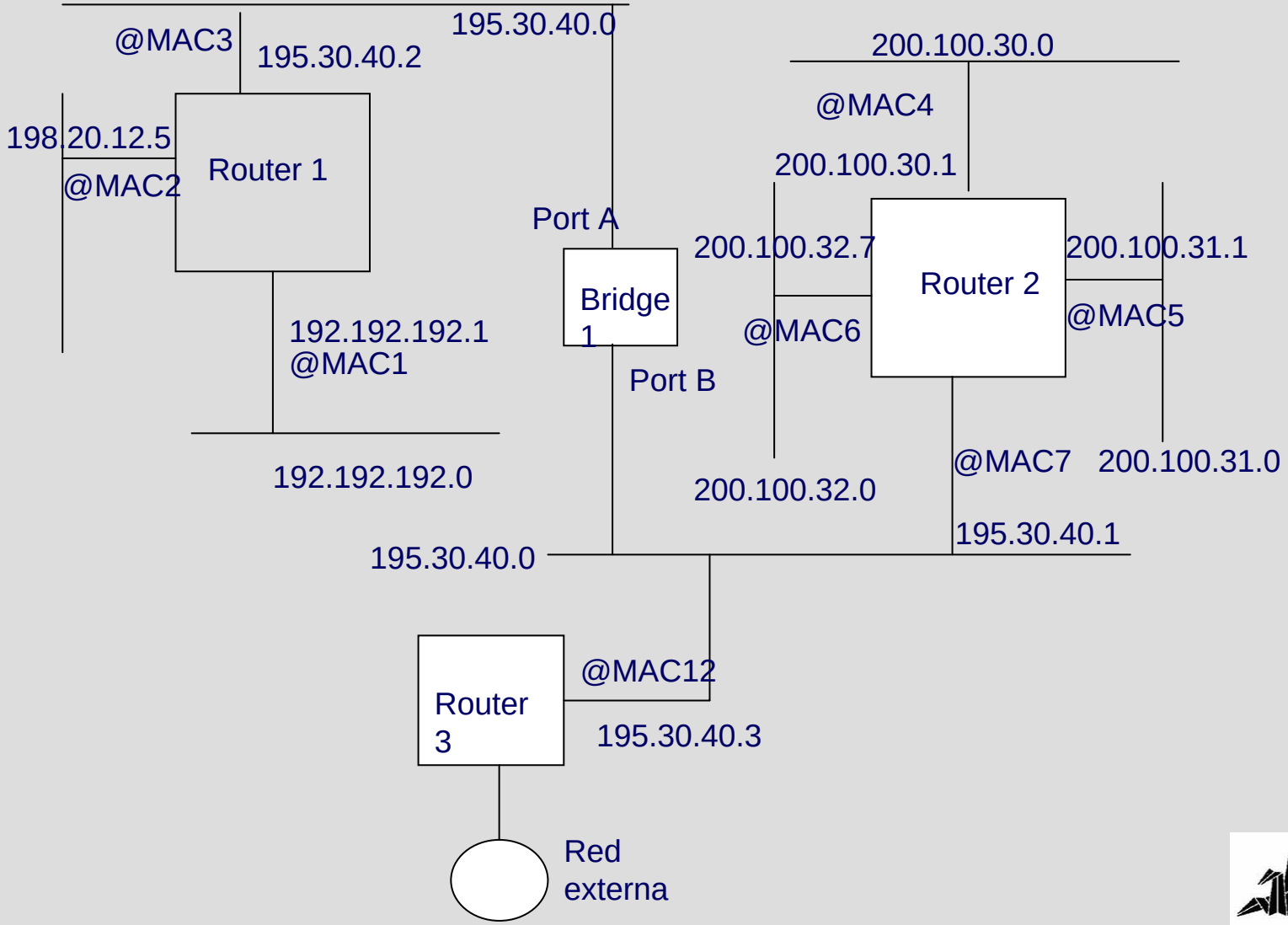
Caso práctico 2

Probad de hacer el esquema de red.

Solución en la siguiente transparencia.

4. Casos prácticos

Caso práctico 2: Solución



4. Casos prácticos

Caso práctico 2

- **La estación con @MAC30 y @IP 200.100.32.101 quiere enviar un paquete IP a la estación con @MAC40 y @IP 198.20.12.101.**
- **Suponiendo que todas las máquinas saben las correspondencias entre @IP - @MAC necesarias, qué direcciones (MAC y IP) contendrá la trama Ethernet en cada segmento que atraviesa?**

4. Casos prácticos

Caso práctico 2: Solución

- ***Las direcciones IP no cambian. Así que en todos los segmentos:***
  - ***IP origen:*** ***200.100.32.101***
  - ***IP destino:*** ***198.20.12.101***
- ***Las direcciones que cambian son las direcciones MAC:***
  - ***Segmento 1 (de MAC30 a router 2):***
    - ***MAC destino:*** ***MAC6***
    - ***MAC origen:*** ***MAC30***
  - ***Segmento 2 (de router 2 a router 1):***
    - ***MAC destino:*** ***MAC3***
    - ***MAC origen:*** ***MAC7***
  - ***Segmento 3 (de router 1 a MAC40):***
    - ***MAC destino:*** ***MAC40***
    - ***MAC origen:*** ***MAC2***

FIN DE LA SESIÓN

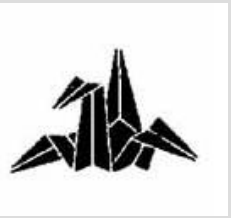
Gracias por su atención!

Deficiencias de seguridad en las tecnologías de comunicaciones

www.shellsec.net

Xavier Vila i Espinosa

Ing. Técnico en Telecomunicaciones – Esp. Telemática



Deficiencias de seguridad en las tecnologías de comunicaciones

1.- Introducción

Deficiencias de seguridad en transmisiones telemáticas

- **Seguridad de host**
  - **Vulnerar la seguridad de host es lo que habitualmente se persigue por parte de los hackers**
  - **Tiene como objetivo general el acceso a información de éste o de otros host**
- **Seguridad de red**
  - **Implican deficiencias en los protocolos de la red**
  - **Se suelen emplear como método para vulnerar la seguridad de host**
- **Errores humanos como factor clave**

Conceptos de seguridad

- **Autenticidad**
  - **Se Dice de lo que es verdadero. El proceso de autenticación nos debe permitir asegurar que el objeto autenticado es quién dice ser**
- **Control de acceso**
  - **Define derechos y privilegios para la utilización de recursos para un objeto o persona auténtica**

Conceptos de seguridad

- **Integridad**
  - **Cualidad de un objeto si no ha sido modificado, ampliado o recortado**
- **Confidencialidad**
  - **Cualidad de la información por la cual solo las personas autorizadas de un mensaje pueden leerlo**

Problemas de seguridad en redes: Nivel físico (I)

- **Redes LAN**
  - **Acceso complejo, detección sencilla.**
- **Redes WAN**
  - **Acceso al canal más sencillo, solución más compleja.**

Problemas de seguridad en redes: Nivel físico (II)

- **Registro de los datos que viajan por un canal**
  - **Dificultad en función del medio**
    - **Aire, cable (bus coaxial), concentrador, cable punto a punto**
  - **Objetivo: sniffing. Precisa decodificación de protocolos a niveles superiores**
- **Alteración de mensajes**
  - **Dificultad en función del medio**
    - **Aire, cable (bus coaxial), concentrador, cable punto a punto**

Problemas de seguridad en redes: Nivel físico (III)

- **Simular averías**
- **Suplantación del origen**
  - **Implica conocimiento de los protocolos de nivel superior**

Problemas de seguridad en redes: Nivel físico (IV)

- **Evitar la comunicación entre los extremos por voluntad expresa (DoS = Denial of Service)**
  - **La dificultad depende del medio físico**
  - **Solución generalmente compleja/cara**
- **Corte de comunicaciones por fenómenos naturales y/o averías**
  - **Es lo más habitual**
  - **Diversos motivos**

Problemas de seguridad en redes: Nivel de enlace (I)

- **Precisamos de un acceso físico a la red**
- **Registro de los datos que viajan por el enlace**
  - **Dificultad: depende del acceso al medio físico**
  - **Es muy peligroso**
- **Modificación de los mensajes de origen a destino**
  - **Dificultad muy elevada**
  - **Detección muy difícil**

Problemas de seguridad en redes: Nivel de enlace (II)

- **Suplantación del origen**
  - **Dificultad baja**
  - **Nos facilita el acceso a servidores**
- **DoS**
  - **Bombardeo de tramas**
  - **Provocar colisiones**
  - **Denegación de paso de token en redes Token Ring**
  - **Impedir que dos estaciones se comuniquen en una red segmentada**

Problemas de seguridad en redes: Caso concreto: IEEE 802.11b

- **Problemas de seguridad de WaveLan**
  - **Es muy sencillo acceder a una red WaveLan**
  - **Tan solo es necesario disponer de una tarjeta de acceso y configurar el ID de red por defecto**
  - **Existen sniffers WaveLan**
- **Soluciones**
  - **Cambiar el ID de red por defecto**
  - **Utilizar la encriptación WEP para la comunicación de la red**

Deficiencias de seguridad en las tecnologías de comunicaciones

2.- Deficiencias protocolo IP

Tipos de ataques (I)

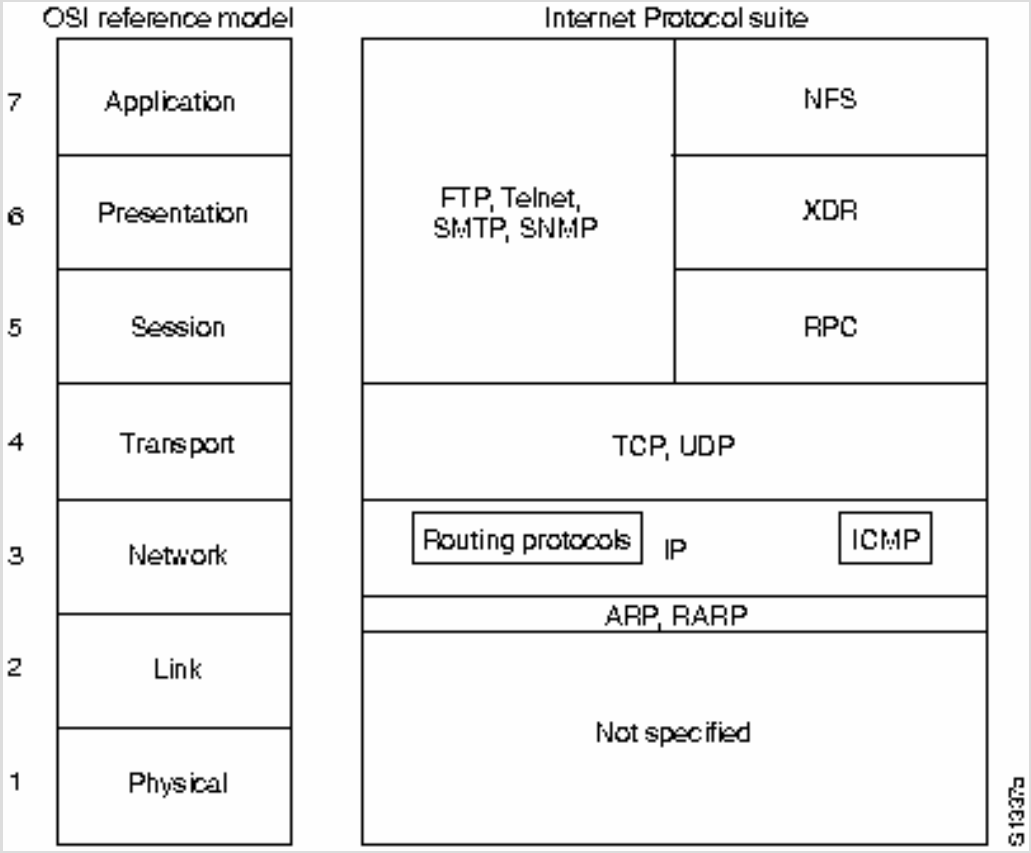
- **Ataques DoS (Denial of Service)**
  - **Ataques que se aprovechan del tratamiento erróneo de las pilas de TCP/IP**
  - **Ataques que se aprovechan de errores concretos de servicios**
- **Ataques DDoS (Distributed DoS)**
  - **Ataques desde varios host.**
  - **Ejemplos: Trinoo, Tribe Flood Network (TFN), TFN2k, Stacheldraht**
- **Buffer Overflow**
- **Tratamiento incorrecto de nombres de ficheros**
  - **Aplicable a servidores web**

Tipos de ataques (II)

- **Comprobaciones inadecuadas de argumentos**
  - **Aplicable a servidores web**
- **Características inseguras de servicios**
  - **Ej: telnet, etc...**
- **Caballos de Troya**
  - **Ej: BackOrifice**
- **Deficiencias en el cifrado o autenticación**
- **Problemas a nivel de kernel de sistemas operativos**
  - **Ej: ping of death**

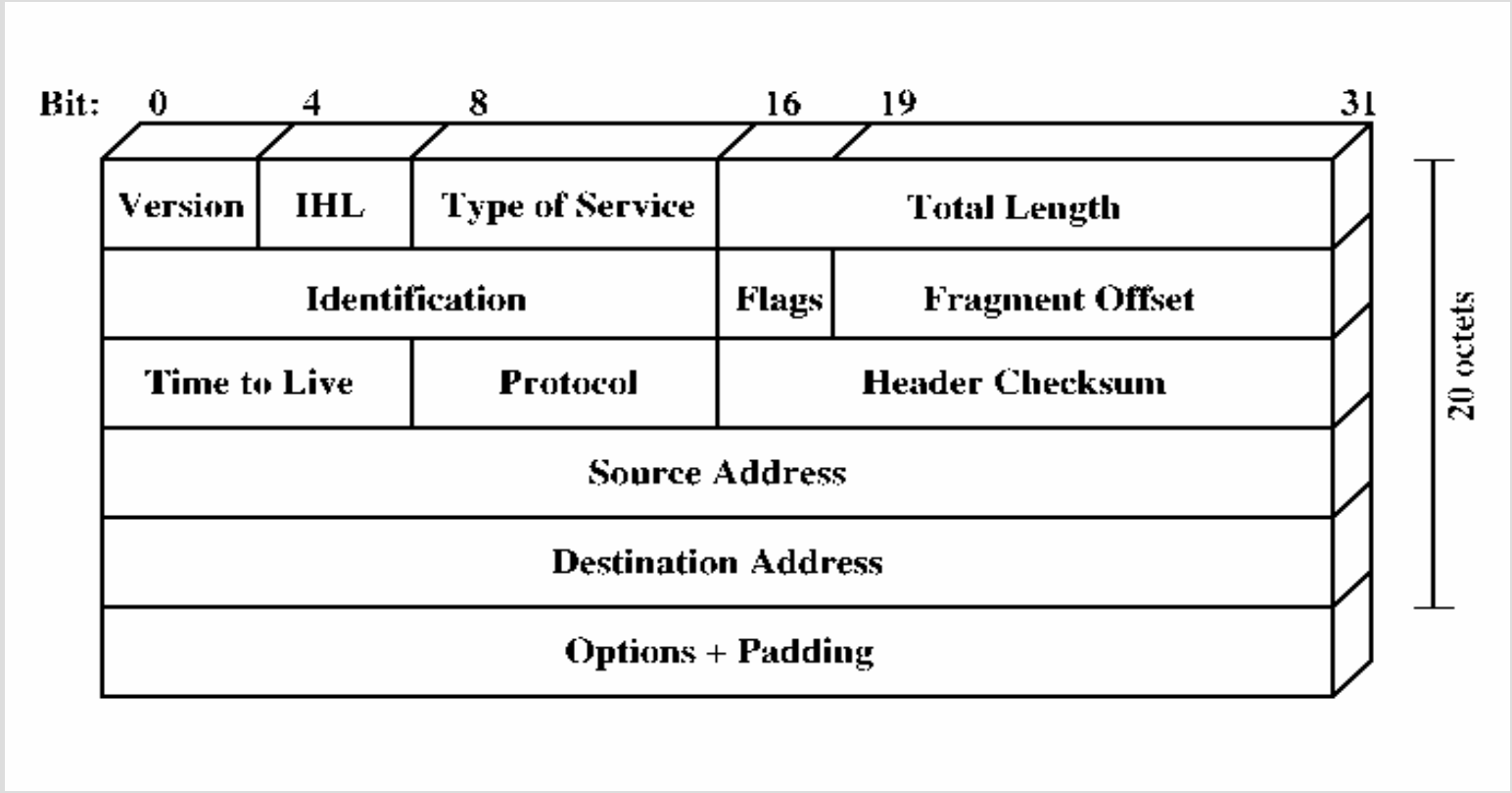
Generalidades

- IP es el protocolo de Internet
  - Breve repaso: correspondencia OSI



Generalidades

- IP es el protocolo de Internet
  - Breve repaso: cabecera IP

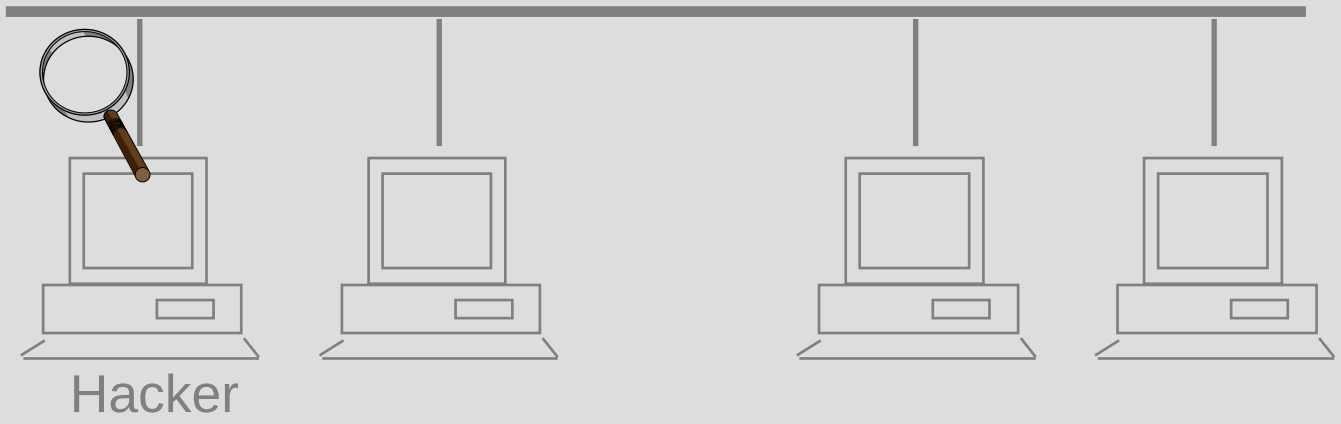


Sniffing o Snooping

- **Ataque muy potente**
- **Es condición indispensable que los paquetes pasen por los canales de comunicación en los cuales el sniffer está conectado**
- **Dos posibilidades**
  - **Conectar un sniffer en la red objeto**
  - **Instalar un sniffer en una estación remota**

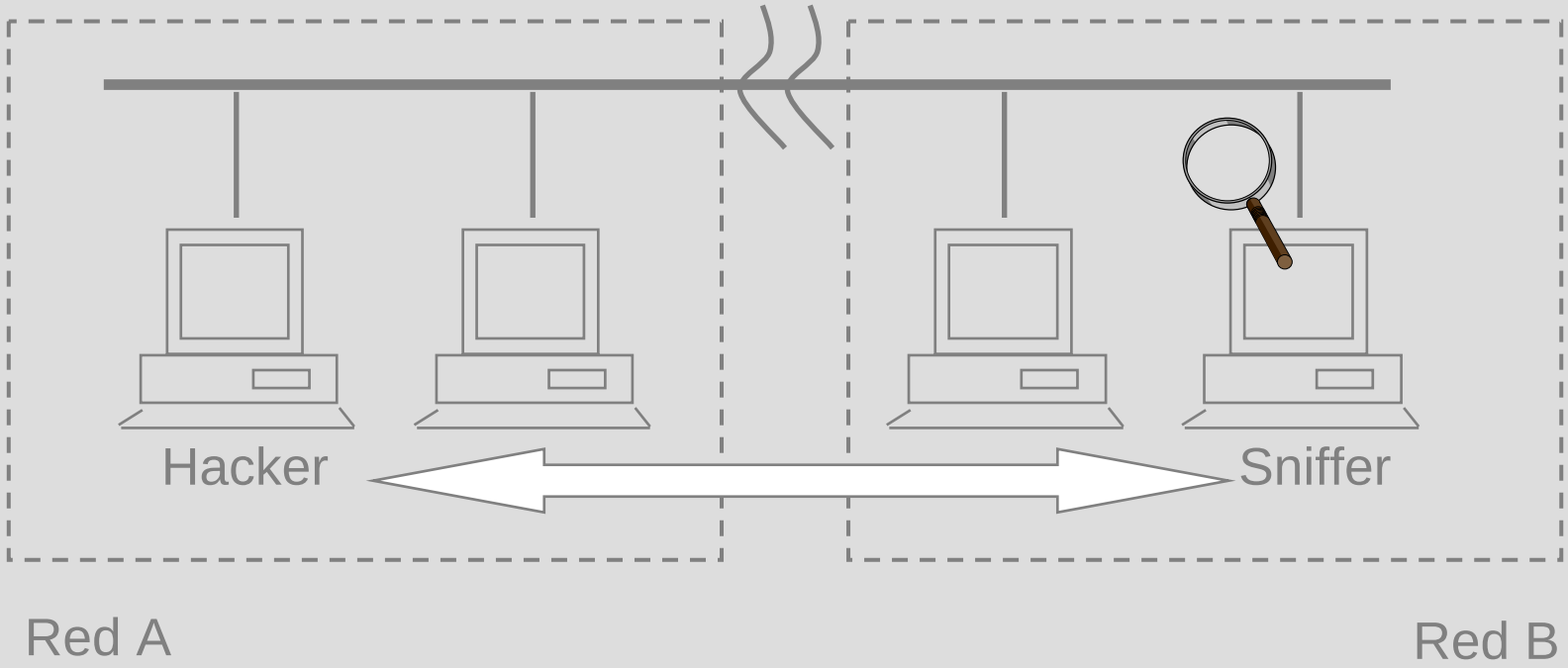
Sniffing o Snooping

- **Sniffer “directo”**



Sniffing o Snooping

- **Sniffer remoto**



Message alteration

- **Viene dado por la falta de control de la integridad de los datos**
- **Es de difícil detección**
- **Precisa de métodos para garantizar la integridad**

Message Delay and Denial

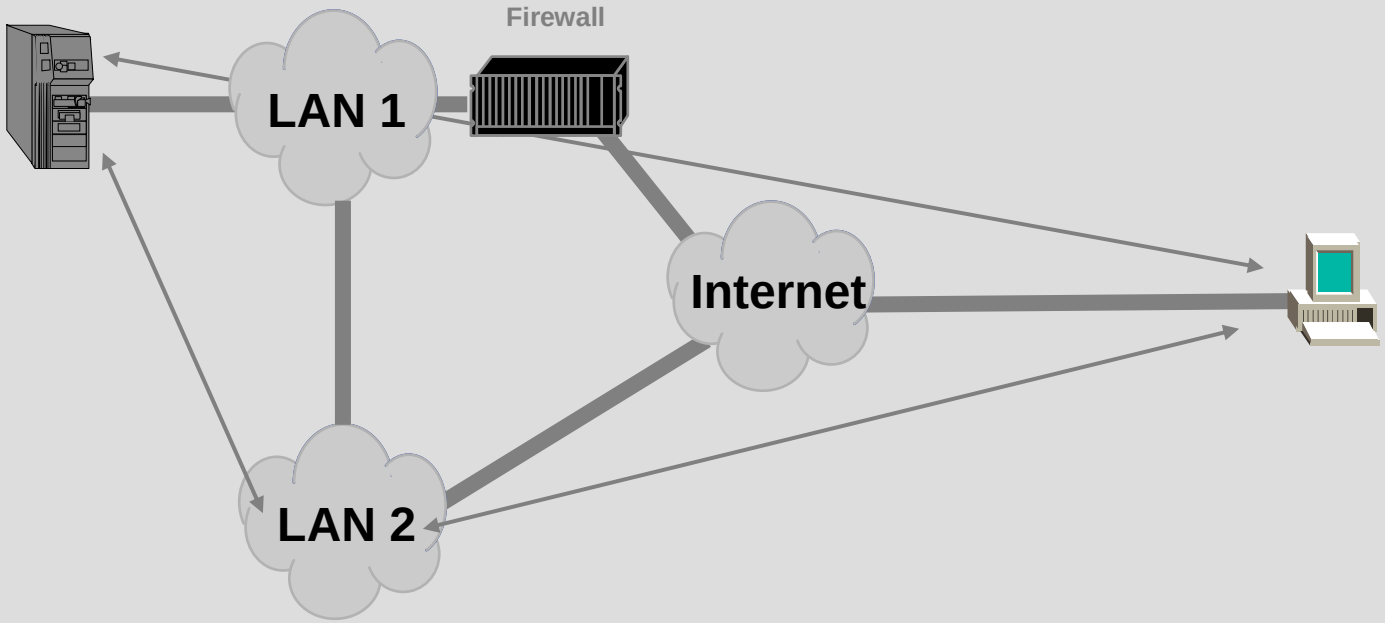
- **Obtenido a partir de modificaciones de parámetros de routers**
- **Delay**
  - **Se modifican las prioridades de paquetes del router**
  - **Precisa obtener acceso al router**
- **Denial (1)**
  - **Se modifican los filtros de acceso al router**
  - **Precisa obtener acceso al router**
- **Denial (2)**
  - **Bombardeo con “basura”**

IP adress masquerading

- Implica suplantación de origen
- Útil cuando tenemos control de acceso por IP
- Dificultad muy baja, fácil detección
- No confundir con IP spoofing!
- Vulnerabilidades
  - Routers
  - Proxys o firewalls
  - SunRPC & NFS
  - Comandos BSD UNIX "r"
  - X windows
  - Otras aplicaciones

Routing attacks (I)

- **Source routing**
  - **Provocado por la definición de IP (source routing option)**
  - **Indica al destino la ruta de retorno de los paquetes**



Routing attacks (II)

- **RIP, BGP, etc**
  - **Se suele enviar información falsa de rutas**
  - **Los routers envían información hacia destinos falsos**
  - **Se utiliza para la captura de información**
  - **También puede utilizarse para DoS**
  - **RIP v2 soluciona el problema utilizando autenticación**

ARP attacks (I)

- **Host Spoofing**
  - **Un host puede responder a tramas ARP que no van dirigidas a el**
  - **Este ataque sólo se puede hacer en una LAN**
  - **2 posibles funcionamientos**
    - **Spoofing**
    - **Intercepción de información**
- **Funcionamiento del spoofing**
  - **En este caso podemos hacer que un equipo responda a las peticiones ARP como si fuera otro equipo (que esté desconectado en ese momento)**
- **Funcionamiento de la intercepción**
  - **En este caso hay que modificar las tablas de ARP de los host origen y destino, de manera que los paquetes se dirijan a un host “interceptor”**

ARP attacks (II)

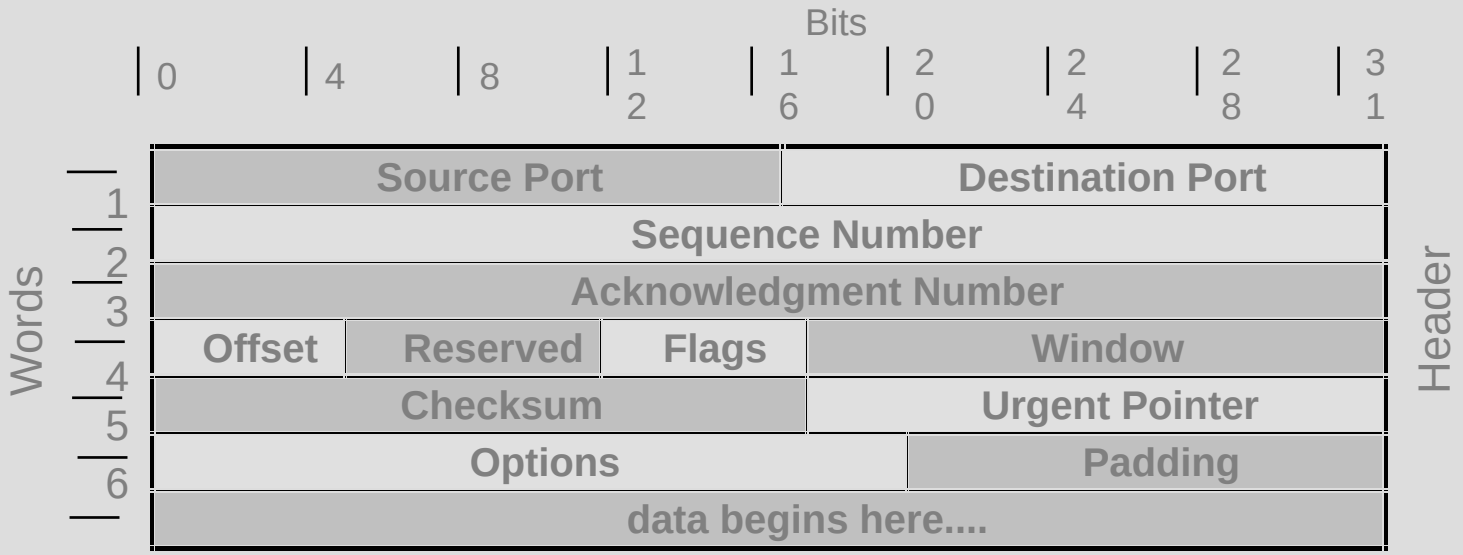
- **DoS**
  - **Actualizar tablas ARP de hosts con información no válida**
    - **Esto provoca que la información no pueda llegar a su destino**
  - **Broadcast storms**
    - **Provocados en una red con más de un router IP**

Deficiencias de seguridad en las tecnologías de comunicaciones

2.- Deficiencias protocolo TCP/UDP

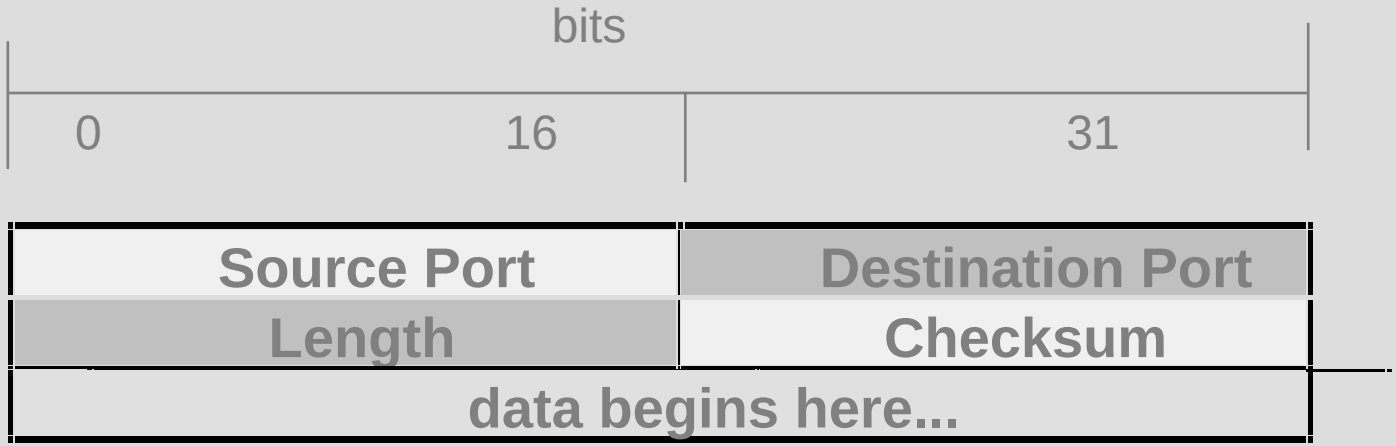
Deficiencias TCP/UDP

- **Repaso funcionamiento TCP: cabecera TCP**



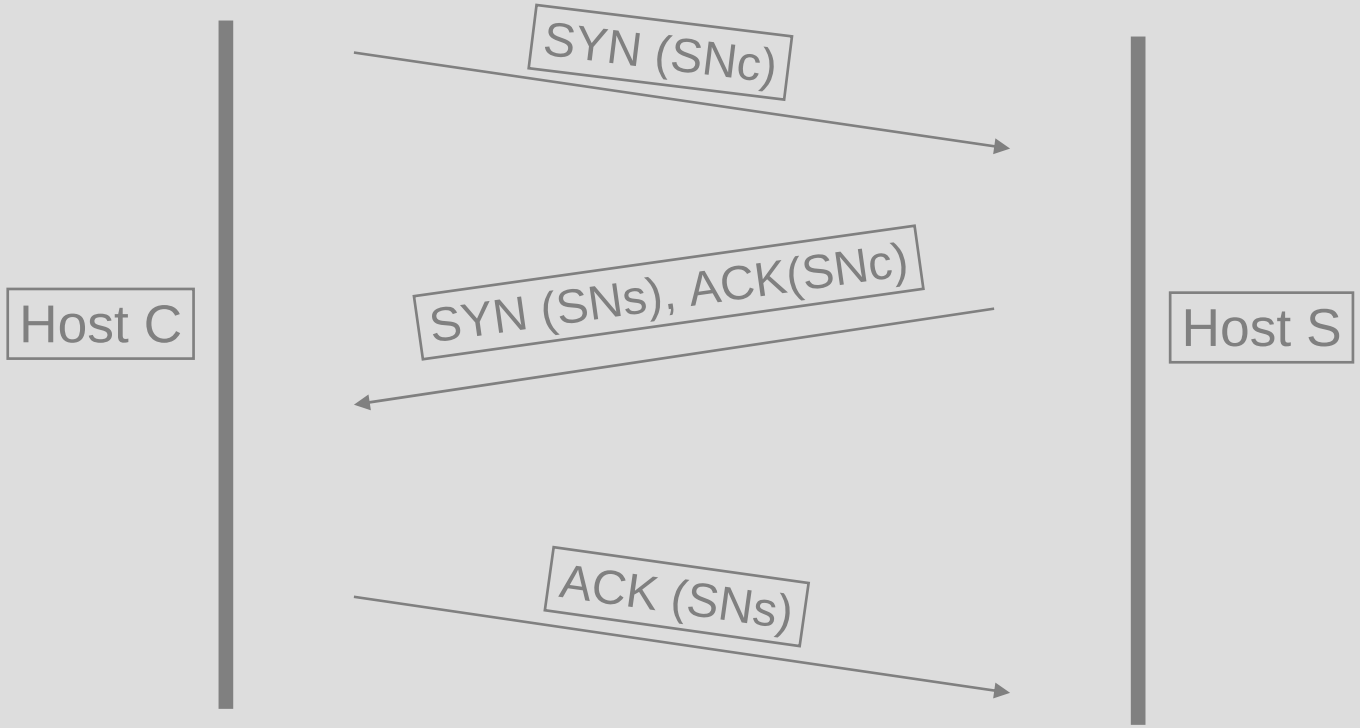
Deficiencias TCP/UDP

- **Repaso funcionamiento TCP: cabecera UDP**



Deficiencias TCP/UDP

- **Repaso funcionamiento TCP: Handshake TCP**

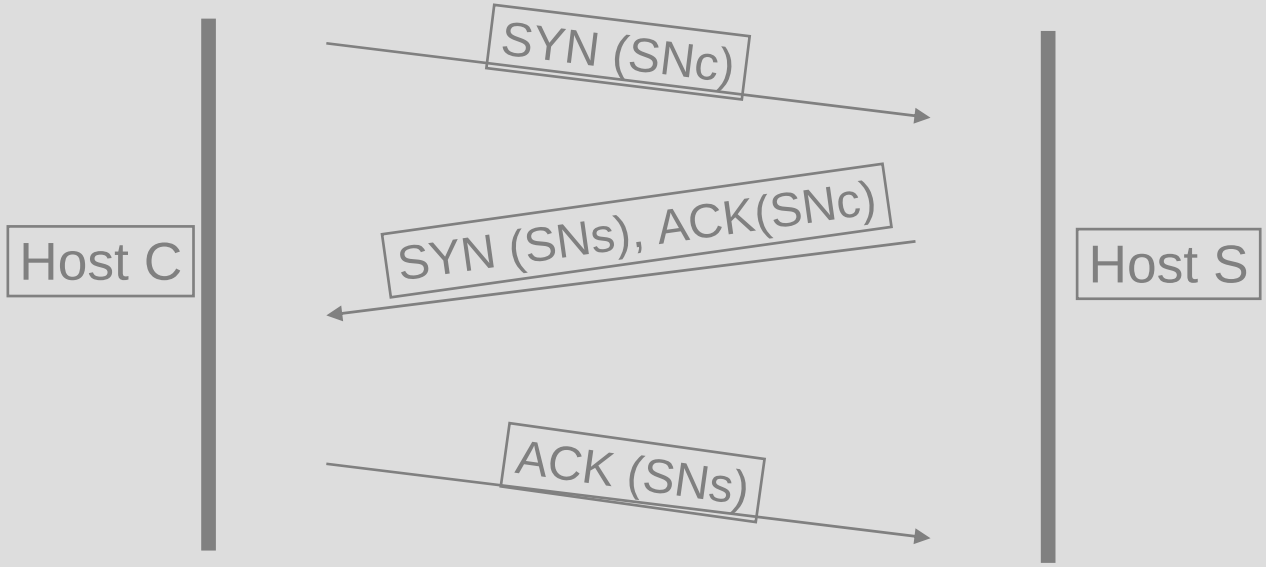


Deficiencias TCP/UDP

- **IP Address Spoofing**
  - **Se utiliza para generar otro tipo de ataques, especialmente el de TCP Sequence Number Prediction**
  - **Solo permite el envío de datagramas IP a un destino, ya que la ruta de retorno no existe**

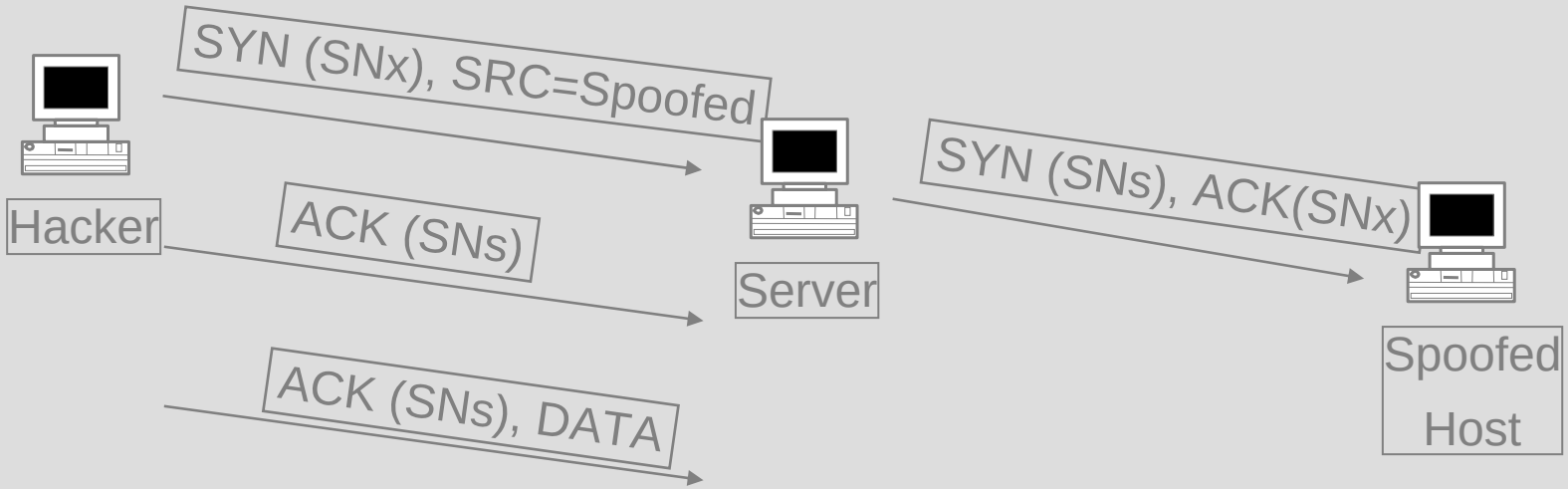
Deficiencias TCP/UDP

- **TCP sequence number prediction**
  - **Utiliza IP address spoofing para como parte del ataque.**
  - **Fundamento: para que una conversación TCP entre dos equipos tenga lugar, el cliente utilizará un número de secuencia SNs**



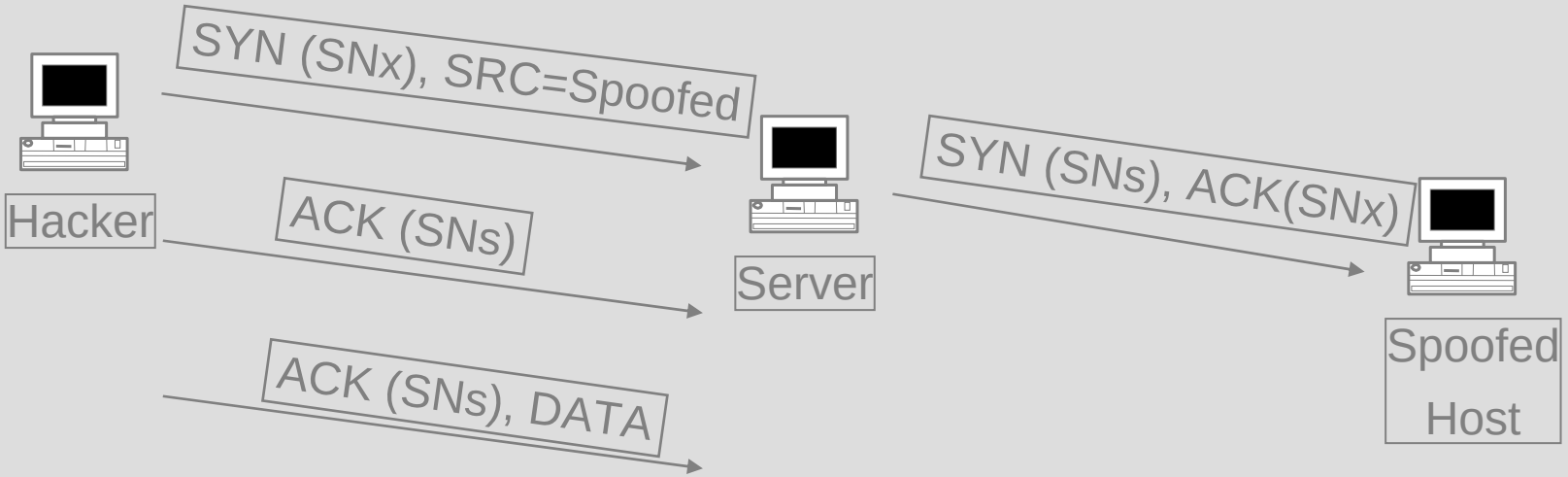
Deficiencias TCP/UDP

- **TCP sequence number prediction**
  - **Si somos capaces de predecir SNs, podremos simular una comunicación TCP provinente de otro host**



Deficiencias TCP/UDP

- **TCP sequence number prediction**
  - **Dificultad: el host impersonado puede resetear el intento de conexión cuando recibe el mensaje del server.**
  - **Se debe atacar a dicho host con un SYN flooding o similar o bien esperar a que el equipo no esté conectado**

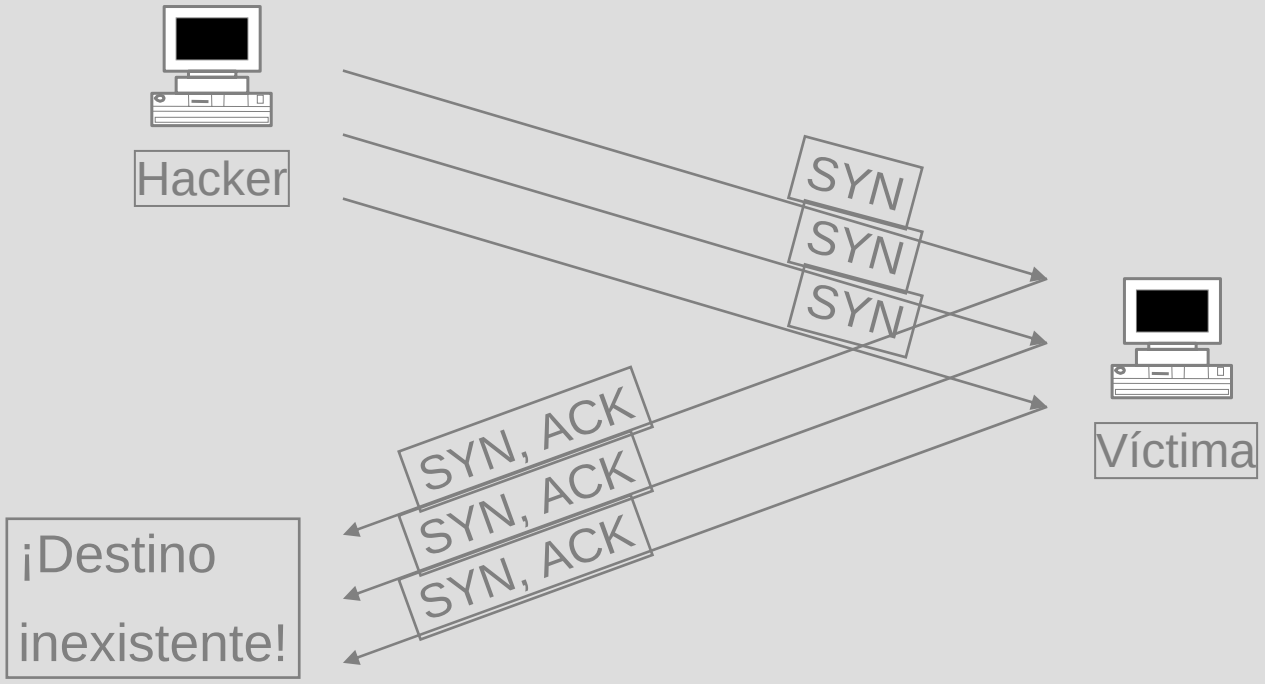


Deficiencias TCP/UDP

- **TCP SYN flooding**
  - **Ataque de tipo Denial of Service**
  - **Se basa en deficiencias del 3-way handshake de TCP**
  - **Se provoca un bombardeo de falsas conexiones, de manera que el equipo atacado no sea capaz de aceptar más conexiones (legítimas)**
  - **Provoca elevada utilización de CPU y memoria**

Deficiencias TCP/UDP

- **TCP SYN flooding: funcionamiento**



Deficiencias TCP/UDP

- **TCP SYN flooding: como detectarlo**
  - **netstat -an: muchas conexiones en estado SYN_RCVD**

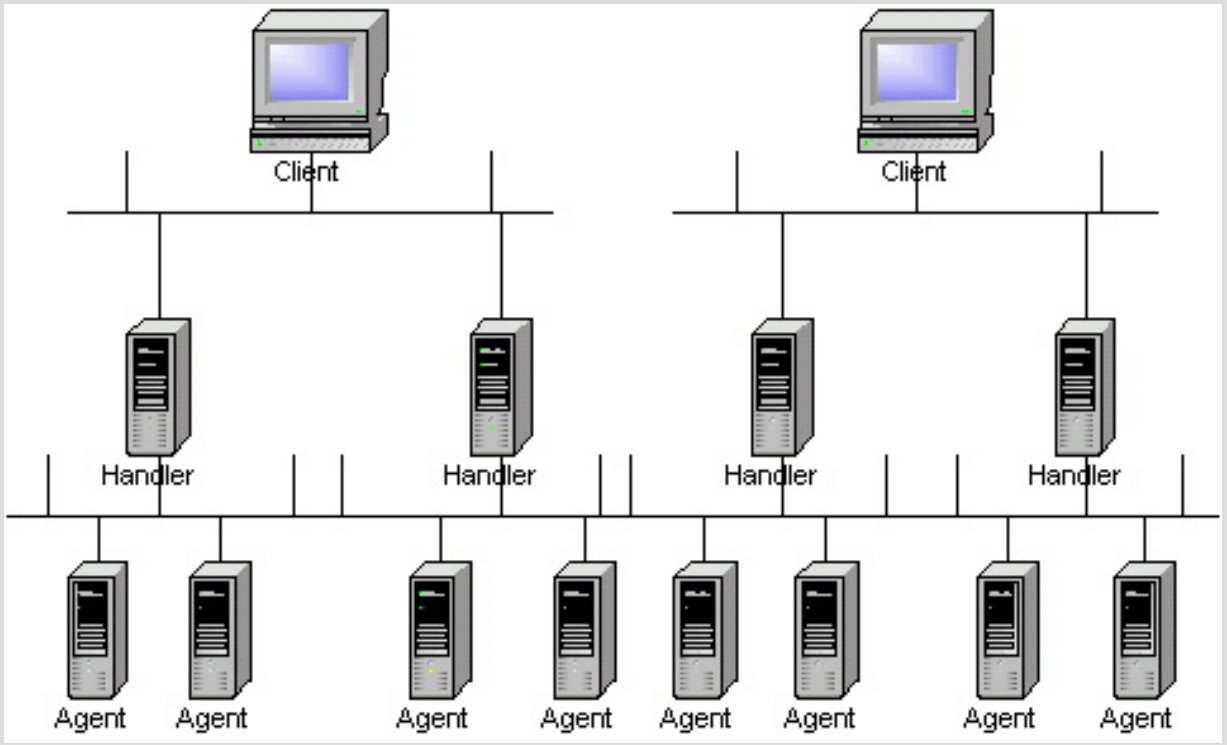
- **Soluciones:**
  - **Incrementar capacidad de los servidores**
  - **Protección firewall**
  - **Decrementar timeout para abortar intentos de conexión**
  - **Aumentar el número de conexiones aceptadas**
  - **Reducir el número de puertos que aceptan conexiones**

Deficiencias TCP/UDP

- **TCP SYN flooding: más características**
  - **El ataque se aplica a cualquier puerto disponible que acepte conexiones**
  - **Elección de dirección IP spoofed**
    - **Sólo una dirección**
    - **Dirección de un rango**
    - **Aleatoriamente**

Deficiencias TCP/UDP

- **TCP SYN flooding: técnica DDoS**



Deficiencias TCP/UDP

- **UDP flooding “pepsi”**
  - **Ataque consistente en el envío de paquetes UDP (spoofed) a puertos de diagnóstico de dispositivos de red (routers, etc…)**
  - **Esto genera una alta utilización de CPU de estos dispositivos, provocando un DoS de la red atacada**

Deficiencias TCP/UDP

- **LAND**
  - **Objetivo: ataque de cualquier tipo TCP/IP**
  - **Funcionamiento: se efectúa una conexión (IP:PORT) a sí mismo**
  - **Requiere spoofing de la dirección IP**
  - **Estrategia útil si no se protege un host de paquetes externos con direcciones IP internas**

BIBLIOGRAFÍA (I)

Libros ,informes y enlaces Internet

- Stuart McClure & Joel Scambray, George Kurtz. *Hacking Exposed (Network Security Secrets & Solutions)*, Osborne/McGraw-Hill, 1999
- Stephen Northcutt & Judy Novak. *Network Intrusion Detection An Analyst's Handbook Second Edition*, New Riders Publishing, 2001
- Guang Yang. *Introduction to TCP/IP Network Attacks*, Department of Computer Science, Iowa State University
- http://astalavista.box.sk
- http://blacksun.box.sk
- http://www.securityfocus.com
- http://www.elfqrin.com/hack/
- Sekar. *Classification of CERT/CC Advisories 1993-1998* http://seclab.cs.sunysb.edu/sekar/papers/
- *Top 50 Security Tools* http://www.insecure.org/tools.html
- Steven M. Bellovin. *Defending Against Sequence Number Attacks*, 1996, AT&T Research
- R.T. Morris. *A Weakness in the 4.2BSD UNIX TCP/IP Software*, CSTR 117, 1985, AT&T Bell Laboratories, Murray Hill, NJ.
- Postel, J. *Transmission Control Protocol*, STD 7, RFC 793, September 1981.
- Atkinson, R. *Security Architecture for the Internet Protocol*, RFC 1825, August 1995.

BIBLIOGRAFÍA (II)

- Postel, J., and J. Reynolds. *Telnet Protocol Specification*, STD 8, RFC 854
- G.R. Wright, W. R. Stevens. *TCP/IP Illustrated, Volume 2*, 1995. Addison-Wesley.
- S. Bellovin. *Security Problems in the TCP/IP Protocol Suite*, Abril de 1989, Computer Communications Review, vol. 19, no. 2, pp. 32-48.
- Rivest, R. *The MD5 Message-Digest Algorithm*, RFC 1321, Abril de 1992.
- Joncheray. *A Simple Active Attack Against TCP*, 1995, Proc. Fifth Usenix UNIX Security Symposium.
- http://www.attrition.org/security/denial/w/synflood.dos.html
- http://www.gncz.cz/kra/index.html
- ftp://ftp.gncz.cz/pub/linux/hunt/
- http://www.l0pht.com/~weld/netcat/
- Synnergy Networks. *Examining port scan methods - Analysing Audible Techniques* ✳ http://packetstormsecurity.org/groups/synnergy/portscan.pdf
- Fyodor. *Art of portscanning*, http://www.phrack.com, http://www.insecure.org/nmap/nmap_doc.html
- N'Ofir Afkin. *Networking Scanning,* http://www.syssecurity.com/archive/papers/Network_Scanning_Techniques.pdf
- Hobbit, *The FTP bounce attack,* http://www.insecure.org/nmap/hobbit.ftpbounce.txt

¡ GRACIAS !