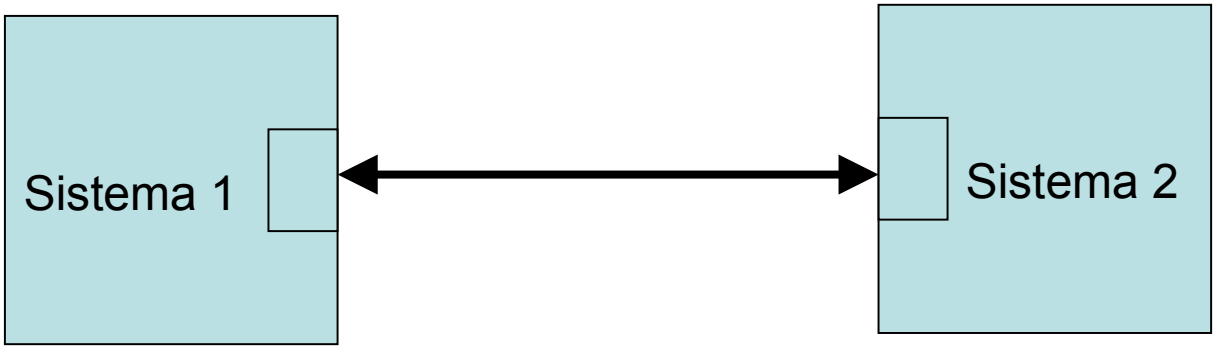
REDES DE COMPUTADORAS

En esta clase:

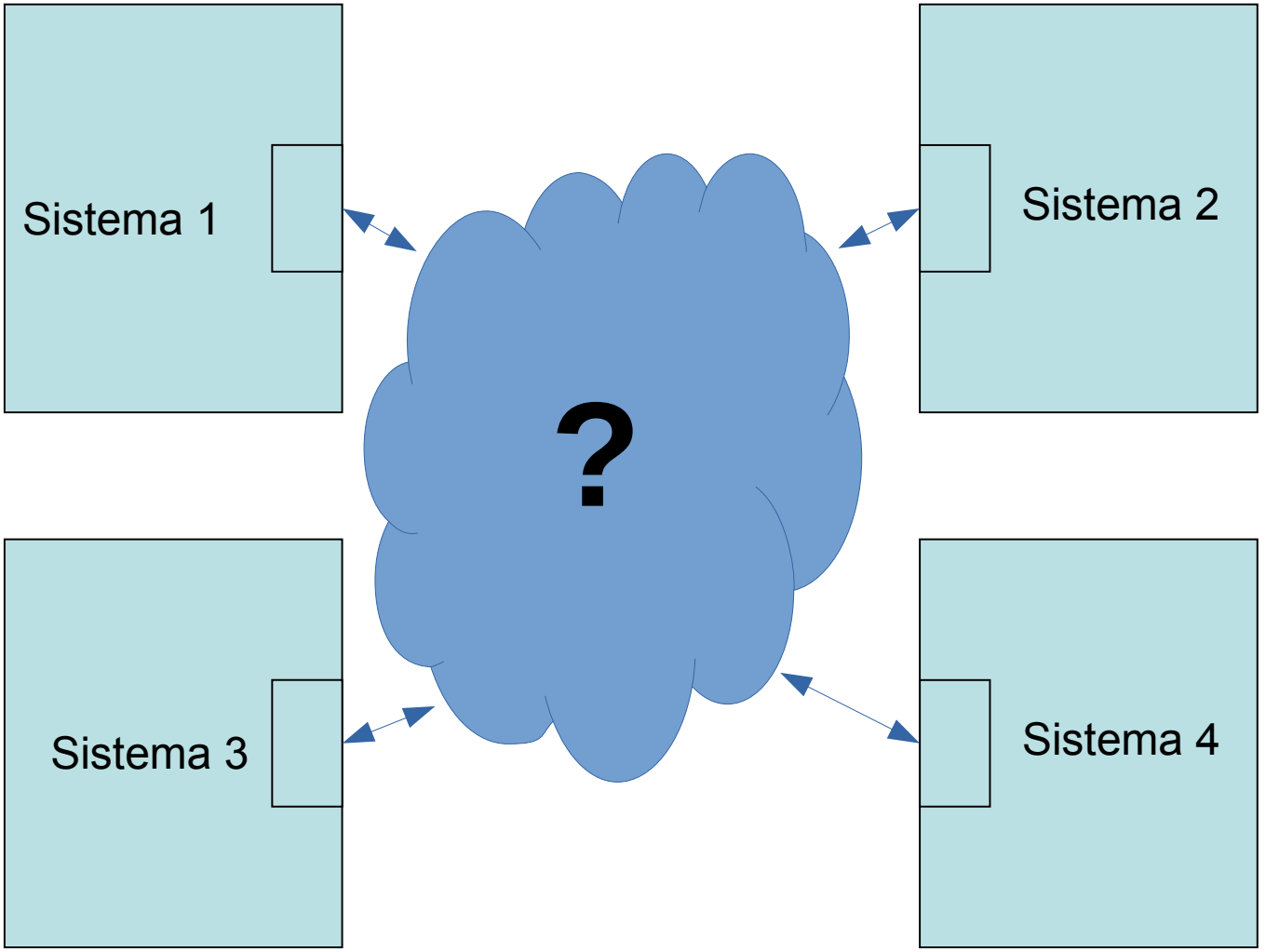
- Topologías de red
- Protocolos de comunicación
- El modelo de capas ISO/OSI.
- Ubicación de Ethernet, IP y TCP en el modelo ISO/OSI

Comunicación entre Computadoras

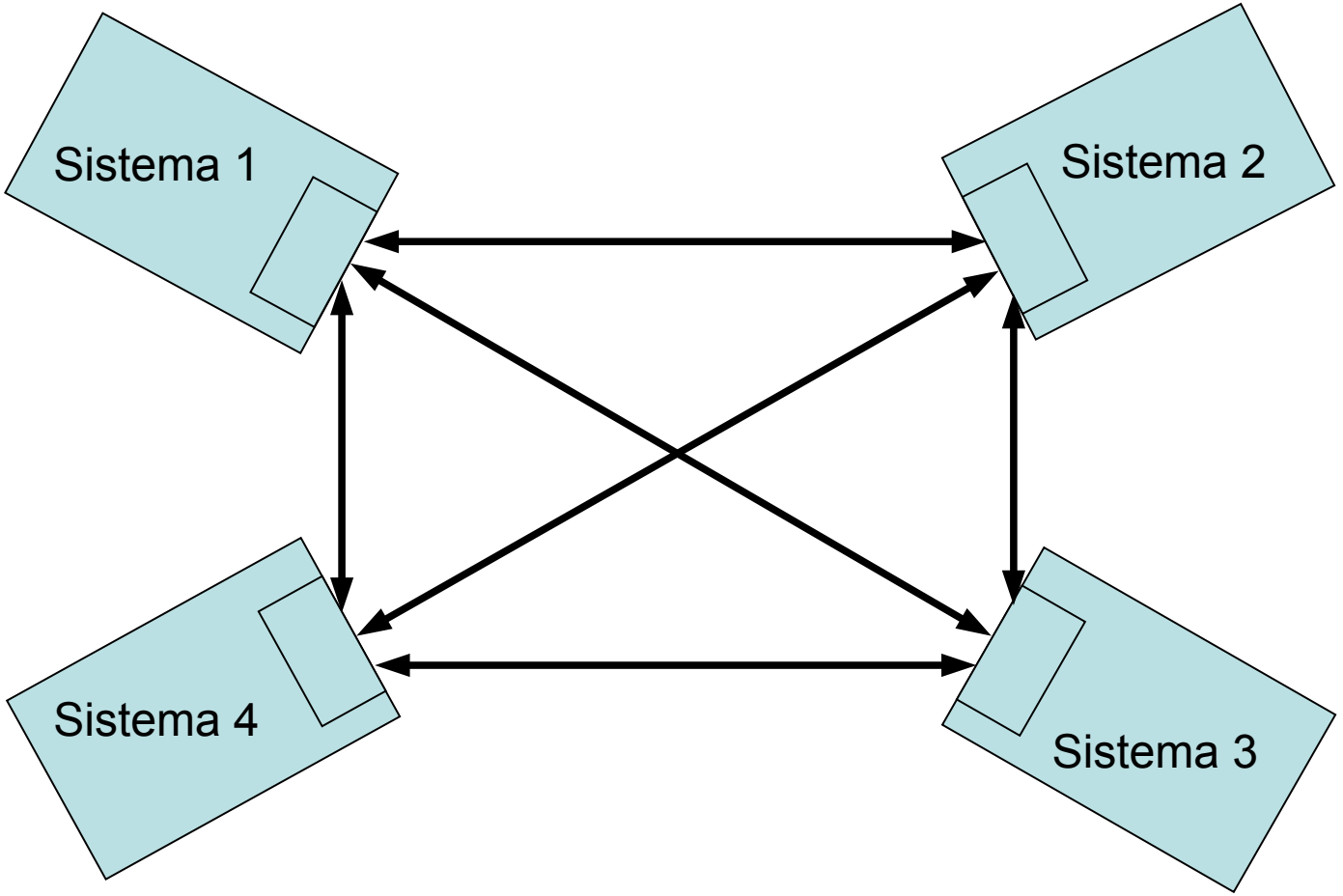
- En general se habla de comunicación entre ***sistemas***.
- Si quiero comunicar ambos sistemas en ambas direcciones debería definir:
  - Quien inicia la comunicación? (uno, el otro o ambos?)
  - Se turnan para enviar la información o transmiten simultáneamente?
  - Cuantos cables necesito para comunicarlos?
  - El flujo de información va a ser continuo o se va a dividir en porciones?
  - Cómo termino la comunicación?
  - Etc…



Comunicación entre Múltiples Sistemas

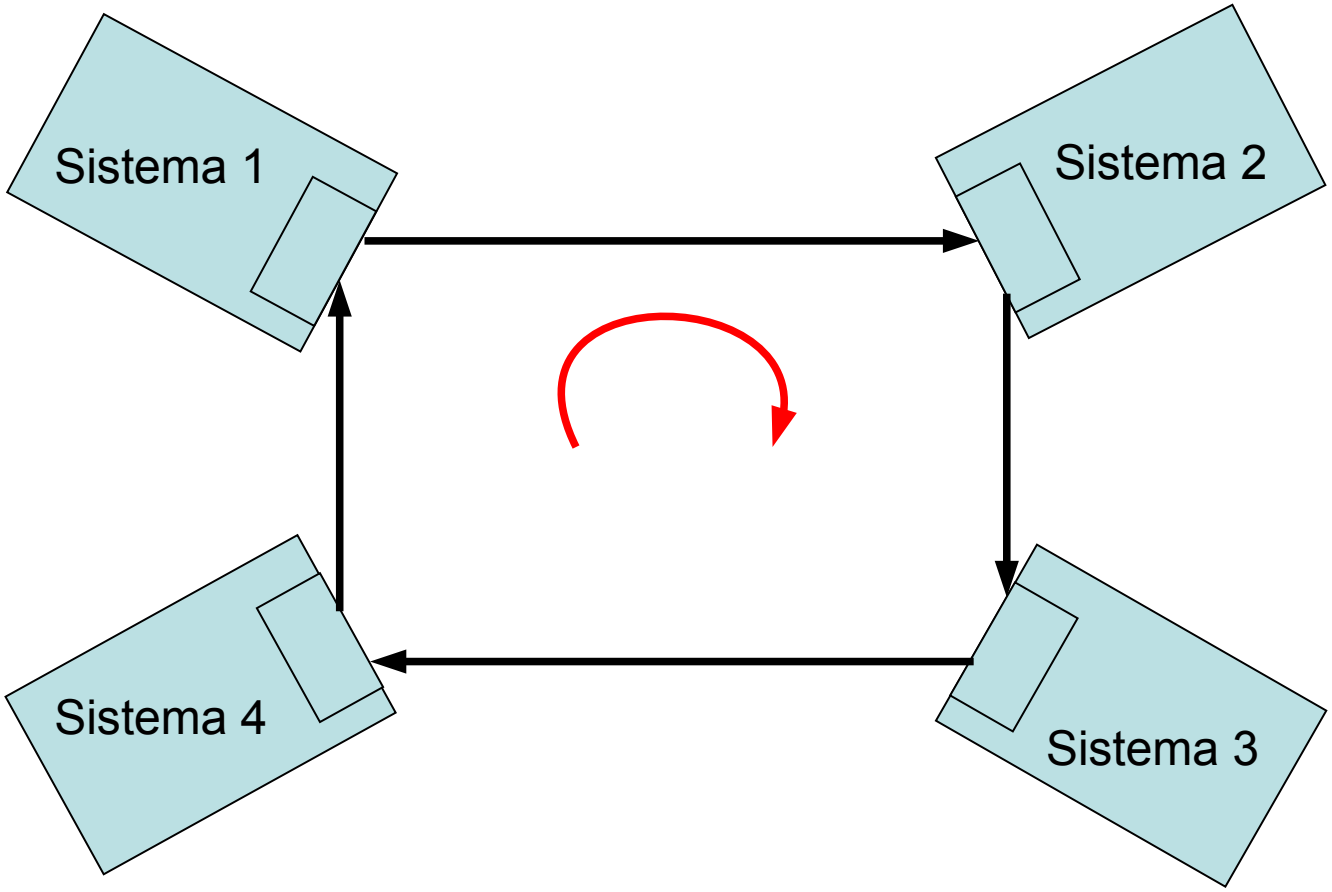


Interconexión Total (Todos con Todos)



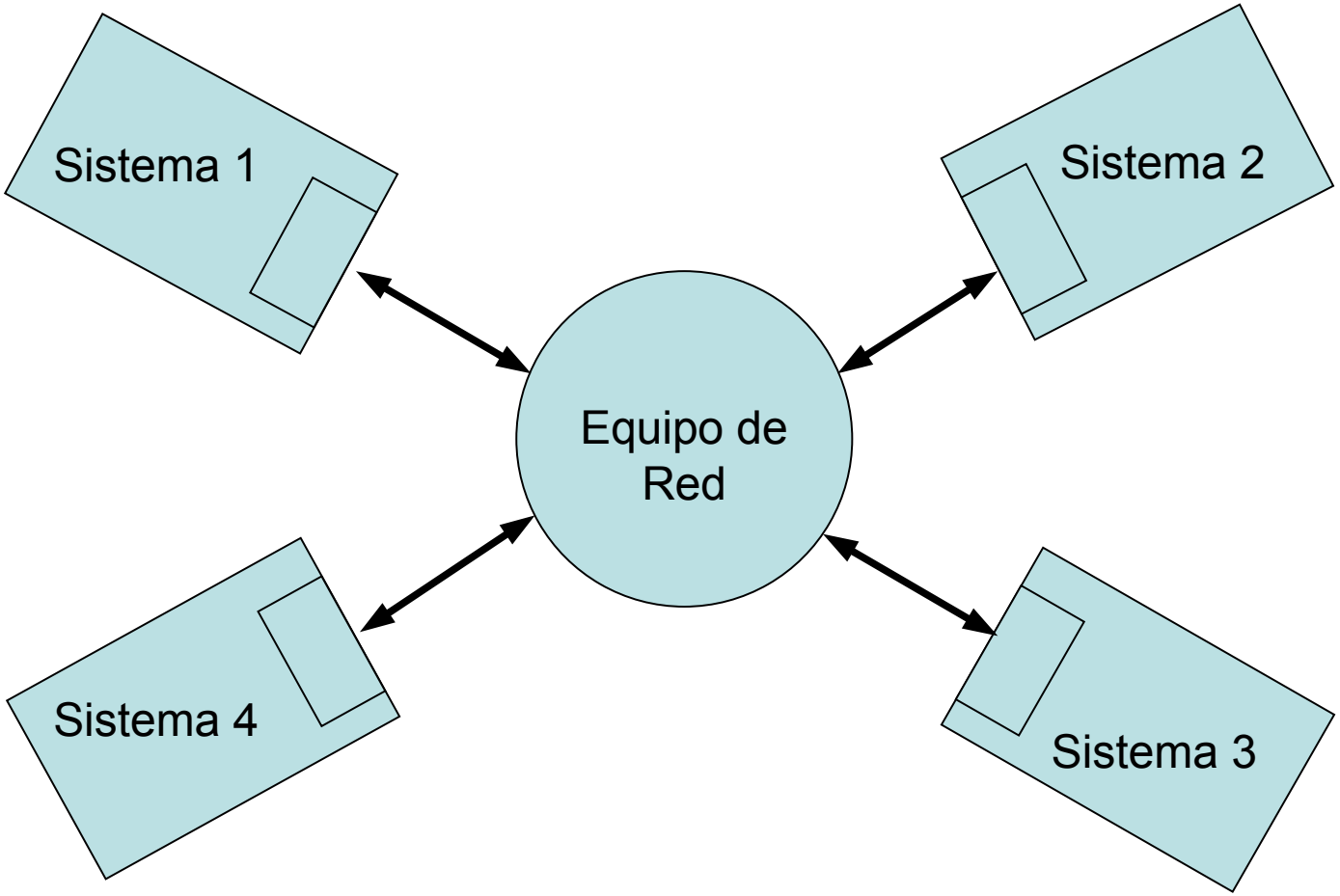
Para N Sistemas, la cantidad de vínculos necesarios crece con N^2

Conexión en Anillo



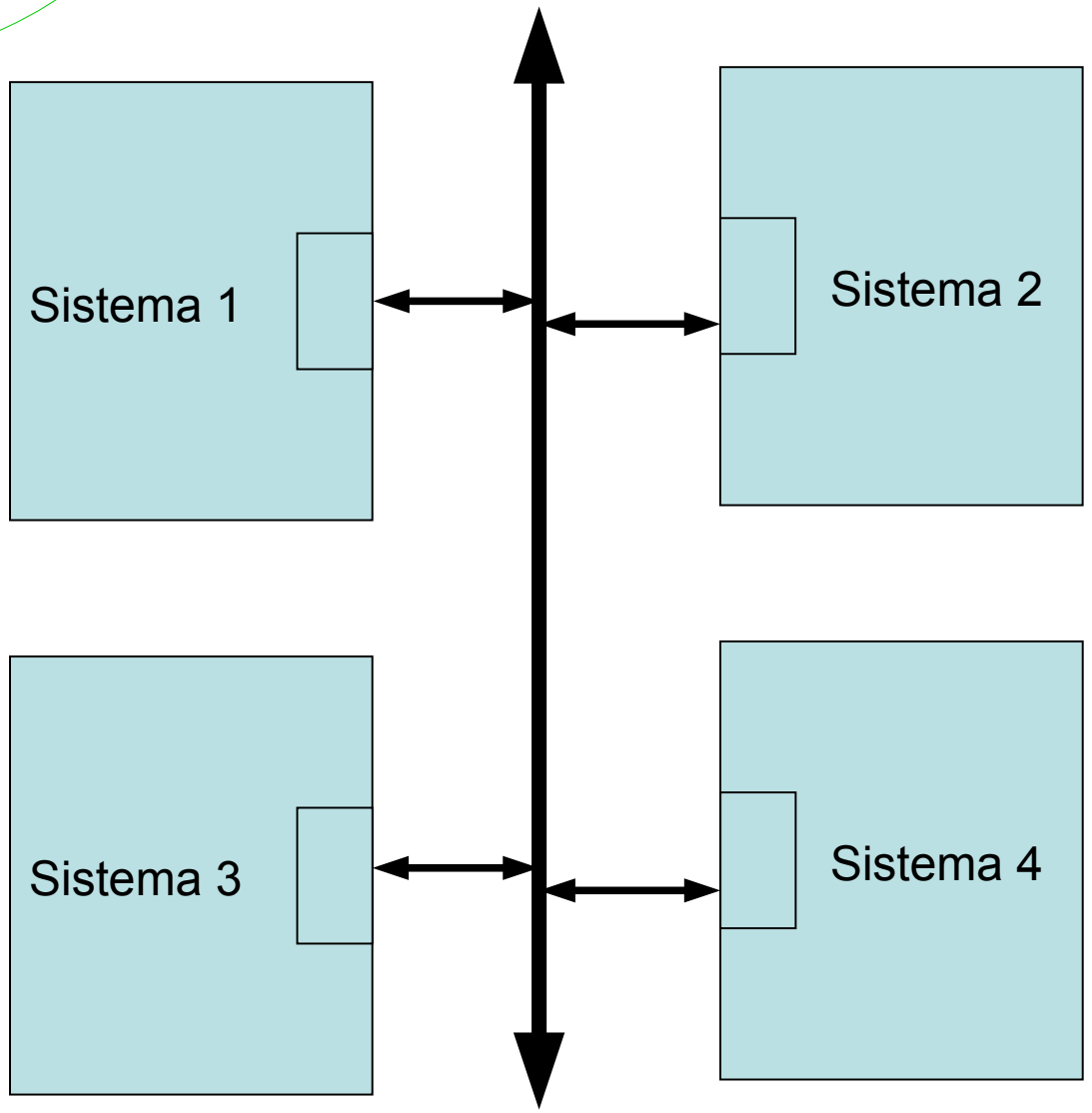
Para N Sistemas, se necesitan N vínculos.
Los vínculos son unidireccionales.
La comunicación debe pasar por hasta (N-2) sistemas intermedios

Conexión en Estrella



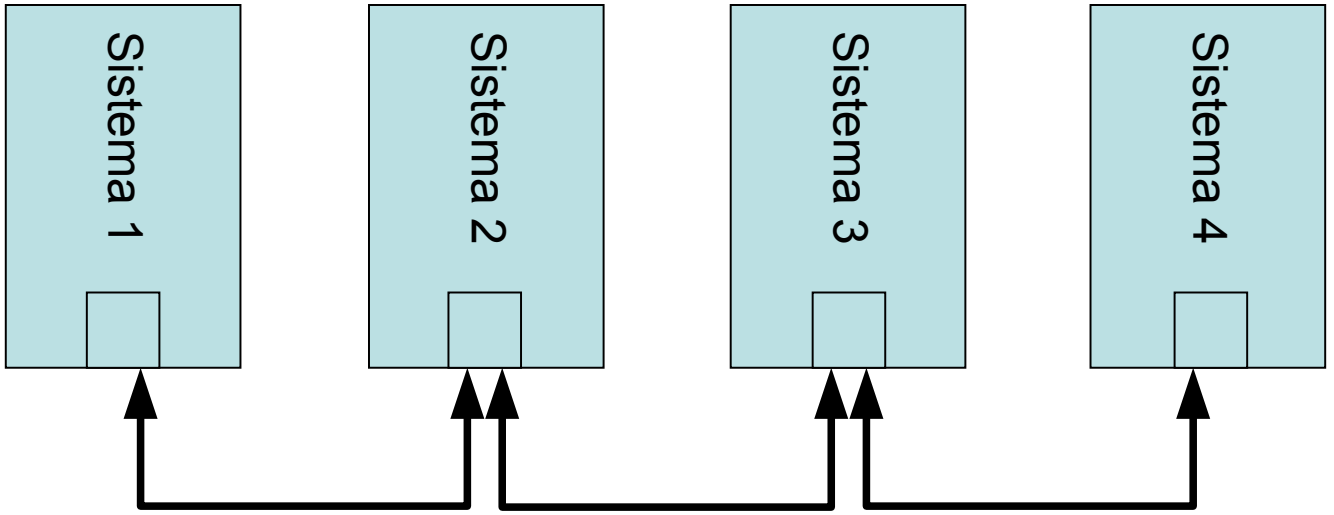
Para N Sistemas, se necesitan N vínculos.
Los vínculos son bidireccionales.
La comunicación debe pasar por un equipo de red

Conexión en BUS



- **Los N sistemas comparten vínculos**
- **Pueden producirse colisiones**

Conexión encadenada (Daisy Chained)

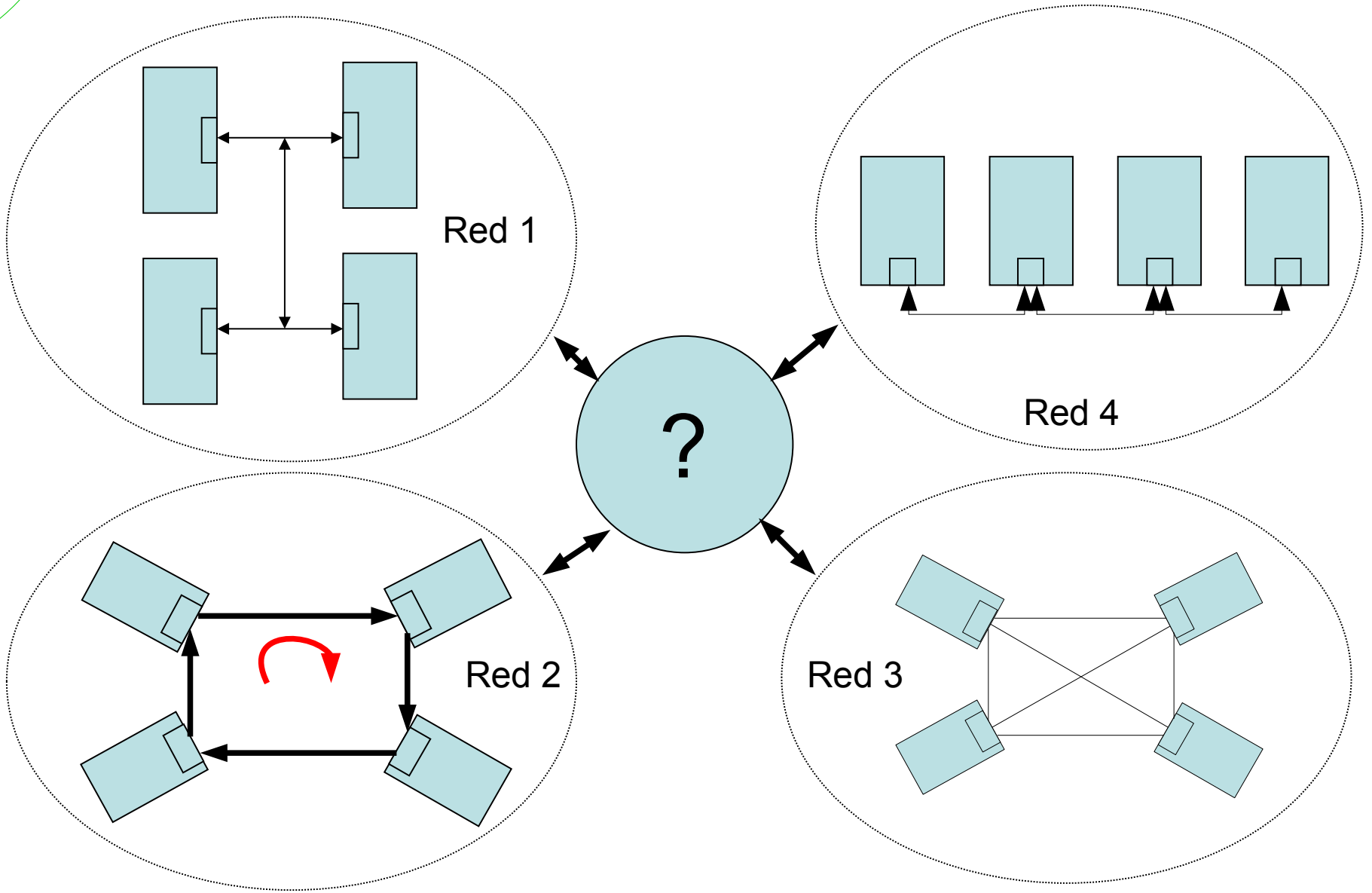


- **Puede pensarse como un anillo abierto**
- **Los vínculos son bidireccionales**

Conexión entre redes

- Las topologías vistas dieron lugar a distintas tecnologías para la interconexión entre sistemas cercanos, formando redes de área local (LAN)
- Cuando se quiere comunicar redes entre sí, el problema se hace un poco más complejo debo tener en cuenta:
  - Redes con distintas topologías.
  - Redes con distintas tecnologías.
  - Redes de distintas velocidades
- Es muy probable que necesite equipos de conexión de Red

Conexión entre redes



Terminología (I)

- Red de Comunicaciones
  - Instalación que provee transferencia de datos
- internet
  - Colección de redes de comunicaciones interconectadas por bridges y/o routers (ver más adelante)
- Internet – notar I mayúscula
  - La colección global de máquinas individuales y redes interconectadas utilizando tecnología TCP/IP
- Intranet
  - internet corporativa utilizada dentro de una organización
  - Usa Tecnología de Internet (TCP/IP y http) para compartir recursos internamente

Terminología (II)

- End System o Sistema Terminal (ES)
  - Dispositivo conectado a una de las redes de una internet
  - Soporta aplicaciones o servicios para el usuario final.
- Intermediate System o Sistema Intermediario (IS)
  - Dispositivo utilizado para conectar dos o más redes.
  - Permite la comunicación entre Sistemas Terminales conectados a distintas redes.

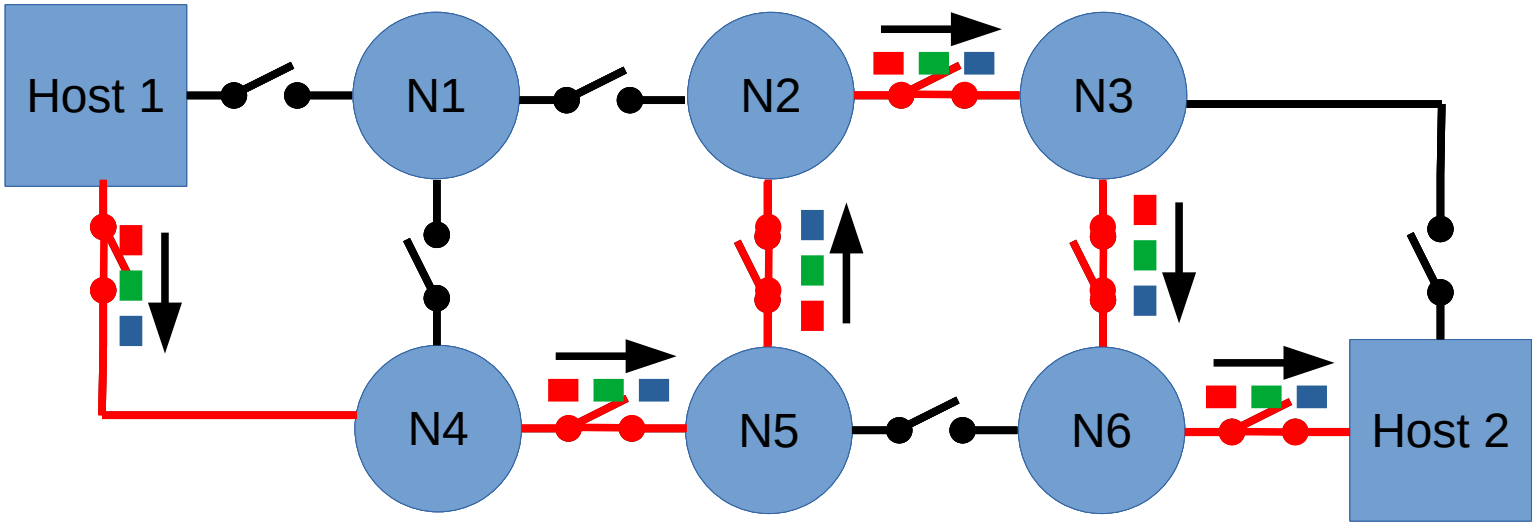
Terminología (III)

- HUB
  - Conecta varios ES entre sí, mediante un Bus Interno.
  - Todos los ES deben utilizar el mismo protocolo de Capa Física (OSI Capa 1).
  - Cuando se recibe la señal de un ES, se regenera previamente a transmitirla al BUS
  - Todos los ES conectados al HUB reciben las señales transmitidas por el resto de los ES.
- Bridge
  - Es usado para conectar dos LAN que utilizan el mismo protocolo
  - Filtra por direcciones pasando paquetes a la red requerida solamente
  - OSI Capa 2 (Data Link o Enlace de datos)
  - Separa dominios de colisión.

Terminología (IV)

- SWITCH
  - Conecta varios ES entre sí, mediante una matriz de switches interna.
  - Puede conectar distintos ES con capas fisicas diferentes.(“Hub mejorado”)
  - Puede funcionar como Bridge. También separa dominios de colisión.
  - Puede inspeccionar protocolos de capa 3 y superiores para proveer filtrado por protocolo.
  - Permite la creación de LAN Virtuales.
- Router
  - Conecta dos o más redes (posiblemente utilizando distintos protocolos)
  - Usa protocolos de interconexión de red.
  - OSI Capa 3 (Network o Red)

Red de conmutación de Circuitos



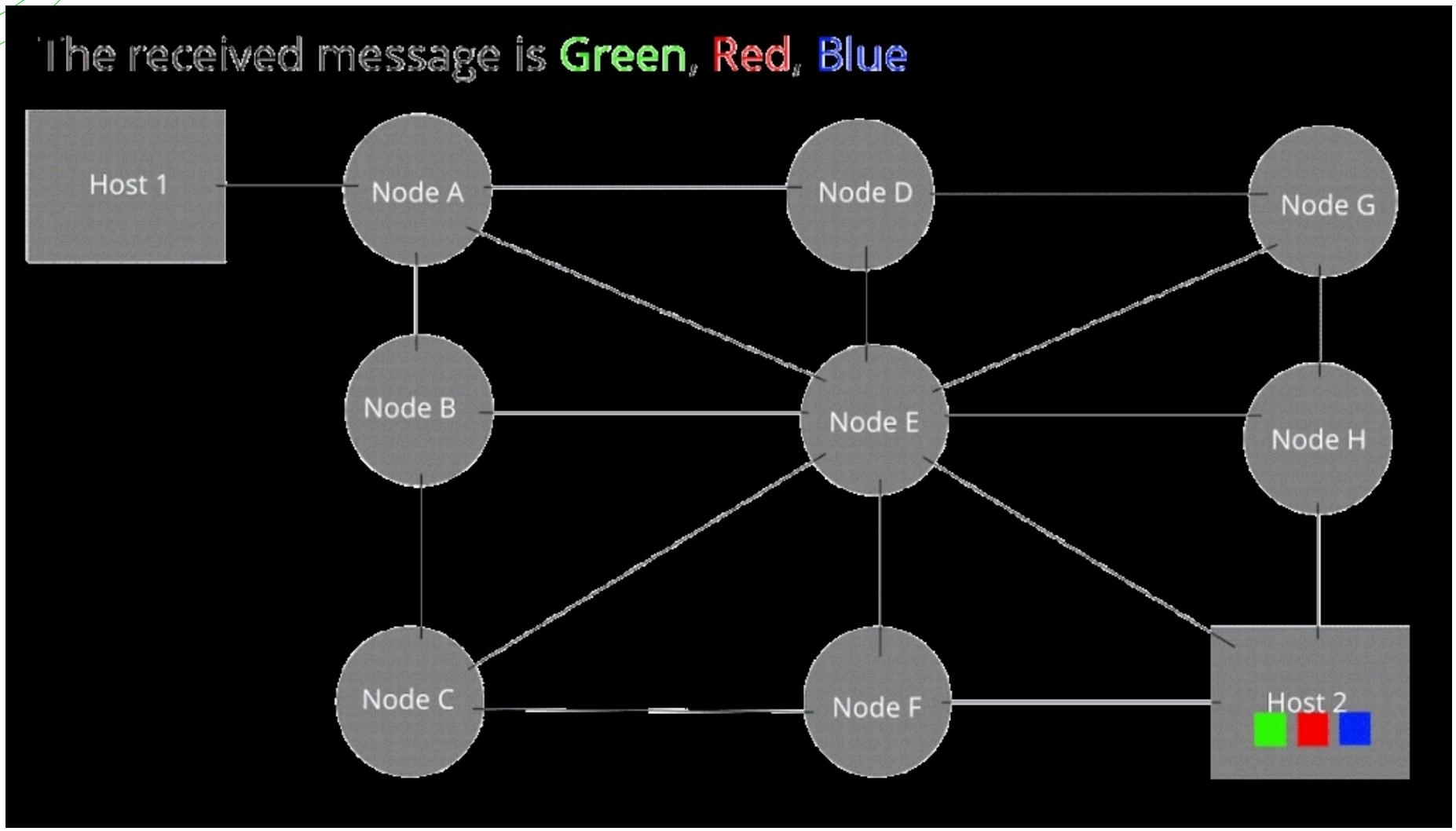
Selección de la ruta

Establecimiento de la ruta (conmutación de circuitos)

Tráfico de Datos

Desconexión de circuitos

Red de conmutación de paquetes



De Oddbodz - Trabajo propio, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=29033823

Redes basadas en conmutación de paquetes.

- Ventajas
  - Flexibilidad
  - Robustez
  - No hay sobrecarga debida al establecimiento de la conexión
- No Confiable
  - No hay entrega garantizada
  - No está garantizado el orden de entrega
  - Los Paquetes pueden tomar distintas rutas
  - La confiabilidad es responsabilidad de una capa superior (por ej. TCP)

Arquitectura de la red

- Basado en conexiones o sin conexión
- Direccionamiento
- Tamaño de paquete
- Mecanismo de acceso
- Timeouts
- Recuperación de Errores
- Informe de estado
- Enrutamiento
- Control de acceso a los Usuarios

Protocolos y Arquitectura de protocolos

- Protocolo : Conjunto de reglas que deben seguir dos entidades para intercambiar datos entre sí.
  - Una entidad es capaz de enviar o recibir información (por ejemplo un programa o aplicación)
  - Un sistema es un objeto físico que contiene una o más entidades.(computadora, router, smartphone, tablet, etc.)

Protocolos y Arquitectura de Protocolos

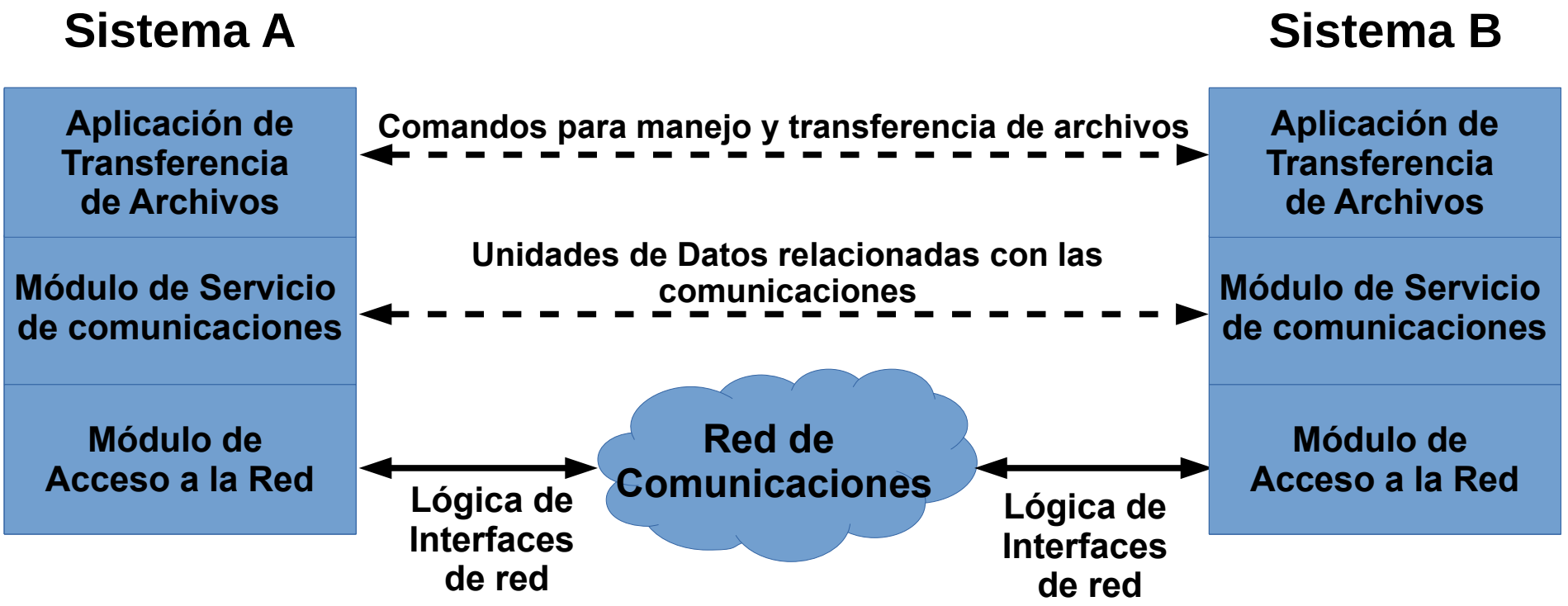
- Elementos de los Protocolos
  - **Sintaxis:** formato de los datos, niveles de señal
  - **Semántica:** Información de control, control de errores.
  - **Temporalidad:** Velocidad de transmisión, secuencias de transmisión y recepción

Protocolos y Arquitectura de Protocolos

- Arquitectura de los Protocolos
  - Es conveniente dividir las tareas de comunicación en módulos que tengan una relación jerárquica entre sí, desde la entidad que desea enviar los datos hasta el vínculo físico que los transporta.
  - La división de tareas entre módulos conforma la arquitectura de los protocolos.

Arquitectura de protocolos

- Dividimos el sistema de transferencia de archivos en tres módulos:
- Toda la información pasa por la red

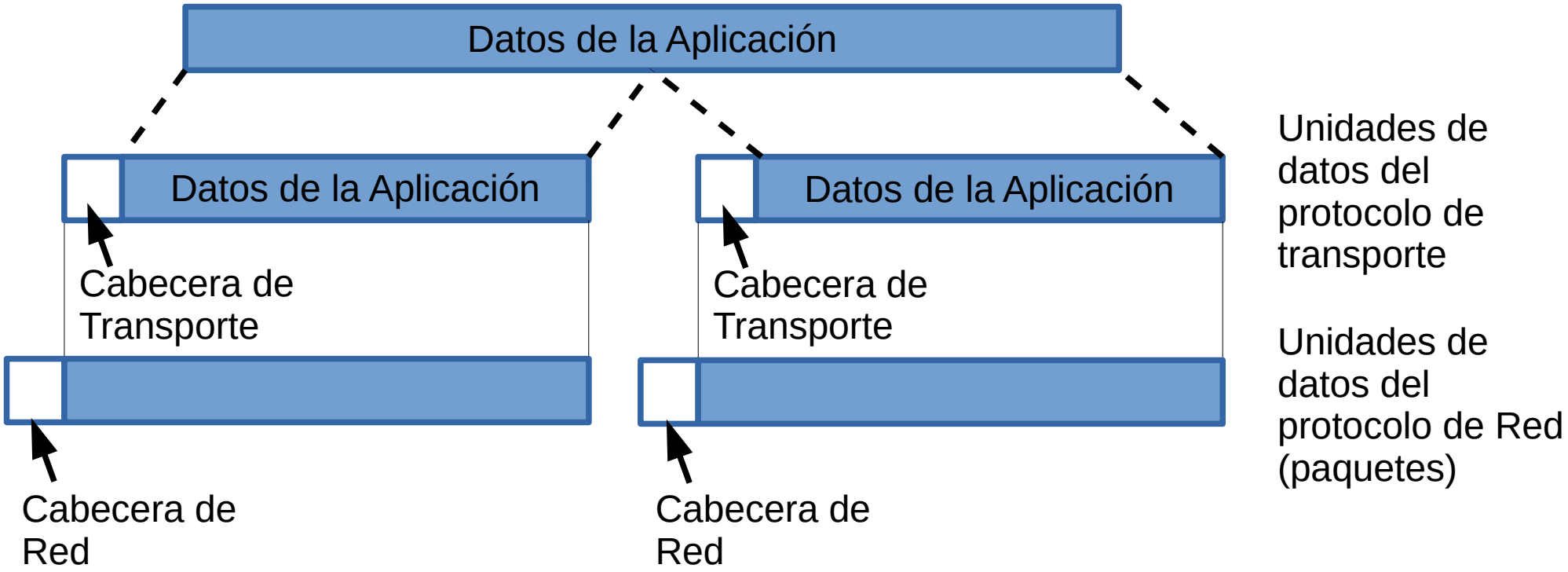


Funciones de los protocolos

1) Encapsulación
2) Segmentación y reensamblado
3) Control de Conexión
4) Entrega en Orden
5) Control de Flujo
6) Control de Errores
7) Direccionamiento
8) Multiplexado
9) Servicios de transmisión

1.- Encapsulación

- Adición de información de control a los datos
- Información de direccionamiento
- Códigos de detección de errores
- Control del protocolo



1.- Segmentación (Fragmentación)

- Bloques de datos de tamaño acotado
- Los datos generados por la aplicación pueden ser grandes
- Los paquetes de red pueden ser más pequeños
- La división de bloques grandes en otros más pequeños se llama segmentación (o fragmentación en TCP/IP)
- Las tramas Ethernet pueden ser de hasta 1530 octetos (bytes), de los cuales hasta 1500 son datos y el resto información del protocolo.
- La segmentación ayuda a la recuperación de errores y verificación de datos

2.- Segmentación: Por que segmentar?

- Ventajas
  - Control de errores mas eficioente
  - Acceso a la red más equitativo
  - Menores retardos
  - Menor tamaño de almacenamiento intermedio (buffers)
- Desventajas
  - Aumento de tamaño debido a las cabeceras (overhead)
  - Mayor frecuencia de interrupción al receptor
  - Mayor tiempo de procesamiento

3.- Control de conexión

- Establecimiento de la conexión
- Transferencia de datos
- Terminación de la conexión
- Puede haber interrupción y recuperación de la conexión
- Se utilizan números de secuencia para:
  - Entrega ordenada
  - Control de flujo
  - Control de errores

4.- Entrega Ordenada

- Las unidades de datos del Protocolo (PDU) pueden recorrer diferentes caminos a través de la red
- Las PDU pueden llegar fuera de orden
- Si se numeran secuencialmente las PDU antes de enviarlas pueden reordenarse al llegar

5.- Control de flujo

- Lo realiza la entidad RECEPTORA
- Se realiza limitando la cantidad o tasa de los datos a recibir.
- Algunos métodos son:
  - Detenerse y esperar (Stop & Wait)
    - (RTS/CTS en RS232)
  - Sistemas que otorgan cupos
    - Ventana deslizante (Sliding window)
- Se necesita en las distintas capas de la red

6.- Control de errores

- Protege contra perdidas o daños en los datos
- Detección de errores
  - El transmisor inserta bits para la detección de errores.
  - Receptor verifica esos bits
  - Si están OK, reconoce haber recibido los datos
  - Si están en error descarta el paquete
- Retransmisión
  - Si no hubo reconocimiento en un tiempo dado (timeout), se retransmite
- Se realiza en distintos niveles

7.- Direccionamiento

- Vamos a considerar distintos tipos:
  1) Nivel de direccionamiento
  2) Alcance del Direccionamiento
  3) Identificadores de conexión
  4) Modo de direccionamiento

7.1- Nivel de Direccionamiento

- Se refiere al nivel dentro de la arquitectura del protocolo
- Dirección única para cada Sistema y y/o router
- Direccionamiento a nivel de red
  - Dirección de Internet o Dirección IP (TCP/IP)
  - Punto de acceso al servicio de red (NSAP) en OSI
- Proceso dentro del sistema
  - Número de Puerto o Port number (TCP/IP)
  - Punto de acceso al Servicio o SAP (OSI)

7.2- Alcance del Direccionamiento

- No ambigüedad global
  - Dirección Global identifica unicamente a un sistema
  - Hay un solo sistema con dirección X
- Es aplicable globalmente
  - Cualquier sistema con cualquier dirección puede identificar a cualquier otro sistema mediante la dirección global de este último
  - La Dirección X de un sistema, lo identifica desde cualquier parte de la red.
- Por ejemplo la dirección MAC en redes IEEE 802

7.3- Identificadores de Conexión

- Se usan en transferencias de datos orientadas a conexión (circuitos virtuales)
- Se asigna un nombre de conexión durante la fase de transferencia
  - Se reduce el overhead, ya que los identificadores de conexión suelen ser mas cortos que las direcciones globales
  - En algunos casos el ruteo puede ser fijo e identificado por el nombre de la conexión
  - Si las entidades establecen multiples conexiones, permite el multiplexado
  - Provee información de estado

7.4- Modo de Direccionamiento

- Direcciones Unicast
  - Se usan cuando una dirección se refiere a un único sistema
  - Se envía a una maquina o persona
- Direcciones de Broadcast
  - Pueden referirse a todas las entidades dentro de un conjunto
  - Se envían a todas las maquinas o usuarios
- Direcciones Multicast
  - Pueden dirigirse a un subconjunto de entidades dentro de un conjunto mayor
  - Se envían a algunas máquinas o a un grupo de usuarios

8.- Multiplexado

- Permite múltiples conexiones en una maquina o entidad
- Permite mapear múltiples conexiones en un nivel de la arquitectura del protocolo a una única conexión en otro nivel, p. ej.
  - Aceptar datos entrantes desde múltiples orígenes remotos para procesarlos con una única aplicación
  - Transportar una cantidad de conexiones en una única fibra óptica.
  - Utilizar múltiples canales de comunicación para aumentar la capacidad o ancho de banda de una única conexión.

9.- Servicios de transmisión

- Prioridad
  - Por ejemplo, un mensaje de control tiene prioridad sobre una transferencia de datos
- Calidad de Servicio
  - Tasa de transferencia de datos (throughput) aceptable mínima
  - Retardo máximo aceptable
- Seguridad
  - Restricciones de acceso

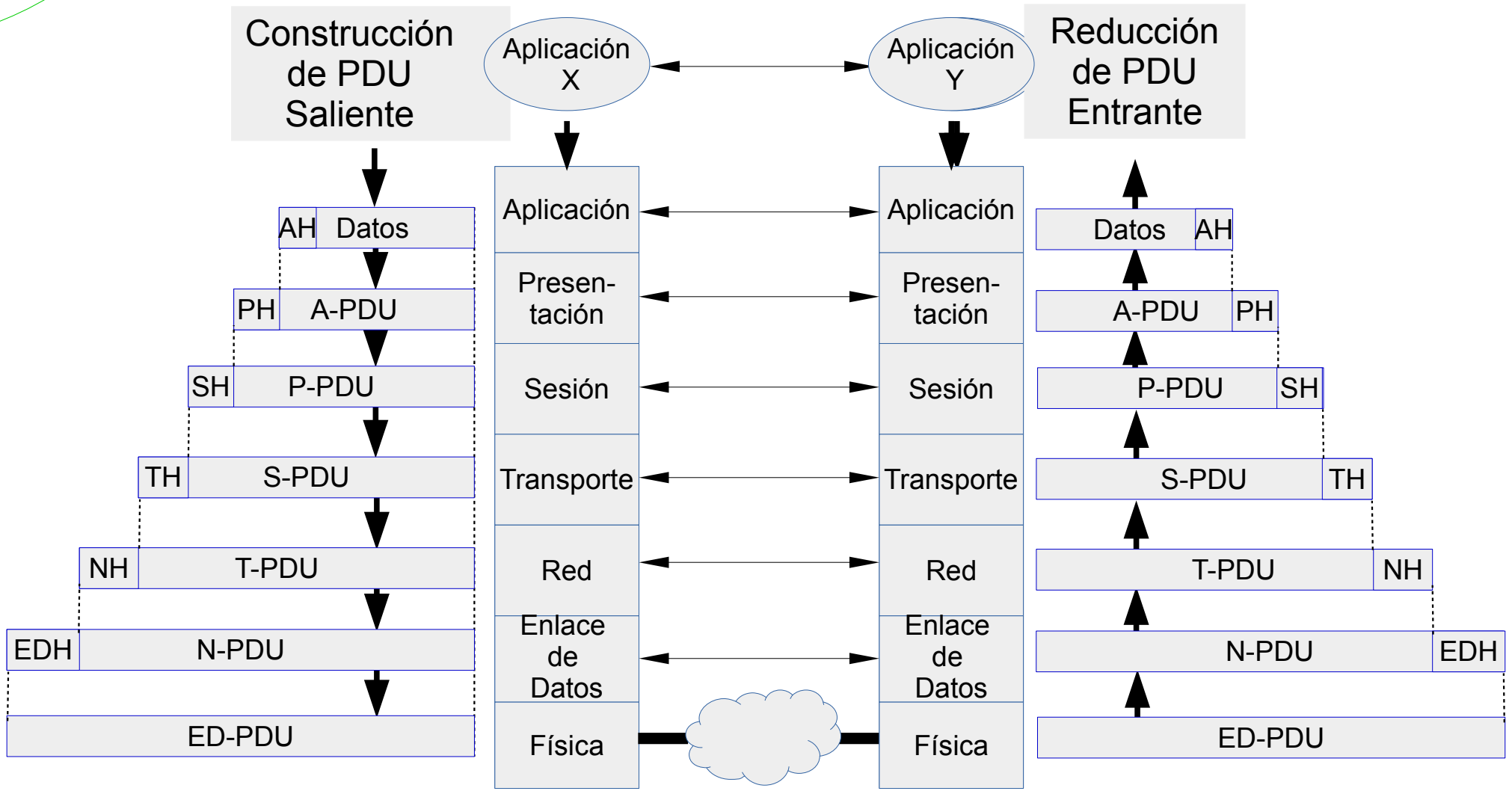
Modelo ISO / OSI

- Es un modelo de capas
- Cada capa realiza un subconjunto de las funciones de comunicación requeridas.
- Cada capa confía en la capa adyacente inferior para realizar funciones más primitivas.
- Cada capa provee servicios a la capa adyacente superior
- Si se realizan cambios en una capa no deberían requerirse cambios en las otras capas

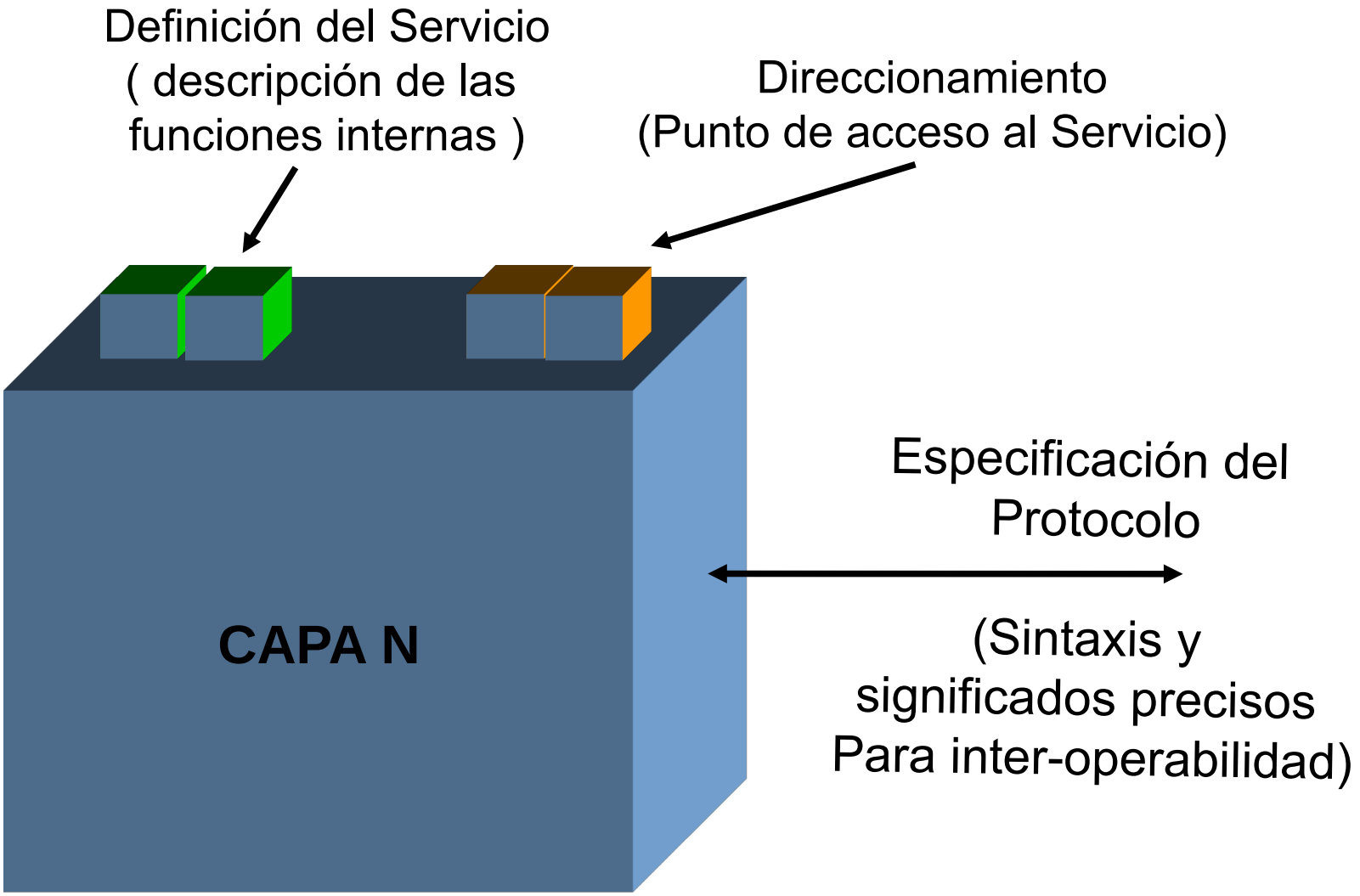
Elementos de la estandarización

- Especificación de Protocolo
  - Opera entre la misma capa en dos sistemas
  - Puede involucrar diferentes sistemas operativos
  - La especificación del protocolo debe ser precisa
    - Formato de las unidades de datos
    - Semántica (significado) de todos los campos
    - Secuencia permitida de Unidades de control de protocolo (PCU)
- Definición de Servicio
  - Descripción funcional de lo que se provee
- Direccionamiento
  - Referenciado por Puntos de Acceso al Servicio (SAP)

Modelo ISO / OSI



Estándares específicos de cada capa



CAPAS OSI (1)

- Física
  - Interfaz Física entre dispositivos
    - Mecánica
    - Eléctrica
    - Funcional
    - Procedural
- Enlace de datos
  - Medios para activar mantener y desactivar un enlace de datos confiable
  - Detección y control de errores
  - Las capas superiores pueden asumir una transmisión libre de errores

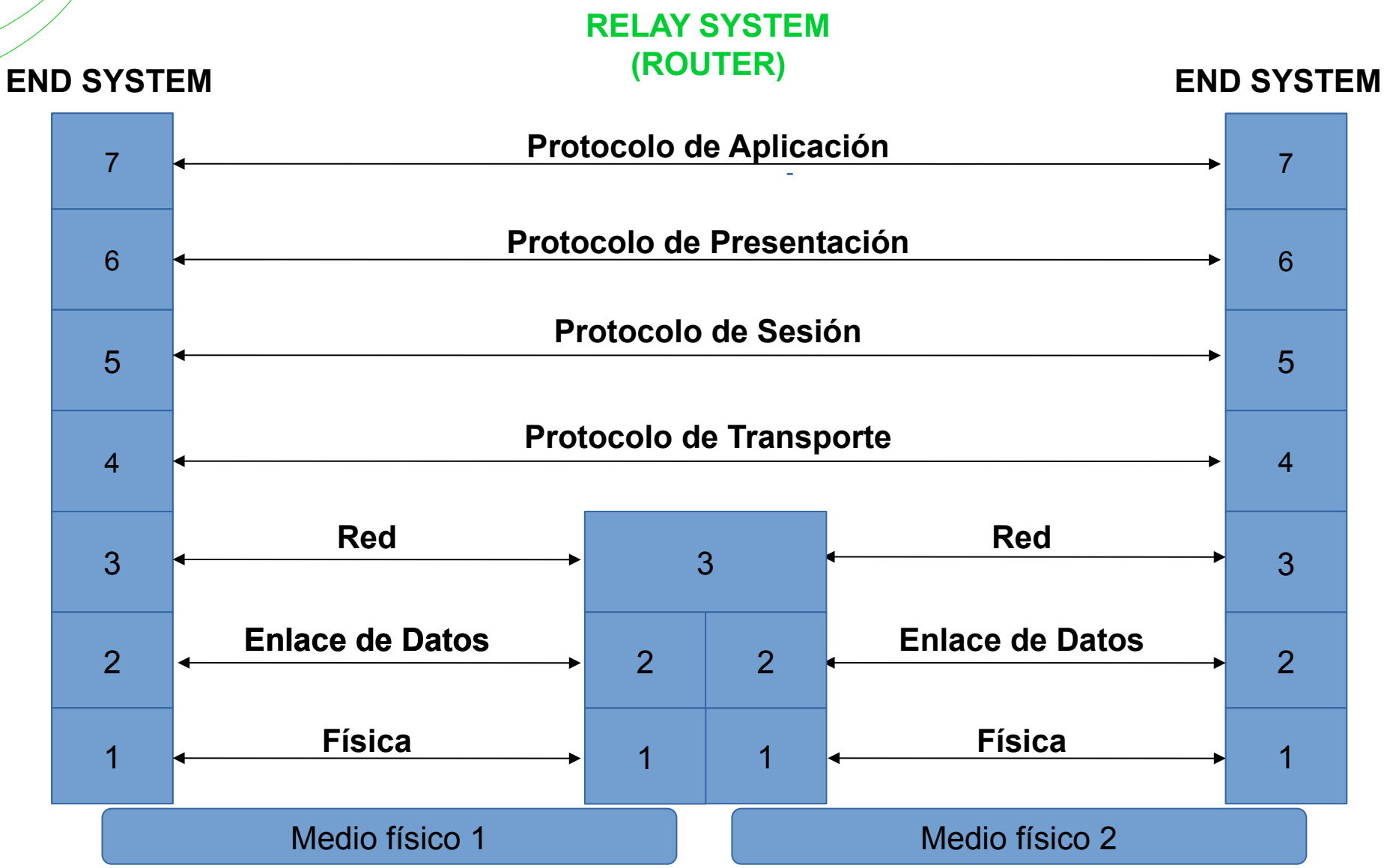
CAPAS OSI (2)

- Red
  - Transporte de información
  - Las capas superiores no necesitan saber acerca de la tecnología utilizada
  - No necesaria en enlaces directos
- Transporte
  - Intercambio de datos entre sistemas terminales (ES)
  - Libre de errores
  - En secuencia
  - Sin Pérdidas
  - Sin Duplicados
  - Calidad de Servicio

CAPAS OSI (3)

- Sesión
  - Control de diálogos entre aplicaciones
  - Disciplina de diálogos
  - Agrupamiento
  - Recuperación
- Presentación
  - Formatos de datos y codificación
  - Compresión de Datos
  - Encriptación
- Aplicación
  - Medios para que las aplicaciones accedan al ambiente OSI

Uso de un router y capas del protocolo



Operación sin Conexión

- Corresponde al mecanismo de transmisión de datagramas en una red de paquetes conmutados
- El protocolo de Red es el mismo para ES y routers
- Conocido genéricamente como protocolo de internet
- Protocolo de Internet
- Protocolo desarrollado para ARPANET
- RFC 791
- Hace falta un protocolo de menor nivel para acceder a una red en particular

Conjunto de Protocolos TCP/IP

- Arquitectura dominante de protocolos comerciales
- Especificado y usado extensivamente antes de OSI
- Desarrollado a partir de investigaciones financiadas por el Departamento de Defensa (DoD) de EEUU
- Usado en Internet

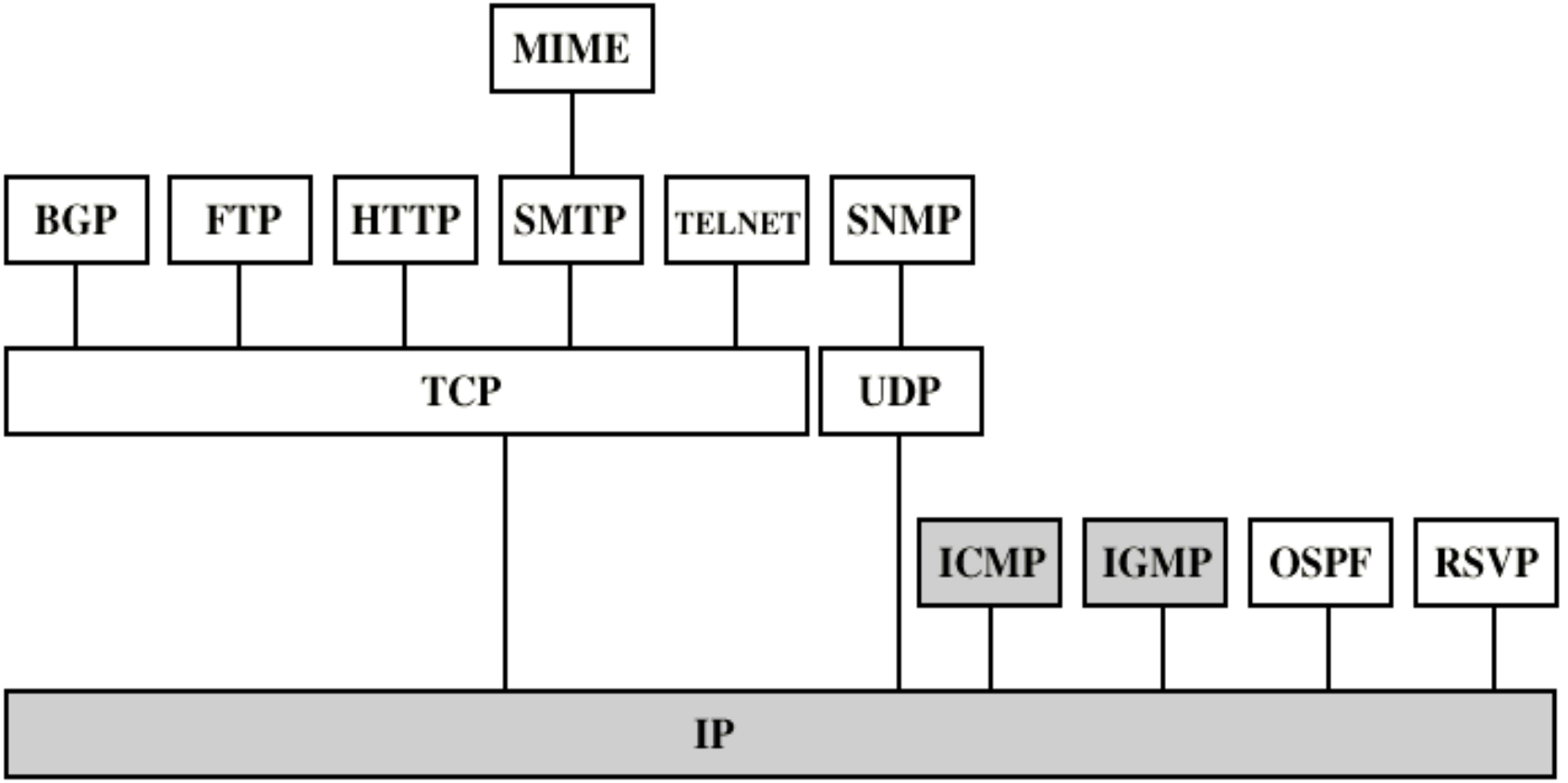
Conjunto de Protocolos TCP/IP

- Capa 4: Aplicación → Capas 5 a 7 OSI
- Capa 3: Transporte (TCP) → Capa 4 OSI
- Capa 2: Red (IP) → Capa 3 OSI
- Capa 1: Acceso al medio → Capa 2 OSI
  - Los protocolos de acceso al medio mas comunes de acceso al medio utilizados con TCP/IP son los definidos por la norma IEEE 802.3 (ethernet) y 802.11 (WiFi).

Temas de diseño

- Enrutamiento
- Tiempo de Vida del datagrama
- Fragmentación y re-ensamblado
- Control de Errores
- Control de flujo

Protocolos TCP/IP



ENRUTAMIENTO

- ES y routers mantienen TABLAS DE ENRUTAMIENTO
  - Indican el próximo router al cual dirigir un datagrama
  - Estáticas (Pueden contener algunas rutas alternativas)
  - Dinámicas (respuesta flexible a congestión y errores)
- Enrutamiento de origen (Source route)
  - El origen especifica la ruta como un secuencia de routers a ser seguidos
  - Seguridad
  - Prioridad
- Grabación de la ruta (route recording)
  - El paquete “aprende” en el viaje de ida la ruta para volver al origen

Tiempo de vida del datagrama

- Los datagramas pueden entrar en un loop infinito.
  - Consume recursos
  - El protocolo de transporte puede necesitar un limite maximo de tiempo de vida del datagrama
- Se marca el Datagrama con un tiempo de vida
  - Campo “Time To Live” en IP
  - Una vez que expira, se descarta el datagrama
  - Se cuentan los “saltos”
  - Se decrementa el tiempo de vida al pasar por cada router

Fragmentación y re-ensamblado

- En distintas redes existen distintos tamaños de paquete.
  - Puede ser necesario fragmentar
- Cuando reensamblar?
  - En el Destino
    - Resulta en paquetes cada vez más pequeños al atravesar la internet
- En puntos Intermedios
  - Necesita buffers enormes en los routers
  - Los Buffers pueden llenarse con fragmentos
  - Todos los fragmentos deben pasar por el mismo router
    - Inhibe el enrutamiento dinámico

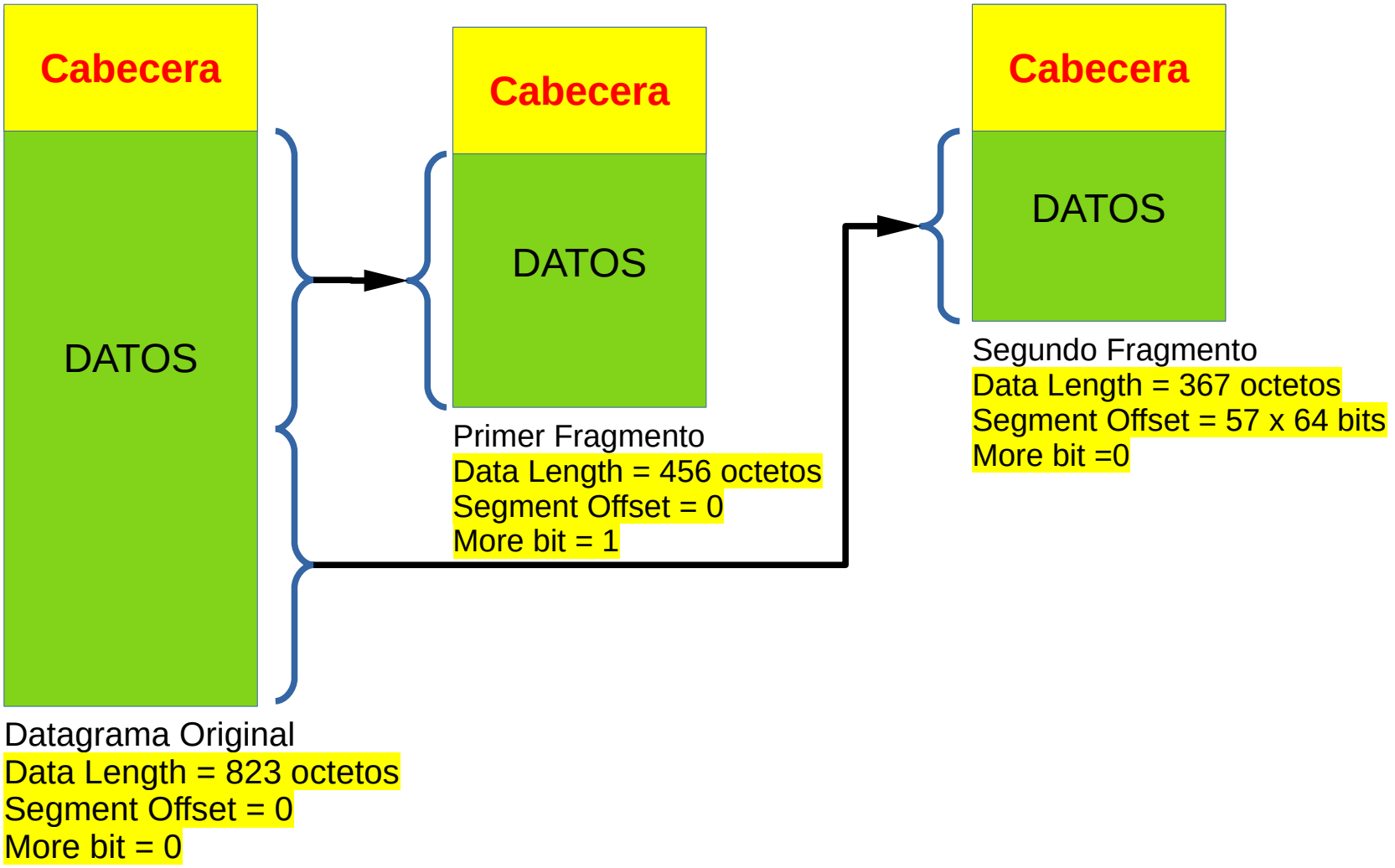
Fragmentacion IP (1)

- IP re-ensambla solo en el destino
- Usa campos en la cabecera
  - Identificación de unidad de datos (ID)
    - Identifica el ES que originó el datagrama
      - Dirección de origen y de destino
      - Capa de protocolo que generó el dato (por ej. TCP)
      - La identificación es provista por esa capa
  - Largo de datos
    - La longitud de los datos de usuario en octetos (bytes)

Fragmentacion IP (2)

- Offset
  - Posición del fragmento de datos de usuario en el datagrama original
  - En múltiplos de 64 bits (8 octetos)
- More flag
  - Indica que este no es el último fragmento

Ejemplo de fragmentación



Como tratar las fallas

- El reensamblado puede fallar si se pierden fragmentos
- Necesidad de detectar fallas
- Se asigna un Time-out de reensamblado
  - Se asigna al primer fragmento en llegar
  - Si se cumple el timeout antes que lleguen todos los fragmentos, se descartan los datos recibidos
- Usar el tiempo de vida (Time To Live en IP)
  - Si el TTL llega a cero se descartan los datos

Control de Error

- No hay garantía de entrega
- El Router debería intentar informar al origen si se descartó el paquete
  - P. ej si expiro el TTL
- El origen podría modificar la estrategia de envío
- O informar a las capas de protocolo superiores
- Se necesita identificar el datagrama

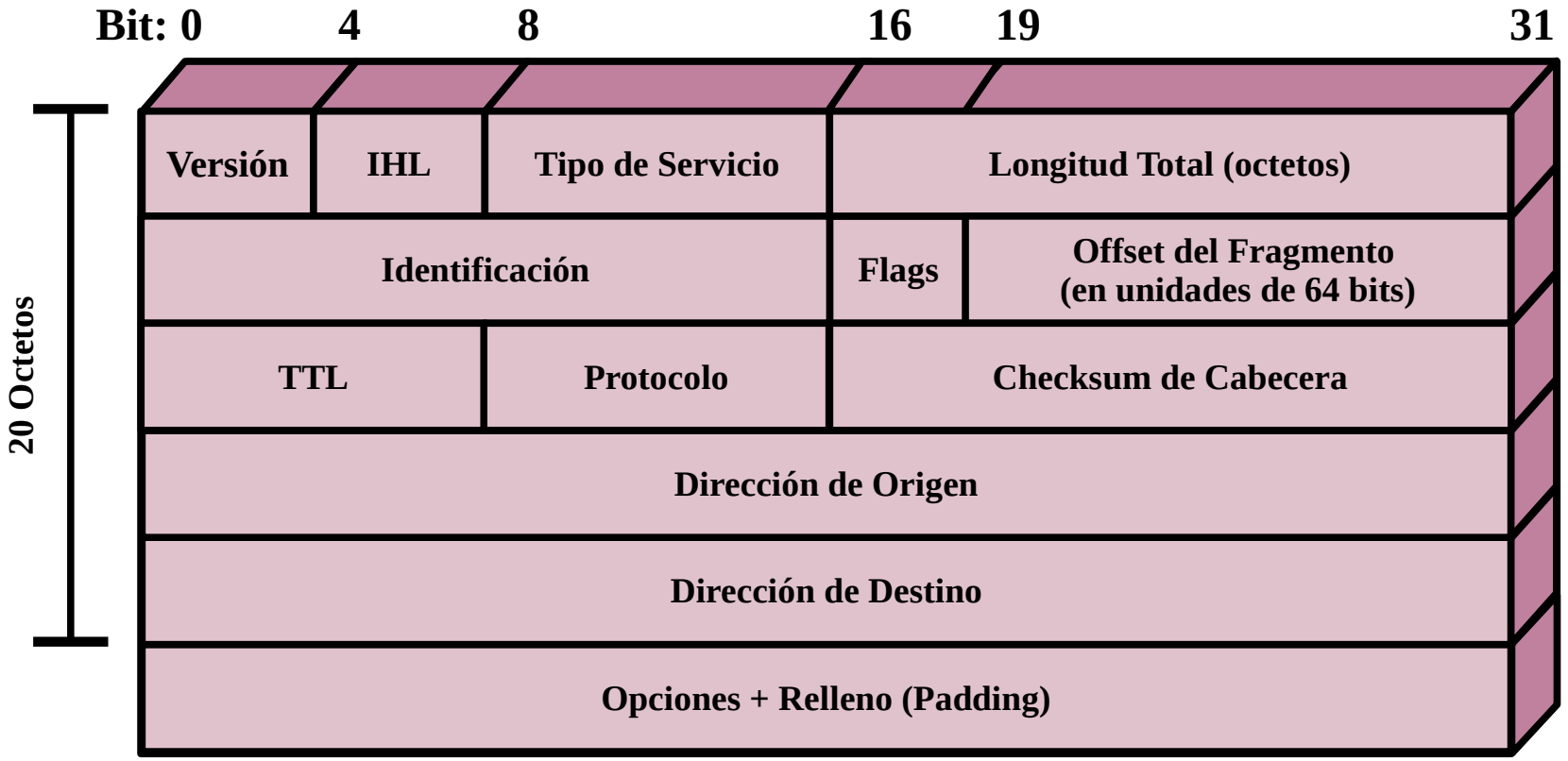
Control de Flujo

- Le permite a routers y/o ES limitar la tasa de datos que recibe
- Limitado en sistemas sin conexión (Red de paquetes conmutadas)
- Se envían paquetes de control de flujo
  - (Pidiendo reducción del flujo entrante)
- P. Ej. ICMP(obsoleto)

Internet Protocol (IP)

- Parte de TCP/IP
  - Usado en Internet
- Especifica Interfaz con capas superiores
  - P ej. TCP
- Especifica formato del protocolo y mecanismos

Protocolo IP . Cabecera



Implementación de servicios provistos por IP

- Primitivas
  - Funciones a realizar
  - Depende de la forma de la implementación de la primitiva
    - P.Ej. Llamado a subrutina, llamado a función
  - Send
    - Requiere la transmisión de una unidad de datos
  - Deliver
    - Notifica al usuario del arribo de una unidad de datos
- Parametros
  - Usados para pasar información de control y datos

Parametros (1)

- Dirección de origen (Source address)
- Dirección de destino (Destination address)
- Protocolo
  - Receptor. P. ej. TCP (6), UDP (17), ICMP(1)
- Tipo de Servicio
  - Especifica el tratamiento de la unidad de datos durante el tránsito por las redes
- Identificación
  - Dirección de origen y destino y protocolo de usuario
  - Identifica unívocamente la unidad de datos del protocolo
  - Necesario para el informe de errores y re-ensamblado
  - Solo el que envía

Parametros (2)

- Indicador Don’t fragment
  - IP puede fragmentar datos?
  - Si no puede hacerlo, podría ser imposible la entrega
  - Solo el que envía
- Indicador More
- Time To Live (TTL)
  - Solo el que envía
- Longitud de datos
- Datos Optativos
- Datos de Usuario

Tipo de Servicio (Type of Service – TOS)

- Actualmente se divide en dos campos:
- Differentiated Services Code Point (DSCP)
  - Default: mejor esfuerzo
  - Expedito: Bajas Pérdidas y Baja Latencia
  - Entrega Asegurada
  - Voz
  - Seleccion de clase (por compatibilidad)
- Explicit congestion notification (ECN)
  - Permite administrar mejor el envio de información cuando hay congestión

Opciones

- Seguridad
- Enrutamiento de fuente
- Grabación de ruta
- Identificación de Flujo
- Estampado de tiempo

Campos de la Cabecera (1)

- Version
  - Actualmente 4
  - IP v6
- Longitud de la cabecera IP
  - En Palabras de 32 bit
  - Incluyendo las Opciones
- Tipo de Servicio
- Longitud Total
  - Del datagrama, en octetos

Campos de la Cabecera (2)

- Identificacion
  - Número de Secuencia
  - Se usa con las direcciones y el protocolo de usuario para identificar unívocamente el datagrama
- Flags
  - More
  - Don’t fragment
- Offset de Fragmentación
- Time to live
- Protocolo
  - Capa superior que debe recibir el campo de datos en el destino

Campos de la Cabecera (3)

- Checksum de la Cabecera
  - Reverificado y recalculado en cada router
  - Complemento a 1 de la suma en 16 bits de todas las palabras de 16 bits en la cabecera
  - Se establece a cero durante el Source Address
- Dirección de Destino
- Opciones
- Padding (relleno)
  - Para llenar la cabecera hasta obtener un largo múltiplo de 32 bits en el campo de datos en el destino

Campo de Datos

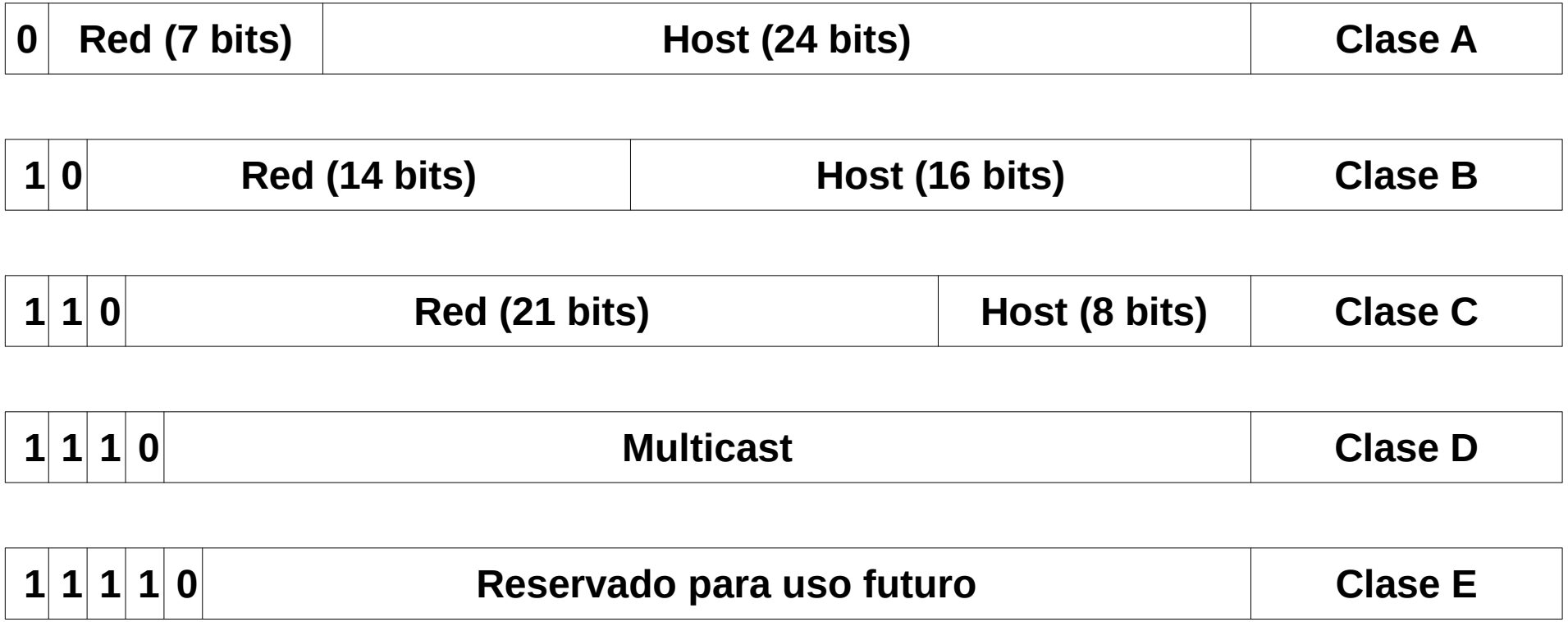
- Transporta los datos de usuario provistos por la capa superior
- Múltiplo entero de 8 bits (octeto)
- Maxima longitud del datagrama (Cabecera mas datos) 65,535 octetos

Direcciones IP

- Están definidas por un número de 32 bits
- La notación mas conocida es la que se obtiene al separar los 32 bits en grupos de 8 y convertir cada grupo de ocho bits a decimal separando los numeros resultantes por puntos (QUAD-DOT).

32 bits				
8 bits	8 bits	8 bits	8 bits	
1 0 0 1 0 0 1 1	1 0 1 1 0 1 1 1	0 0 1 1 0 0 1 1	0 0 0 1 1 1 1 1	Binario
0x93	0xB7	0x33	0x1F	Hexa
147	.183	.51	.31	Quad Dot
0x93B7331F				Hexa 32 bits
2478256927				Decimal sin signo
-1816710369				Decimal con signo (CA2)

Direcciones IP - Clases



Direcciones IP - Clase A

- Dirección global de 32 bits
- Una parte corresponde a red y la otra a Host
- Class A
  - Comienza con 0 en binario
  - Todos ceros reservada
  - 01111111 (127) reservada para loopback
  - Rango 1.x.x.x a 126.x.x.x
  - Todas utilizadas

Direcciones IP - Clase B

- Comienzan con 10 en binario
- Rango 128.x.x.x a 191.x.x.x
- La dirección de red tambien incluye el segundo octeto
- 214 = 16,384 direcciones clase B
- Todas asignadas

Direcciones IP - Clase C

- Comienzan con 110 en binario
- Rango 192.x.x.x a 223.x.x.x
- La dirección de red tambien incluye el segundo y tercer octeto
- 221 = 2,097,152 direcciones
- Casi todas Asignadas
  - Ver IPv6

Direcciones IP - Clase D

- Comienzan con 1110 en binario
- Rango 224.x.x.x a 239.x.x.x
- Estaba destinada a el uso en MULTICAST, es decir comunicaciones de uno a muchos. Nunca se implementó masivamente

Direcciones IP - Clase E

- Comienzan con 11110 en binario
- Rango 240.x.x.x a 255.x.x.x
- Se dejó como reserva para otros usos futuros, pero no se utilizó nunca.

Direcciones IP - Classless

- Luego de la expansión masiva de Internet a partir de principios del siglo XXI se acordó asignar los números IP por zona geográfica, mediante el uso de agrupamientos de bloques numéricos.
- Actualmente la tecnología permite que los routers internacionales puedan manejar tablas de enrutamiento mayores.

Máscara de red.

- Mascara natural es la máscara que corresponde a una clase determinada.
- Al realizar la operación AND bit a bit entre una dirección IP y su máscara natural obtenemos la dirección de la red.

1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**Clase A / 8 bits**
255								**.0**								**.0**								**.0**								
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**Clase B / 16 bits**
255								**.255**								**.0**								**.0**								
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	**Clase C / 24 bits**
255								**.255**								**.255**								**.0**								

Uso de la Máscara de red para determinar la red.

- Ejemplo: dirección IP del servidor de la Facultad de Ingeniería 163.10.11.65
- Vemos que el primer octeto es 163 decimal – 0xA3 hexadecimal o bien 10100011 binario, esto dice que es una dirección clase B
- Se hace el AND de la dirección IP con la Máscara y obtengo la Red.
- Este procedimiento es el que realizan los Routers para encontrar una ruta que lleve a esa red, a partir del número IP

1	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**Número IP**
163								**.10**								**.11**								**.65**								
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**Máscara Clase B / 16 bits**
255								**.255**								**.0**								**.0**								
1	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**Dirección de red**
163								**.10**								**.0**								**.0**								

Uso de la Máscara de red para determinar el Host.

- Ejemplo: dirección IP del servidor de la Facultad de Ingeniería 163.10.3.65
- Vemos que el primer octeto es 163 decimal – 0xA3 hexadecimal o bien 10100011 binario, esto dice que es una dirección clase B
- Se hace el AND de la dirección IP con la Máscara negada y se obtiene el Host.
- Este procedimiento debería realizar un router a la entrada de la organización para determinar a que host debe enviar el datagrama recibido. En este caso interpretamos que todos los hosts están conectados a una única LAN.

1	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**Número IP**
163								**.10**								**.11**								**.65**								
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**Máscara Clase B Negada**
0								**.0**								**.255**								**.255**								
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**Host**
0								**.0**								**.11**								**.65**								

Subredes y máscara de subred

- Usar una única LAN para una organización con muchos Hosts no es práctico.
- Extendiendo la cantidad de bits de máscara se pueden dividir las redes asignadas en SUBREDES.
- Permiten una complejidad arbitraria de LANs interconectadas dentro de la organización
- Aísla la internet corporativa y la Internet global del crecimiento de números de red y la complejidad de enrutamiento
- La organización se ve para el resto de la Internet como una sola red.
- Permite asignar una subred a cada LAN

Subredes y máscara de subred

- La porción de Host de la dirección se divide en un número de subred y un número de host
- Los routers locales dirigen el tráfico entre las distintas subredes
- La Máscara de subred indica cuales bits son subred y cuales son número de host
- Se considera como ***dirección de subred*** a la dirección IP más baja de la subred.
- Se considera como d***irección de Broadcast*** a la dirección IP más alta de la subred
- La dirección de subred y la dirección de broadcast no pueden asignarse a ningun Host de la red

Subredes y máscara de subred

- Por ejemplo, la UNLP ha dividido su espacio de direcciones en subredes de 255 direcciones IP cada una.
- Esto equivale a agregar 8 bits a la mascara natural de la clase B que tiene asignada.
- Puedo distinguir las subredes 163.10.x.0 como subredes separadas y asignarlas a distintas dependencias.
- En el caso de ingeniería por ejemplo, tiene asignadas las subredes 163.10.3.0, 163.10.11.0, 163.10.12.0 y 163.10.27.0 con una mascara de 24 bits o en notación quad-dot 255.255.255.0

Uso de la Máscara de subred para determinar la subred. Máscara de 24 bits

- Ejemplo: dirección IP del servidor de la Facultad de Ingeniería 163.10.3.65
- Vemos que el primer octeto es 163 decimal – 0xA3 hexadecimal o bien 10100011 binario, esto dice que es una dirección clase B
- Se hace el AND de la dirección IP con la Máscara y obtengo la Red.

1	0	1	0	0	0	1	1	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	1	**Número IP**
163								.10								.3								.65							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	**Máscara de subred / 24 bits**
255								.255								.255								.0							
1	0	1	0	0	0	1	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**Dirección de red**
163								.10								.3								.0							

Otras Máscaras

- Una subred puede dividirse a su vez en subredes más pequeñas ampliando las máscaras.
- Las mascaras no están restringidas a múltiplos de 8 bits
- Por ejemplo podrían ser de 26 bits y en ese caso la subred corresponde a los 26 bits más significativos de la dirección y el Host a los 6 bits menos significativos. Para el ejemplo anterior:

1	0	1	0	0	0	1	1	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	1	**Número IP**
163								.10								.11								.65								
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	**Máscara de subred / 26 bits**
255								.255								.255								.192								
1	0	1	0	0	0	1	1	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	**Dirección de red**
163								.10								.11								.64								

Otras Máscaras

- Es conveniente conocer los valores decimales que representan máscaras de menos de 8 bits:

Bits de la Máscara	**Mascara en binario**								**Decimal**
1	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**128**
2	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**192**
3	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**224**
4	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**240**
5	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**248**
6	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**252**
7	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**254**

Otras Máscaras Ejemplo con 26 Bits

Máscara 26 bits: 0xFFFFFFC0 = 255.255.255.192

$$192_{10} = C0_{16} = 11000000_2$$

Subred 0:
163.10.3.0/255.255.255.192
163.10.3.0/26
Hexa: 0xA30A0300/FFFFFFC0
Broadcast: 163.10.3.63

Subred 128:
163.10.3.128/255.255.255.192
163.10.3.128/26
Hexa: 0xA30A0380/FFFFFFC0
Broadcast: 163.10.3.191

Subred 64:
163.10.3.64/255.255.255.192
163.10.3.64/26
Hexa: 0xA30A0340/FFFFFFC0
Broadcast: 163.10.3.127

Subred 192:
163.10.3.192/255.255.255.192
163.10.3.192/26
Hexa: 0xA30A03C0/FFFFFFC0
Broadcast: 163.10.3.255