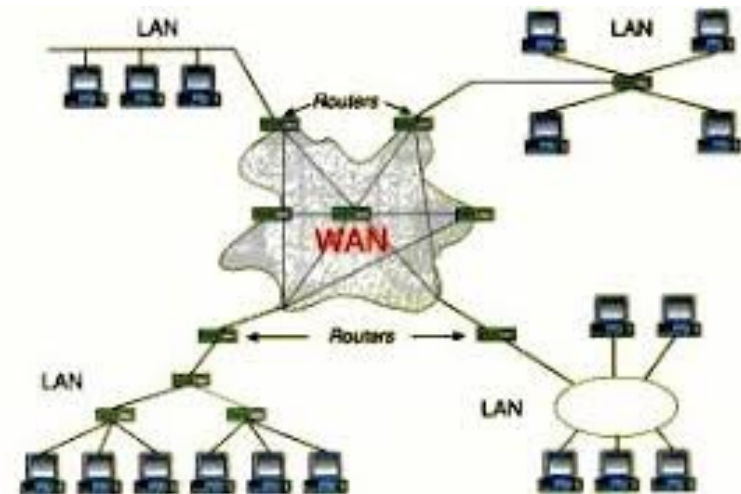
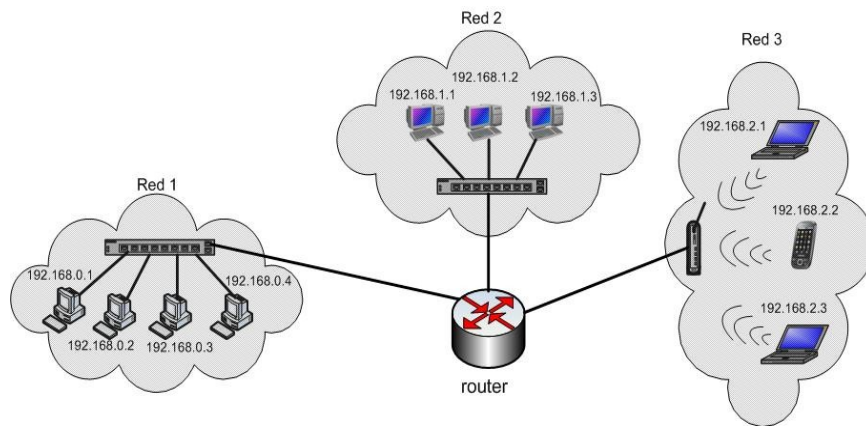




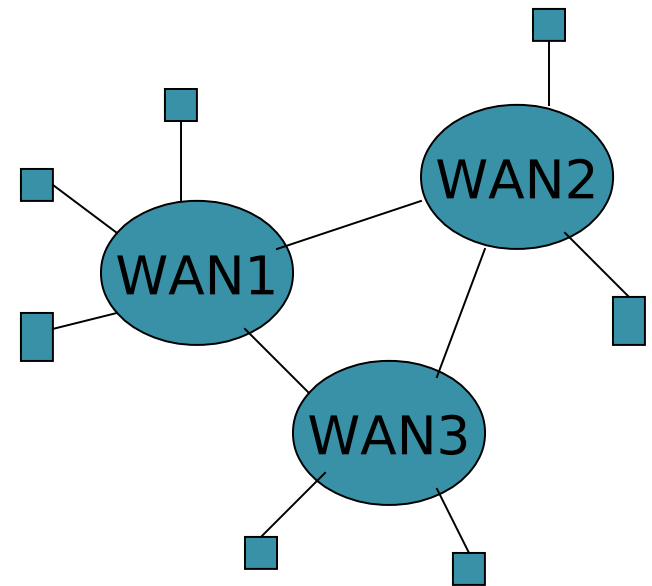
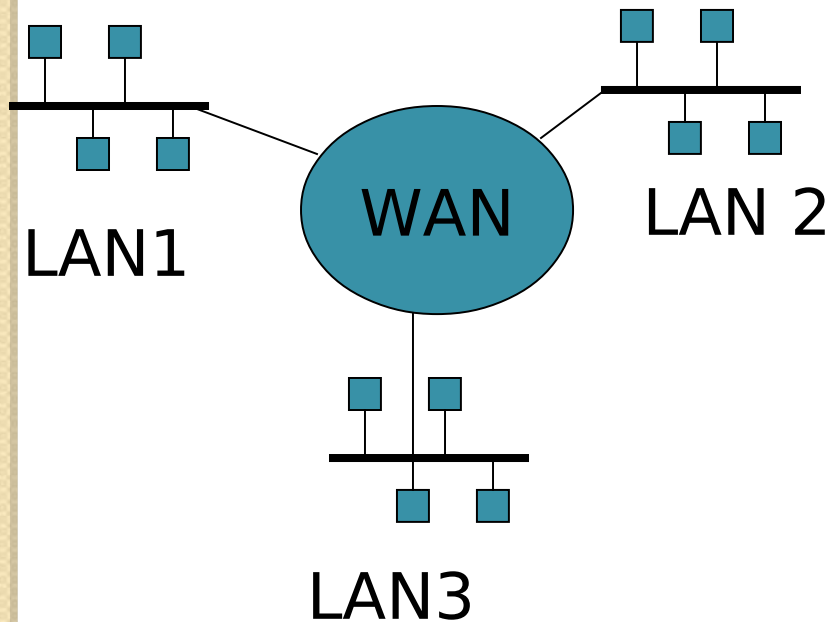
Redes de Datos- Interconexión de redes

Especialización en Telecomunicaciones
UPB Bucaramanga

Interconexión de redes



Interconexión de redes



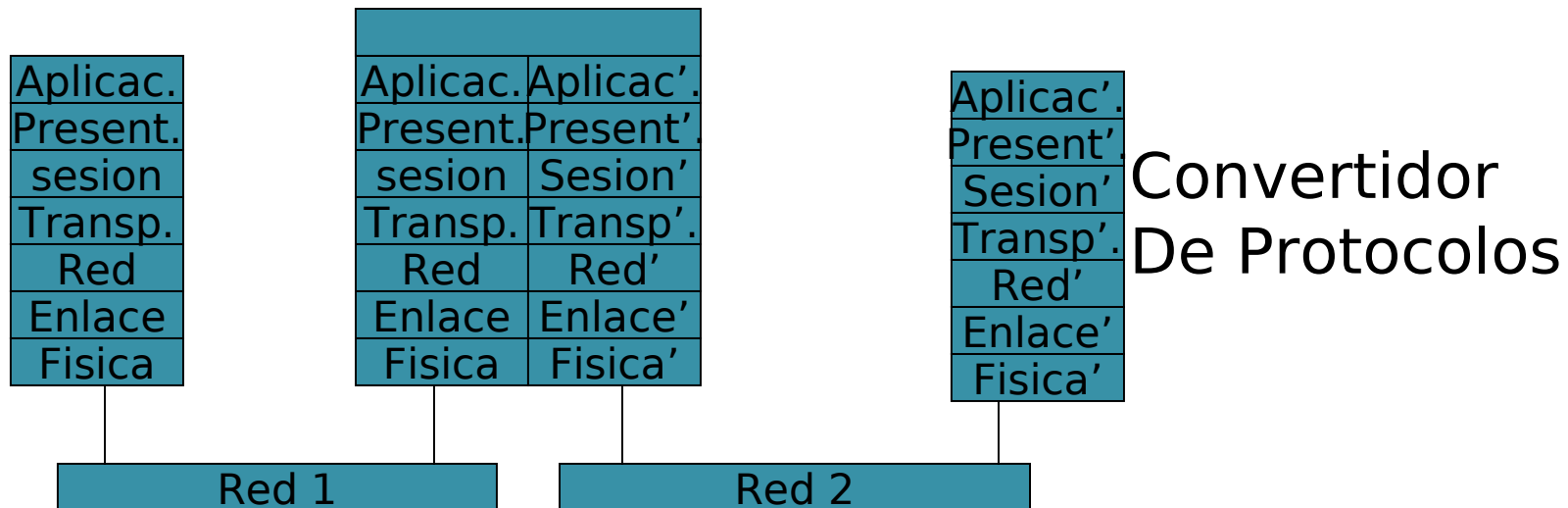
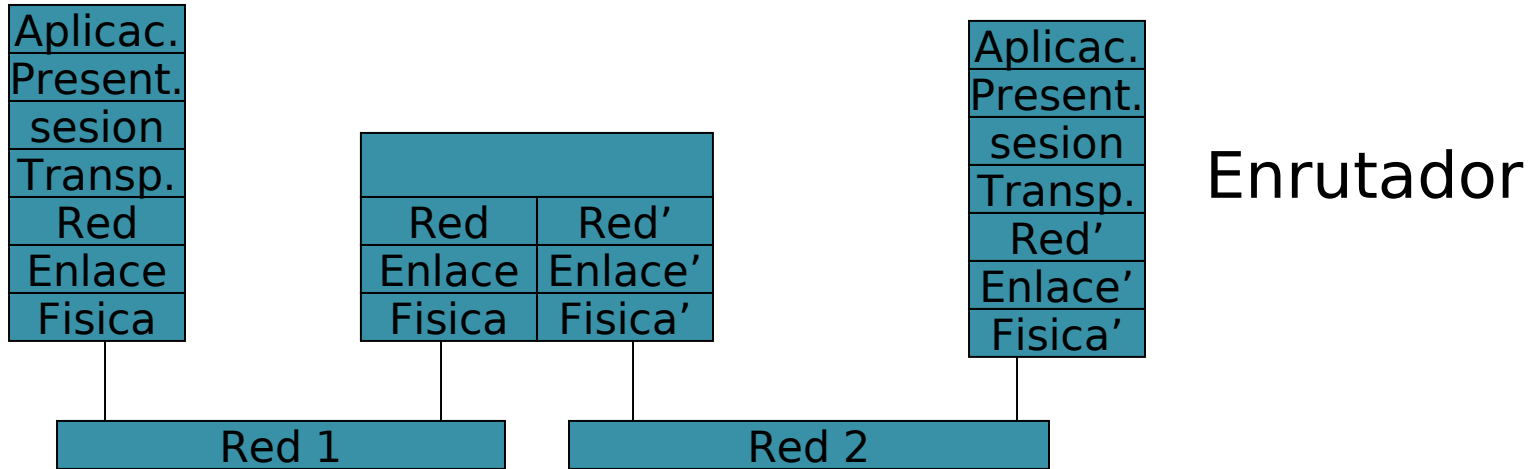
Conceptos básicos

- Internetworking
 - Modo de operación en que estaciones se conectan a un conjunto de redes interconectadas entre sí.
- Internet
 - Conjunto de redes de diferentes tipos (LAN, MAN, WAN) interconectadas entre sí.
- Subred
 - Cada una de las redes que componen una internet

Conceptos básicos

- IS: Intermediate System
 - Dispositivo que interconecta dos subredes
 - Otros nombres: IWU (Internetworking Unit), Router (enrutador), Gateway (Pasarela)
- Convertidor de protocolos
 - Dispositivo que comunica dos redes con arquitecturas de protocolos diferentes
- Datagrama
 - Modo de funcionamiento
 - Paquete

Enrutador vs. Convertidor



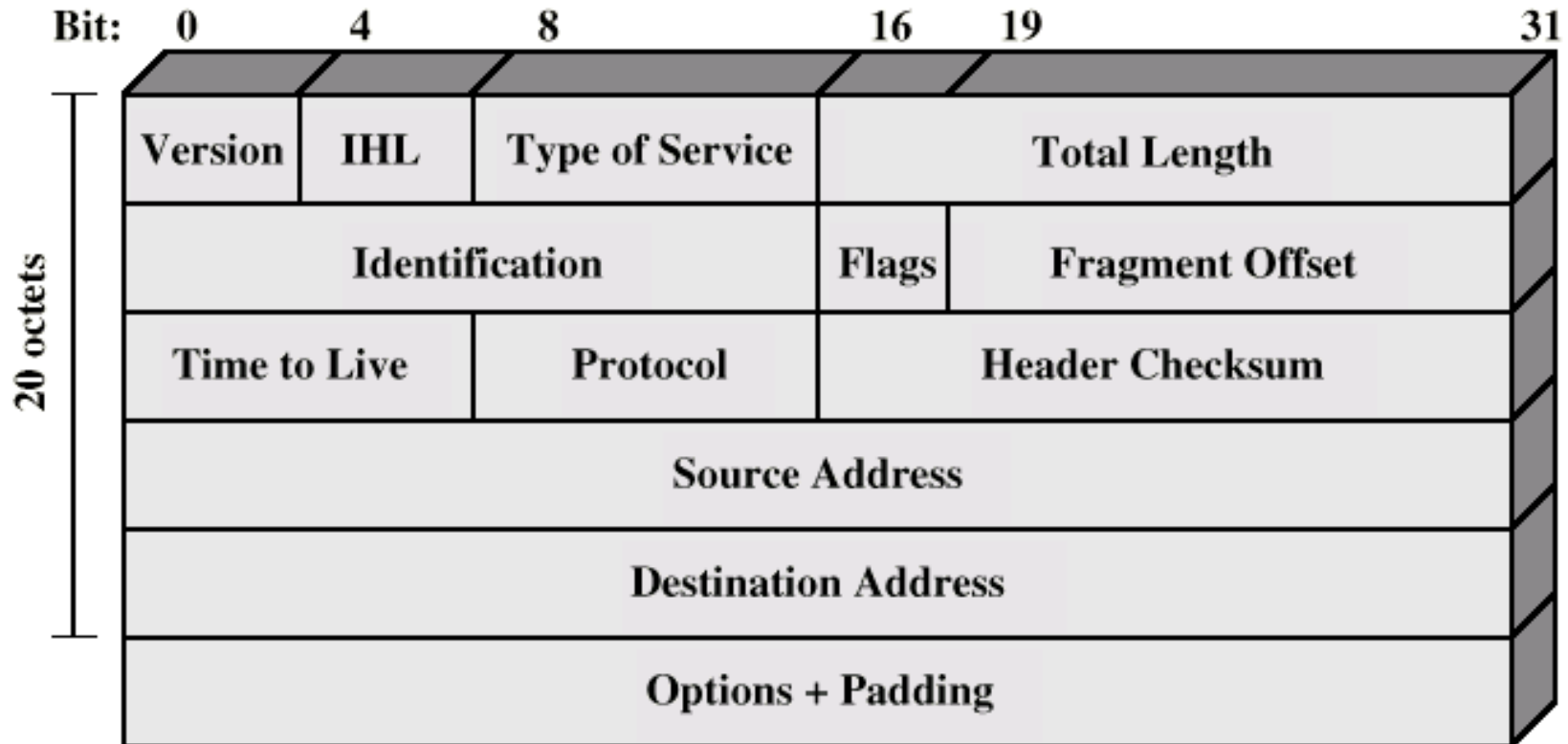


El protocolo IP

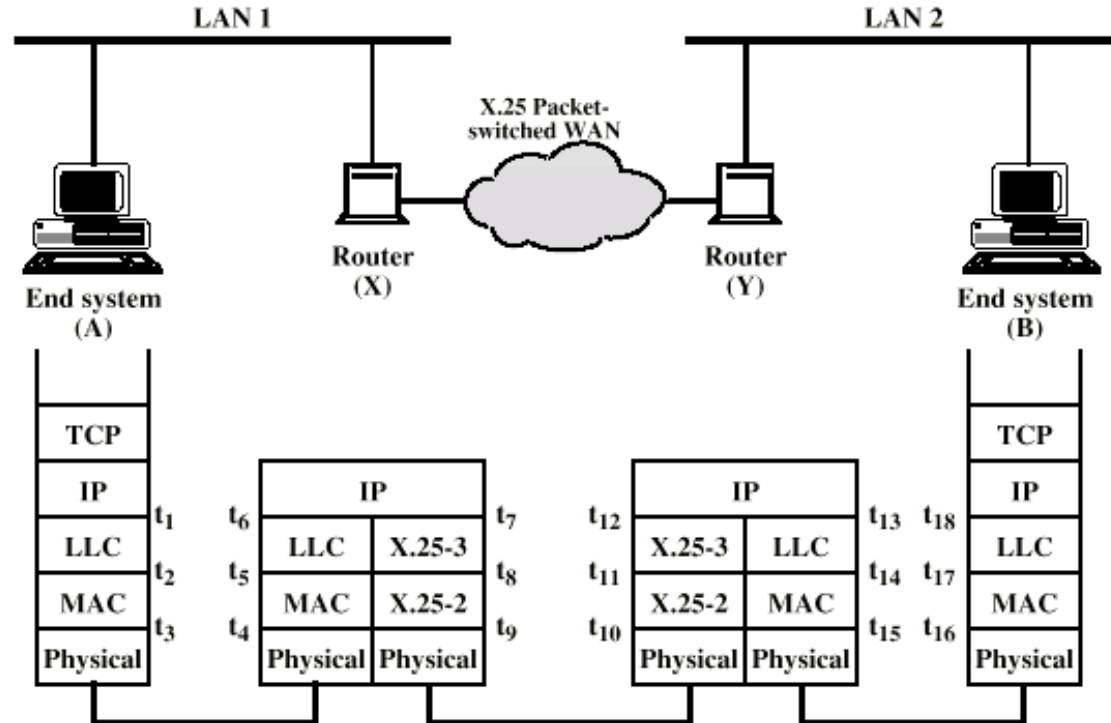
Interconexión de redes con IP

- IP: Internet Protocol
- Tiene dos versiones: IPv4 e IPv6 (ó IPng)
- Proporciona un servicio sin conexión (modo datagrama) entre sistemas finales
- Ventajas de esta característica:
 - Es flexible: Gran variedad de redes. Usa poca información de las redes que atraviesa.
 - Es robusto: Ante problemas en segmentos de ruta, los paquetes se encaminan por una ruta alterna.

Protocolo IPv4: Formato de la trama



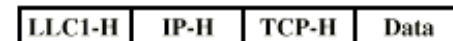
Operación de IP



$t_1, t_6, t_7, t_{12}, t_{13}, t_{18}$



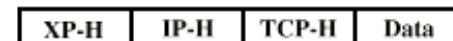
t_2, t_5



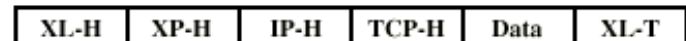
t_3, t_4



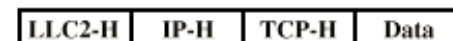
t_8, t_{11}



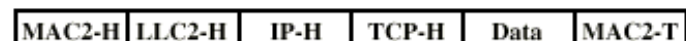
t_9, t_{10}



t_{14}, t_{17}



t_{15}, t_{16}



TCP-H = TCP header
 IP-H = IP header
 LLCi-H = LLC header
 MACi-H = MAC header

MACi-T = MAC trailer
 XP-H = X.25 packet header
 XL-H = X.25 link header
 XL-T = X.25 link trailer

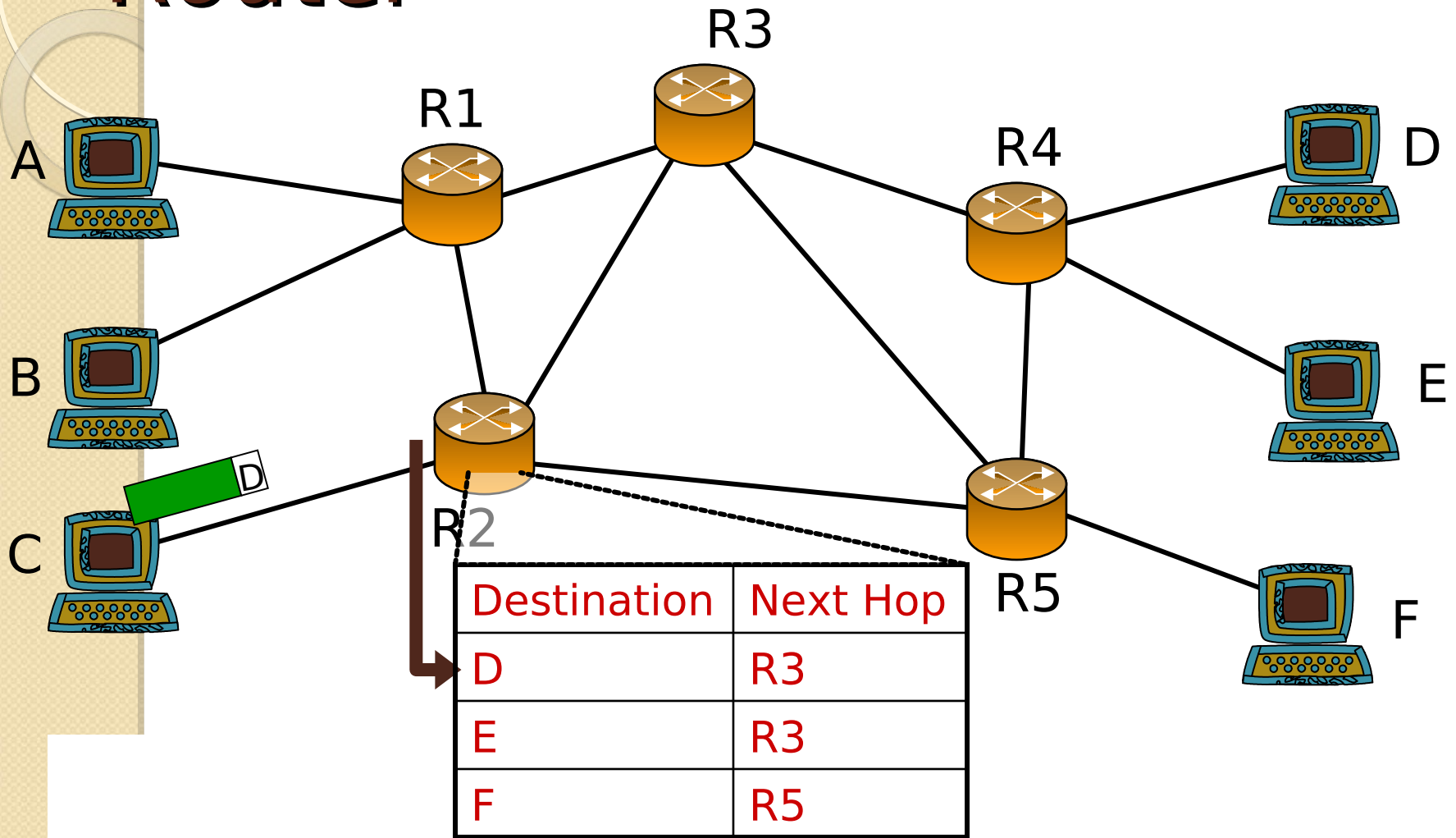
Características de la interconexión de redes con IP

- Internet como una red de conmutación de paquetes:
 - Nodos → Enrutadores
 - Enlaces → Subredes
- Características:
 - Encaminamiento
 - Tiempo de vida de los datagramas
 - Segmentación y re-ensamblado
 - Control de errores
 - Control de flujo

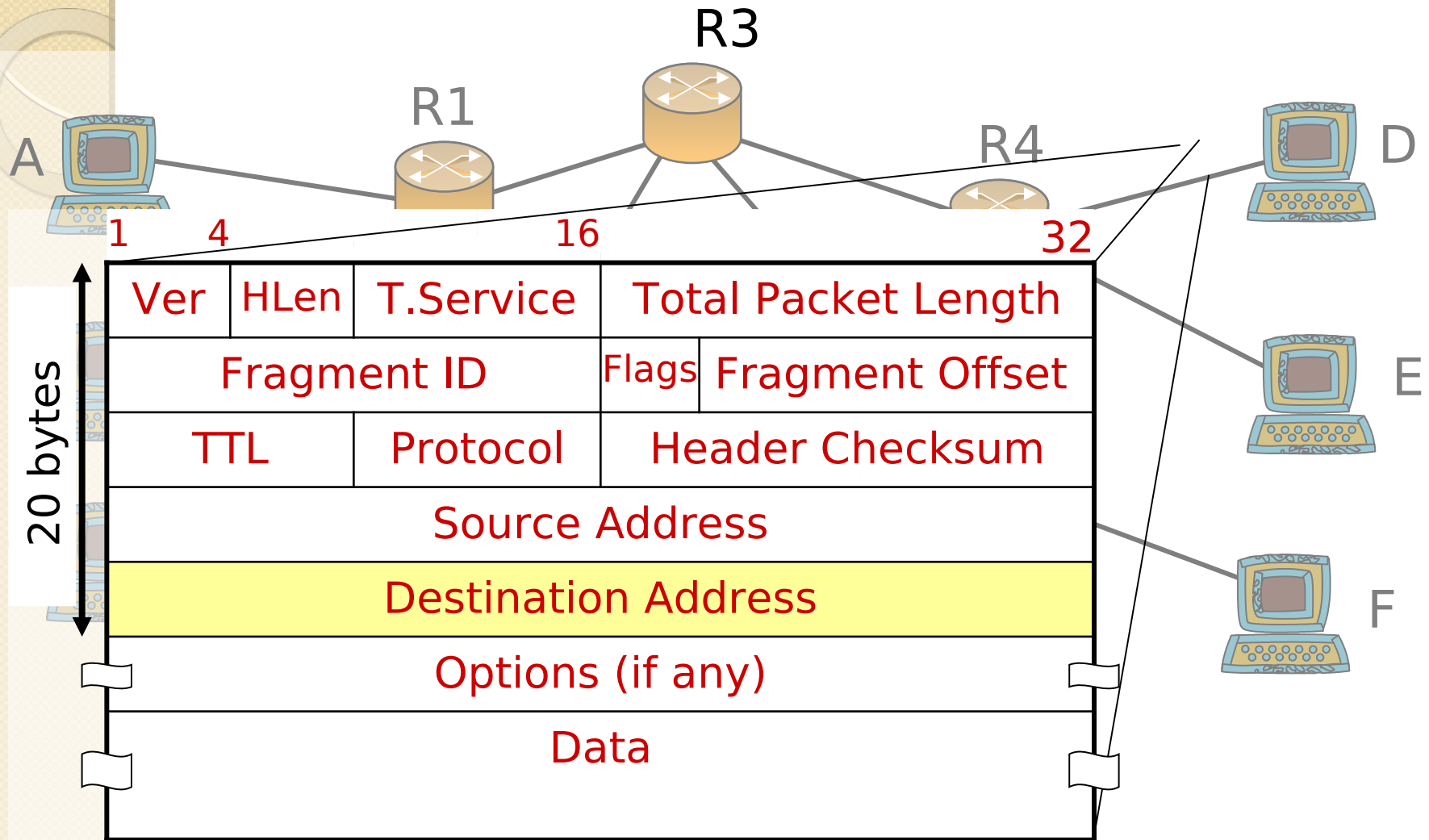
Encaminamiento

- Usa tablas de encaminamiento en los Routers y sistemas finales: siguiente router según el destino (dirección IP destino) del Datagrama.
- **Campo Cabecera IP: Dirección IP Destino**
- Tipos: Estático, Dinámico
- Cuando un dispositivo de encaminamiento se desconecta, todos sus vecinos emiten un informe de estado.
- Esto permite que otros Routers y estaciones actualicen sus tablas de encaminamiento.

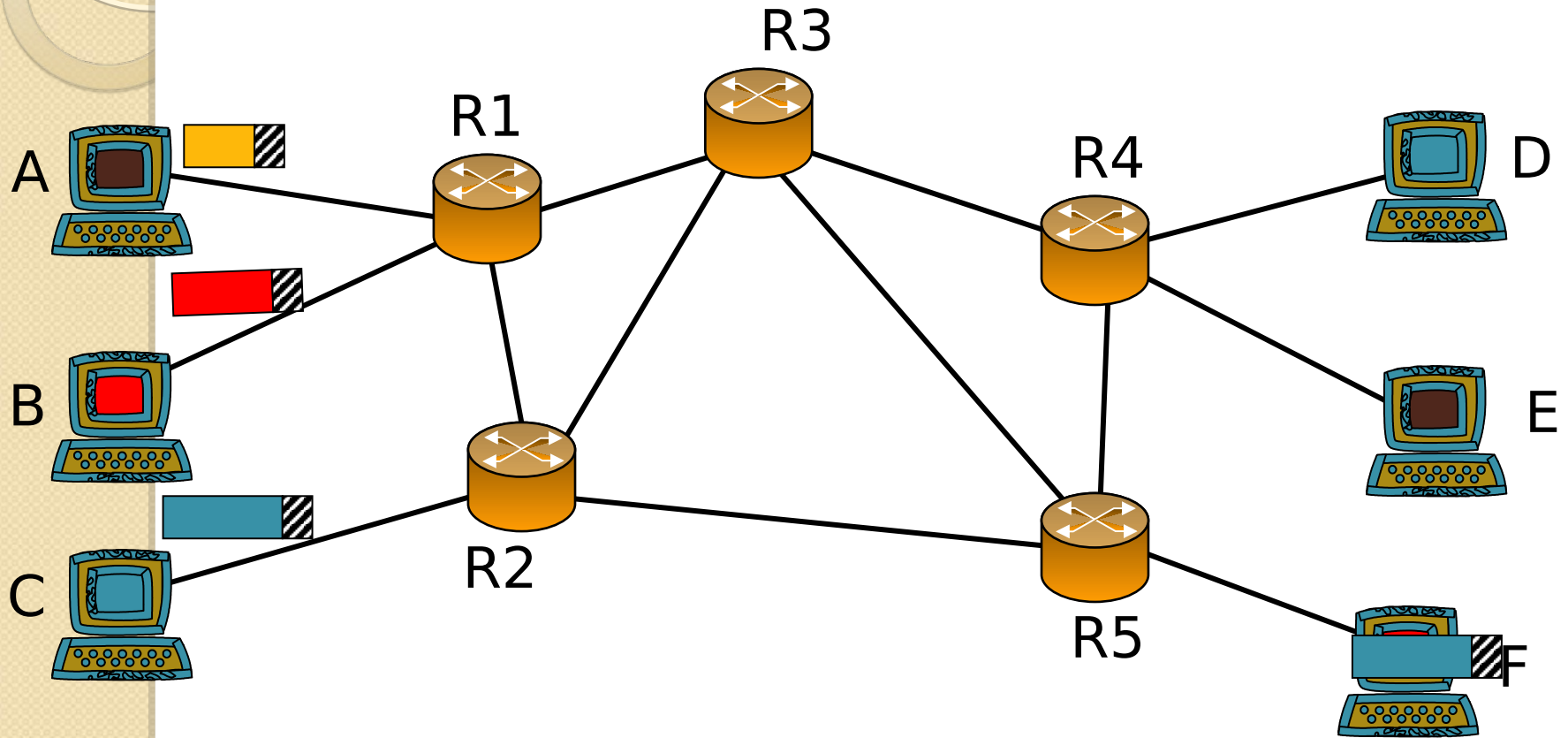
Operacion basica de un Router



Que hace un router?



Que hace un router?



Encaminamiento

- Debe asegurar que los datos de cierto nivel de seguridad no se les permita pasar a través de redes no acreditadas para gestionarlos.
- Encaminamiento por la fuente: usado si se quiere dar seguridad.
- Registro de ruta: cada router anexa su dirección internet a una lista que lleva el datagrama (comprobación de rutas)

Tiempo de vida de los datagramas

- Existe la posibilidad de que un datagrama viaje indefinidamente a través del conjunto de redes:
 - Consume recursos
 - Podría funcionar mal el protocolo de la capa de transporte
- Una vez transcurrido el tiempo de vida, el datagrama se descarta
- Implementación: Contador de saltos (se decrementa con cada router), también se podría trabajar con tiempo pero se requiere sincronización de la red.
- **Campo cabecera IP: TTL (Time To Live)**

Segmentación y reensamblado

- Las subredes podrían especificar tamaños máximos de paquetes diferentes.
- Podría requerirse que los routers segmenten los paquetes de entrada en unidades más pequeñas llamadas fragmentos para transmitirlos a la siguiente red.
- ¿Dónde reensamblarlos?
 - Destino
 - Routers intermedios

Segmentación y reensamblado

- Reensamblado en el Destino:
 - Los paquetes pueden volverse demasiado pequeños, lo que afecta la eficiencia de las redes.
 - Simple
- Re-ensamblado en Routers intermedios:
 - Grandes memorias temporales para almacenar datagramas parciales
 - Todos los segmentos de un datagrama deberían pasar por el mismo router de salida (no permite enrutamiento dinámico)

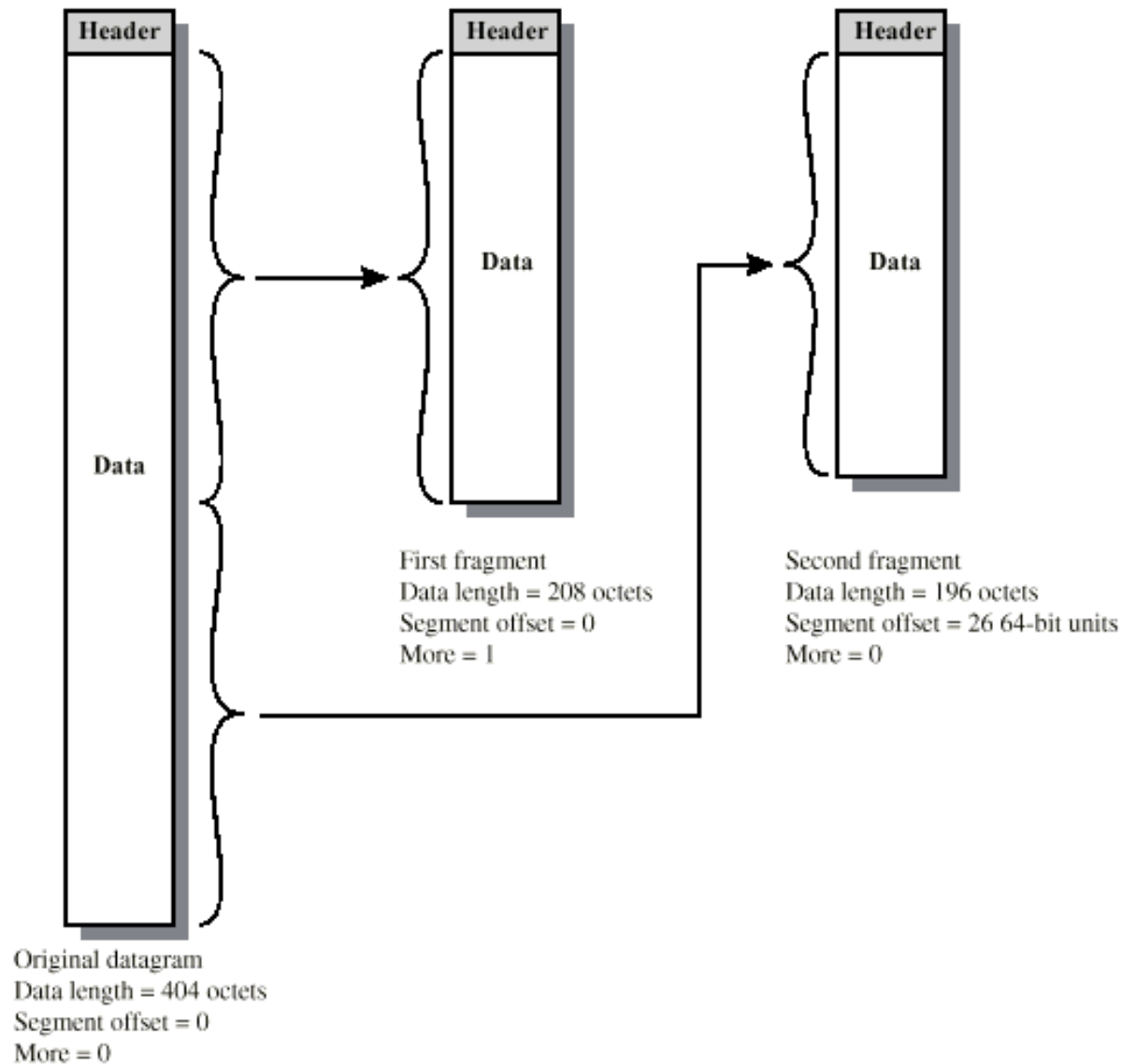
Segmentación y reensamblado

- IP reensambla los fragmentos de un datagrama en el sistema final destino.
- Campos de la cabecera IP:
 - ID: Identificador de la unidad de datos
 - Longitud de datos
 - Desplazamiento
 - Indicador de más datos

Segmentación y reensamblado: Campos Cabecera IP

- **ID** identifica de forma única un datagrama originado por un sistema final.
- **ID**= Dir. IP Origen + Dir. IP Destino + Protocolo (capa superior) + número de secuencia
- **Total Length:** (Longitud de datos) longitud de datos de usuario en octetos
- **Fragment Offset:** (Desplazamiento) Posición de un fragmento de los datos de usuario en el campo de datos en el datagrama original (múltiplos de 64 bits).

Ejemplo Fragmentación



Re-ensamblado

- Los datos de fragmentos con el mismo ID se almacenan en una memoria temporal en la posición correcta de acuerdo al desplazamiento indicado.
- Este proceso se repite hasta que el campo de datos está completo (inicia con un desplazamiento=0 y termina con un indicador de más datos puesto a falso).
- Se requiere una buena cantidad de memoria

Reensamblado

- Qué pasa si se pierden segmentos?
 - IP no garantiza la entrega
 - Alternativas:
 - ▮ Asignar un tiempo de vida al reensamblaje del primer segmento que llega: Temporizador que al expirar desecha todos los segmentos que intentaron reensamblarse.
 - ▮ Uso del campo de tiempo de vida de los datagramas IP. Al llegar al destino, se decrementa este campo periódicamente hasta llegar a cero (se descartan los fragmentos).

Control de errores

- Cuando un router descarta un datagrama, debe intentar devolver alguna información al origen (si es posible).
- El protocolo IP del origen avisa a las capas superiores.
- Razones para descartar un datagrama:
 - Expiración tiempo de vida
 - Congestión
 - Error en la suma de comprobación de la cabecera

Control de flujo

- Permite a los routers o a las estaciones receptoras limitar la velocidad de entrega de paquetes del origen.
- En internet los mecanismos son limitados ya que el servicio es sin conexión.
- Se usa el mensaje SOURCE QUENCH del protocolo ICMP para avisarle al origen que disminuya la tasa de envío de paquetes.

Protocolo ICMP

- ICMP: Internet Control Messages Protocol
- Proporciona información de realimentación sobre problemas del entorno de comunicación.
- En general, un mensaje ICMP se envía en respuesta a un datagrama, ya sea por un router o por un sistema final destino.
- *ICMP es un usuario de IP*: Los mensajes ICMP se envían como datagramas (no es seguro que lleguen)

Mensajes ICMP

Mensaje	Significado
Destino inalcanzable	Un router no sabe llegar al dest.
Tiempo excedido	Ha expirado t. Vida datagrama
Ralentización del origen	Disminuir tasa envío datos
Redirección	Se indica una mejor ruta
Eco	Obliga al dest. A contestar
Respuesta a Eco	Resp. A solíc. Eco
Marca de tiempo	Origen envía info. De tiempo
Respuesta a marca de tiempo	Destino envía info. De tiempo
Petición de máscara de dirección	Solicitud del origen al destino
Respuesta a máscara de direcc.	Máscara enviada al origen

Protocolo ICMP: Formato de los mensajes

0	8	16	31
Type	Code	Checksum	
Unused			
IP Header + 64 bits of original datagram			

(a) Destination Unreachable; Time Exceeded; Source Quench

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Originate Timestamp			

(e) Timestamp

0	8	16	31
Type	Code	Checksum	
Pointer	Unused		
IP Header + 64 bits of original datagram			

(b) Parameter Problem

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Originate Timestamp			
Receive Timestamp			
Transmit Timestamp			

(f) Timestamp Reply

0	8	16	31
Type	Code	Checksum	
Gateway Internet Address			
IP Header + 64 bits of original datagram			

(c) Redirect

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	

(g) Address Mask Request

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Optional data			

(d) Echo, Echo Reply

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Address Mask			

(h) Address Mask Reply

Servicios IP

- Son la interfaz con la capa superior (TCP)
- Se expresan mediante primitivas (funciones) y parámetros (datos a pasar).
- IP especifica dos primitivas:
 - Send (envío de una unidad de datos)
 - Deliver (entrega de unidad de datos)

Servicios IP

Send{

Dirección origen

Dirección destino

Protocolo

Indicadores tipo servicio

Identificador

Indicador de no
fragmentación

Tiempo de vida

Longitud de los datos

Datos de opción

Datos

}

Deliver{

Dirección origen

Dirección destino

Protocolo

Indicadores tipo servicio

Longitud de los datos

Datos de opción

Datos

}

Parámetros de los servicios IP

- Tipo de servicio:
 - Usado para solicitar una calidad de servicio particular
 - Parámetros:
 - ▢ Precedencia (similar a prioridades, 8 niveles)
 - ▢ Seguridad (alta, normal: intentar no perderlo)
 - ▢ Retardo (normal, bajo: minimizar retardo)
 - ▢ Rendimiento (normal, alto: maximizar velocidad)

Parámetros de los servicios IP

- Opciones (Datos de opción):
 - Se incluyen parámetros que normalmente no se invocan
 - Opciones:
 - ▢ Seguridad (etiqueta adicional)
 - ▢ Encaminamiento por la fuente (lista de routers a seguir)
 - ▢ Registro de la ruta (lista de routers visitados por el datagrama)
 - ▢ Identificación de secuencia: identifica recursos reservados para servicios con secuencia (ej. voz)
 - ▢ Marcas de tiempo (entidad IP origen o routers colocan una marca temporal (precisión mseg) a los datagramas)



DIRECCIONAMIENTO IP

Direccionamiento IP

- Las direcciones IP de las redes y sus computadores son asignadas por la IANA (Internet Assigned Numbers Authority)
- Para IPv4 son de 32 bits
- Para IPv6 son de 128 bits
- Una dirección IP se organiza de manera jerárquica: Dirección de Red + Dirección de Host
- Existen diferentes tipos de direcciones: Clase A, Clase B y Clase C

Direcciones IPv4

- El origen y destino tienen una dirección de 32 bits
- Dirección = ID. Red + ID. Computador
- Clases de redes
 - Clase A: 0 + Red(7bits) + Computador (24bits)
 - Clase B: 10+Red (14bits) + Computador (16 bits)
 - Clase C: 110+Red(21bits)+Computador(8bits)
- Notación punto decimal:
 - 11000000 11100100 000010001 00111001
 - 192 . 228 . 17 . 57

Clases de Direcciones IPv4

Clase A:

Network	Host	Host	Host
---------	------	------	------

Clase B:

Network	Network	Host	Host
---------	---------	------	------

Clase C:

Network	Network	Network	Host
---------	---------	---------	------

Clase D: Multicast

Clase E: Research

Rangos Direcciones de red

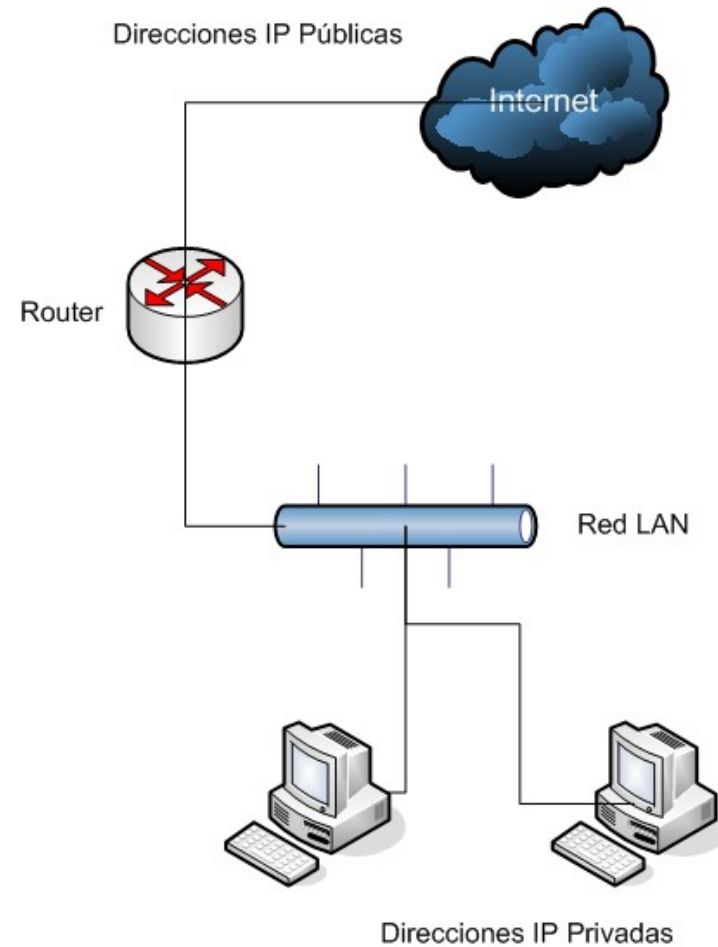
Tipo de Red	Rango Direcciones de Red
Clase A	0-127
Clase B	128-191
Clase C	192-223
Clase D y E	224-255

Direcciones de Propósito Especial

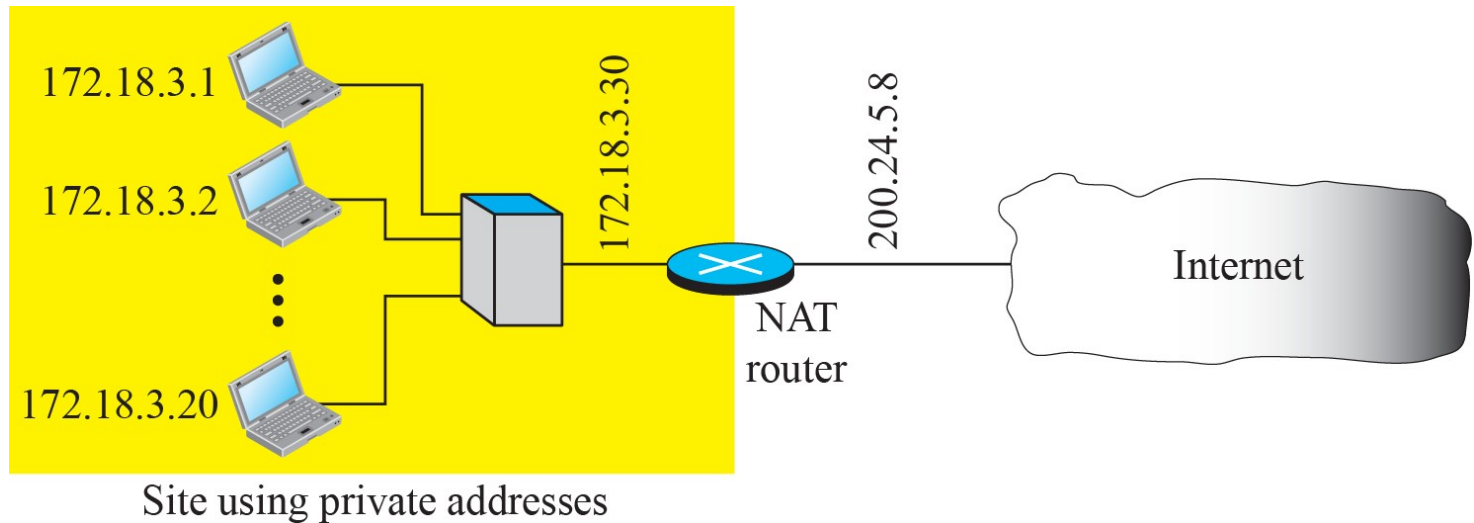
Dirección	Función ó Significado
Todos los Bits de dirección de red en ceros	“Esta red o segmento”
Todos los bits de dirección de red en unos	“Todas las redes”
127.0.0.1	Pruebas de lazo cerrado (un nodo se manda paquetes a sí mismo sin generar paquetes a la red)
Todos los Bits de Dirección de nodo en ceros	“Cualquier host en la red especificada”
Todos los bits de dirección de nodo en unos	“Todos los nodos en la red especificada” (Ej: 128.2.255.255 son todos los nodos de la red 128.2)
Todos los bits de dirección IP en ceros	“Cualquier Red” ó “Ruta por defecto” (En Routers Cisco)
Todos los bits de dirección IP en unos (255.255.255.255)	Todos los nodos en la red actual. También llamado “Broadcast de todos en 1” ó “Broadcast limitado”

Direcciones IP Privadas

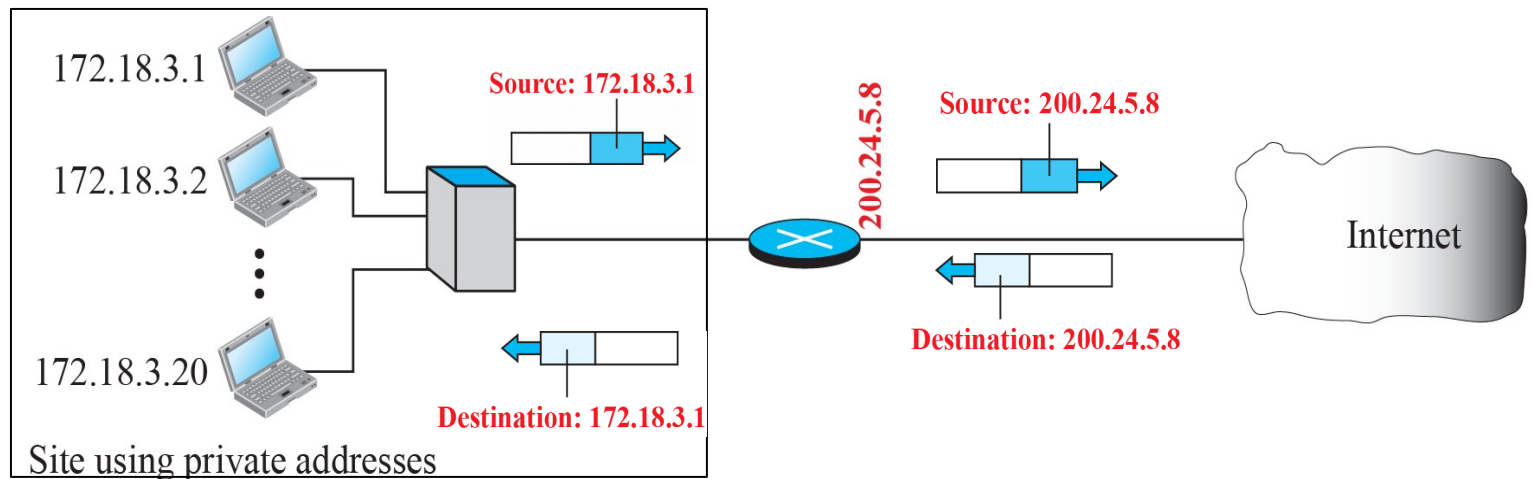
- Son utilizadas en una red privada, pero no son enrutables hacia Internet.
- Ventajas:
 - Seguridad
 - Ahorro de espacio de direcciones IP
- ISPs, empresas y usuarios de hogar sólo requieren de unas pocas direcciones para conectar sus redes a Internet
- Las direcciones IP privadas sólo se usan en las redes internas
- Se requiere de un servicio NAT (Network Address Translation) para convertir direcciones IP privadas a Públicas y viceversa



Network Address Translation (NAT)



Address translation



Translation

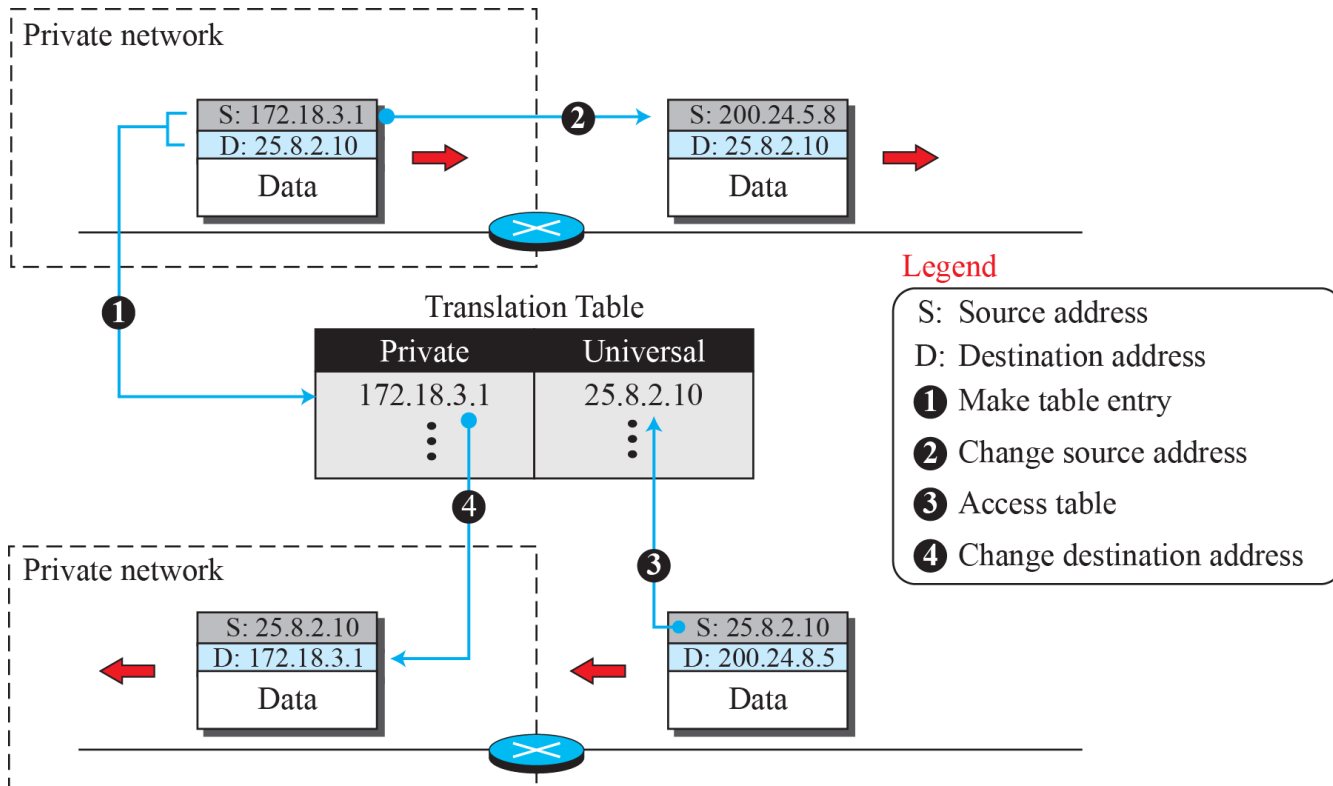


Tabla de Traducción de 5 Columnas

<i>Private address</i>	<i>Private port</i>	<i>External address</i>	<i>External port</i>	<i>Transport protocol</i>
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
⋮	⋮	⋮	⋮	⋮

Direcciones IP Privadas

Clase de dirección	Espacio de direcciones reservado
Clase A	10.0.0.0 hasta 10.255.255.255
Clase B	172.16.0.0 hasta 172.31.255.255
Clase C	192.168.0.0 hasta 192.168.255.255

Cuál usar?

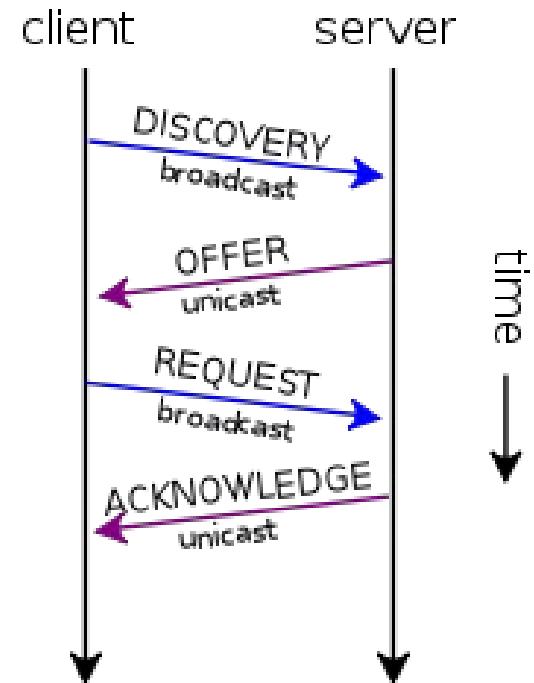
- Se podría usar cualquiera
- **Redes Corporativas:** Usar direcciones de red Clase A (Brinda flexibilidad y opciones de crecimiento)
- **Redes de Hogar:** Preferible Clase C (más fáciles de entender y configurar con hasta 254 hosts)

Asignación dinámica de direcciones IP con DHCP

- DHCP: Dynamic Host Configuration Protocol
- Permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.
- Se trata de un protocolo de tipo cliente/servidor
- Un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres
- El servidor conoce en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.
- Este protocolo se publicó en octubre de 1993, estando documentado actualmente en la RFC 2131.
- DHCPv6 se publica el RFC 3315.

Lista de opciones configurables:

- Dirección del servidor DNS
- Nombre DNS
- Puerta de enlace de la dirección IP
- Dirección de Publicación Masiva (*broadcast address*)
- Máscara de subred
- Tiempo máximo de espera del ARP (*Protocolo de Resolución de Direcciones* según siglas en inglés)
- MTU (*Unidad de Transferencia Máxima* según siglas en inglés) para la interfaz
- Servidores NIS (*Servicio de Información de Red* según siglas en inglés)
- Dominios NIS
- Servidores NTP (*Protocolo de Tiempo de Red* según siglas en inglés))
- Servidor SMTP
- Servidor TFTP
- Nombre del servidor WINS



Formato de los mensajes DHCP

0	8	16	24	31
Opcode	Htype	HLen	HCount	
Transaction ID				
Time elapsed		Flags		
Client IP address				
Your IP address				
Server IP address				
Gateway IP address				
Client hardware address				
Server name				
Boot file name				
Options				

Fields:

Opcode: Operation code, request (1) or reply (2)

Htype: Hardware type (Ethernet, ...)

HLen: Length of hardware address

HCount: Maximum number of hops the packet can travel

Transaction ID: An integer set by client and repeated by the server

Time elapsed: The number of seconds since the client started to boot

Flags: First bit defines unicast (0) or multicast (1); other 15 bits not used

Client IP address: Set to 0 if the client does not know it

Your IP address: The client IP address sent by the server

Server IP address: A broadcast IP address if client does not know it

Gateway IP address: The address of default router

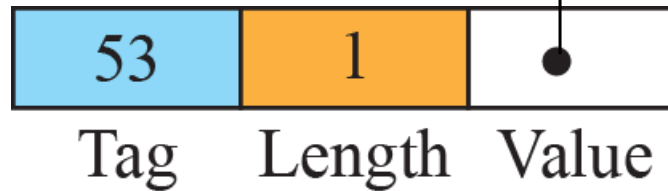
Server name: A 64-byte domain name of the server

Boot file name: A 128-byte file name holding extra information

Options: A 64-byte field with dual purpose described in text

Formato de las Opciones

1 DHCP DISCOVER	5 DHCP ACK
2 DHCP OFFER	6 DHCP NACK
3 DHCP REQUEST	7 DHCP RELEASE
4 DHCP DECLINE	8 DHCP INFORM



Operacion de DHCP

Se usa el canal de broadcast

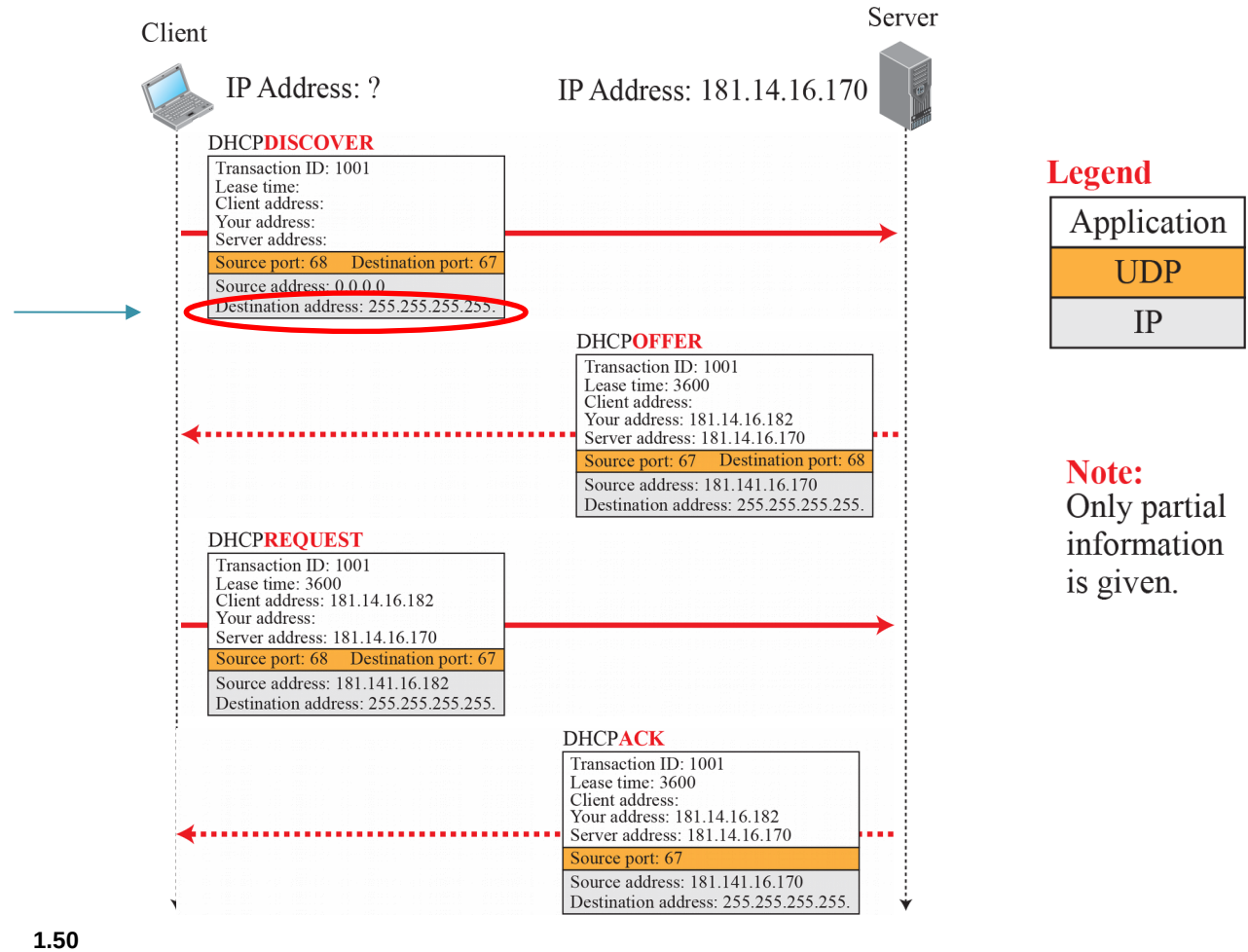
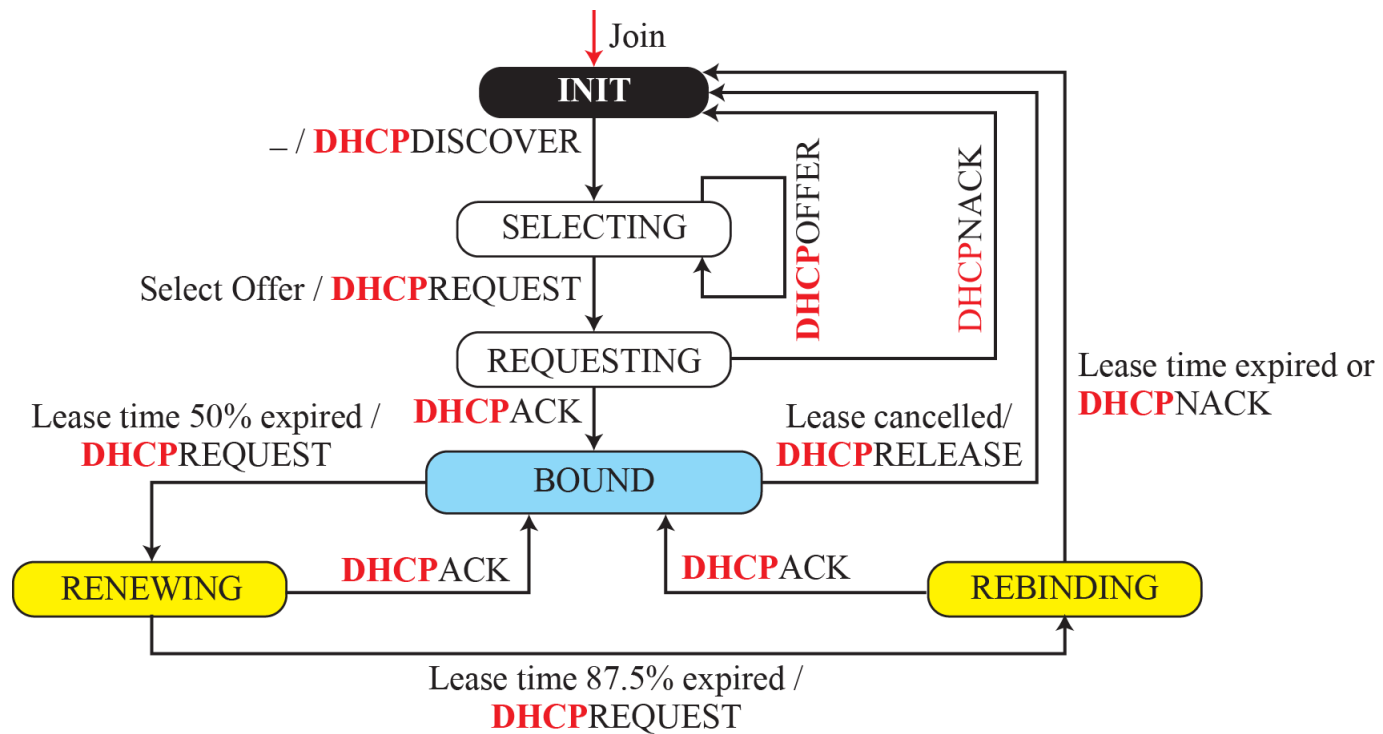


Figure 4.41: FSM for the DHCP client



Protocolo de Resolución de Direcciones (ARP)

- Se usa en redes de acceso
- Para enviar una trama desde un Host origen a un Host Destino dentro de la misma red de Acceso, debe descubrirse cuál es la dirección física (MAC Address) del nodo destino.
- El protocolo ARP sirve para traducir automáticamente entre dirección física y dirección IP.

ARP (Address Resolution Protocol)

- Cuando un Host desea transmitir una trama con otro Host Local, busca la dirección IP del otro en su tabla ARP.
- Si no existe una entrada para esa dirección de IP, el host difunde una solicitud de ARP que contiene la dirección IP de destino (¿Quién tiene la IP xxxx?)
- El Host destino contesta enviando su dirección física (Yo soy MMMM)

Cómo ver la tabla ARP?

- En windows:
 - arp -a

```
C:\USERS\DV4-14~1>arp -a
```

```
Interfaz: 10.150.78.XX --- 0xa
```

Dirección de Internet	Dirección física	Tipo
10.150.78.1	40-01-c6-68-5f-01	dinámico
10.150.78.13	10-1f-74-44-6b-d7	dinámico
10.150.78.66	f0-4d-a2-1f-c6-86	dinámico
10.150.78.255	ff-ff-ff-ff-ff-ff	estático
224.0.0.22	01-00-5e-00-00-16	estático
224.0.0.251	01-00-5e-00-00-fb	estático
224.0.0.252	01-00-5e-00-00-fc	estático
239.255.255.250	01-00-5e-7f-ff-fa	estático
255.255.255.255	ff-ff-ff-ff-ff-ff	estático

Creación de subredes (Subnetting)

- Las subredes se crean con el fin de dividir una red LAN grande en subredes más pequeñas
- Esto requiere de utilizar Switches de capa 3 (manejan direcciones IP en lugar de direcciones Ethernet)
- Beneficios de hacer Subnetting:
 - **Reducción de tráfico de red:**
 - ▮ El tráfico de las subredes permanece en cada una de ellas. Sólo los paquetes que van a otra subred pasan por el Switch capa 3.
 - ▮ Los paquetes a direcciones de Broadcast sólo van a los hosts de la subred.
 - **Rendimiento de la red optimizado:** Esto resulta de la reducción del tráfico
 - **Gestión de red simplificada:** Facilidad para identificar y aislar problemas de red

Direcciones IP y máscara de subred

	Representación binaria	Notación de Punto decimal
Dirección IP	11000000.11100100.00010001.00111001	192.228.17.57
Máscara de subred	11111111.11111111.11111111.11100000	255.255.255.224
Resultado And bit a bit	11000000.11100100.00010001.00100000	192.228.17.32
Número de subred	11000000.11100100.00010001.001	1
Número de computador	00000000.00000000.00000000.00011001	25

La máscara de subred sirve para determinar la dirección de subred y la identificación del Host



Rango:

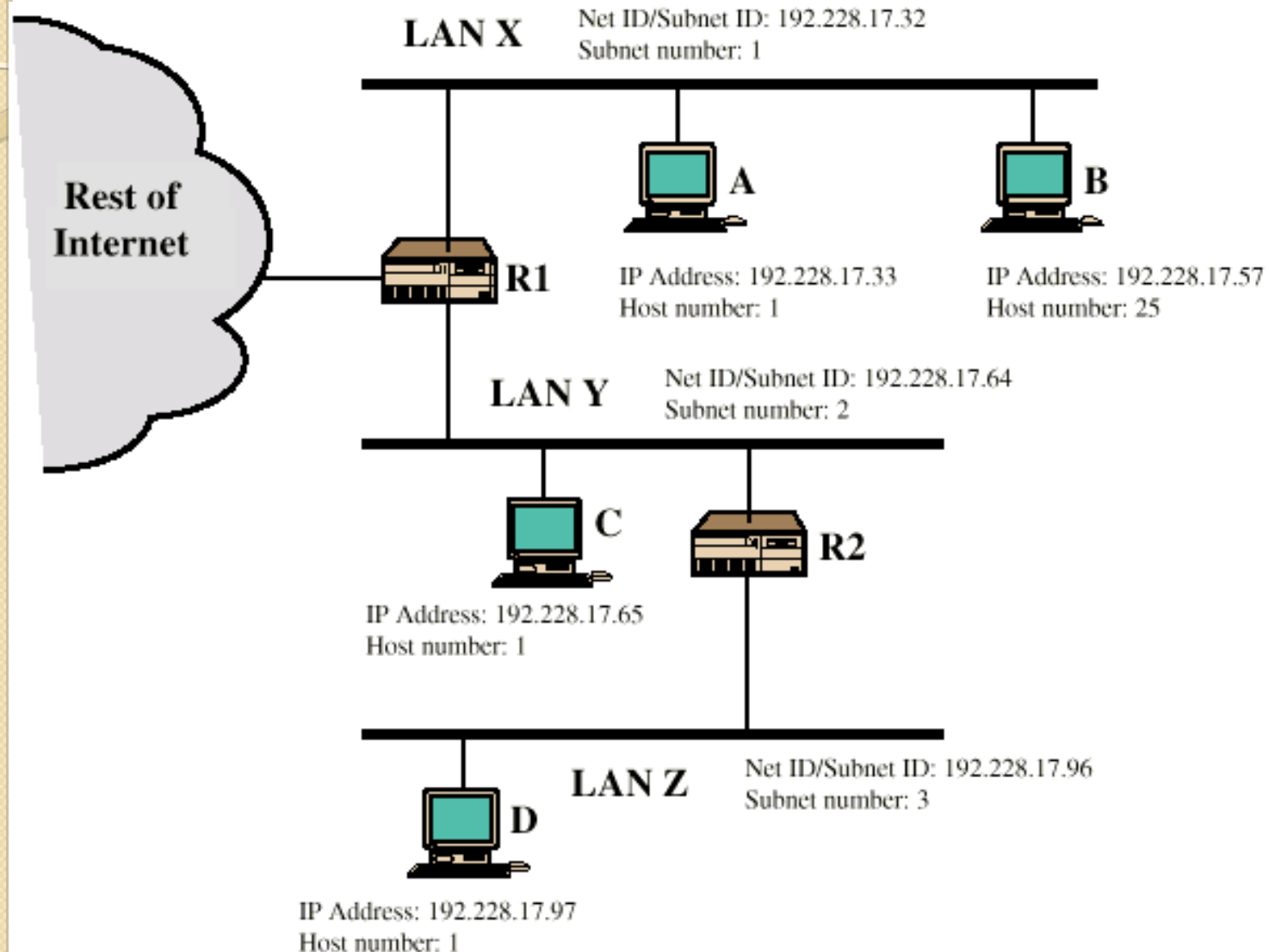
Ip inicial: 192.228.17.32

(32=00100000)

Ip final: 192.228.17.63

(63=00111111)

Enrutamiento usando subredes




Nomenclatura CIDR

- CIDR: Classless Inter-Domain Routing
- CIDR es un método que utilizan los ISPs (Internet Service Providers) para asignar una cantidad de direcciones a una empresa o un hogar cliente.
- Los ISPs proveen un bloque de direcciones y lo especifican así:
 - Ejemplo: 192.168.10.32/27
- El término /27 indica cuál es la máscara de subred. Esto significa que los primeros 27 bits de la dirección IP deben estar en “uno” para su máscara de subred (máscara: 255.255.255.224).

Ejemplos de Máscaras

Máscara de Subred	Valor CIDR	Tipo de Red
255.0.0.0	/8	Clase A
255.128.0.0	/9	Clase A
255.192.0.0	/10	Clase A
255.255.0.0	/16	Clase B
255.255.128.0	/17	Clase B
255.255.192.0	/18	Clase B
255.255.255.0	/24	Clase C
255.255.255.128	/25	Clase C
255.255.255.192	/26	Clase C
255.255.255.252	/30 (máximo posible)	Clase C



Protocolos de Enrutamiento en Internet

Introducción

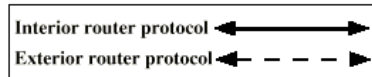
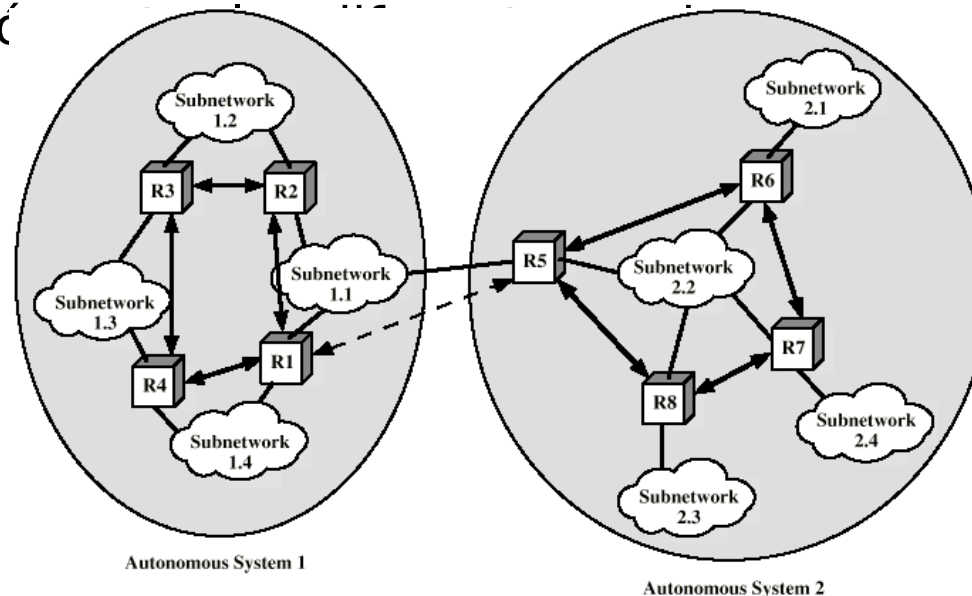
- En topologías complejas se requiere cooperación dinámica entre los routers para:
 - Evitar porciones de red con fallos
 - Evitar porciones de red con congestión
- Se requiere que los routers intercambien información sobre:
 - Qué redes son accesibles?
 - A través de qué Routers se puede acceder?
 - Características de retardo de las rutas?
- **Solución:** Protocolos de encaminamiento

Protocolos de encaminamiento

- Información necesaria
 - Entre ES y IS: Destino en la misma red o en otra?
 - Entre IS's: Información global de la red
- Sistema autónomo (AS):
 - Conjunto de redes interconectado por IS's pertenecientes a un mismo dominio administrativo

Sistema Autónomo

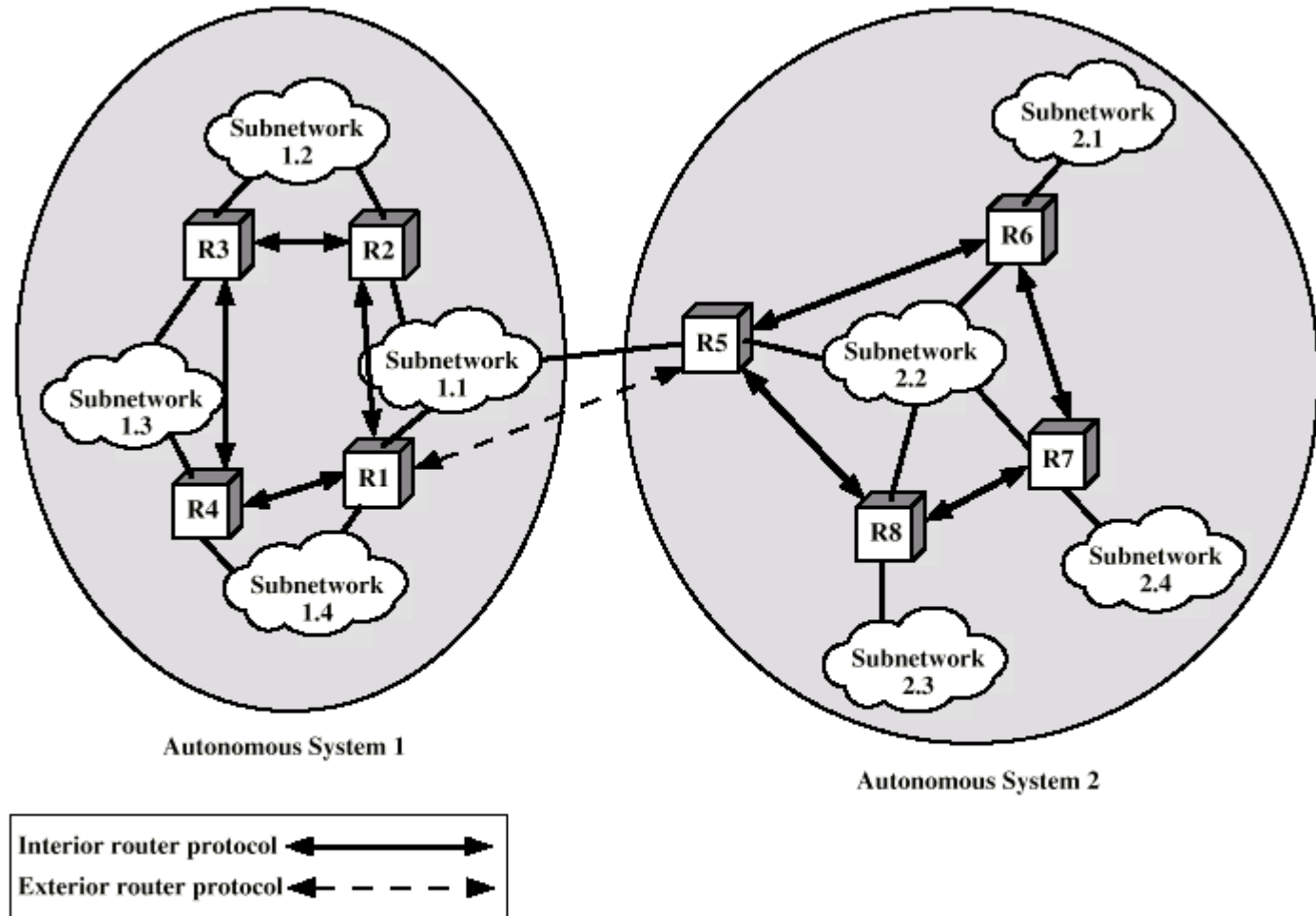
- Un AS contiene un grupo de encaminadores intercambiando información a través de un protocolo de encaminamiento común
- Un AS es un conjunto de redes y dispositivos de encaminamiento gestionados por una única organización
- En todo momento (excepto cuando hay fallos), existe conexión



Tipos de Protocolos de Encaminamiento

- Interiores a un Sistema Autónomo:
 - IRP: Interior Router Protocol (También conocido como IGP- Interior Gateway Protocol)
 - Funciones de encaminamiento dentro del sistema Autónomo
 - Los IRPs pueden cambiar de un SA a otro
 - Ejemplos de IRP: RIP (Routing Information Protocol), Algoritmo OSPF (Open Shortest Path First)
- Exterior a un sistema Autónomo:
 - ERP: Exterior Router Protocol (También conocido como EGP- Exterior Gateway Protocol)
 - Intercambia información de encaminamiento con otros Sistemas Autónomos (A quiénes se puede alcanzar por un AS específico)
 - Ejemplo: BGP (Border Gateway Protocol)

Aplicación de IRP y ERP



Internet: BGP, Border Gateway Protocol (ERP)
OSPF, Open Shortest Path First (IRP)

OSPF

- Open Shortest Path First
- Protocolo de enrutamiento de estado de enlace
- En el RFC 1131, la especificación de OSPFv1 fue publicada en 1989. La segunda versión de OSPF fue desarrollada en 1998 y publicada en el RFC 2328. La tercera versión de OSPF fue publicada en 1999 y destinadas principalmente para la compatibilidad con IPv6.
- Basado en la comunicación hop- by-hop del enrutamiento de la información
- Específicamente diseñado para el enrutamiento de Dominios interiores de una red IP

OSPF

- Cada Encaminador mantiene la información del estado de sus enlaces locales
- El Encaminador transmite la información de estado de los enlaces periódicamente a los Encaminadores que conoce
- Cada Encaminador que recibe un paquete de actualización, debe enviar una confirmación al emisor.
- Cada Encaminador mantiene una base de datos que refleja la topología conocida del sistema Autónomo del que forma parte.

Características OSPF

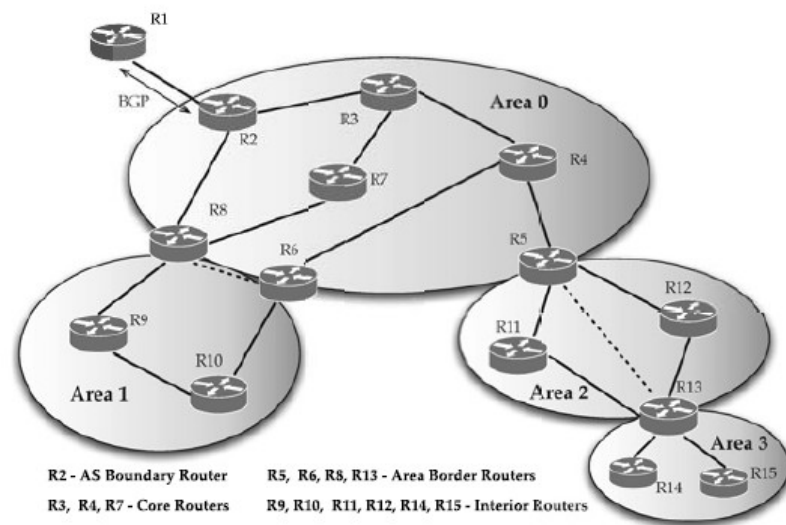
- Un protocolo de enrutamiento requiere:
 - Información sobre el estado (costo) de enlace
 - La habilidad de anunciar la fiabilidad de este estado de enlace a través de la comunicación en la red.
- Además un protocolo de estado de enlace utiliza dos sub-protocolos, uno para establecer una relación de vecinos a través del protocolo hello, y otro para la sincronización de bases de datos

Distribución de LSAs

- La inundación del anuncio del estado de enlace (LSA) no siempre es necesaria ya que una red puede tener diversos tipos de medios de transmisión.
- Por ejemplo, si hay N routers en una red, por decir, en la misma área local (LAN), se crea innecesariamente $N(N - 1)$ enlaces mientras que la definición de un solo enlace podría ser suficiente

Jerarquía de la red en OSPF

- OSPF proporciona la funcionalidad de dividir una red intradomain (un sistema autónomo) en subdominios, comúnmente conocidos como áreas
- Cada red intradomain debe tener un área central, referida como **área troncal**; lo que se identifica con el **Área ID 0**.
- Las áreas se identifican a través de un campo de área de 32 bits; por lo que Area ID 0 es lo mismo que 0.0.0.0.
- Por lo general, las áreas (aparte del área troncal) se numeran secuencialmente como Área 1 (es decir, 0.0.0.1), Área 2, y así sucesivamente.
- OSPF permite una configuración jerárquica con el área troncal como el nivel superior, mientras que todas las otras áreas, conectadas con el área troncal, se conocen como áreas de bajo nivel



Clasificación de los Routers en OSPF

- **Routers de borde de área:** Son routers que se sitúan entre el borde del área troncal y las áreas de bajo nivel. Cada router de borde de área debe tener al menos una interfaz al área troncal; también debe tener al menos una interfaz para cada área a la cual está conectada.
- **Routers internos:** Son routers ubicados en cada área de bajo nivel que sólo tienen interfaces para los routers internos en la misma área.
- **Routers del área troncal:** Son routers localizados en el Área 0 con al menos una interfaz que une a otro router en el área troncal.
- **Routers frontera AS:** Estos routers están localizados en el Área 0 con conectividad a otros AS; deben ser capaces de manejar más de un protocolo de enrutamiento. Por ejemplo, intercambiar información con otros AS, deben ser capaces de comunicar BGP. Estos routers también tienen interfaces internas para conectividad a otros routers del área troncal.

Tipos de Redes que soporta OSPF

- (1) Redes punto a punto:
 - conectar un par de routers directamente por una interface/enlace como es el OC-3.
 - Los enlaces punto a punto se utilizan típicamente cuando un dominio OSPF es expandido en una región distribuida geográficamente.
- (2) Redes de radiodifusión:
 - Redes tales como las LANs, conectadas con una tecnología como Ethernet.
 - Las redes radiodifusión, por naturaleza, son multiaccesos donde todos los routers en una red de radiodifusión pueden recibir un sólo paquete transmitido.
 - En estas redes, un router es elegido como **Designated Router** (DR) y otro como **Backup Designated Router** (BDR).

Tipos de Redes que soporta OSPF

- (3) Redes multiacceso sin radiodifusión (NBMA)
 - Las redes *multi acceso sin-radiodifusión* utilizan tecnologías tales como ATM o frame relay donde más de dos routers pueden ser conectados sin capacidad de radio difusión.
 - Así, se requiere transmitir explícitamente un paquete OSPF a cada router de la red.
 - Tales redes requieren una configuración extra para emular la operación de OSPF sobre una red de radio difusión. Como las redes de radio difusión, las redes NBMA elijen un DR y un BDR.
- (4) Redes punto a multipunto
 - Son también redes sin radio difusión como las redes NBMA, sin embargo, el modo de operación de OSPF es diferente y de hecho similar a los enlaces punto a punto.
- (5) Enlaces virtuales
 - Son utilizados para conectar un área con el área troncal.
 - Los enlaces virtuales se configuran entre dos routers de borde de área.
 - Los enlaces virtuales pueden ser utilizados también si el área troncal está dividida en dos partes en caso de que un enlace falle; en tal caso, los enlaces virtuales son tunelizados a través del área (sin área troncal).

Sub-Protocolos de OSPF

- Los mecanismos de sub-protocolos son también utilizados para el funcionamiento de un protocolo de estado de enlace además de la función de LSA a través de inundación.
- Dos sub-protocolos claves son:
 - El protocolo hello
 - El protocolo database synchronization protocol.

Protocolo Hello

- Durante la inicialización/activación, el protocolo hello se utiliza para la búsqueda de vecinos así como muchos parámetros antes de establecer dos routers vecinos;
- Esto significa que al usar el protocolo hello, las adyacencias lógicas son establecidas; esto se hace para punto a punto, punto a multipunto, y redes de enlaces virtuales.
- Para redes de radio difusión y redes NBMA, no todos los routers se convierten en adyacencias lógicas; aquí, el protocolo Hello se utiliza para elegir DRs y BDRs.

Protocolo Hello

- Después de la inicialización, para todos los tipos de redes, el protocolo hello se utiliza para mantener viva la conectividad, que garantiza la comunicación bidireccional entre vecinos.
- Esto significa, que si el mensaje hello de permanencia de conectividad no es recibido durante un intervalo de tiempo que se estableció durante la inicialización, se supone que el enlace/conectividad entre los routers no está disponible.

Database synchronization protocol

- Dos routers adyacentes necesitan construir adyacencia.
- La base de datos del estado de enlace mantenida por estos dos routers puede cambiarse fuera de sincronización durante el tiempo de fallo de un enlace. Por tanto, es necesario sincronizarlos de nuevo.
- Con el fin de mantener un intercambio completo de LSA de todos los enlaces en la base de datos de cada router, se debe usar un proceso de descripción especial de la base de datos para optimizar este paso.
- Por ejemplo, durante la de descripción de la base de datos, sólo las cabeceras del LSA son intercambiadas; las cabeceras sirven como una información adecuada para comprobar si un lado tiene el último LSA.
- Ya que un proceso de sincronización puede requerir intercambio de información de la cabecera sobre muchos LSAs, el proceso de sincronización de la base de datos permite para tales intercambios dividir en múltiples pedazos. Estos pedazos son comunicados mediante la descripción de la base de datos de los paquetes indicando si es un pedazo de un paquete inicial (utilizando I-bit) o una continuación/más paquetes o el último paquete (con M-bit).
- Además, un lado necesita servir como maestro (MS-bit) mientras que el otro lado sirve como esclavo, esta negociación es permitida; típicamente, el router vecino con el ID más bajo será el esclavo.

Formato de paquetes OSPF

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
version (1 byte)								type (1 byte)								Packet Length (2 bytes)															
Router ID (4 bytes)																Area ID (4 bytes)															
Checksum (2 bytes)								Authentication Type (2 bytes)																							
Authentication (4 bytes)																Authentication (4 bytes)															

- **Cabecera Común**

- **Version:** Este campo representa el número de la versión de OSPF; la correspondiente versión es 2.
- **Type:** Este campo especifica el tipo del paquete. OSPF tiene 5 tipos de paquetes: hello (1), database description (2), link state request (3), link state update (4), y LSA (5).
- **Packet length:** Este indica la longitud del paquete OSPF
- **Área ID:** Este es el ID del área donde el paquete OSPF es originado. El valor 0.0.0.0 está reservado para el área backbone (área troncal).
- **Checksum:** Este es el checksum IP sobre todo el paquete OSPF.
- **AuType and Authentication Field:** AuType trabaja con el campo de (Authentication field) para la autenticación. Existen tres tipos de autenticación: El valor 0 (sin autenticación), 1 (password de texto claro) y 2 (autenticación criptográfica MD5 de checksum).

Formato de paquetes OSPF

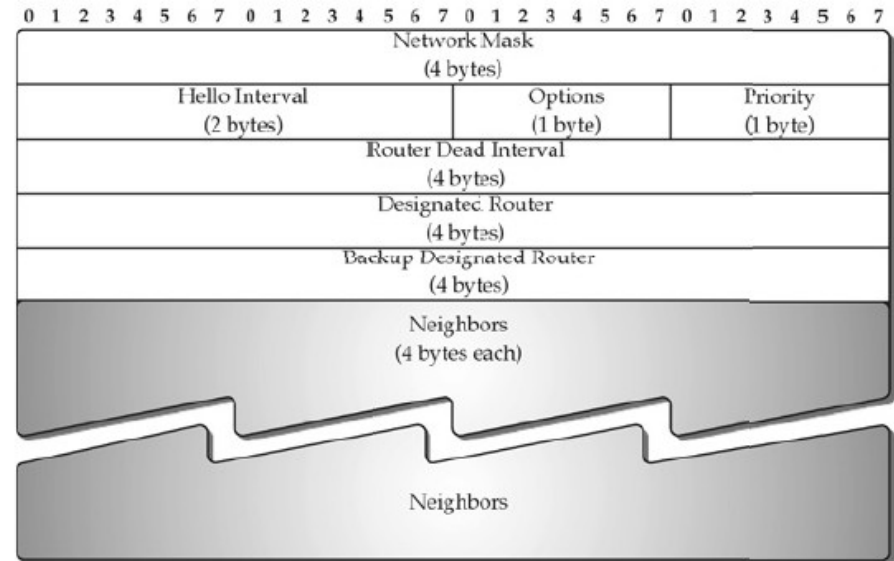
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
version (1 byte)								type (1 byte)								Packet Length (2 bytes)							
Router ID (4 bytes)																							
Area ID (4 bytes)																							
Checksum (2 bytes)								Authentication Type (2 bytes)															
Authentication (4 bytes)																							
Authentication (4 bytes)																							

- **Router ID:**

- ▮ Este campo indica el ID del router origen.
- ▮ Ya que un router tiene múltiples interfaces, no hay un modo definitivo para determinar cual interface de dirección IP debería ser el ID del router. De acuerdo al RFC 2328, podría ser también la dirección IP más larga o más corta que pertenece a todas las interfaces.
- ▮ Cabe señalar que si un router es creado sin una interface de conexión, no tiene la habilidad para adquirir el ID del router. Para evitar este escenario, **una interfaz de loopback**, siendo una interface virtual, puede usarse para adquirir el ID de un router. En general, el ID de un router que es basado sobre una interface de loopback proporciona mucha más flexibilidad a las funciones de la red en términos de administración que una interface física basada en el direccionamiento.

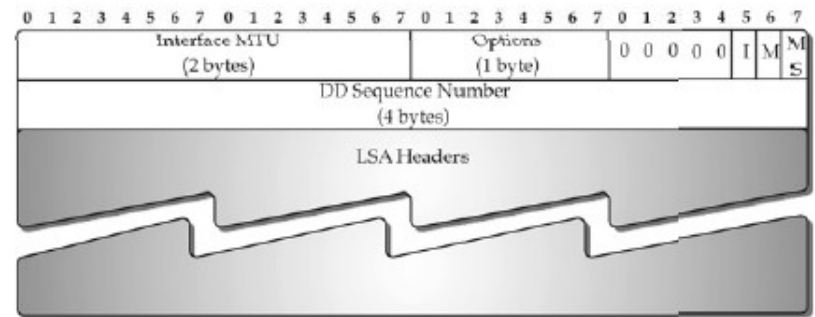
Paquete Hello

- **Network Mask:** Esta es la dirección de la máscara de una interface del router desde el cual el paquete es enviado.
- **Hello Interval:** Este campo designa la diferencia de tiempo en segundos entre cualquiera de dos paquetes hello. Los routers transmisores y receptores son requeridos para mantener el mismo valor, si no, la relación de vecindad entre los dos routers no se establece. Para red punto a punto y redes radio difusión, valor por defecto es 10 segundos, mientras para una red sin radio difusión el valor por defecto es 30 segundos.
- **Options:** El campo options permite compatibilidad con un router vecino por ser revisado.
- **Priority:** Este campo se utiliza cuando elige el router designado y el router de apoyo.
- **Router Dead Interval:** Esta es la diferencia de tiempo en el cual un router declara a un vecino para ser eliminado si no recibe paquete hello.
- **Designated Router (DR) (Backup Designated Router (BDR):** El campo DR (BDR) enumera las direcciones IP de la interface del DR (BDR) sobre la red, pero no la identificación del router. Si el campo DR(BDR) es 0.0.0.0, esto significa que no hay DR (BDR).



Data Base Description Packet

- **Interface Maximun Transmission Unit (MTU):** Este campo indica el tamaño de la unidad de transmisión que la interface puede manejar sin fragmentación.
- **Options:** Los campos de opciones consisten de muchos bits de campos de nivel. El más crítico es el E-bit, el cual se establece cuando el área próxima es capaz de procesar AS - externos LSA.
- **I/M/MS bits:** I-bit (initial-bit) se inicializa en uno para un paquete inicial que empieza una sesión de la descripción de la base de datos; para otros paquetes en la misma sesión, este campo se establece en 0. M-bit (more bit) se utiliza para indicar que este paquete no es el último para la sesión de descripción de la base de datos. MS-bit (bit maestro-esclavo) se utiliza para indicar que el originador es el maestro y se estable este campo en 1, mientras el esclavo se establece en 0.
- **DD Sequence number:** Este campo se utiliza para incrementar el número de secuencias de los paquetes desde el lado del maestro durante la sesión de descripción de la base de datos; el maestro establece el valor inicial para el número de secuencia.
- **LSA Header:** Este campo enumera las cabeceras de los LSAs en el originador de la base de datos de estado de enlace; podría enumerar algunos o todos.



Soporte de múltiples métricas en OSPF

- La tecnología actual hace que sea posible soportar varias métricas en paralelo.
- Evaluando el camino entre dos nodos en base a diferentes métricas es tener distintos mejores caminos según la métrica utilizada en cada caso, pero surge la duda de cuál es el mejor. Esta elección se realizara en base a los requisitos que existan en la comunicación.
- Diferentes métricas utilizadas pueden ser: Mayor rendimiento, Menor retardo, Menor costo, Mayor fiabilidad.
- La posibilidad de utilizar varias métricas para el cálculo de una ruta, implica que OSPF provea de un mecanismo para que una vez elegida una métrica en un paquete para realizar su routing esta sea la misma siempre para ese paquete, esta característica dota a OSPF de un routing de servicio de tipo en base a la métrica.

BGP

- Border Gateway Protocol (RFC 1771)
- BGP se utiliza para comunicar información sobre las redes que actualmente residen en un sistema autónomo a otros sistemas autónomos.
- El intercambio de información de la red se realiza mediante la creación de una sesión de comunicación entre sistemas autónomos de frontera

BGP

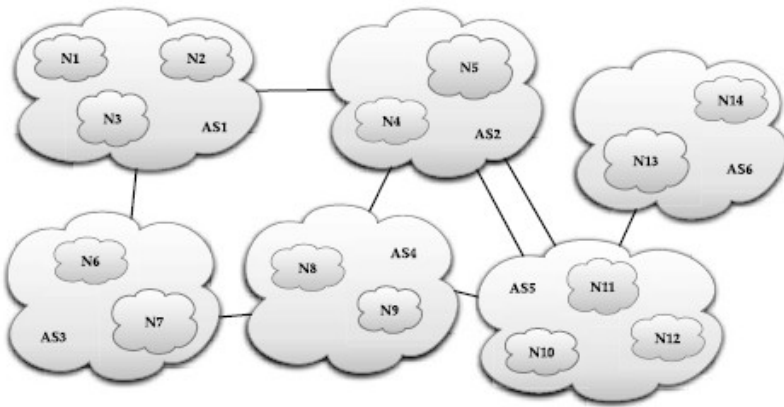
- BGP se diseñó para permitir la cooperación en el intercambio de información de encaminamiento entre dispositivos de encaminamiento, llamados pasarelas, en sistemas autónomos diferentes.
- El protocolo opera en términos de mensajes, que se envían utilizando el protocolo TCP

Comunicación entre SA con BGP

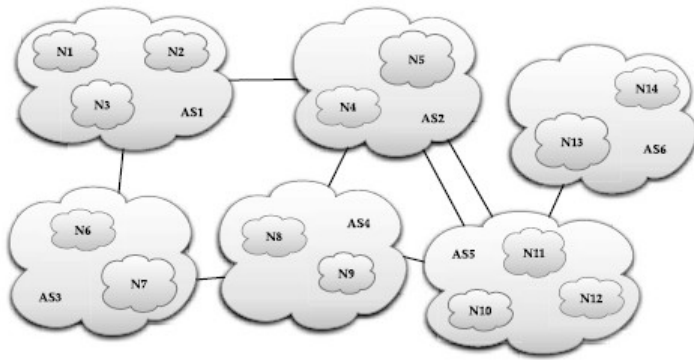
- Para la entrega fiable de información, se establece una sesión de comunicación basado en el protocolo TCP entre sistemas autónomos de frontera utilizando el número de puerto TCP 179
- Cuando por alguna razón se rompe la conexión TCP, cada parte está obligada a dejar de utilizar la información que ha obtenido desde el otro lado. En otras palabras, la sesión TCP sirve como un enlace virtual entre los dos sistemas autónomos vecinos, y la falta de comunicación significa que este vínculo virtual esta caído.
- Cada sistema autónomo puede considerarse como un *supernodo virtual*

Topología BGP

- Se pueden apreciar seis supernodos virtuales (sistemas autónomos) AS1 a AS6, conectados por enlaces virtuales, utilizando el protocolo TCP basado en sesiones BGP para la comunicación entre dos supernodos virtuales adyacentes.
- Cada supernodo virtual contiene una o más redes identificadas como N1, N2, N3 en AS1, y así sucesivamente



Topología BGP



- Hay más de un camino posible entre sistemas autónomos determinados.
- También es posible tener un supernodo en el borde de toda la red, tal como AS6.
- Además está permitido que existan múltiples enlaces virtuales entre dos sistemas autónomos vecinos, así como se puede apreciar entre AS2 y AS5, existen dos enlaces virtuales.

Mensajes de BGP

- 1. OPEN
- 2. UPDATE
- 3. KEEPALIVE
- 4. NOTIFICACION

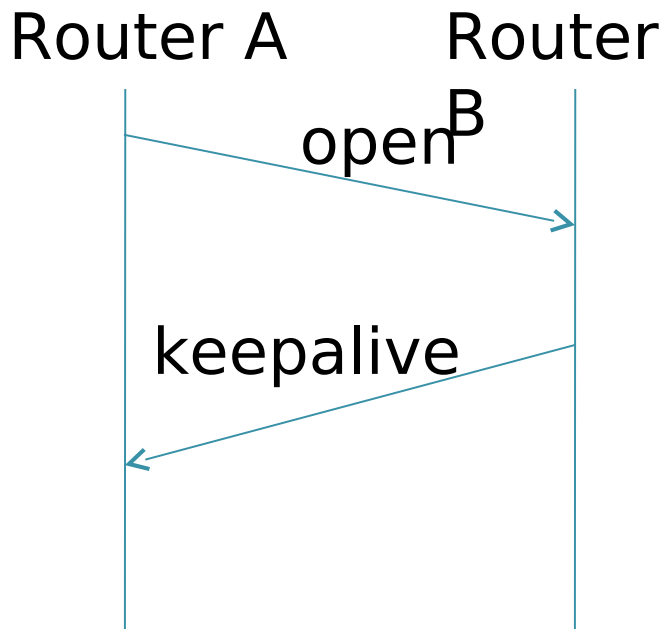
Procedimientos de BGP

- Adquisición de vecinos
- Detección de vecino alcanzable
- Detección de red alcanzable

Adquisición de Vecinos

- Dos dispositivos de encaminamiento se consideran que son vecinos si están en la misma subred.
- Si los dos dispositivos de encaminamiento están en sistemas autónomos diferentes, podrían desear intercambiar información de encaminamiento.
- Para este cometido es necesario realizar primero el proceso de adquisición de vecino.
- Se requiere un mecanismo formal de encaminamiento ya que alguno de los dos vecinos podría no querer participar. Existirán situaciones en las que un vecino no desee intercambiar información esto se puede deber a múltiples factores como por ejemplo que este sobresaturado y entonces no quiere ser responsable del tráfico que llega desde fuera del sistema.

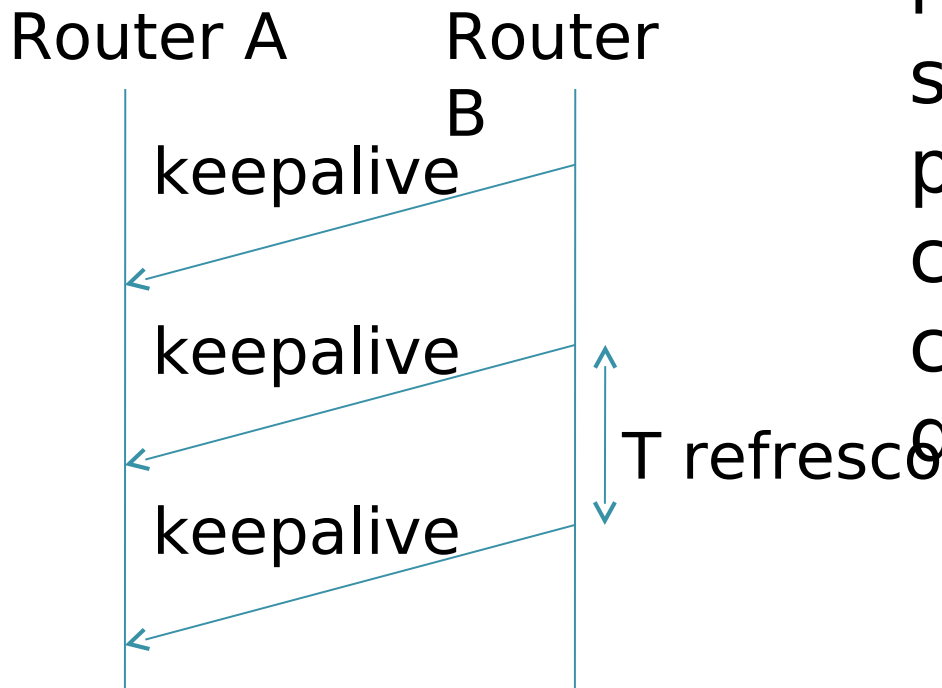
BGP: Adquisición de Vecinos



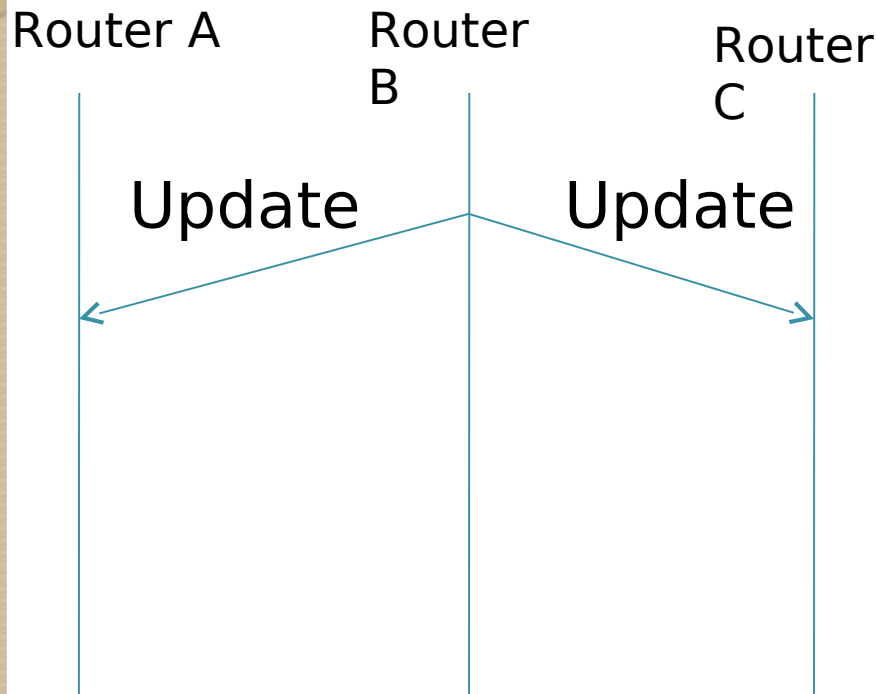
- Es un procedimiento para que dos Encaminadores vecinos se pongan de acuerdo en que intercambiarán información de Encaminamiento.
- Alguno podría no querer hacerlo por tener demasiada congestión.

BGP: Detección de vecino alcanzable

- Cada Router necesita estar seguro de que su par existe y está comprometido con la relación de vecino



BGP: Detección de Red Alcanzable



- Cada Encaminador mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para alcanzar esa red.
- Cada vez que hay un cambio, este se informa a los demás vecinos (mensaje Update)

Mensajes BGP

- Los mensajes BGP tienen una cabecera común de 19 octetos que contiene los siguientes tres campos:
 - **Marcador:** reservado para autenticación. El emisor puede insertar un valor en este campo para permitir al receptor comprobar la veracidad del emisor.
 - **Longitud:** longitud del mensaje en octetos.
 - **Tipo:** tipo de mensaje; OPEN, UPDATE, NOTIFICATION, KEEPALIVE.

Mensaje Open

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1
Versión	1
AS	2
Tiempo permanente.	2
Identificador BGP	4
Long. Opciones	1
Opciones	Variable

- **Versión:** indica la versión del protocolo del mensaje. La versión actual es 4.
- **AS:** identifica al sistema autónomo del emisor del mensaje.
- **Tiempo de permanencia:** indica el tiempo de que propone el emisor como Hold Time.
- **Identificador de BGP:** identifica al BGP emisor.

Mensaje **KEEPALIVE**

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1

- El mensaje **KEEPALIVE** consta solo de la cabecera. Cada dispositivo de mantenimiento envía regularmente estos mensajes para evitar que expire el temporizador mantenimiento.

Mensaje Update

- El mensaje UPDATE facilita dos tipos de información:
 - Información sobre una ruta particular a través del conjunto de redes. Esa información se puede incorporar a la base de datos de cada dispositivo de encaminamiento que la recibe.
 - Una lista de rutas previamente anunciadas por este dispositivo de encaminamiento que van a ser eliminadas.

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1
Longitud Rutas no factibles	2
Rutas retiradas	Variable
Longitud Total atributos de camino	2
Atributos de camino	Variable
Información. De accesibilidad de la capa de red	Variable

Mensaje Update

Campo			Long (bytes)
Marcador			16
Longitud			2
Tipo			1
Longitud factibles	Rutas	no	2
Rutas retiradas			Variable
Longitud de camino	Total	atributos	2
Atributos de camino			Variable
Información. De accesibilidad de la capa de red			Variable

- La información sobre una ruta particular a través de la red implica tres campos, campo de información sobre la capacidad de alcanzar la capa de red (NLRI), campo de longitud de los atributos del camino total, y el campo de los atributos de camino. El campo NLRI contiene una lista de identificadores de redes que se pueden alcanzar por esta ruta. Cada red se identifica por su dirección IP, que es en realidad una parte de la dirección IP completa.
- El campo atributos de camino contiene una lista de atributos que se aplican a esta ruta particular.

Distancias Administrativas

- Una distancia Administrativa (AD) se utiliza para medir la confiabilidad de la información de enrutamiento recibida por un router desde otros routers vecinos.
- Rango: 0-255
 - 0: significa más confiabilidad
 - 255: significa que no pasa tráfico por esa ruta.

Decisiones de actualización de rutas con ADs

- Si un router recibe dos actualizaciones que indican una misma red remota:
 - Chequea el AD de ambas actualizaciones
 - La ruta con menor AD será la que se ubica en la tabla de enrutamiento
- Si ambas actualizaciones advierten sobre la misma red y tienen el mismo AD:
 - Se utilizan otras métricas tales como el número de saltos ó el ancho de banda de los enlaces.
- En caso de que tanto el AD, como las métricas de enlaces sean iguales se hace un balance de la carga (se envían paquetes intercaladamente por uno y otro enlace de salida)

Distancias administrativas por defecto (Routers Cisco)

Origen de la Ruta	AD por defecto
Interfaz directamente conectada	0
Ruta estática	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Desconocido	255 (esta ruta no será usada nunca)

- Ejemplos:
 - Si la red está conectada directamente, se usará esta ruta siempre hacia esa red
 - Si la ruta ha sido configurada de forma estática y hay actualizaciones RIP y de IGRP, se prefiere la ruta estática.

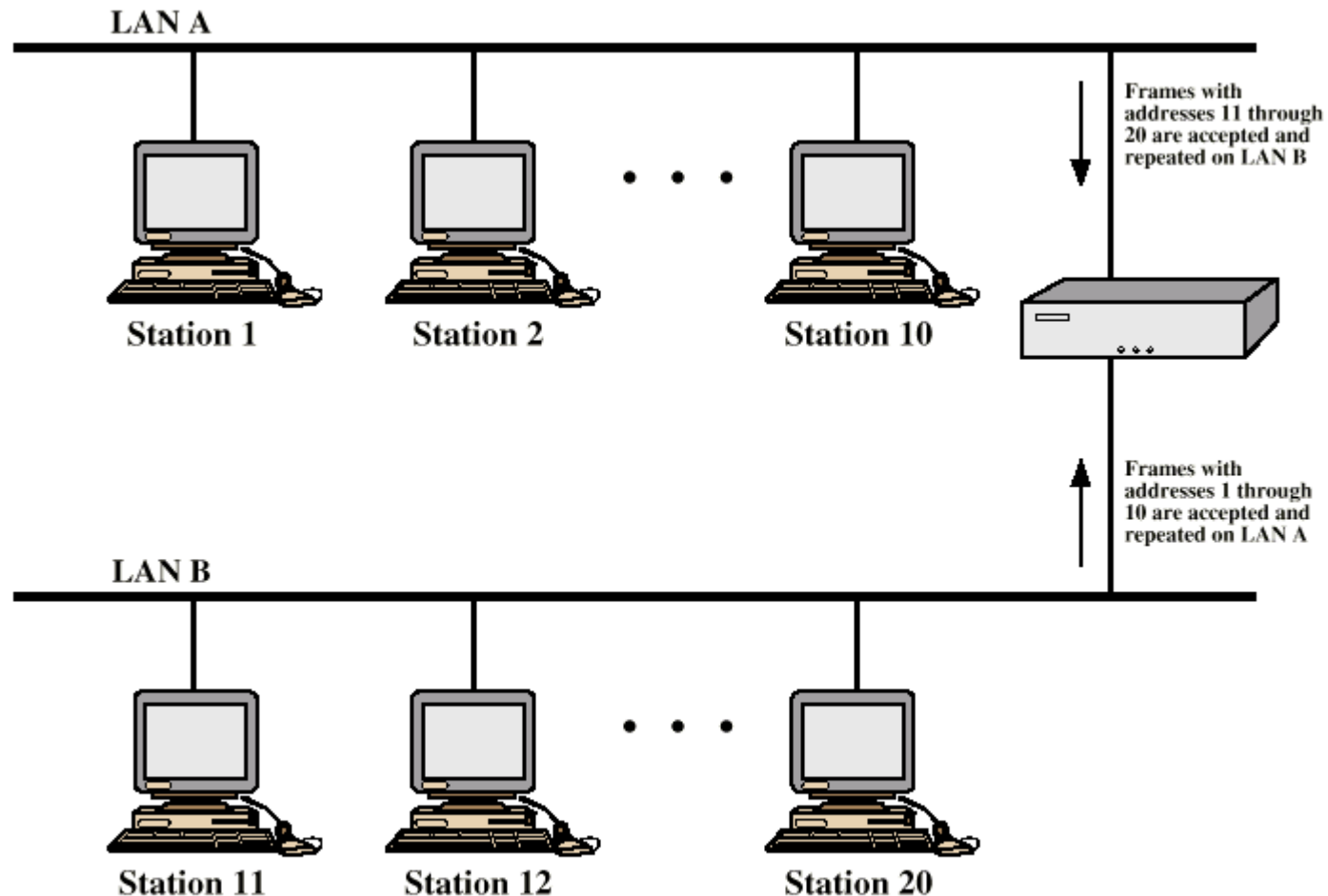


Interconexión de LANs con Puentes

Operación con Puentes

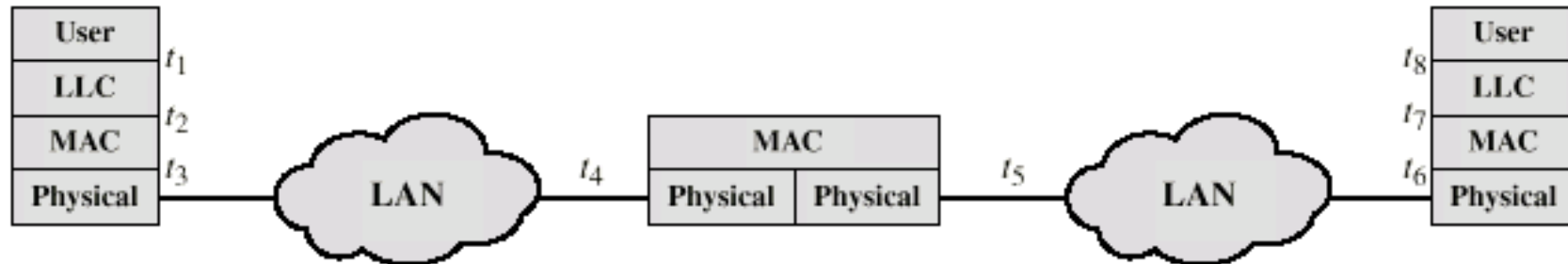
- A veces se requiere interconectar varias LAN
- Si las LAN son del mismo tipo (el mismo estándar), se pueden unir mediante un PUENTE.
- Razones para no usar una sola LAN grande:
 - Fiabilidad (Si se daña todos los host quedan incomunicados)
 - Prestaciones: Aumenta el número de colisiones y se vuelve muy lenta la red
 - Seguridad: Se pueden trabajar grupos de usuarios con diferentes niveles de seguridad

Operación con Puentes

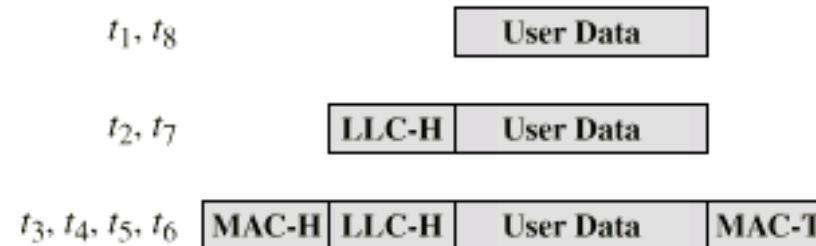


Las estaciones ven
Una sola red.

Conexión de dos LAN



(a) Architecture



(b) Operation

Uso de puentes con múltiples LAN

- Un puente debe poseer capacidad de encaminamiento entre las LAN
- Técnicas de encaminamiento usadas:
 - Encam. Estático
 - Arbol de expansión (Spanning Tree)
 - Encaminamiento por el origen

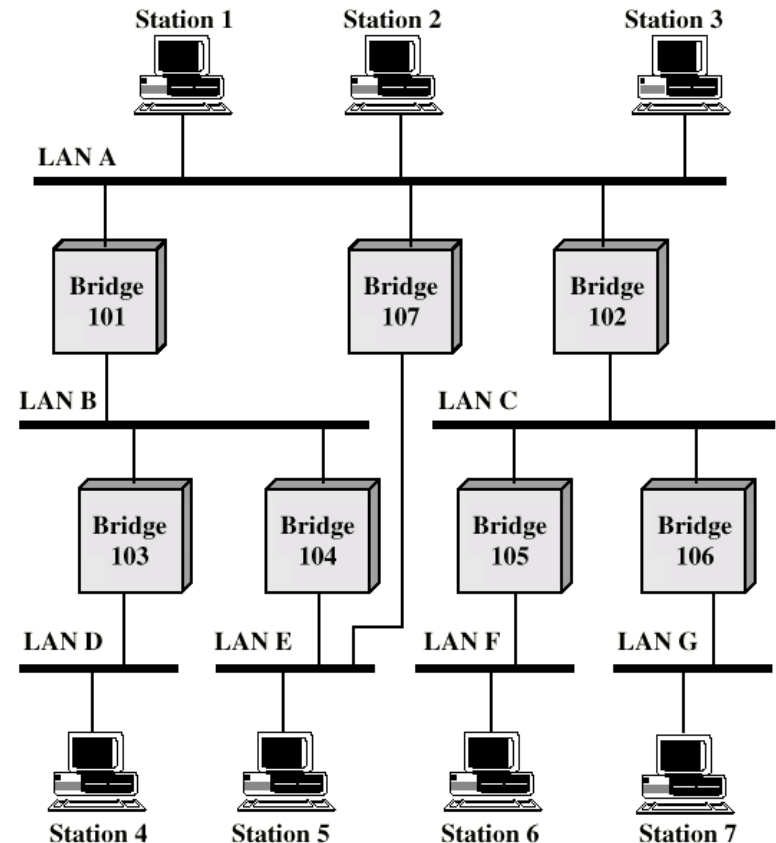
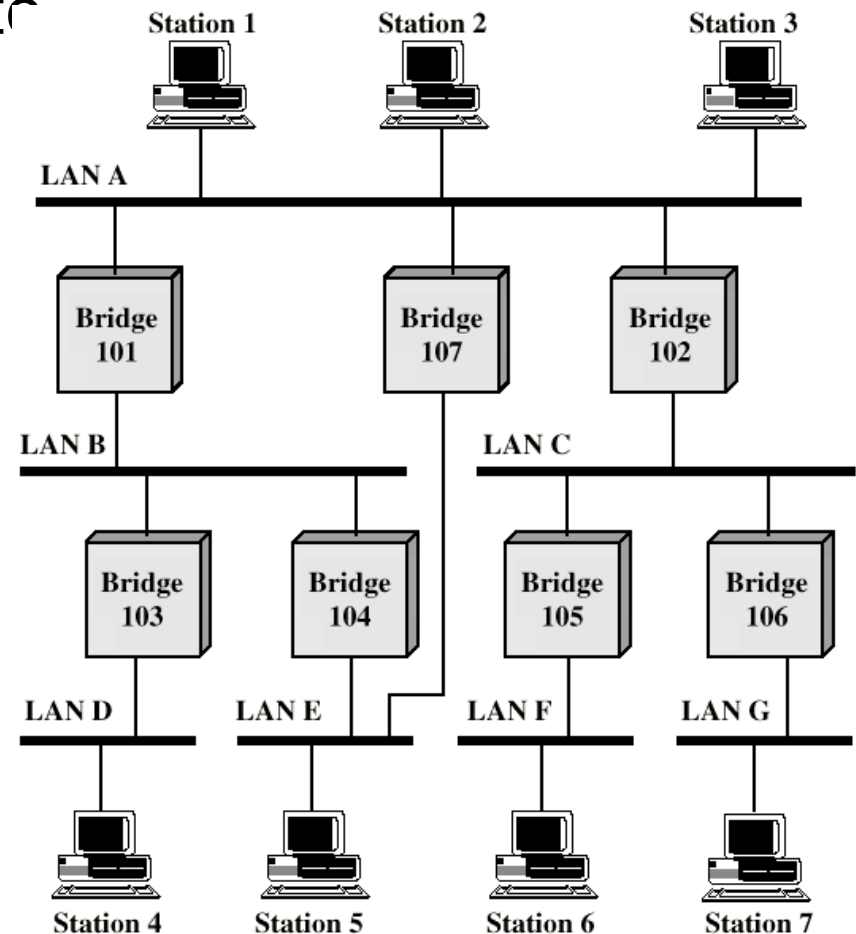


Figure 13.16 Configuration of Bridges and LANs, with Alternate Routes

Encaminamiento estático

Tabla de Encaminamiento para el Puente 105:

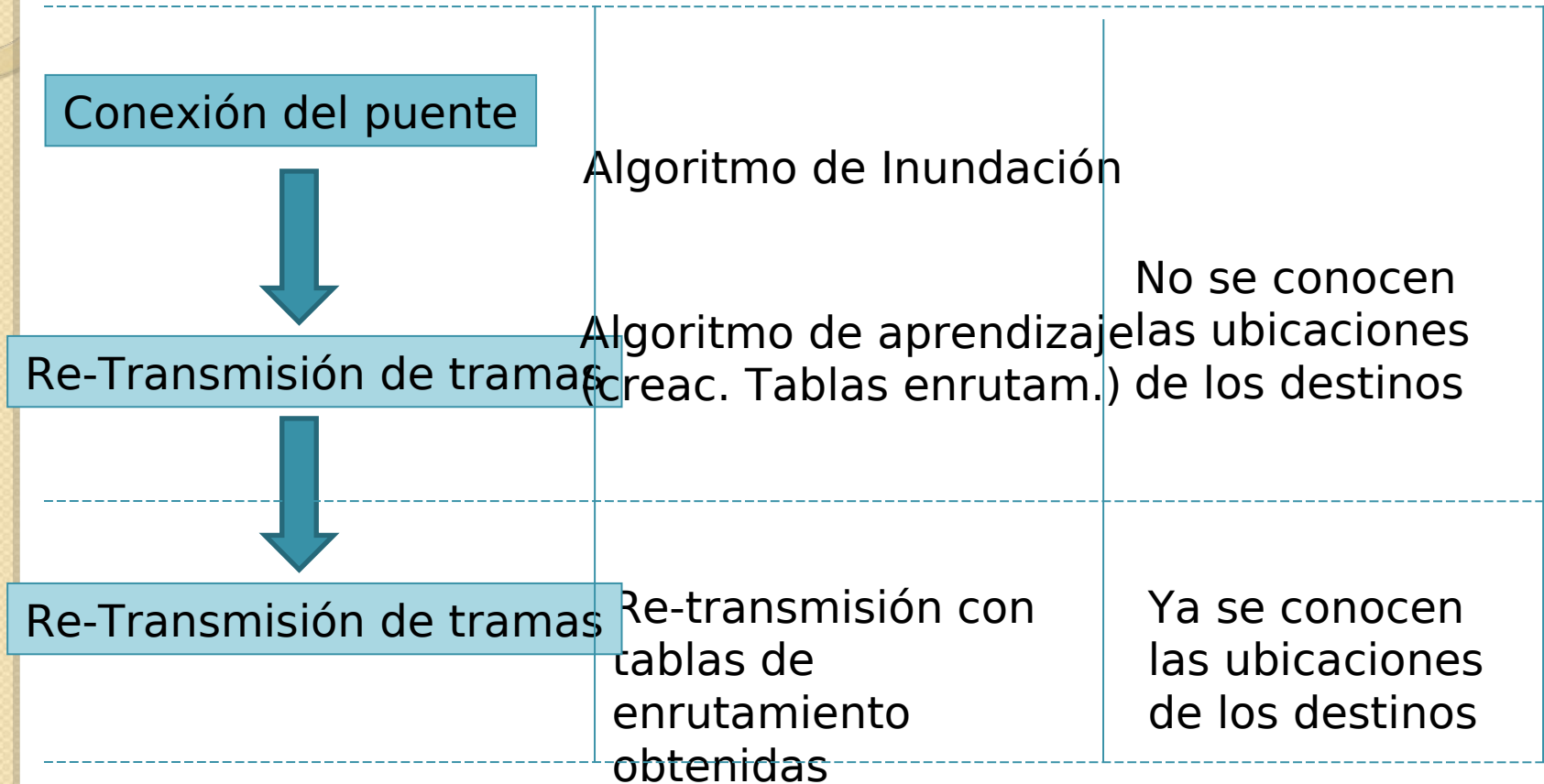
Origen Tramas	Dirección MAC Destino	LAN Destino
LAN C	Estación 6	LAN F
LAN F	Estación 3	LAN C
	Estación 2	LAN C
	Estación 1	LAN C
	Estación 4	LAN C
	Estación 5	LAN C



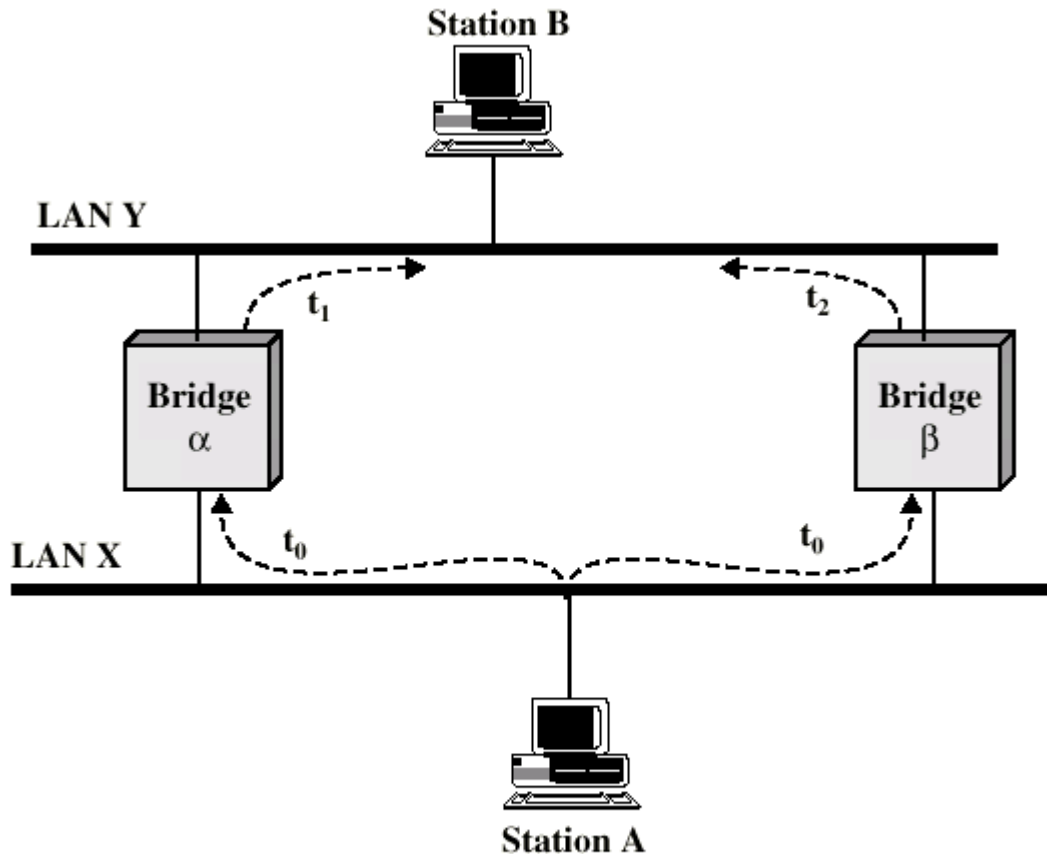
Encaminamiento con Árbol de Expansión (Spanning Tree)

- Los puentes desarrollan automáticamente la tabla de encaminamiento y la actualizan según los cambios de topología
- Posee 3 mecanismos:
 - Retransmisión de tramas
 - Aprendizaje de direcciones
 - Rompimiento de bucles
- Se busca que al conectar los puentes todo funcione perfectamente y al instante (No requiere de programación de tablas)

Operación Spanning Tree

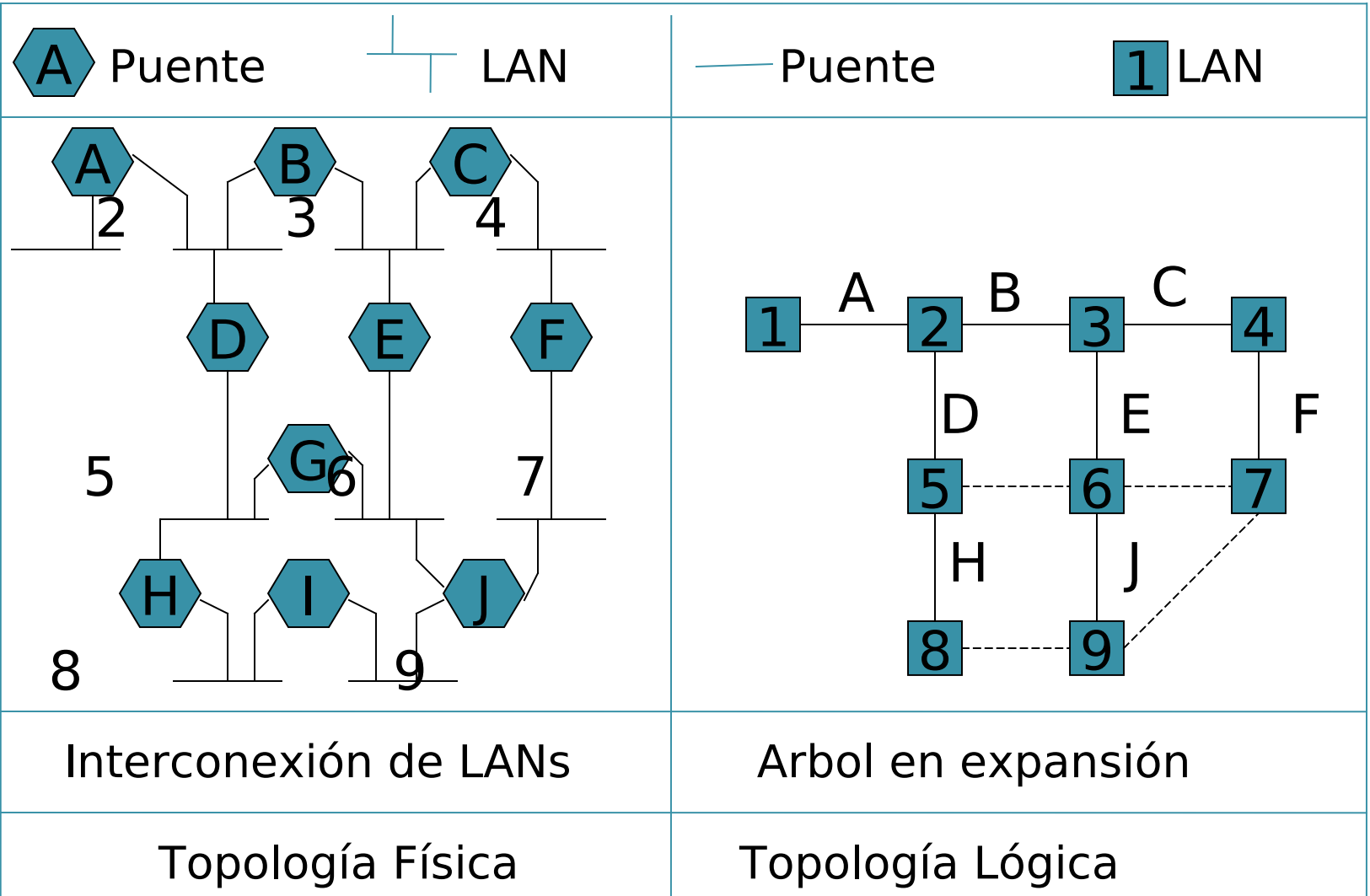


Arbol de expansión-Bucle de puentes



Problemas con tramas con destinatario desconocido

Arbol de expansión



Construcción del árbol de expansión

- Se escoge un puente raíz (suele ser el de menor número de serie)
- Se construye un árbol de trayectorias mínimas desde la raíz a cada puente y LAN
- Si falla un puente o una LAN, se calcula un árbol nuevo
- Si hay cambios en la topología, se actualiza el árbol