

IN3501 - Tecnologías de Información y
Comunicaciones para la Gestión

EQUIPOS DE INTERCONEXIÓN

PROFESORES

Juan D. Velásquez
Gastón L'Huillier
Víctor Rebolledo Lorca

Equipos de Interconexión de Redes

- Aparte de los computadores, existe una “jungla” de otros dispositivos que hacen que una red pueda funcionar:



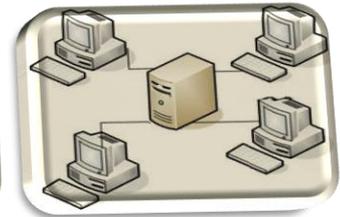
Hub



Switch



Router

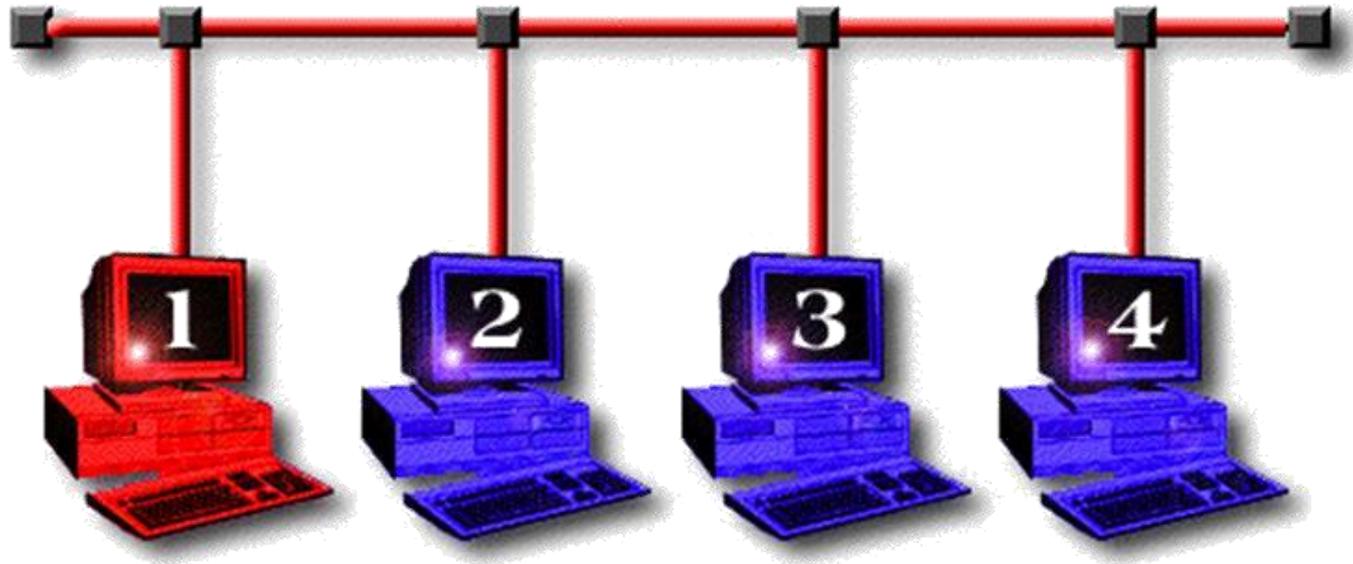


Gateway

Hub

- Es un **repetidor simple**.
- Cualquier paquete que le llega al HUB se **transmite a todos los computadores conectados**.
- Sólo aquel computador que es el verdadero **destinatario**, toma el paquete.
- El resto **escucha**.
- El resultado es una conexión simple, pero con un uso **muy poco eficiente** del ancho de banda.
- Trabaja en la **capa física** del modelo OSI
- Han ido quedando **obsoletos** con el abaratamiento de los *switch*.
- En que casos pueden ser útiles:
 1. Analizadores de la red: **IDS** (Intrusion Detection System)
 2. **Computer Cluster**: todos reciben señal de todos.

Ethernet: Funcionamiento de un HUB

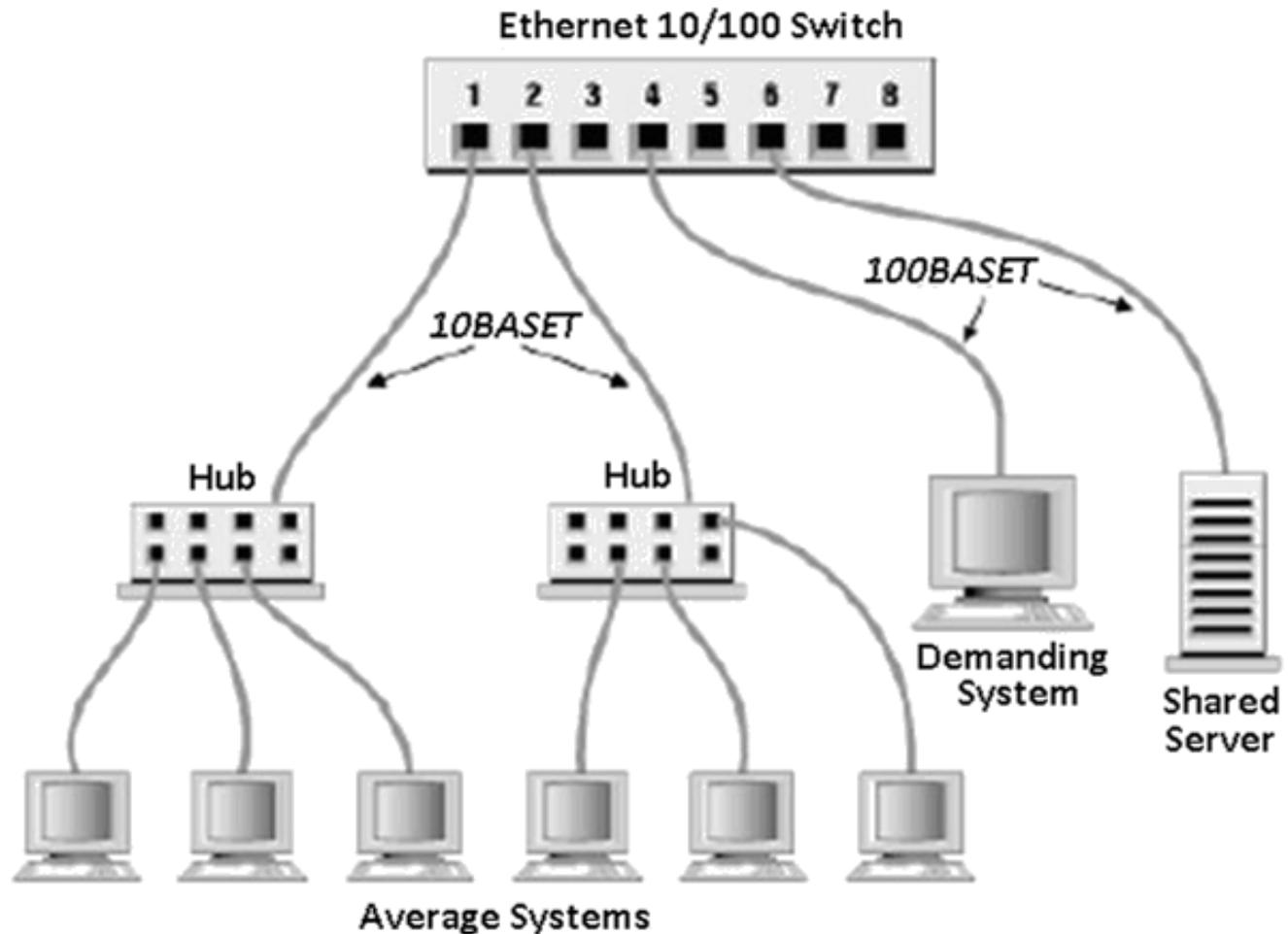


CPU **1** emite el paquete, el cual es recibido por **2**, **3** y **4**
(**Broadcast**)

Switch

- Se trata de un dispositivo de propósito especial, diseñado para **resolver problemas de escasez** de ancho de banda en la red.
- Opera en la capa de **enlace** y **red** del modelo **OSI** y reenvía los paquetes en base a la dirección MAC.
- Utilizados para **segmentar la red** en pequeños dominios de colisión.

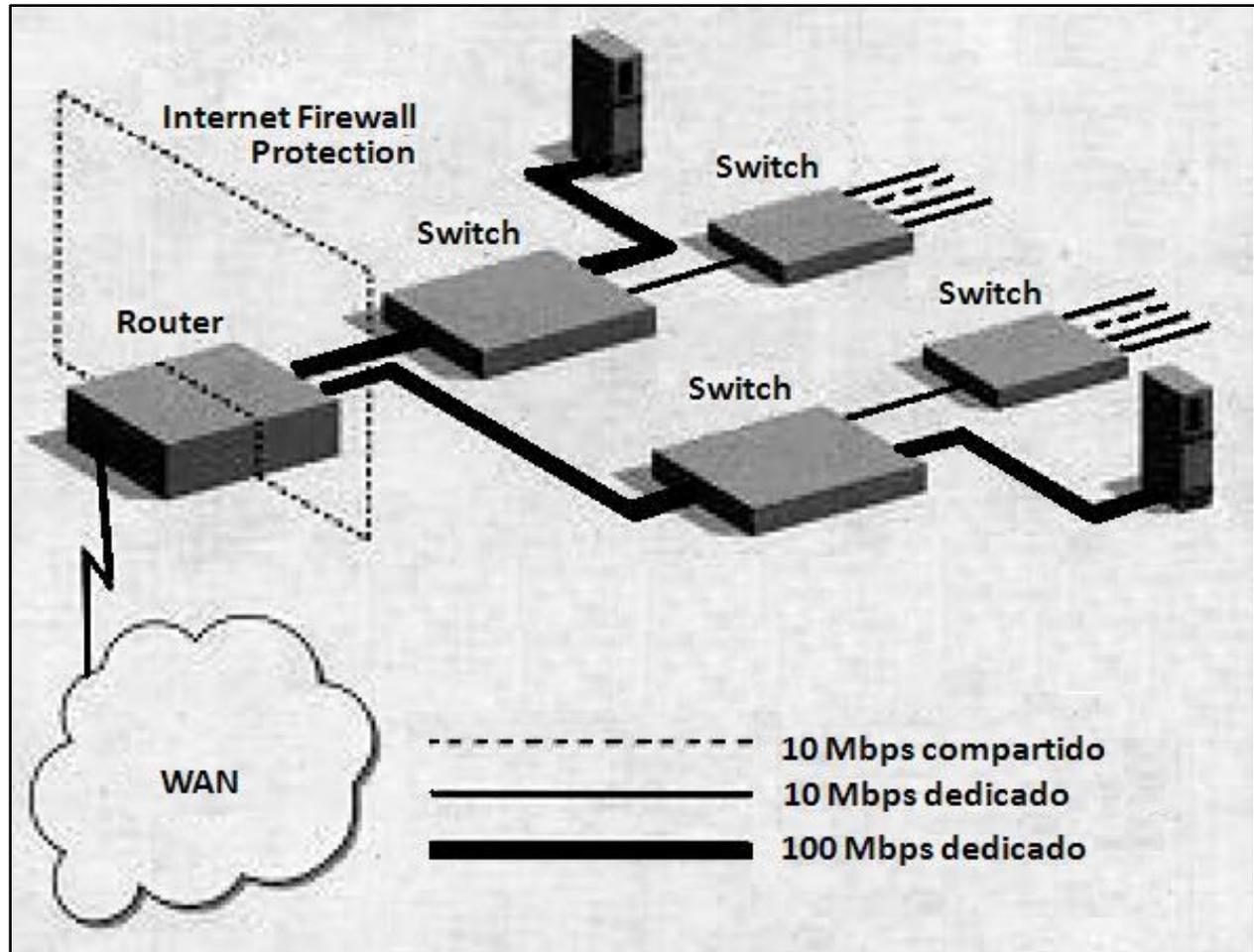
Switch: la visión antigua.



Router

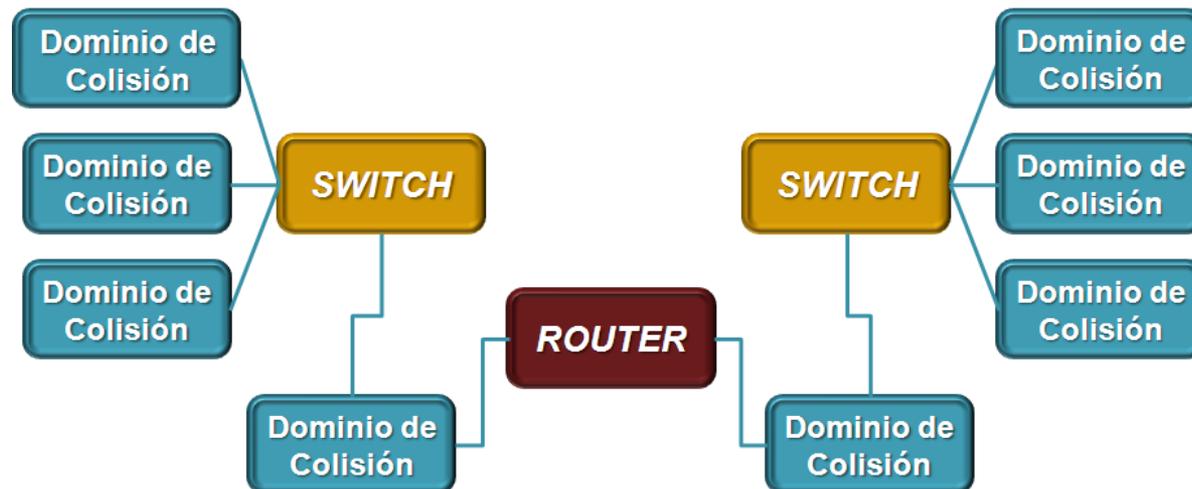
- Es un dispositivo diseñado para **segmentar la red**, **limitar el Broadcast** y **proporcionar seguridad**.
- Opera en la **tercera y cuarta capa** del modelo **OSI**. (capa de red)
- Tiene más **facilidades de software**: puede ser configurado como *firewall*.
- Tiene memoria. Por ello es **más lento que un Switch**.
- Es responsable de:
 - **Crear y mantener** tablas de ruteo.
 - Selecciona la ruta según el protocolo que se use.
 - Selecciona **heurísticamente** la mejor ruta.

Arquitectura típica con un Router.

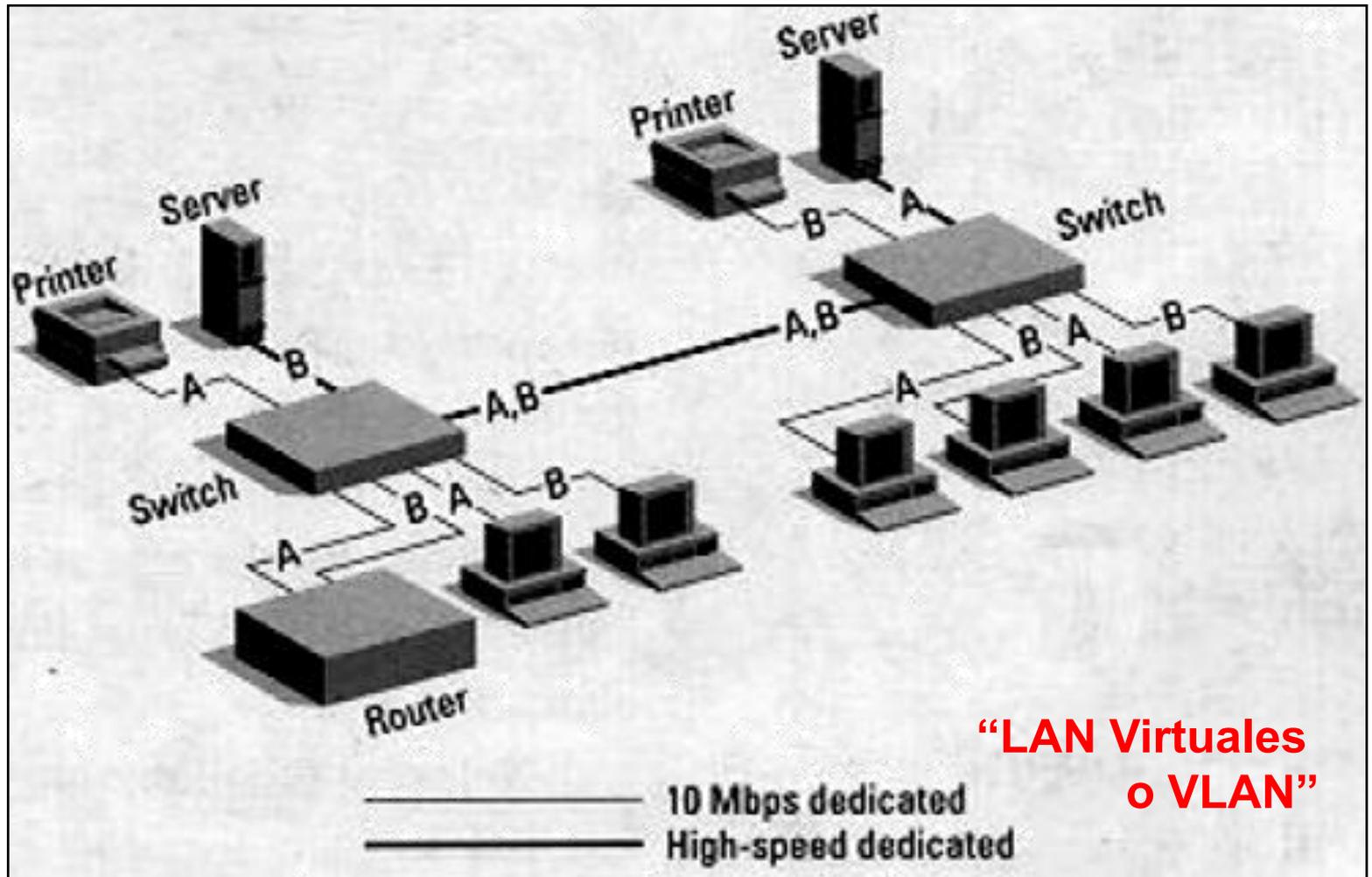


¿Cuándo se usa un Router o un Switch ?

- Si la idea es **segmentar el dominio de colisiones** en la red → **se usa un Switch**.
- Si además se desea segmentar la red en dominios individuales de broadcast, **suministrar envío de paquetes entre redes** y **soportar rutas redundantes en la red** → **se usa un Router**.



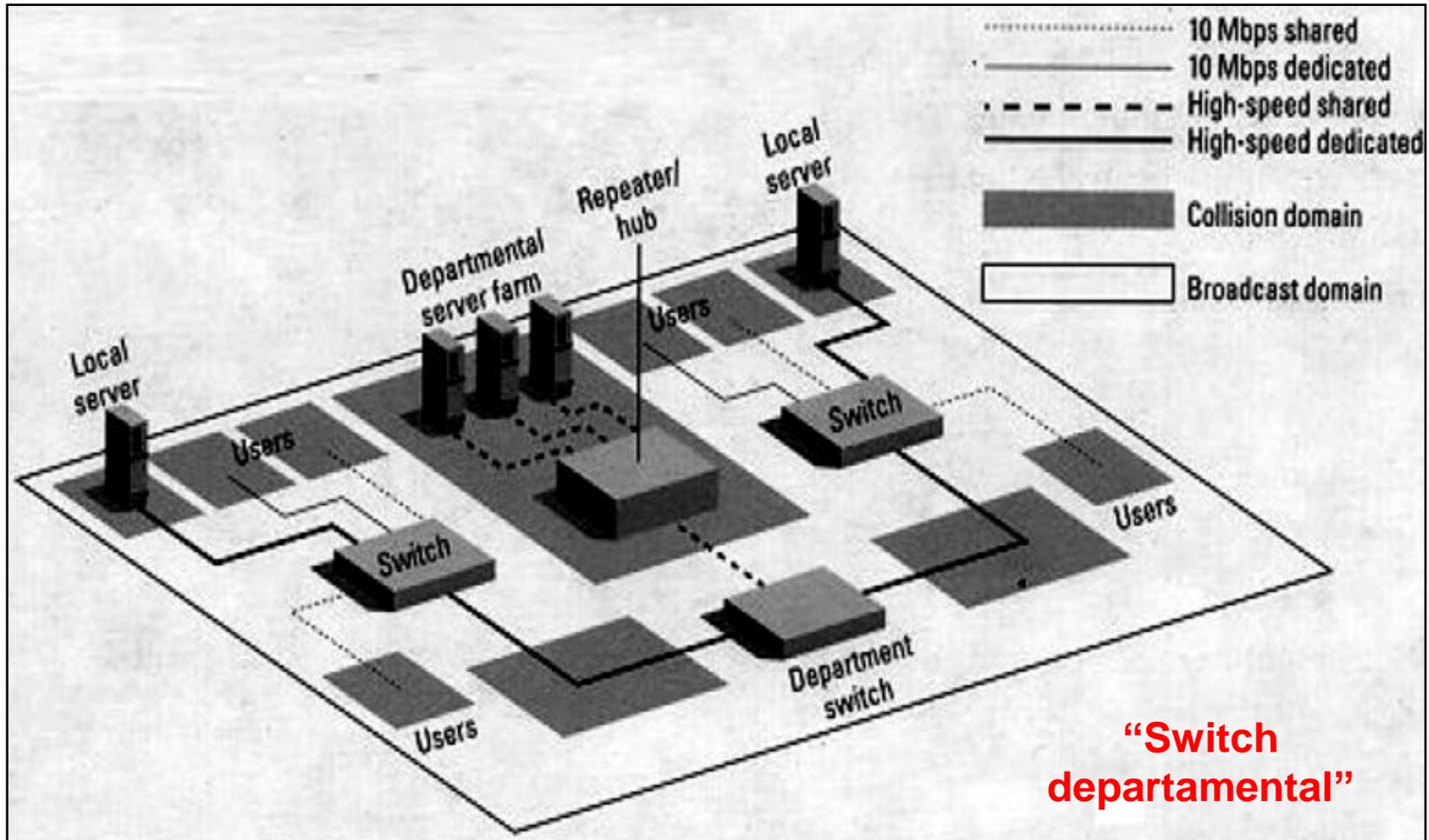
Arquitectura de redes para grupos de trabajo



Arquitectura de redes para grupos de trabajo (2)

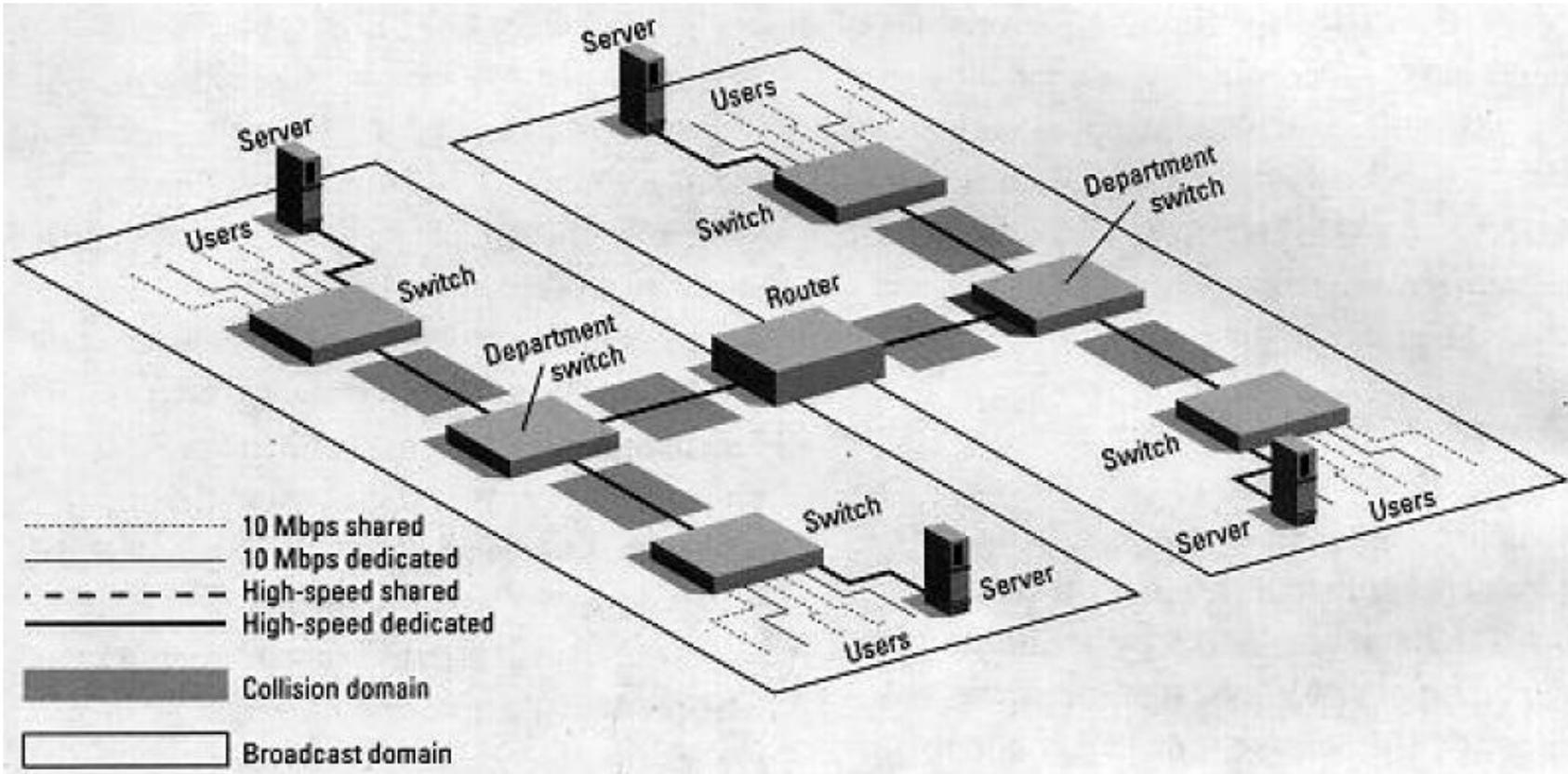
- LAN Virtuales o **VLAN**
- Los switch pueden configurarse para que sólo conecten paquetes de **de A a A** y **de B a B**.
- Esto genera **sub-redes** virtuales A y B
- Mecanismo que permite **controlar el trafico interno**.
- Redes A y B son **lógicamente independientes** en una red física.
- Generalmente utilizadas para **separar la conectividad** entre departamentos de una empresa

Arquitectura de redes para grupos de trabajo (3)



**“Switch
departamental”**

Arquitectura de redes para grupos de trabajo (4)



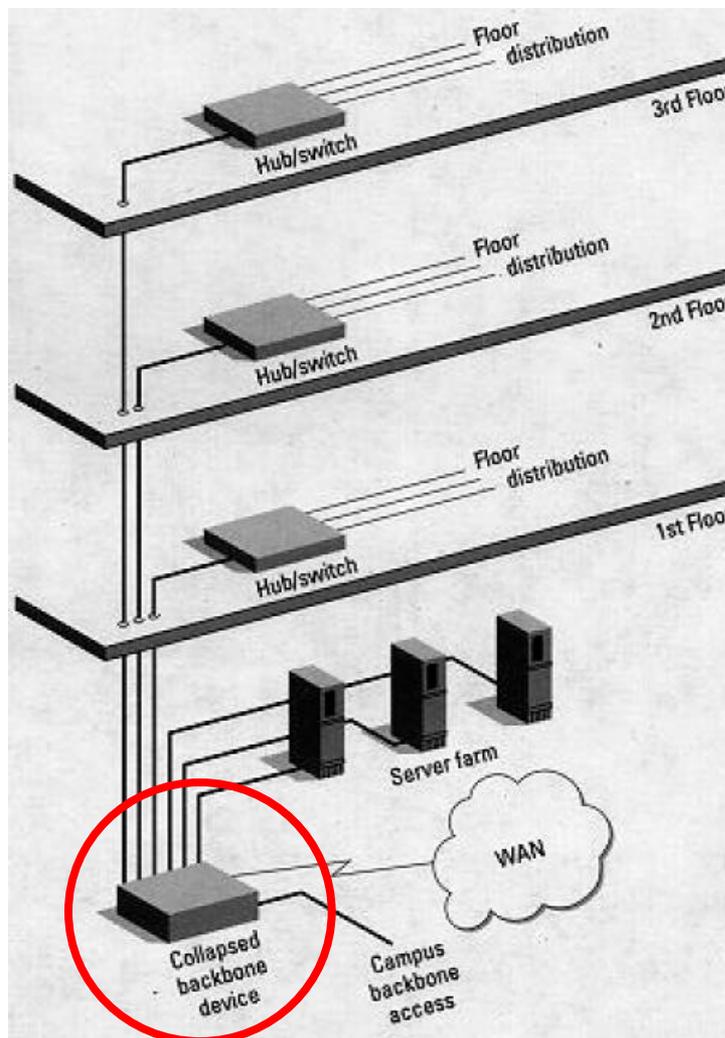
**“Router
inter-departamental”**

Arquitectura de redes para grupos de trabajo (5)

Router inter-departamental

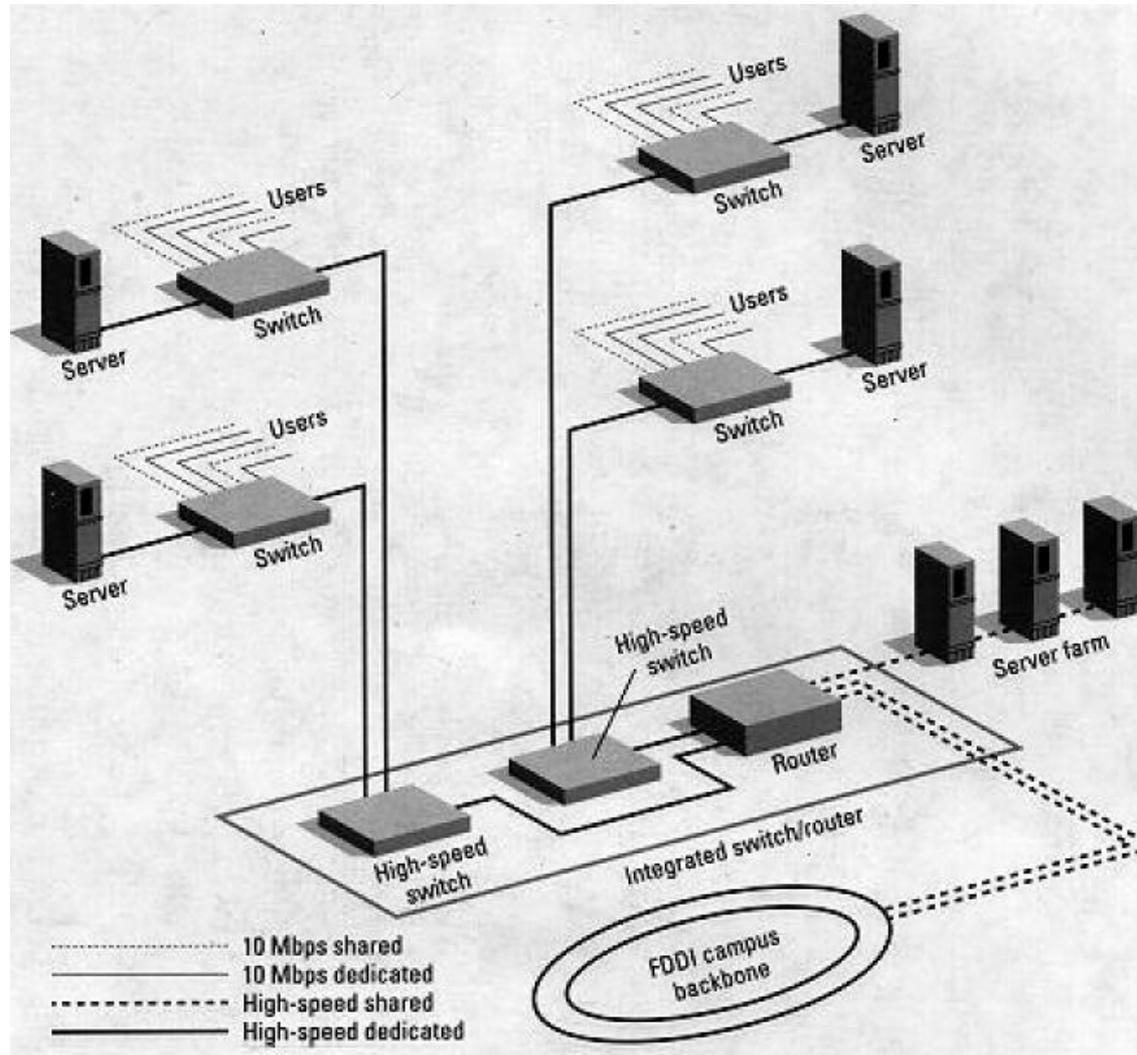
- Cada departamento conectado a una entrada del Router.
- Cada departamento queda **aislado** del “ruido” de los **Broadcast** de los departamentos vecinos por el router que **rutea selectivamente** los paquetes.
- Los Switch se encargaran del **re-envío de los paquetes** a los servidores locales.

Arquitectura de redes para grupos de trabajo (6)

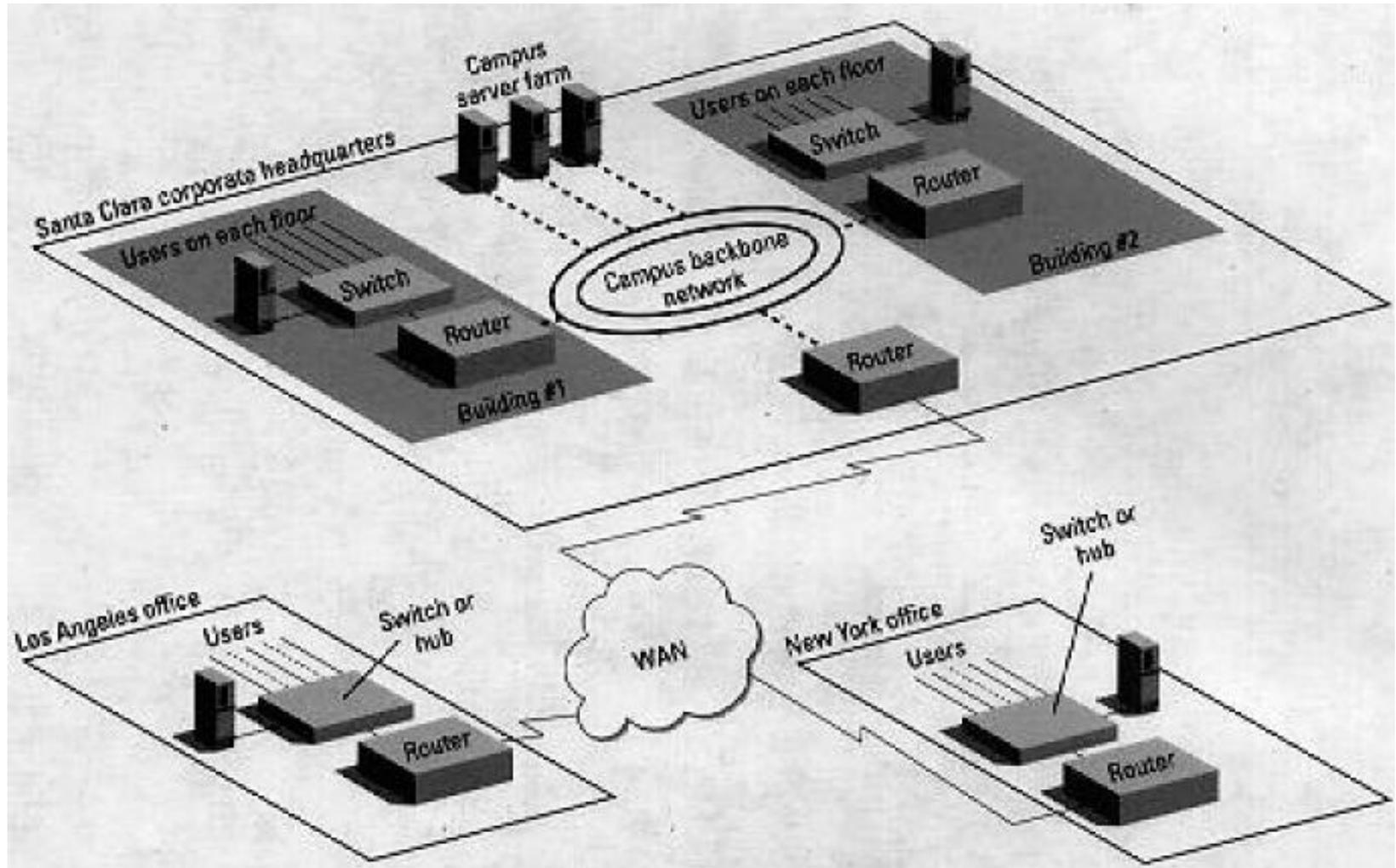


Antigua arquitectura de
BACKBONE Multi-departmental
→ **Colapsada**

Arquitectura de redes para grupos de trabajo (6)



Arquitectura de redes para grupos de trabajo (7)



En resumen (Router vs Switch)

- Router y Switch son **complementarios**.

Router ofrece	Switch ofrece
Control de broadcast	Costo bajo
Redundancia	Rapidez
Control de protocolos	Segmentación
Acceso a WAN	Fácil instalación

Gateway

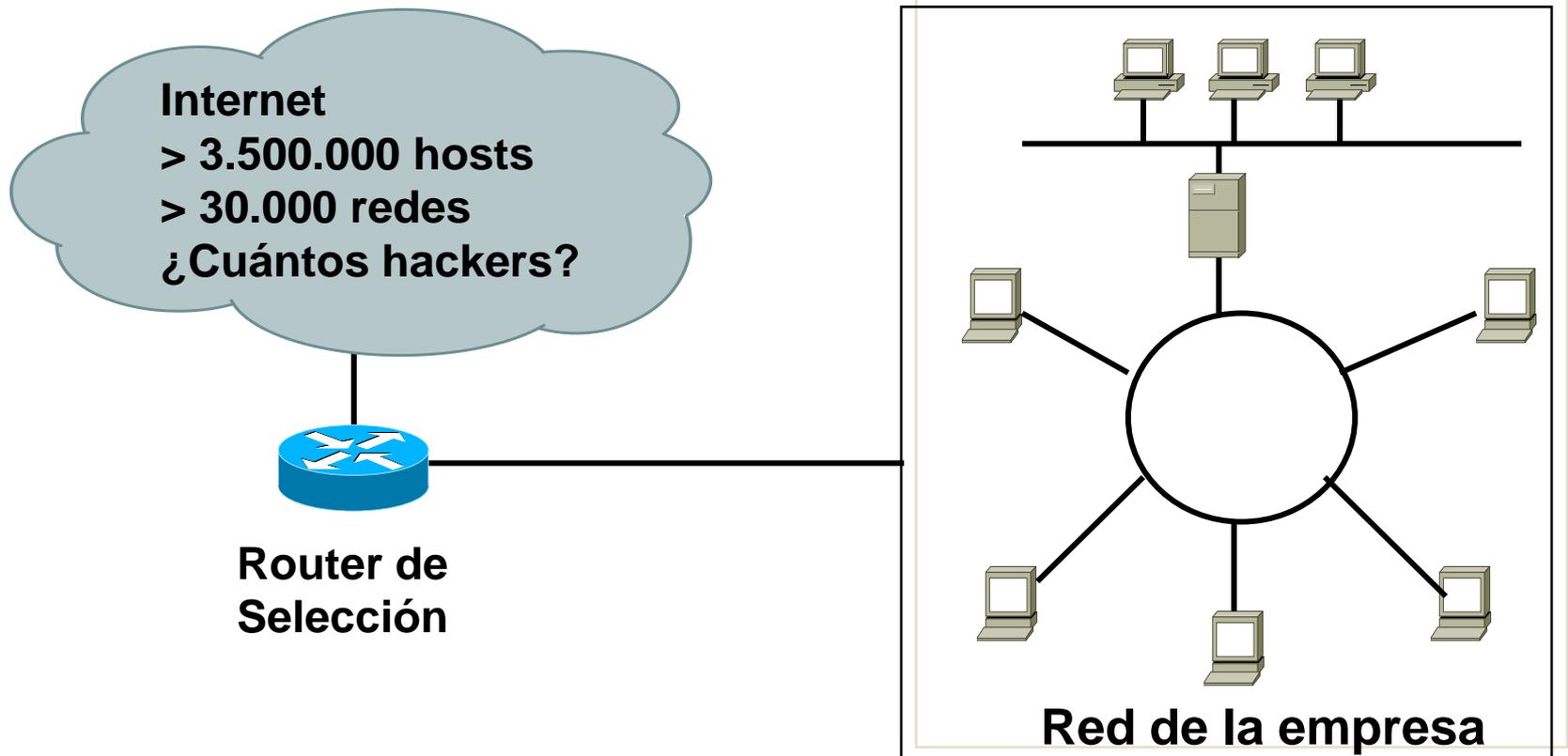
- Dispositivo que conecta 2 redes con protocolos distintos.
- Trabajan en todos los niveles del modelo OSI.
- En general los **Router** tienen capacidades de ser Gateway.
- En internet es muy usado para conectar **LAN** con **WLAN** → **Gateway es el router de salida.**

Servidor

- Es un programa que **responde** desde la capa de aplicación a los **requerimientos** que llegan por la red.
- Debe estar en algún **host**.
- Utiliza un **protocolo propio** sobre las capas del modelo OSI.
- Los **clientes** del servidor conocen el protocolo e **interactúan** con el servidor.
- Ejemplos:
 - Servidor de Bases de datos
 - Servidor de Aplicaciones
 - Servidor de correos

Routers de Selección (1)

- Zonas de riesgo



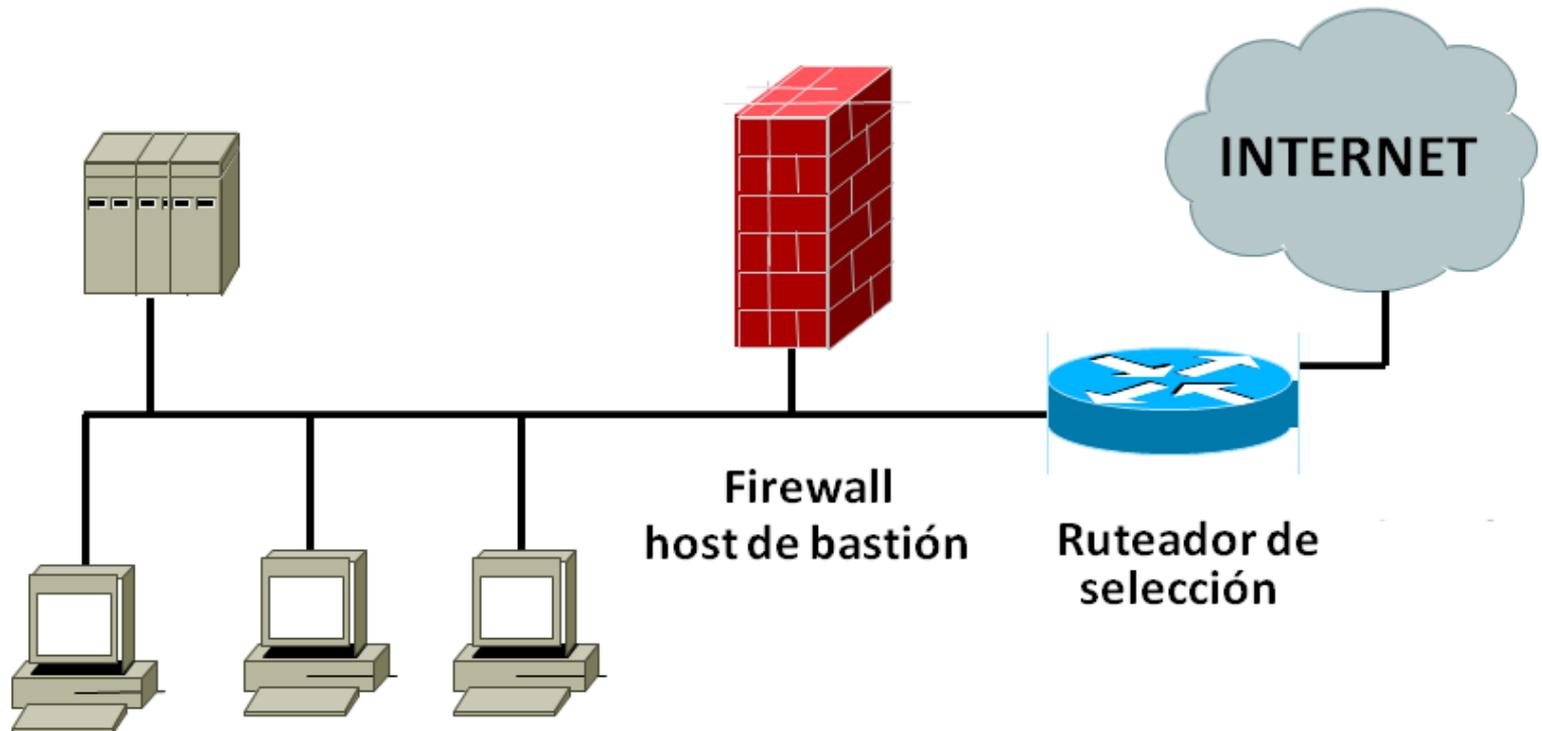
Routers de Selección (2)

- Se trata de routers que pueden **filtrar los paquetes** en base a criterios de selección.
- Básicamente estos criterios son :
 - El **tipo** de **protocolo** (TCP, UDP, ... y puerto).
 - Dirección **IP de origen**.
 - **Servicio** al cual se desea acceder.
- Este tipo de routers, **controla** qué **servicios** están **permitidos** en un segmento de red.

Firewall

- Se instala entre la conexión de la red interna y su enlace a Internet.
- **Todo** el tráfico que viene o sale a Internet, **pasa por el firewall**.
- Su configuración, debe estar en concordancia con la **política de seguridad** definida.
- Hoy en día, una red conectada a Internet **sin un firewall es altamente riesgosa**.
- Qué **no** puede hacer:
 - Proteger contra personas maliciosas internas a la red.
 - Proteger las conexiones que no pasan por él.
 - Proteger contra amenazas desconocidas.

Firewall (2)



Firewall y Routers de Selección

Routers de selección

- Los filtros de paquetes, son una forma eficaz de control del tráfico que entra y sale de la red.
- Trabaja sobre **capas TCP/IP**.
- El número de reglas puede ser muy limitado. Se requieren reglas adicionales y con un grado mayor de cobertura

Firewall

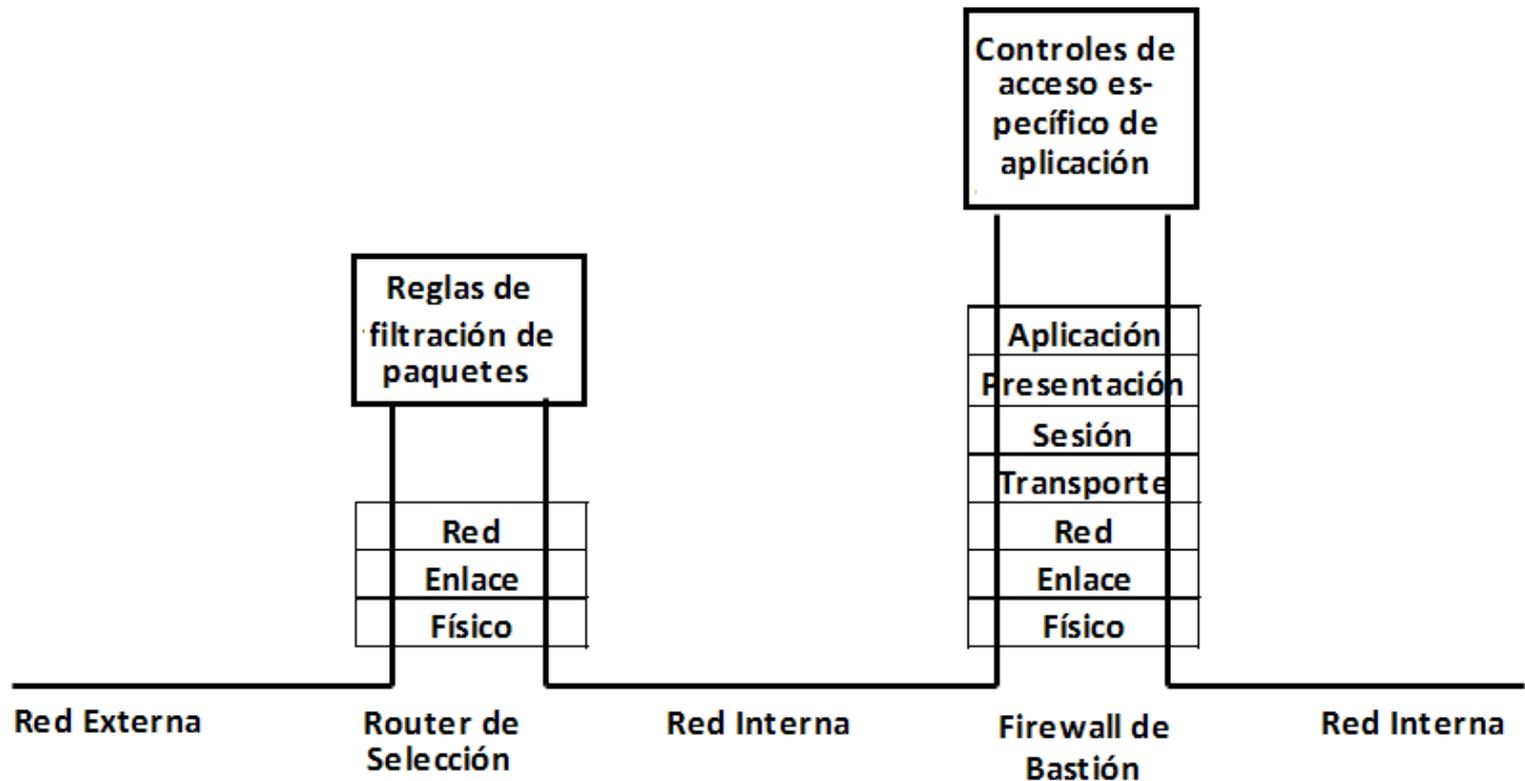
- Instrumento principal para ejecutar la política de seguridad de la organización.
- Trabaja por **sobre todas las capas** del modelo OSI.
- Son **complementarios** a los filtros de paquetes

Firewall y Routers de Selección (2)

- El router de selección, es la **primera línea de defensa**.
- Debe estar configurado para **enviarle** los **paquetes** ya **filtrados** al firewall.
- Se rechaza todo tráfico que no pase las reglas impuestas en el router.
- El *firewall de bastión*, utiliza funciones de **nivel de aplicación**.
- Firewall permite **aceptar** o **rechazar** las solicitudes que vienen de la red externa **no filtradas previamente**.

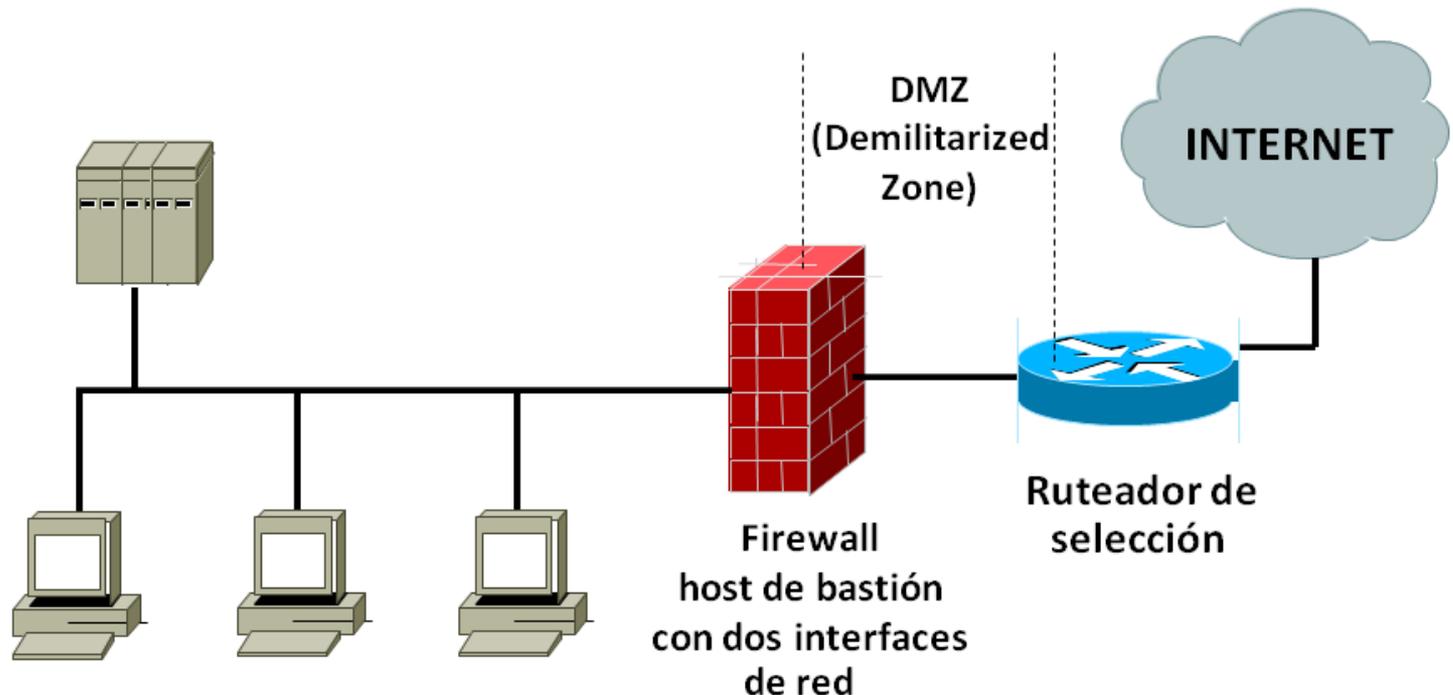
Firewall y Routers de Selección (3)

- Al nivel de capas del modelo OSI

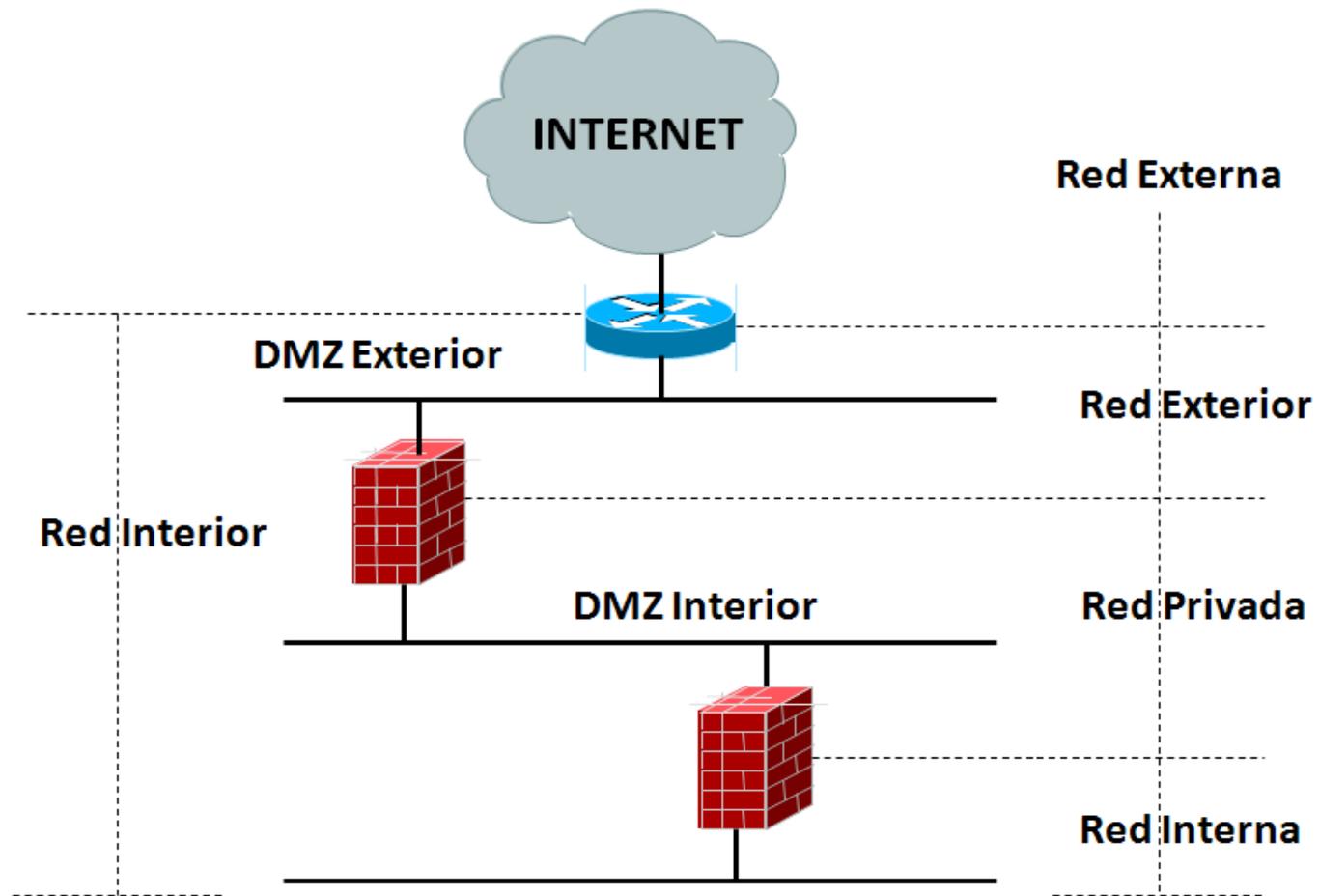


Zona Desmilitarizada

- Se define una “**Zona Desmilitarizada**” (**DMZ** Demilitarized Zone), una parte de la red interna en la cual no hay computadores.



Zona Desmilitarizada (2)



DMZ Interior y Exterior

- Dejan **traza** de posibles violaciones de **seguridad**.
- Permite conectar computadores en dos zonas, con **distintos grados de protección**.
- En la **red privada**, pueden estar los **hosts menos delicados**. (e.g. Web server)
- La configuración se **puede** usar para **impedir ataques internos**.
- Se pueden colocar algunos hosts en la red exterior, si se desea dar algunos servicios.

IDS: Intrusion-detection system

- Se utilizan **sensores** en los diferentes elementos de la red que **generan eventos** de riesgos de seguridad.
- **Servidores** que almacenan en una base de datos la **información recolectada** por los sensores y el tráfico de red que pasa por ellos.
- Monitor que **analiza la base de datos** y entrega reportes de seguridad de la red y gatilla alarmas en caso de detectar riesgos.

NAT: Network Address Translation

- Actúa en la **capa de red y transporte** modelo OSI
- **Re-escibe** el encabezado del datagrama en la parte de **IP** de **origen-destino**.
- Mantiene un registro de **qué flujo** que salió **fue re-escrito**.
- Con esto puede re-escribir los paquetes **entrantes** para **direccionarlos al lugar interno correcto**.
- **Desventajas:**
 - No puede iniciarse la comunicación desde afuera.
 - No hay comunicación simétrica *end to end*.
- **Ventajas:**
 - Aumenta la disponibilidad de direcciones IP.

DHCP: Dynamic Host Configuration Protocol

- Sistema **Cliente-Servidor**
- Entrega los parámetros de **configuración** a máquinas que se **conectan por vez primera a la red**.
- Comienza con un broadcast y el servidor establece una conexión UDP (User Datagram Protocol) con quien haya efectuado el llamado.
- Asigna un **IP dinámico** y otros parámetros de configuración.
- El servidor debe estar ubicado en el **dominio de broadcast** del computador afectado, típicamente el **primer switch**.
- **Utilidad:** configuración dinámica de las estaciones de trabajo, lo que da robustez a la configuración de la red.
- **En contra:** es un punto de falla y de baja seguridad.

IN3501 - Tecnologías de Información y
Comunicaciones para la Gestión

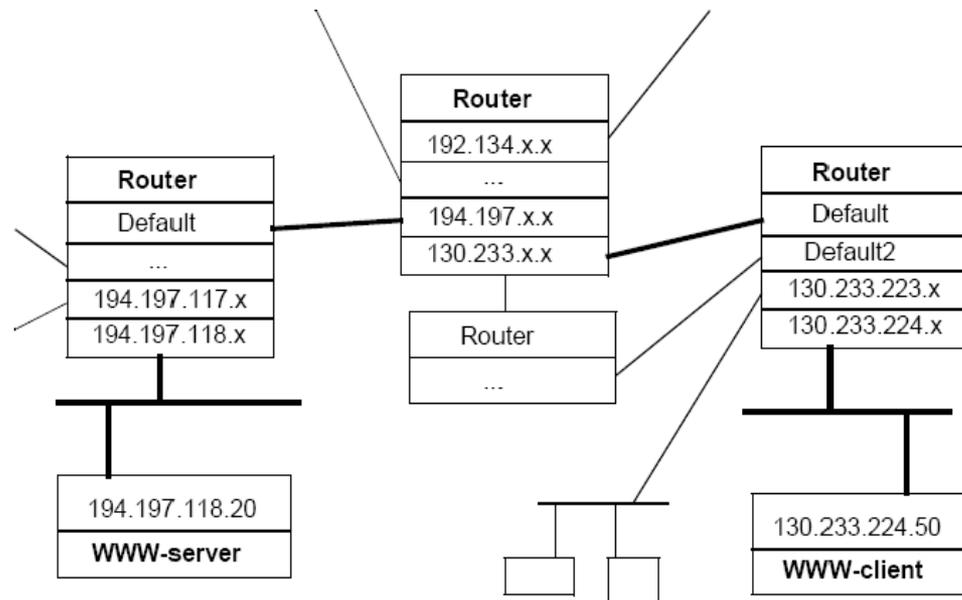
ENRUTAMIENTO DE REDES

PROFESORES

Juan D. Velásquez
Gastón L'Huillier
Víctor Rebolledo Lorca

Ruteando

- **LANs** están interconectadas por **routers**
- Cada **router** tiene una tabla que dice a **qué dirección de Internet puede llegar y bajo qué conexión.**
- Los routers *Backbone* **actualizan esta información** automáticamente.



Ruteo Básico

- Es el proceso a través del cual **dos computadores se comunican**, privilegiando la mejor trayectoria de una red TCP/IP.
- En el ruteo asumiremos que el problema de enviar el paquete dentro de la misma red, está resuelto.
- El paquete **viaja entre redes** hasta llegar a la red de destino:
 - El computador inicial necesita saber cómo y cuando comunicarse con un ruteador.
 - El ruteador necesita saber cómo determinar la mejor trayectoria para llegar a una red remota.
 - El ruteador de la red destino, necesita saber como comunicarse con el computador final.

Tablas de rutas

- Cada **router** y cada **host** mantienen una **tabla de rutas**
- Un **router** está conectado directamente a una o más redes.
- El algoritmo de ruteo que toda implementación IP debe realizar, se basa en una **tabla de rutas**

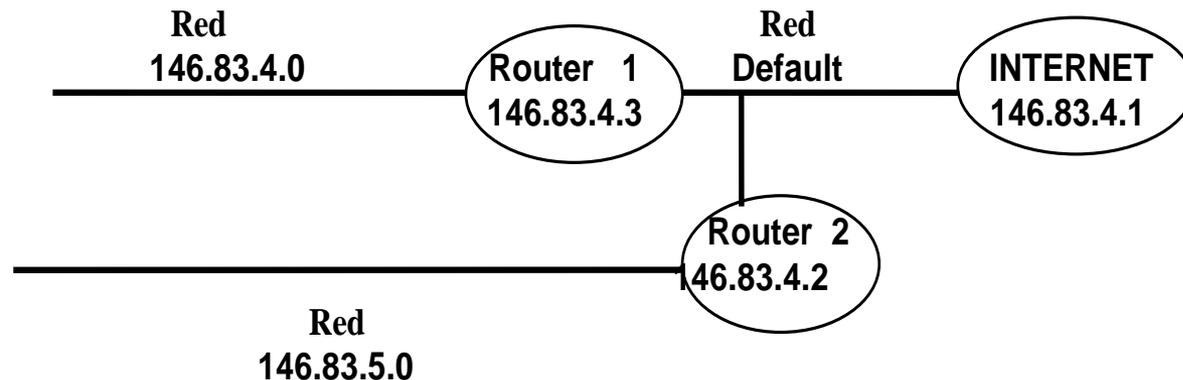
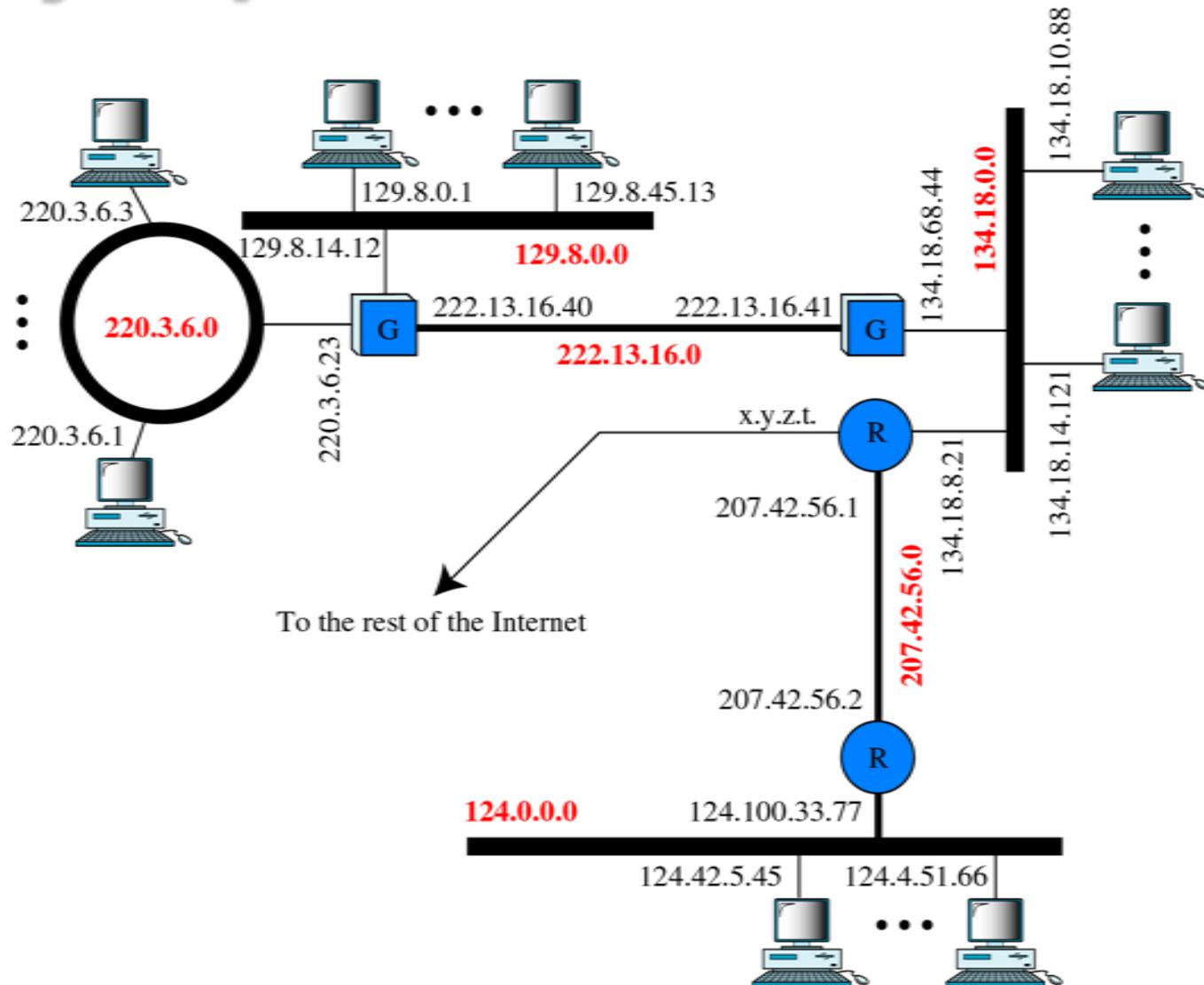


Tabla para router 1

<i>Net</i>	<i>Gateway</i>	<i>Type</i>
146.83.4.0	146.83.4.3	DIR
146.83.5.0	146.83.4.2	GW
Default	146.83.4.1	GW

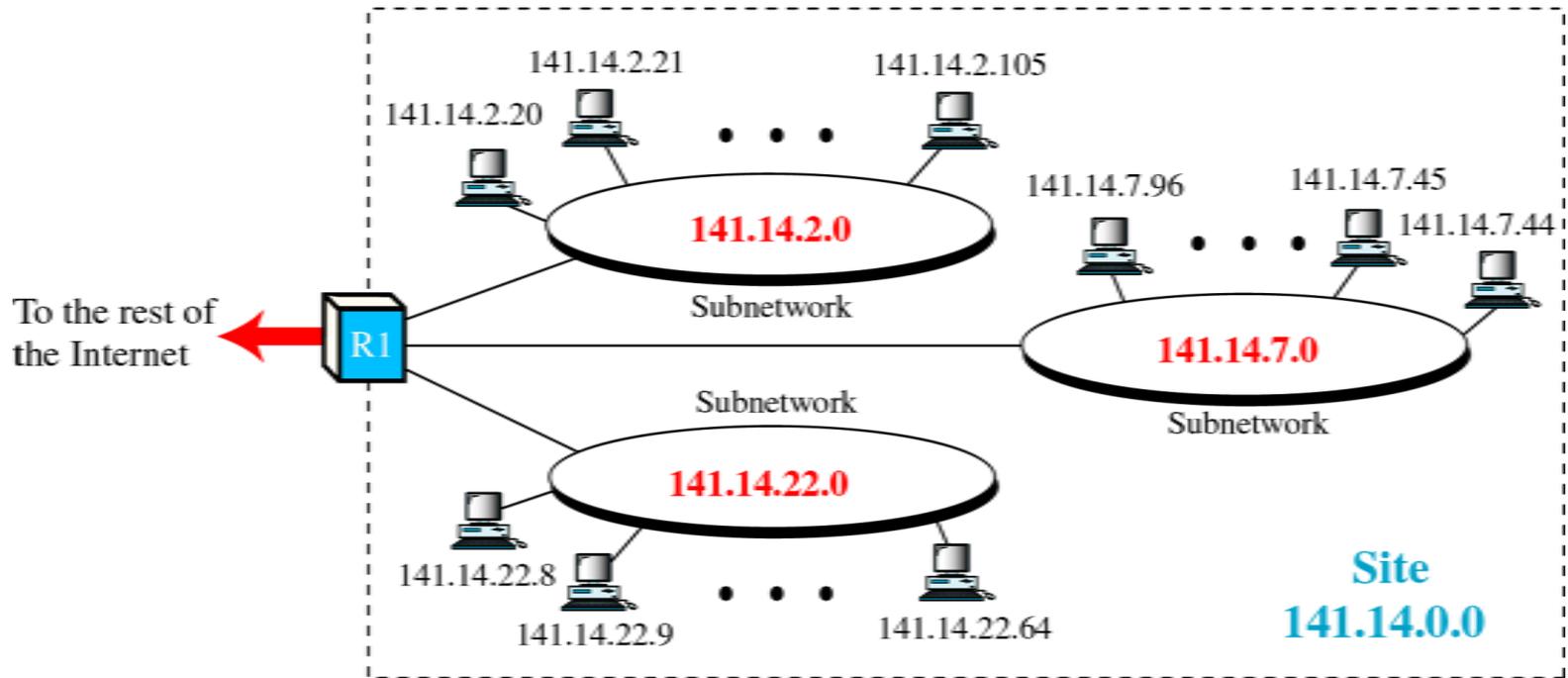
Ejemplo



Ruteo Interno

- Una vez que el datagrama llega al **router de destino**, hay que revisar a que computador en la red se envía el paquete.
- El envío es en base al **tipo de red**.
 - Por ejemplo, si la red es una Ethernet, se encapsula el paquete IP en uno Ethernet.
- El **router** y los computadores internos **mantienen una tabla dinámica** con la dirección IP y la Ethernet.
- Cuando un computador no identifica un par IP/Ethernet, envía un mensaje a la red preguntando cual de los computadores posee la IP.

Ruteo Interno (2)



IN3501 - Tecnologías de Información y
Comunicaciones para la Gestión

TRANSMITIENDO UN ARCHIVO

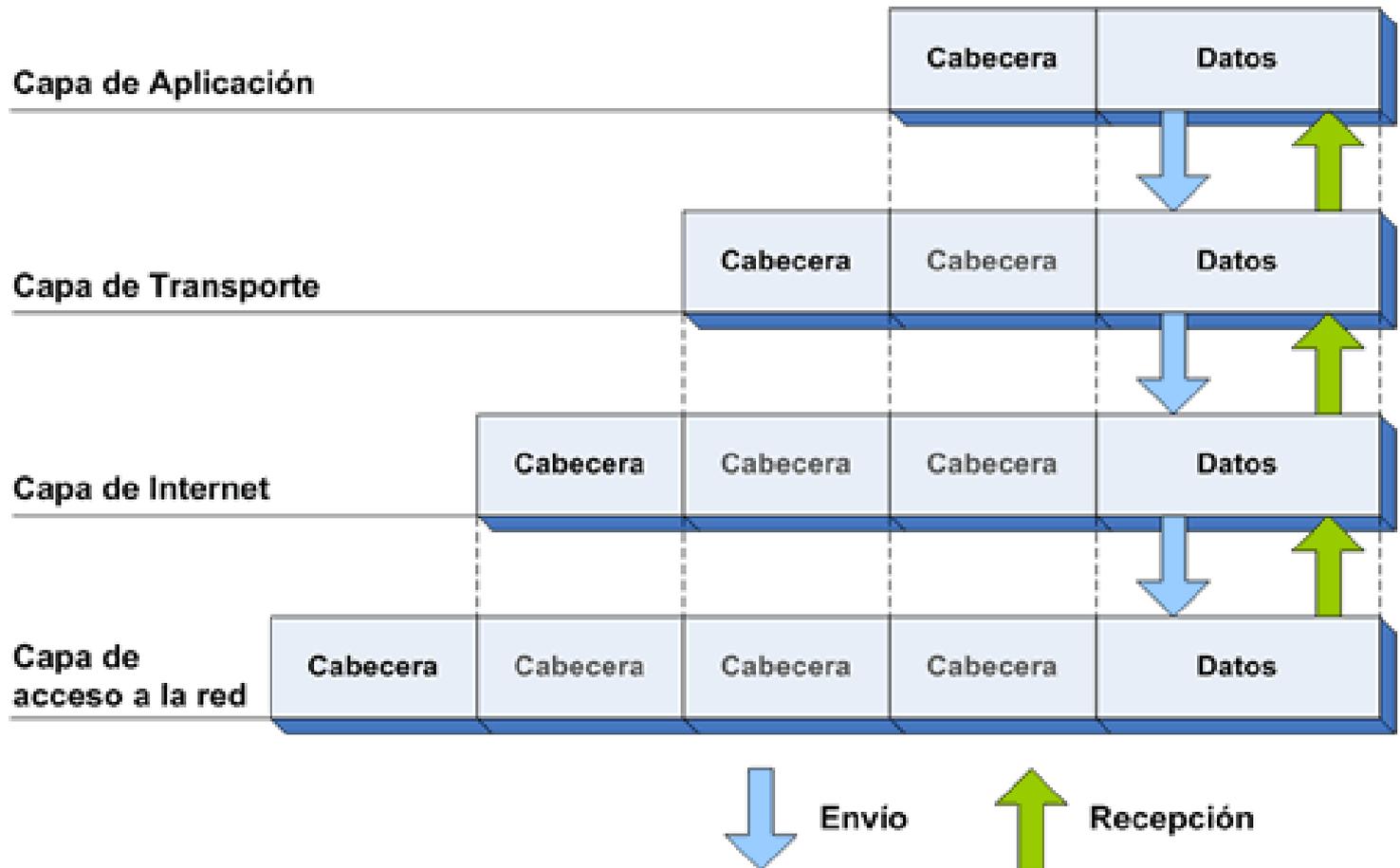
PROFESORES

Juan D. Velásquez
Gastón L'Huillier
Víctor Rebolledo Lorca

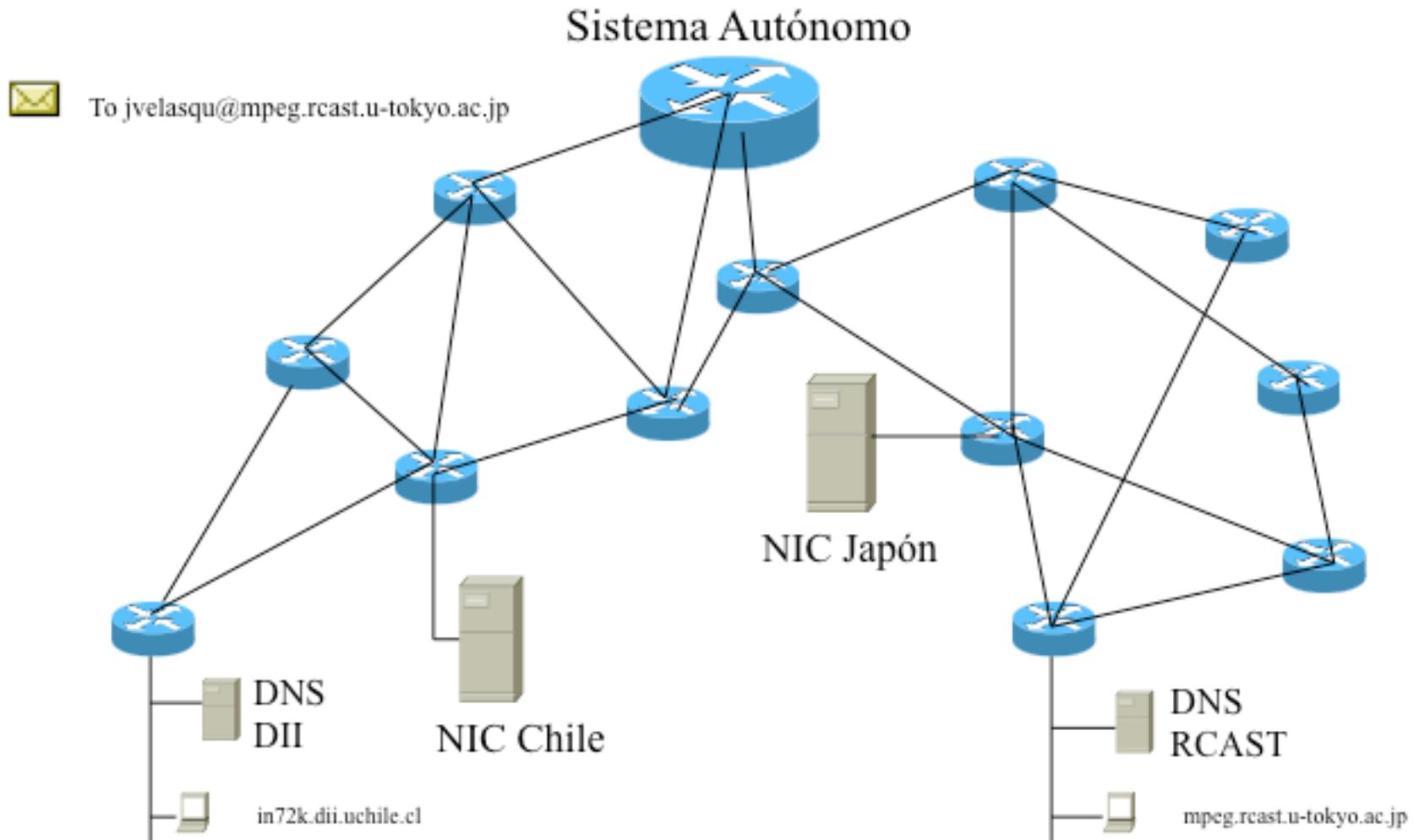
Enviando un archivo por e-mail

- Queremos enviar un archivo “**attachado**” en un e-mail a un computador en Tokio.
- Una vez que se aplica el “**send**”, el archivo el e-mail es “**paquetizado**” y enviado al servidor de correos de nuestra red.
- Cada trozo del archivo debe ser encapsulado y transformado en un datagrama.

Encapsulando los datos



TCP/IP en acción: ejemplo

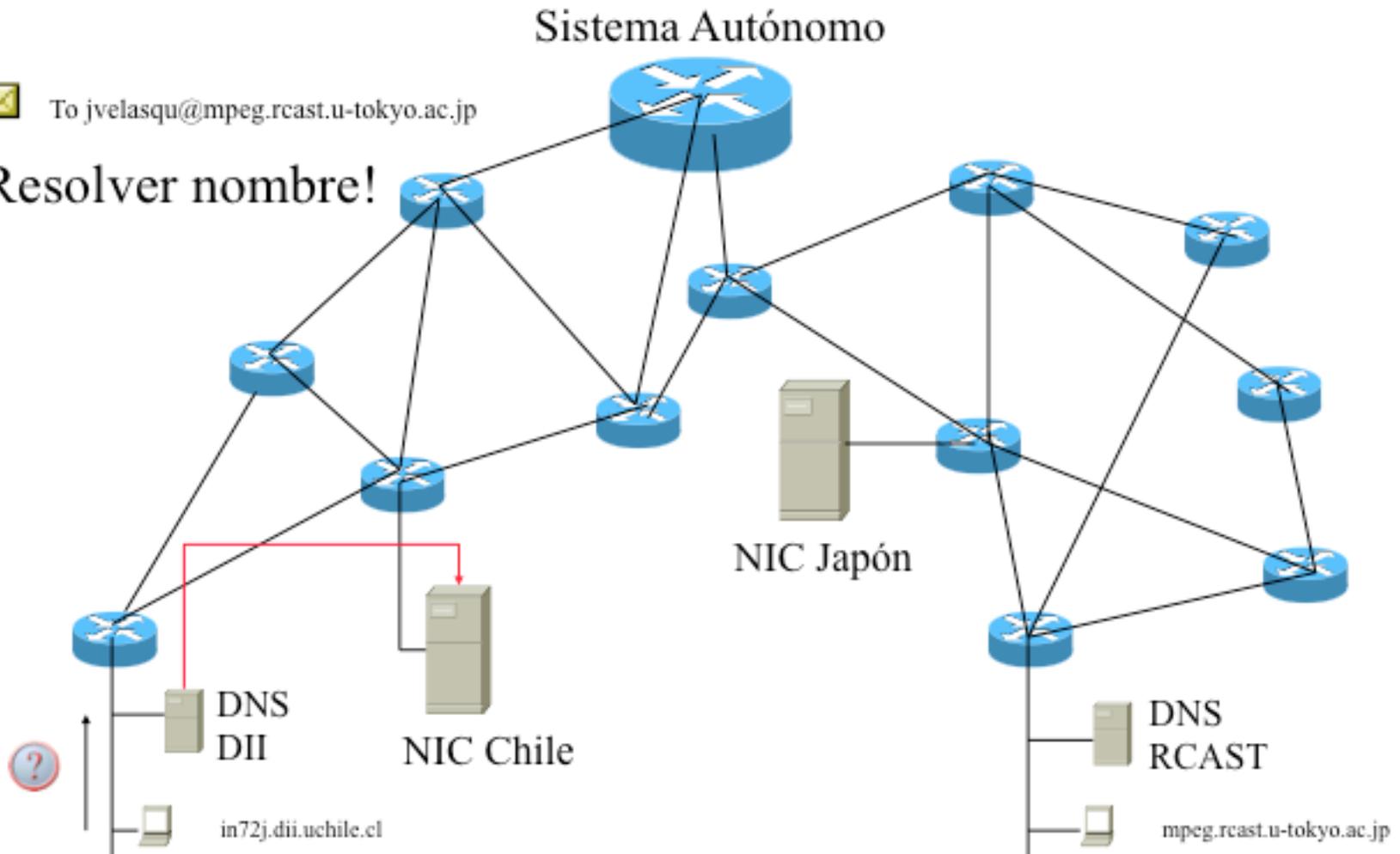


TCP/IP en acción: ejemplo



To jvelasqu@mpeg.rcast.u-tokyo.ac.jp

Resolver nombre!

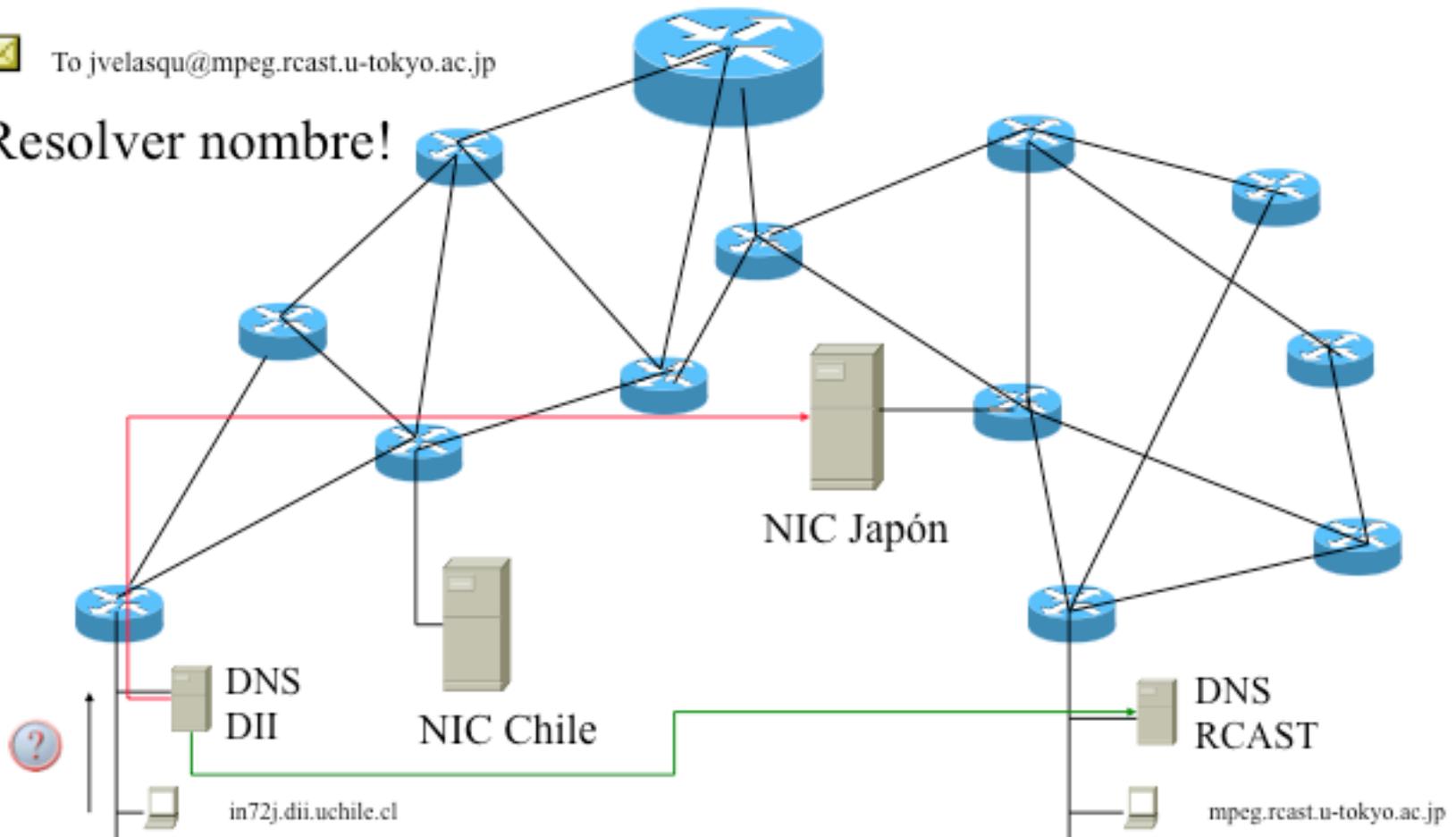


TCP/IP en acción: ejemplo



To jvelasqu@mpeg.rcast.u-tokyo.ac.jp

Resolver nombre!



TCP/IP en acción: ejemplo

