

Redes de computadoras

Introducción: segunda parte

Las diapositivas están basadas en en libro:

“Redes de Computadoras – Un enfoque descendente”
de James F. Kurose & Keith W. Ross

Introducción - ¿Qué es Internet?

Temario

¿Qué es internet?

Descripción de los componentes esenciales

Descripción de los servicios

¿Qué es un protocolo?

La frontera de la red

El núcleo de la red

Retardos, pérdidas y tasa de transferencia

Capas de protocolos y sus modelos de servicio

Ataques a las redes

Historia de Internet y las redes de computadoras

Medio físico

bit

- Se propaga entre las entidades que transmiten/reciben.

Enlace físico:

- Medio entre el transmisor y el receptor

Medio “guiado”

- Señales se propagan en medios sólidos

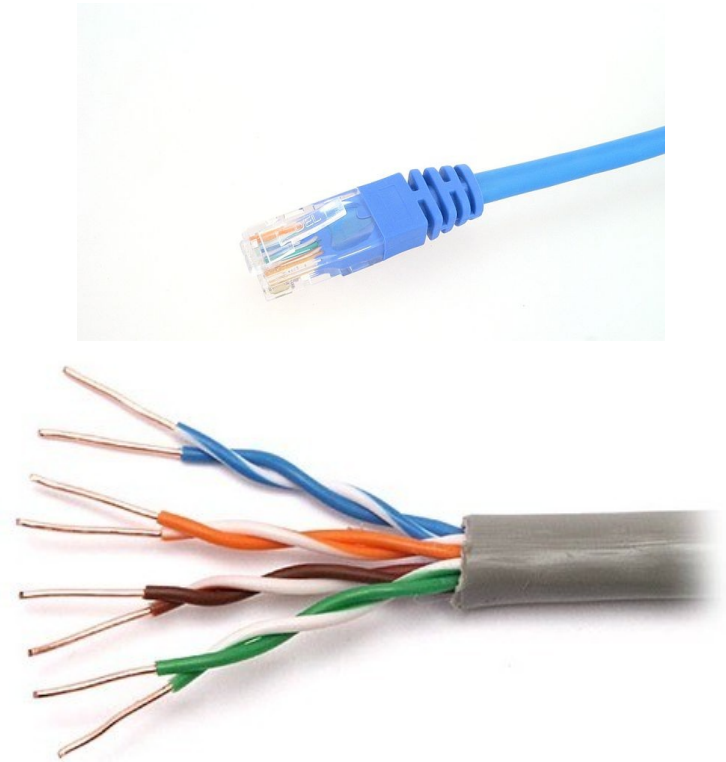
Medio “no guiado”

- Señales se propagan mediante antenas

Medio físico

Twisted Pair (Par de cobre trenzado)

- Cable compuesto por ocho hilos de cobre aislados entre sí, trenzados de dos en dos y entrelazados.
- Unshielded twisted pair (UTP) par trenzado sin blindaje
- Shielded twisted pair (STP) par trenzado blindado
- Existen varias categorías, las más comunmente utilizadas son Cat 3 (teléfono central), Cat 5 y Cat 6 para redes de área local (LAN)
- velocidades entre 10 Mbps y 100 Mbps.



Medio físico

Cable coaxial

- Par de conductores de cobre concéntricos
- Bidireccional
- Banda base:
 - Canal único de cable
 - “legacy” Ethernet
- Broadband:
 - Múltiples canales de cable
 - HFC (Hybrid Fiber Coax)

para cables de 1km, por ejemplo, es factible obtener velocidades de datos de hasta 10Mbps



Medio físico

Fibra óptica

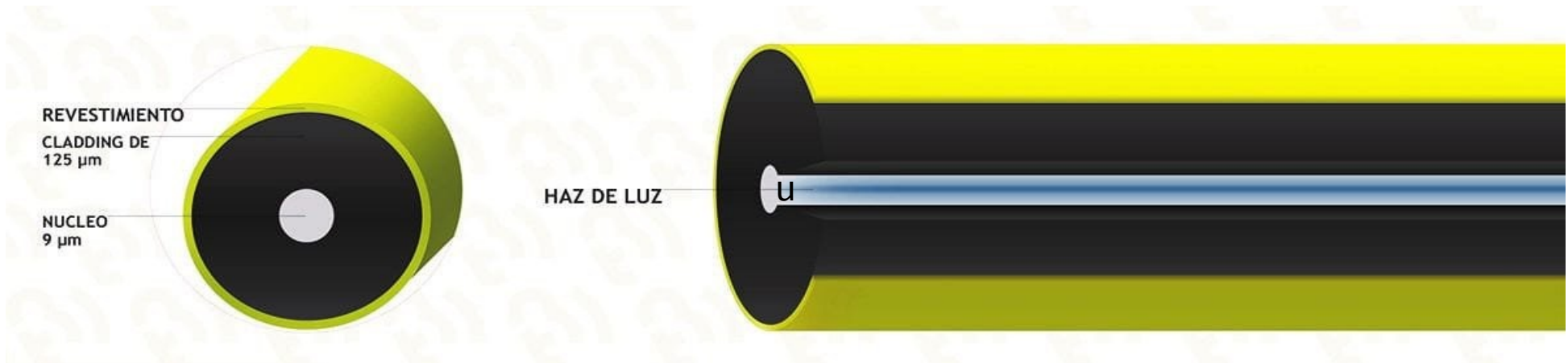
- Fibra de vidrio que transporta pulsos de luz
cada pulso es un bit
- Alta velocidad:
Transmisión punto a punto 10-100 Gbps
- Baja tasa de error
inmune a ruido electromagnético,
repetidores espaciados.
- 2Km multimodo
- 300Km monomodo



Medio físico

Fibra óptica monomodo

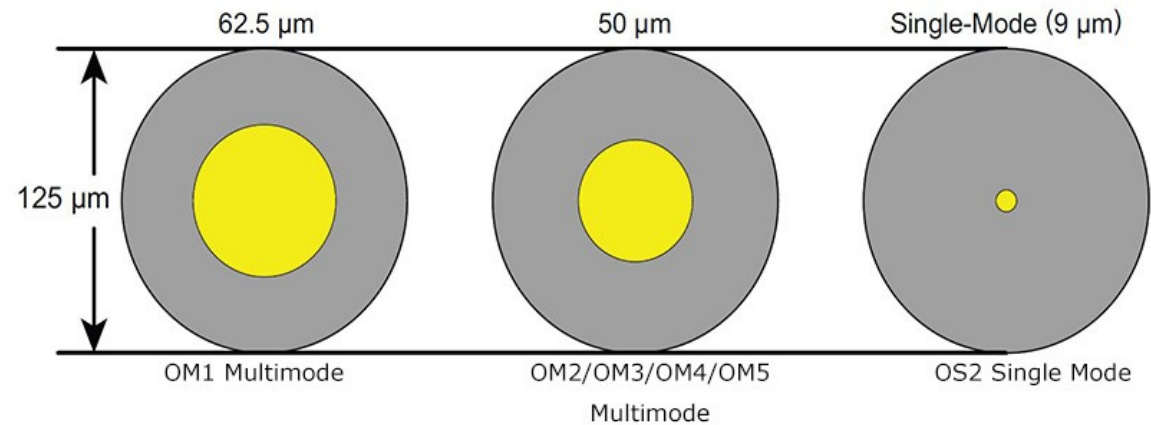
- Fibra de vidrio que transporta pulsos de luz
- Cable monomodo: La luz viaja sin rebotar - velocidad de transferencia más alta
- OS1 y OS2, no muy flexibles, adecuados para exteriores.- distancias de hasta 10Km
- 1 a 10Gb



Fibra óptica multimodo

- Mayor cantidad de haces de luz viajando al mismo tiempo
- Mayor ancho de banda
- Pierde calidad de señal en distancias largas

Optical Fiber Core Diameters



REVESTIMIENTO

CLADDING DE
125 μm

NUCLEO
50 μm

HAZ DE LUZ

Radio - Señal transportada en el espectro electromagnético

Efectos del entorno en la propagación

- reflexión
- obstrucción por objetos
- interferencia

Microonda terrestre: STM-1, STM-4 (155 Mbps / 622 Mbps)

LAN: Wifi (11Mbps, 54 Mbps)

Wide-Area: 3G celular ~ 1 Mbps

Satélite: desde Kbps a decenas de Mbps, retardo 270 msec
geoestacionarios ~36.000Km o baja altitud ~2.000Km (Low Earth Orbit)

El núcleo de la red

Conmutación de circuitos
Conmutación de paquetes
Estructura de la red

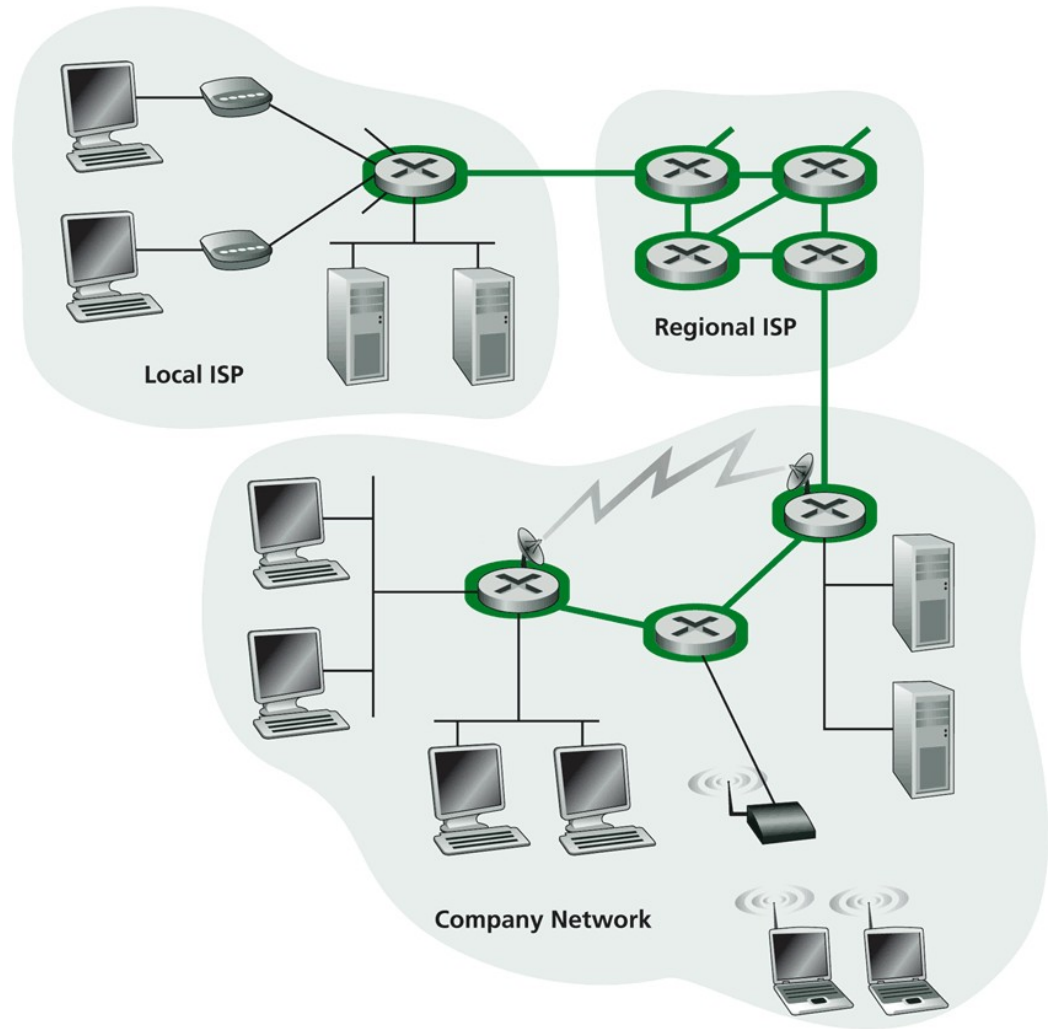


Figure 1.4 ♦ The network core

El núcleo de la red

Malla de routers interconectados

¿cómo se transfieren los datos a través de la red?

- Conmutación de circuitos:

Circuito dedicado para cada llamada: red telefónica.

- Conmutación de paquetes:

Los datos se envían en “trozos” a través de la red.

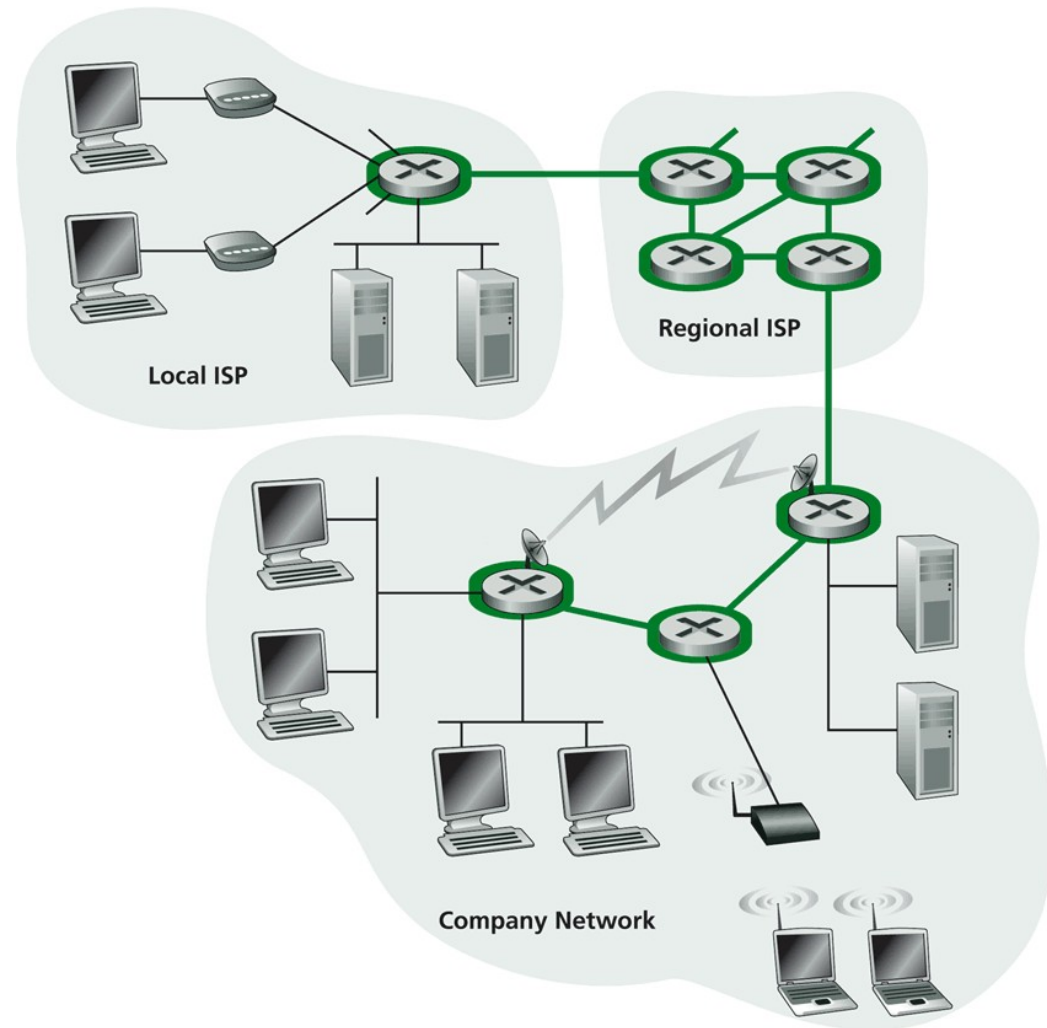


Figure 1.4 ♦ The network core

Núcleo de Red: Conmutación de circuitos

Reserva de recursos de extremo a extremo para cada “llamada”

- Ancho de banda capacidad de conmutación
- Recursos dedicados
- Parámetros de calidad garantizada
- Se requiere un procedimiento de establecimiento de llamada (señalización).

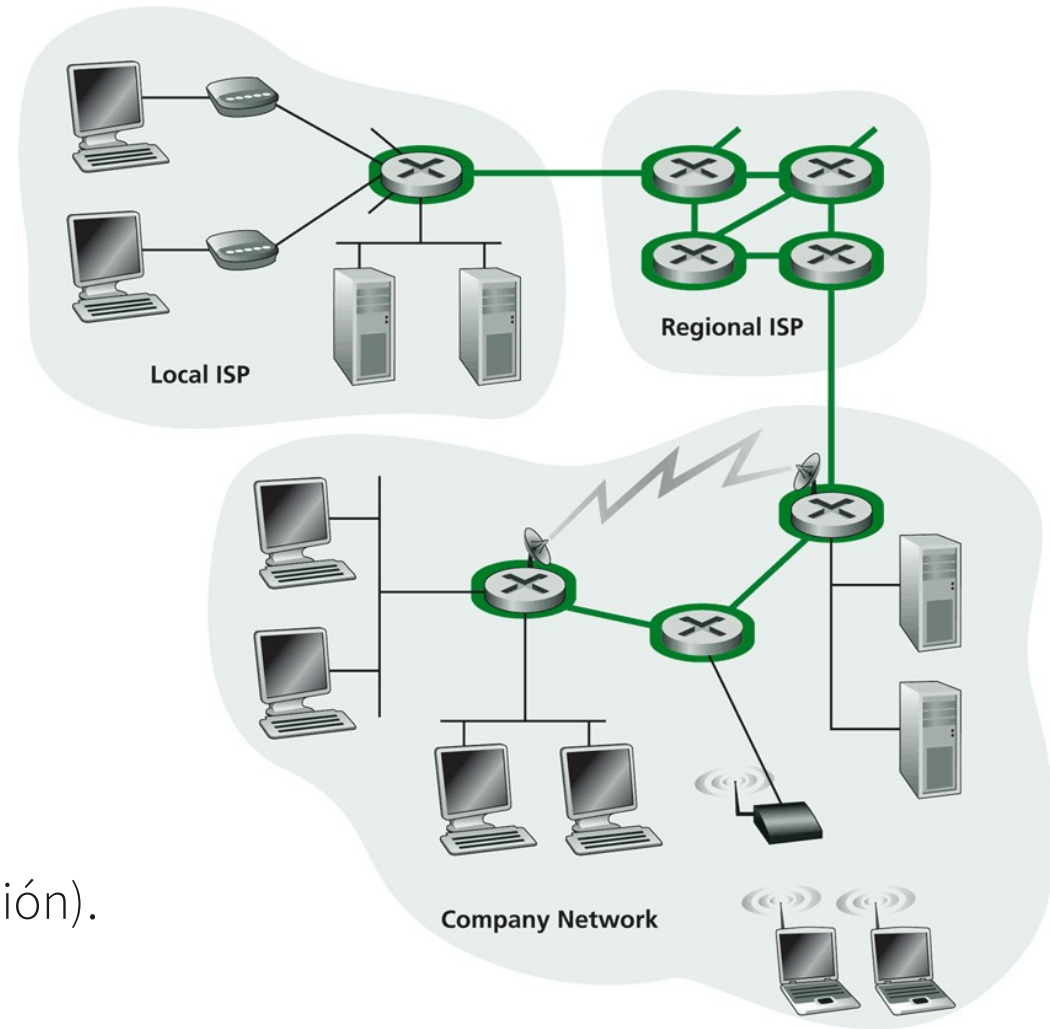


Figure 1.4 ♦ The network core

Núcleo de Red:

Conmutación de circuitos

Recursos de red (ancho de banda) divididos en secciones fijas

- “secciones” asignadas a llamadas
- no se comparten recursos, si no se usan se desperdician.

¿cómo se realiza la división de recursos?

- división en frecuencia
- división por tiempo

Núcleo de Red:

Conmutación de circuitos

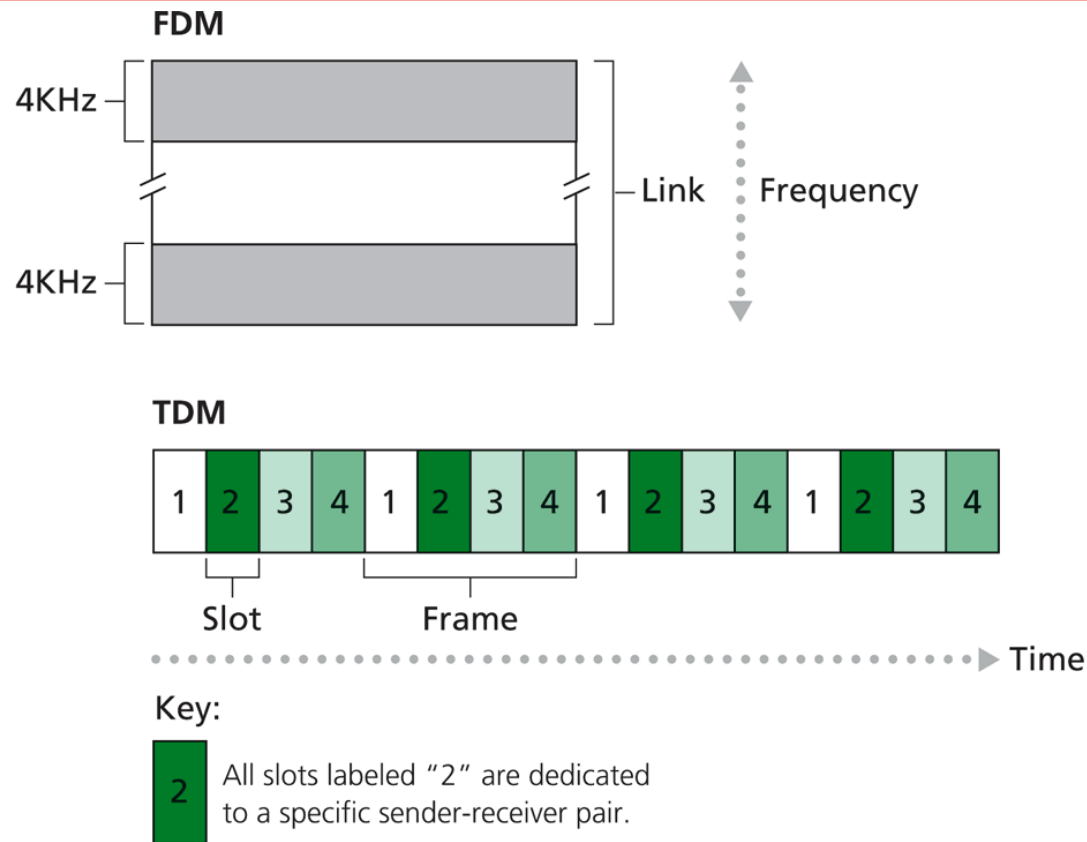


Figure 1.6 ♦ With FDM, each circuit continuously gets a fraction of the bandwidth. With TDM, each circuit gets all of the bandwidth periodically during brief intervals of time (that is, during slots).

Núcleo de Red:

Conmutación de paquetes

Flujo de datos dividido en paquetes

- Los paquetes de distintos usuarios comparten los recursos de red
- Cada paquete utiliza el ancho de banda disponible
- Los recursos se usan cuando se necesitan

Contención (disputa) de recursos:

- La demanda agregada de recursos puede exceder la disponibilidad
- Congestión: Paquetes deben esperar para usar los enlaces (colas, buffers)
- “store & forward”: los paquetes van avanzando de un salto (“hop”) a la vez.

Cada nodo recibe el paquete completo antes de re-enviarlo.

Núcleo de Red: Multiplexado Estadístico

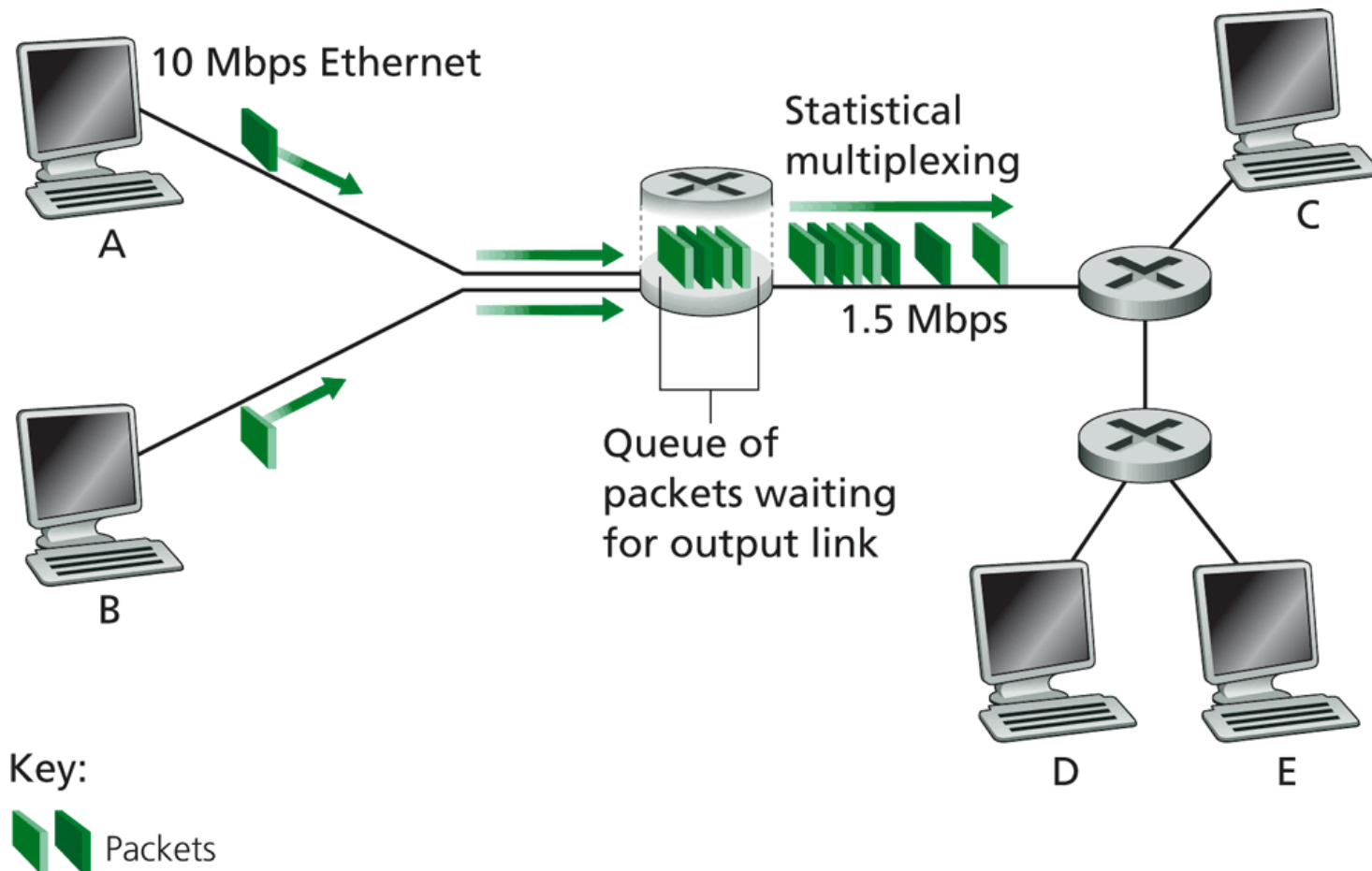


Figure 1.7 ♦ Packet switching

Conmutación de paquetes vs Conmutación de circuitos

La conmutación de paquetes permite que más usuarios utilicen la red

- Enlace de 1 Mb/s

Cada usuario:

- 100 kb/s cuando está “activo”
- activo 10% del tiempo

Conmutación de circuitos

- 10 usuarios

Conmutación de paquetes:

- Con 40 usuarios la probabilidad de que la cantidad de usuarios activos sea > 10 es menor que 0.001

Conmutación de paquetes vs Conmutación de circuitos

¿La conmutación de paquetes es la solución?

- bueno para transmisión de datos en ráfagas
 - Compartir recursos
 - Simple, no es necesario establecer llamadas
- Posible congestión: Retardos y pérdidas de paquetes
 - Se necesitan protocolos para asegurar la transferencia de datos y control de congestión

¿Cómo proveer un comportamiento similar a la conmutación de circuitos?

¿Garantías de ancho de banda y variación del retardo para aplicaciones de audio/video?

Estructura de Internet

Red de redes

- Estructura jerárquica
- En el núcleo: ISP tier-1
 - Ej: Sprint, AT&T, Cable and Wireless
- Cobertura nacional/Internacional
- “diálogo de iguales (peers)”

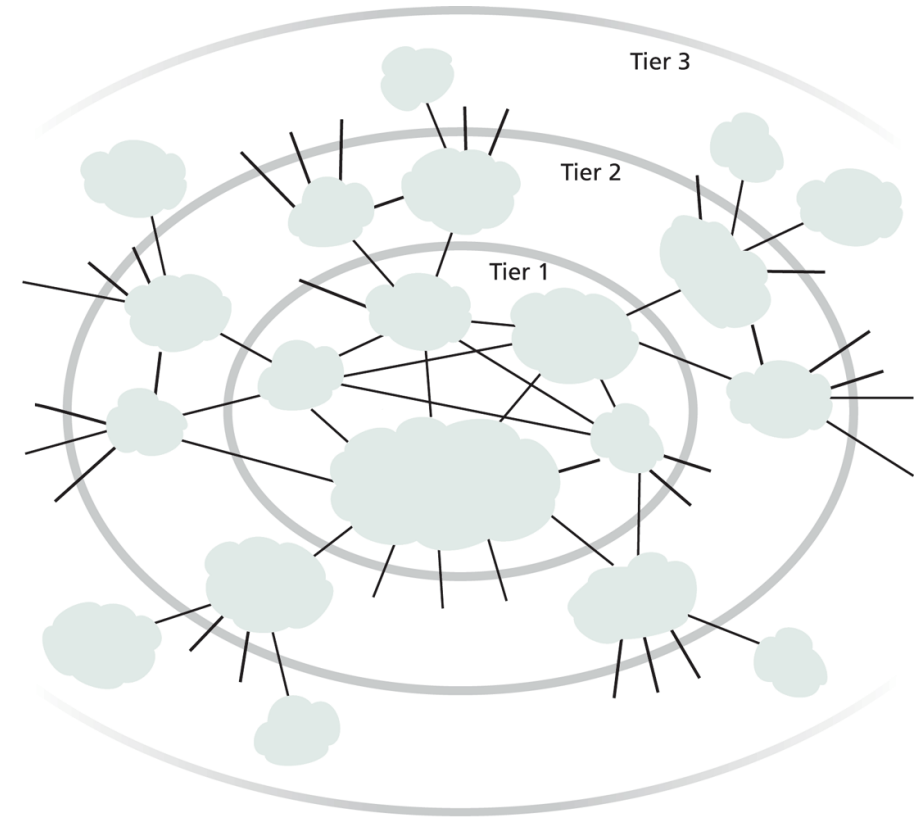


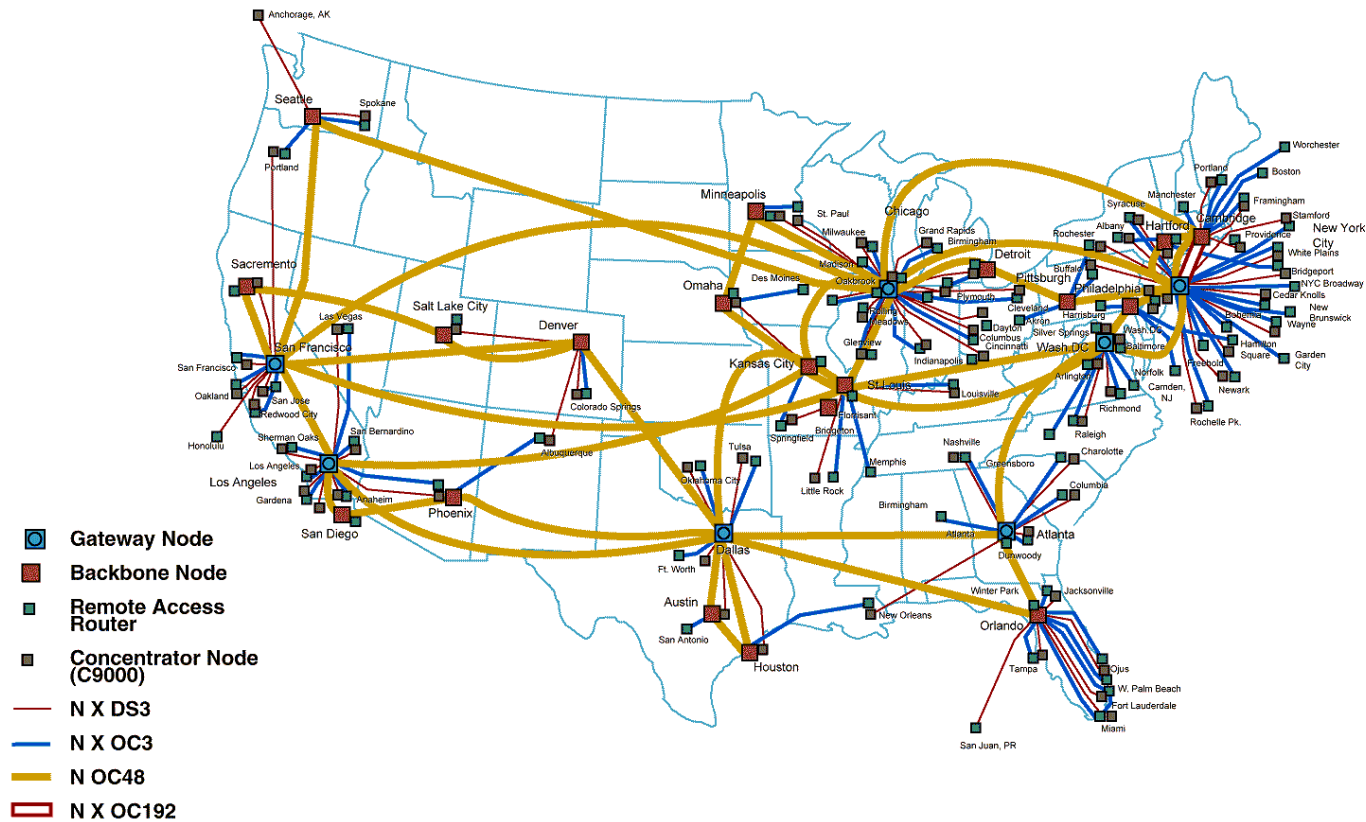
Figure 1.12 ♦ Interconnection of ISPs

Estructura de Internet

Red de redes



AT&T IP BACKBONE NETWORK 2Q2000



Note: map is not to scale.

Estructura de Internet

Red de redes

ISP Tier-2: más pequeños (regionales)

- Conectados a uno o más ISP's Tier-1, y posiblemente a otros ISP's Tier-2

Isp Tier 2

paga al Tier 1 por la conectividad al resto de Internet

El ISP Tier 2 es cliente del proveedor Tier 1.

El ISP Tier 2 también tiene conexiones privadas entre ellos.

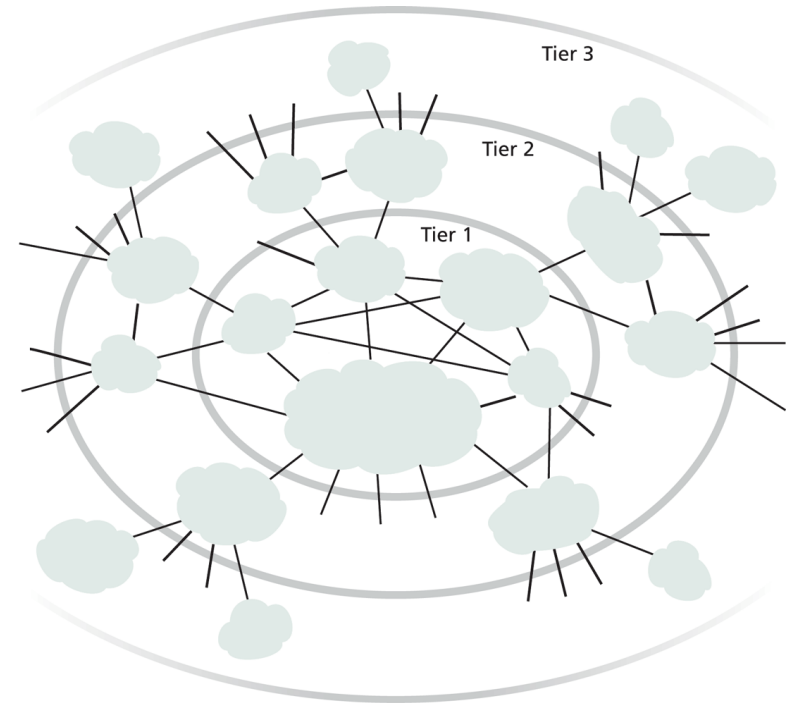
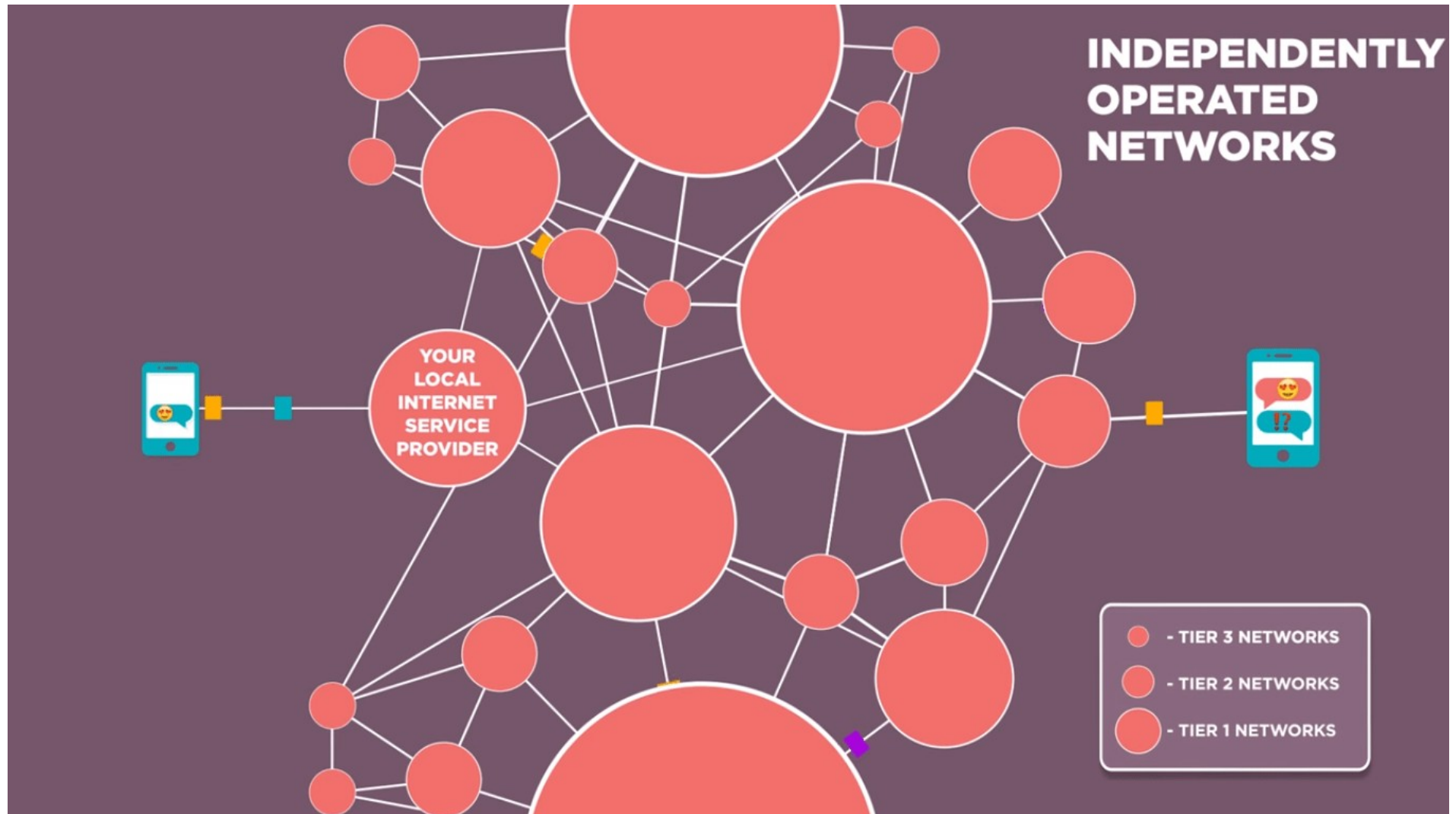


Figure 1.12 ♦ Interconnection of ISPs

Estructura de Internet

Red de redes



Estructura de Internet

Red de redes



Redes de paquetes: Retardo, pérdidas y throughput



Redes de paquetes: Retardo, pérdidas y throughput

¿cómo ocurren pérdidas y retardos?

- Los paquetes se encolan en los buffers de los routers si la tasa de arribos supera la capacidad del enlace la cola crece.

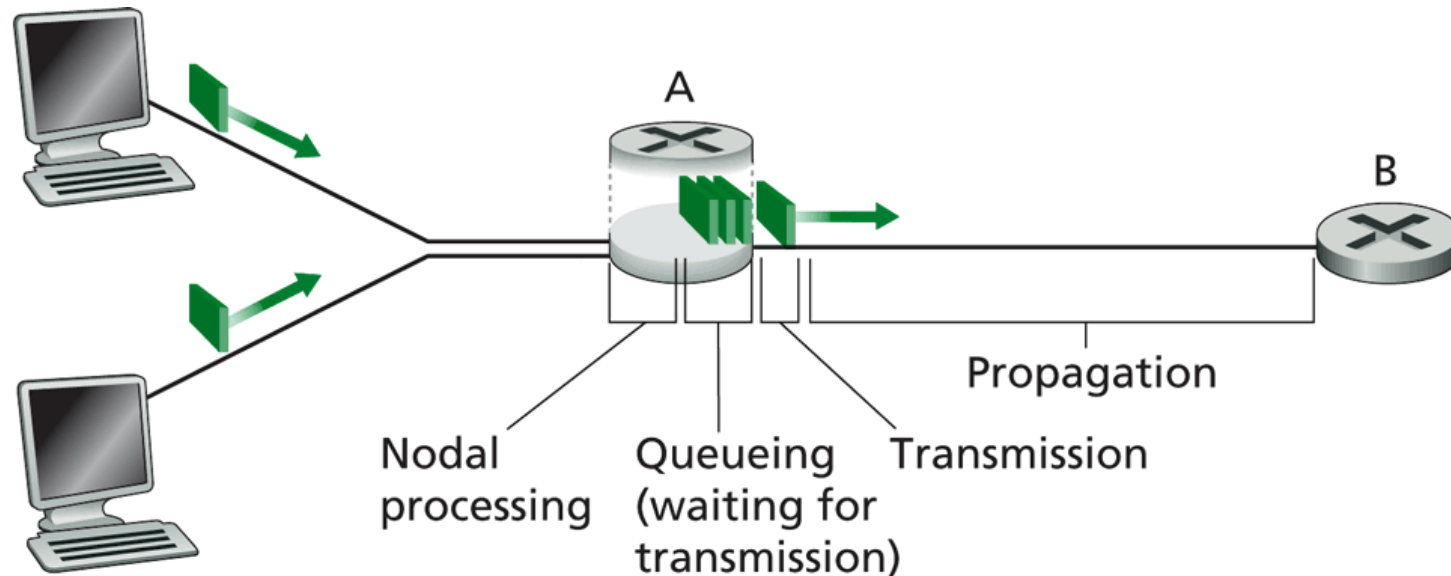


Figure 1.13 ♦ The nodal delay at router A

Redes de paquetes: Las fuentes del retardo

1- Procesamiento en el nodo

- Chequeo de paridad (CRC, verificación de redundancia cíclica)
- Determinar el enlace de salida (enrutamiento)

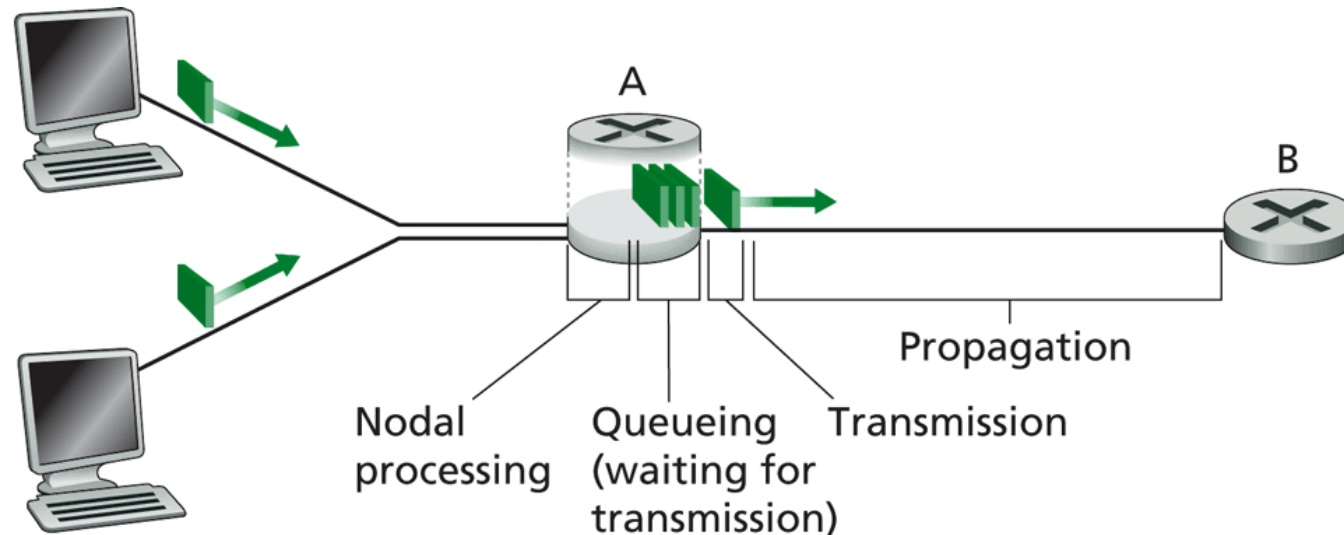


Figure 1.13 ♦ The nodal delay at router A

Redes de paquetes: Las fuentes del retardo

2- Encolamiento

- Espera en colas del enlace de salida para la transmisión
- Depende del nivel de congestión del router

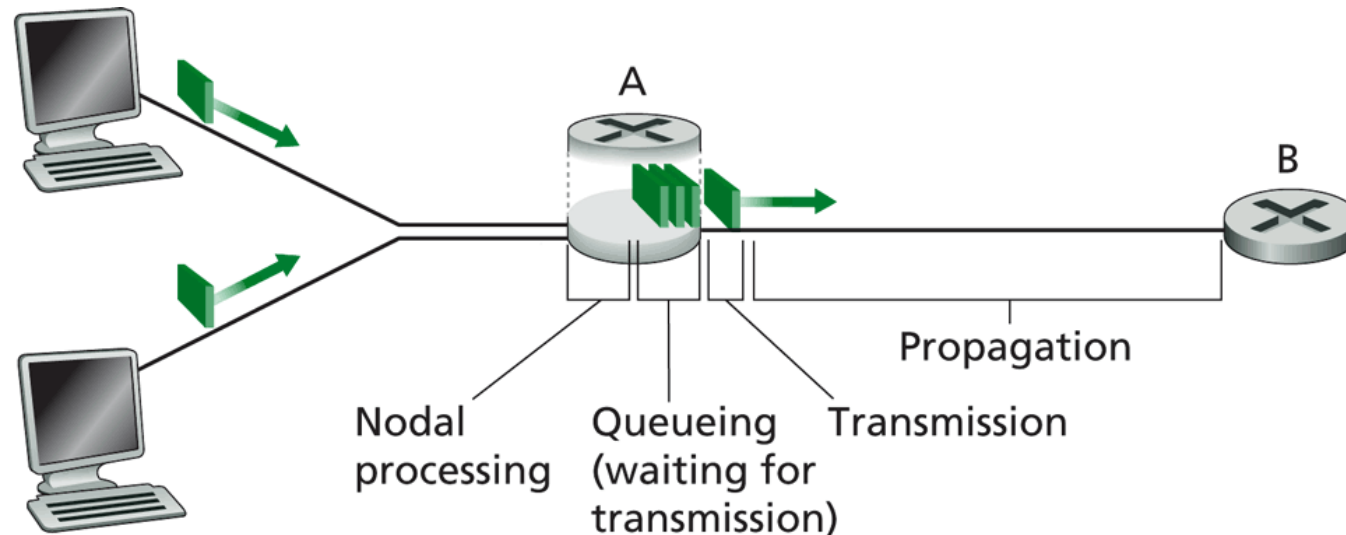


Figure 1.13 ♦ The nodal delay at router A

Redes de paquetes: Las fuentes del retardo

3- Retardo de transmisión

- R = ancho de banda del enlace (bits/s) L = Longitud del paquete (bits)

$$\text{Tiempo de envío} = L/R$$

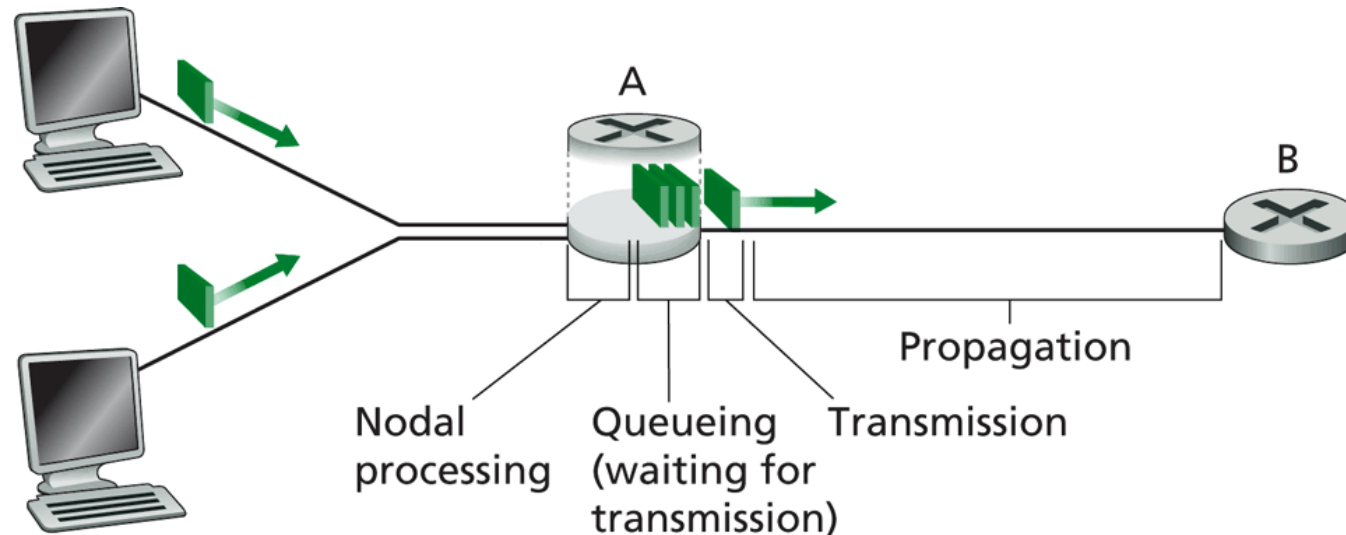


Figure 1.13 ♦ The nodal delay at router A

Redes de paquetes: Las fuentes del retardo

4- Retardo de propagación

- d = longitud del enlace físico s = velocidad de propagación en el medio

Tiempo de propagación = d/s

(propagación en el cobre $\sim 2 \times 10^8$ m/s)

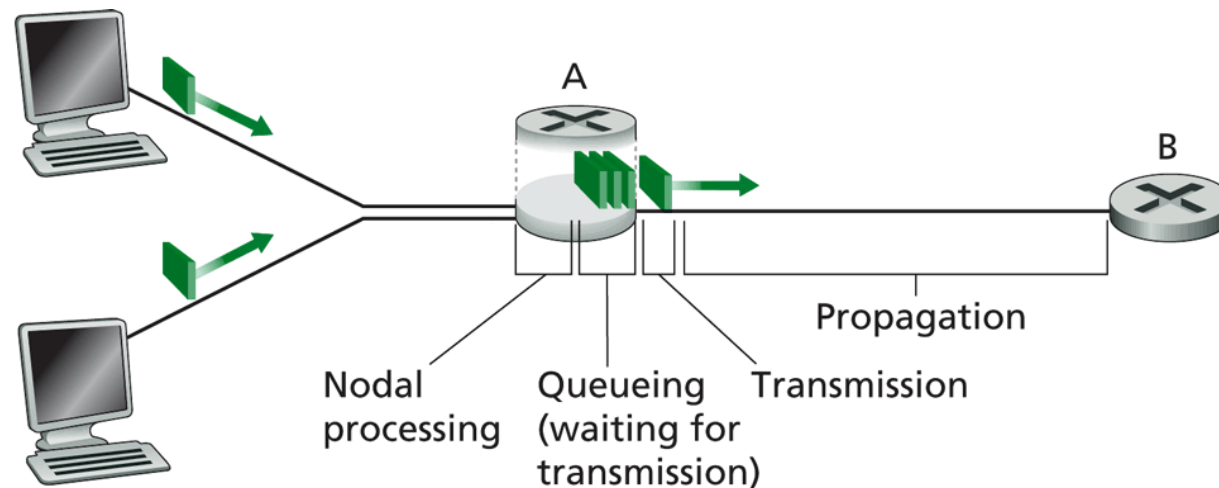


Figure 1.13 ♦ The nodal delay at router A

Retardo en el nodo

$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{cola}} + d_{\text{trans}} + d_{\text{prop}}$$

d_{proc} = retardo de procesamiento

- en el rango de los microsegundos o menos

d_{cola} = retardo de cola

- depende de la congestión

d_{trans} = retardo de transmisión

- L/R significativo en enlaces de baja velocidad

d_{prop} = retardo de propagación

- desde pocos a miles de microsegundos

Retardo de cola

R = ancho de banda del enlace (b/s)

L = Longitud del paquete (bits)

a = promedio de arribos de paquetes/s

Intensidad del tráfico = $\lambda a / R$

- $\lambda a / R \sim 0$ poco retardo
- $\lambda a / R \rightarrow 1$ aumenta el retardo
- $\lambda a / R \sim 1$ más trabajo de llegada que de servicio en el nodo, retardo infinito.

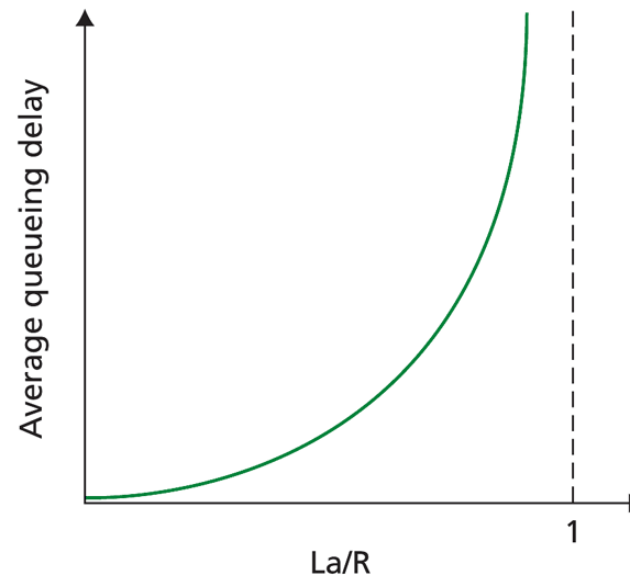


Figure 1.14 ♦ Dependence of average queuing delay on traffic intensity

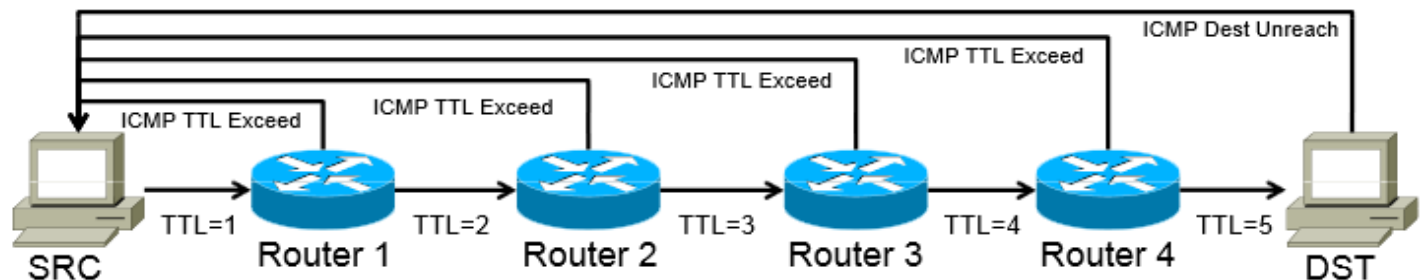
Retardos “reales” y rutas de Internet

¿Cómo se puede medir?

tracert / traceroute

Provee medida del retardo a cada router en el camino de origen al destino a través de Internet para cada nodo.

- Se envían 3 paquetes que llegan al router n del camino al destino.
- El router n devuelve los paquetes al remitente.
- Se mide el intervalo entre la transmisión y la respuesta: “round-trip time”



Retardos “reales” y rutas de Internet

Traceroute

```
C:\WINDOWS\system32\cmd.exe

Tracing route to dilemak.com [212.1.208.1]
over a maximum of 30 hops:

  1    6 ms    4 ms    4 ms  192.168.1.1 [192.168.1.1]
  2    9 ms   10 ms   13 ms  tia2bras3.antel.net.uy [200.40.78.198]
  3   10 ms   10 ms   11 ms  ibb2agu4-3-0-0.antel.net.uy [200.40.78.50]
  4    *      *      *      Request timed out.
  5    *      *      *      Request timed out.
  6    *      *      *      Request timed out.
  7  239 ms  201 ms  201 ms  te0-0-0-8.ccr21.mia03.atlas.cogentco.com [38.104.95.245]
  8  187 ms  201 ms  201 ms  be3401.ccr22.mia01.atlas.cogentco.com [154.54.47.29]
  9  215 ms  201 ms  201 ms  be3483.ccr42.atl01.atlas.cogentco.com [154.54.28.49]
 10  189 ms  161 ms  242 ms  be2848.ccr41.atl04.atlas.cogentco.com [154.54.6.118]
 11  180 ms  258 ms  201 ms  38.122.46.70
 12  285 ms  304 ms  303 ms  bbr01atlga-tge-0-1-0-8.atln.ga.charter.com [96.34.0.132]
 13  301 ms  303 ms  303 ms  bbr01gnvlsc-bue-800.gnvl.sc.charter.com [96.34.0.134]
 14  202 ms  202 ms  184 ms  crr02gnvlsc-bue-1.gnvl.sc.charter.com [96.34.2.55]
 15  291 ms  303 ms  201 ms  dtr01gnvlsc-bue-101.gnvl.sc.charter.com [96.34.66.251]
 16  256 ms  243 ms  305 ms  esr01gnvlsc-tge-0-0-0-0.gnvl.sc.charter.com [96.34.64.29]
 17  295 ms  201 ms  201 ms  68-191-7-206.static.gnvl.sc.charter.com [68.191.7.206]
 18  207 ms  201 ms  202 ms  74.112.175.39
 19  245 ms  304 ms  304 ms  74.112.174.251
 20  298 ms  203 ms  201 ms  74.112.175.17
 21  306 ms  304 ms  236 ms  ashv1.main-hosting.com [208.69.231.10]
 22  234 ms  304 ms  303 ms  srv208-1.hosting24.com [212.1.208.1]

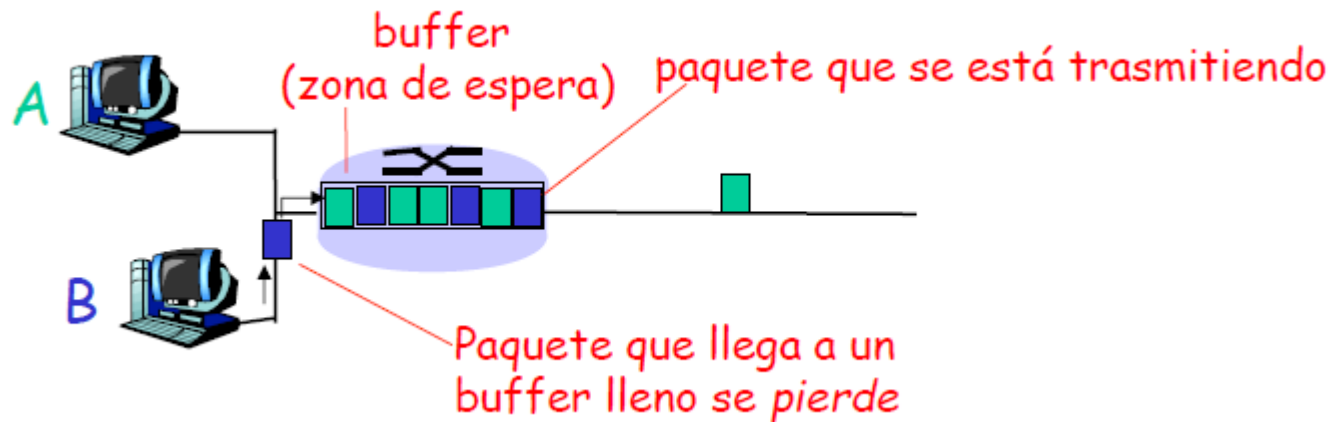
Trace complete.

C:\Users\lenovo>
```

Pérdidas de paquetes

El buffer del enlace tiene capacidad finita

- Cuando un paquete llega a una cola llena se tira (drop)
- Un paquete perdido puede ser retransmitido por el nodo previo, o la fuente, o no...



Bandwidth

Bandwidth

Máximo número de bits que pueden fluir a travez de una conexión de red en determinado periodo de tiempo.

- Unidad fundamental de medida bps
- Si un ISP brinda un ancho de banda de 1Mbps se podrá transferir como máximo 1.000.000 bits por segundo.

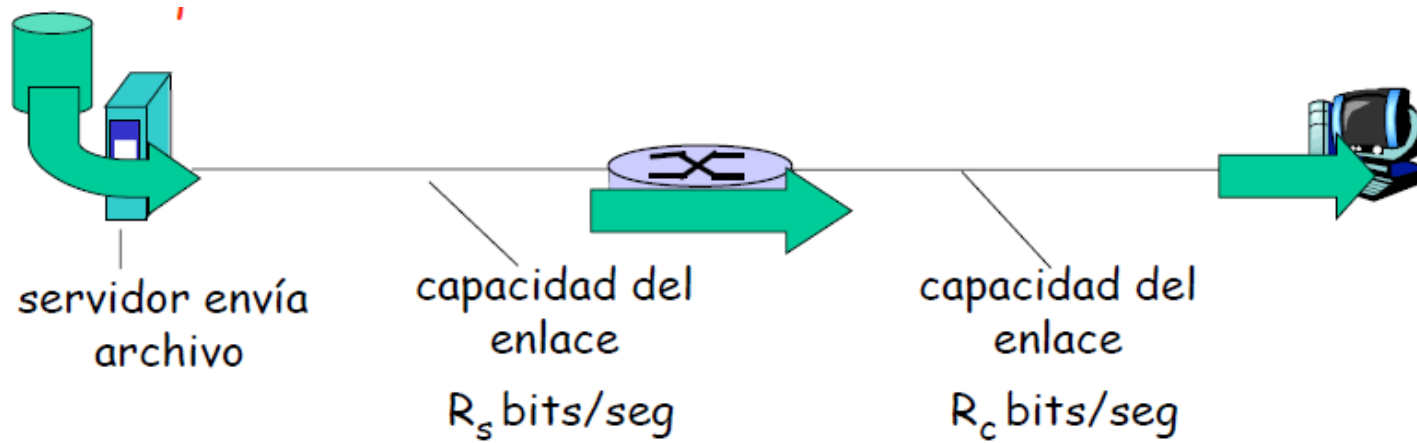
Throughput (tasa de transferencia efectiva)

Throughput

Actual número de bits que fluyen a través de una conexión de red en determinado periodo de tiempo.

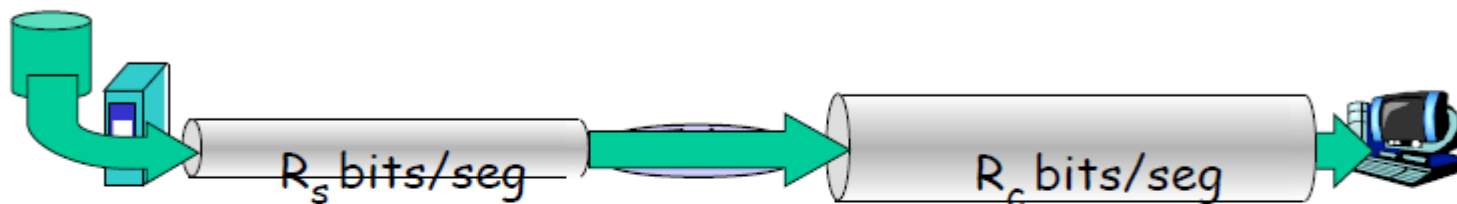
- Esta tasa de transferencia será siempre menor o igual que el ancho de banda.

Se puede considerar el throughput instantaneo o promedio

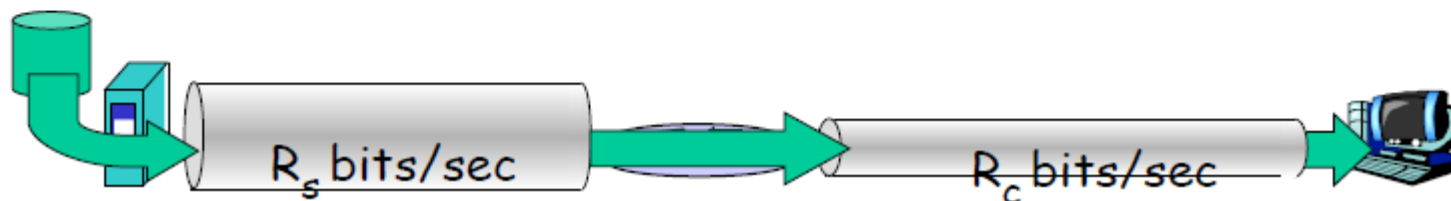


Throughput

$R_s < R_c$ ¿Cuál es el throughput promedio?



☐ $R_s > R_c$ ¿Cuál es el throughput promedio?

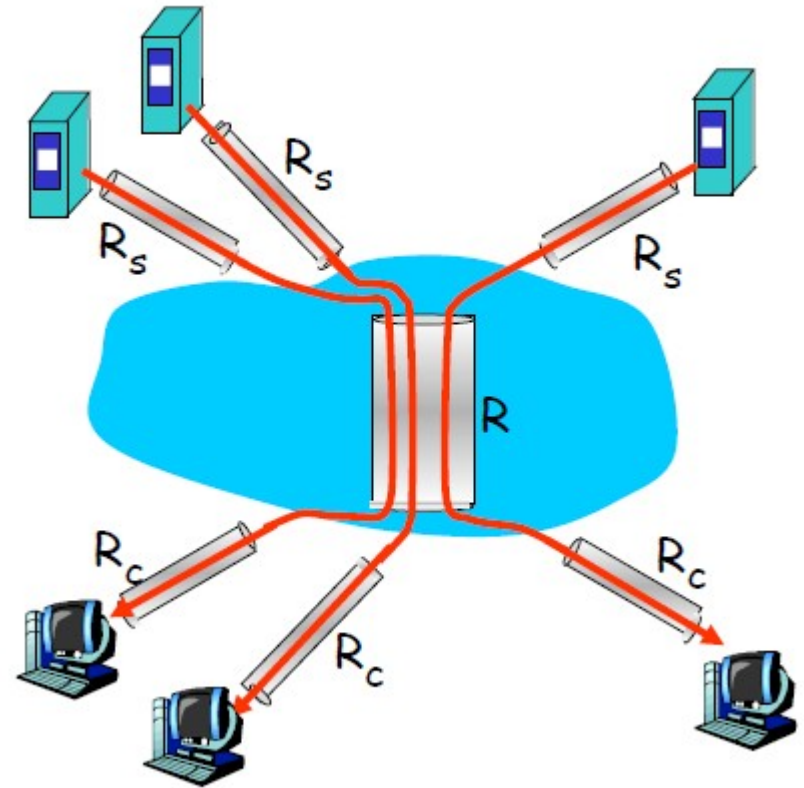


Cuello de botella

Enlace del camino de extremo a extremo que restringe el throughput

Throughput – Escenario en Internet

- Throughput extremo a extremo por conexión:
 $\min(R_c, R_s, R/10)$
- En la práctica:
 R_c o R_s suelen ser el cuello de botella.



10 conexiones comparten (igualmente) el enlace backbone de R bps

Protocolos: Modelos de capas



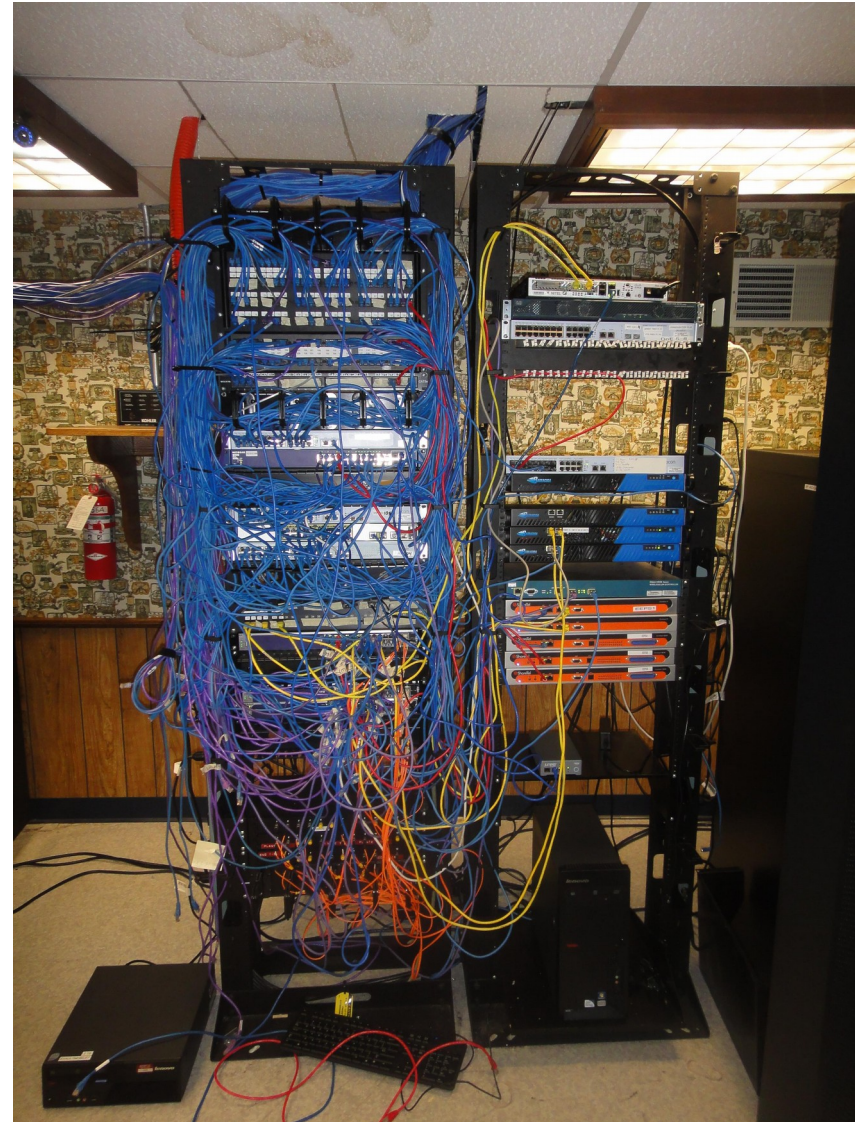
Protocolos: “Capas”

Las redes son complejas

- Muchos elementos

- Hosts
- Routers
- Enlaces de varios medios
- Aplicaciones
- Protocolos
- Software

¿Se puede organizar la estructura de la red?



Organización de un viaje aéreo

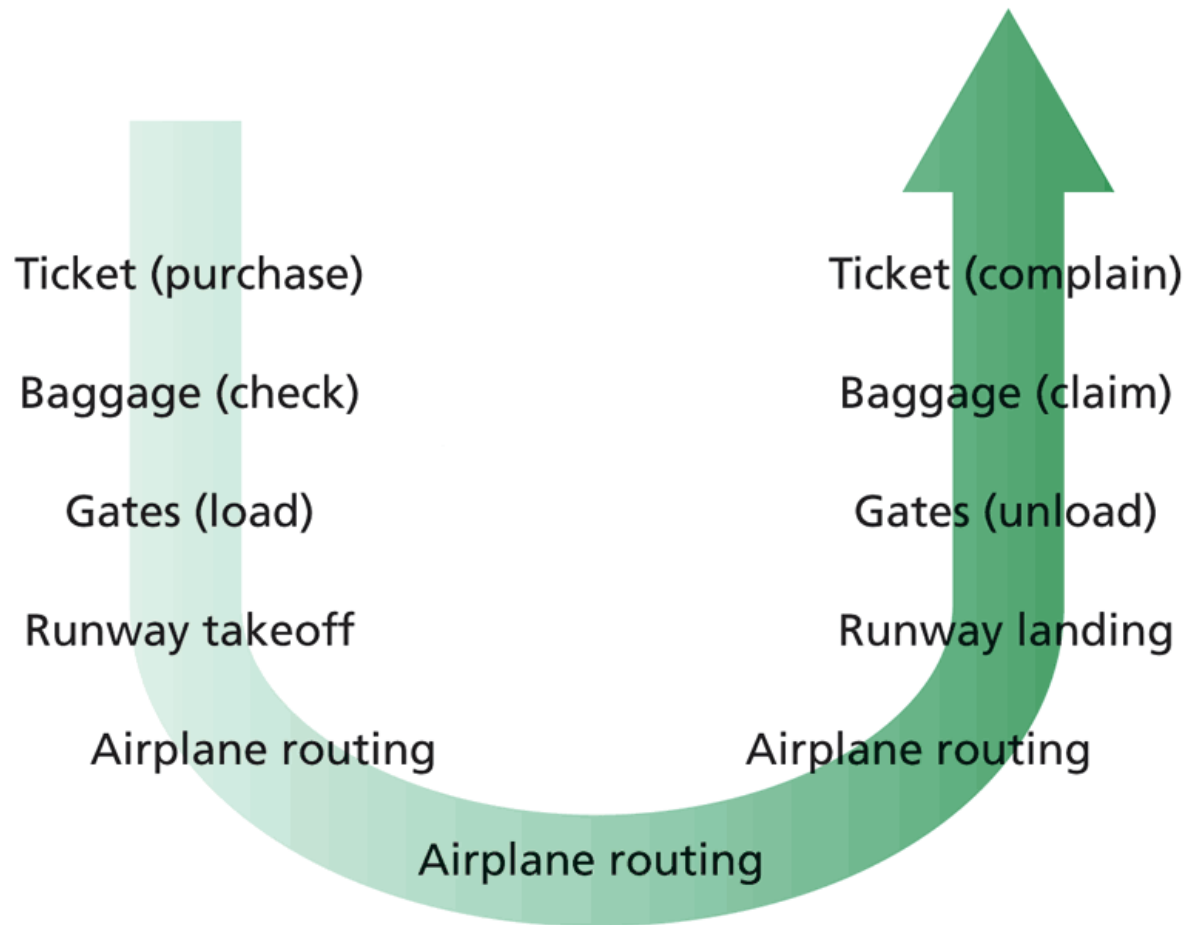


Figure 1.15 ♦ Taking an airplane trip: actions

Modelo en capas de un vuelo

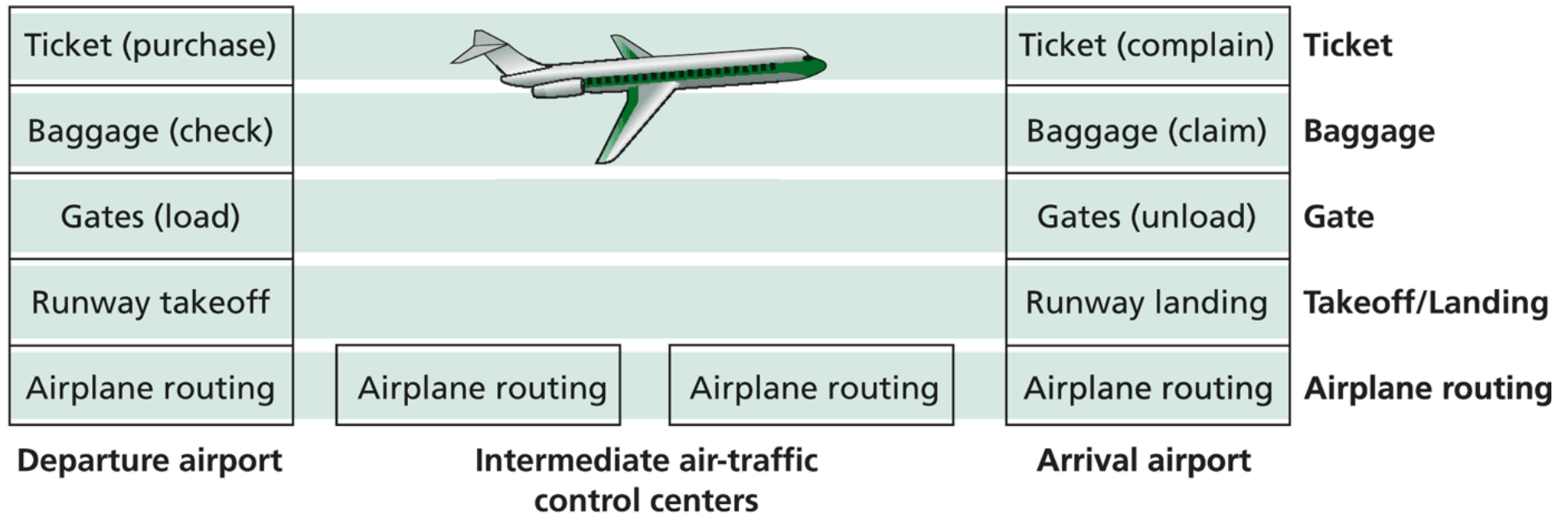


Figure 1.16 ♦ Horizontal layering of airline functionality

Cada capa implementa un servicio

- Usando su propia lógica interna
- Consume servicios provistos por las capas inferiores

¿Por qué usar capas?

Manejar sistemas complejos:

- Permite identificar las relaciones entre los componentes del sistema
- La modularización facilita el mantenimiento y actualización del sistema
 - Cambios en la implementación de un servicio provisto por una capa es transparente al resto del sistema
- ¿Potenciales desventajas?
 - duplicación de funciones
 - necesidad de datos de otra capa para implementar un servicio.

Stack de protocolos de Internet

Aplicación:

Soporta las aplicaciones de la red (FTP, SMTP, HTTP)

Transporte:

Procesamiento de la transferencia de datos de extremo a extremo (TCP, UDP)

Red:

Enrutamiento de datagramas desde fuente a destino (IP, protocolos de enrutamiento)

Enlace:

Transferencia de datos entre elementos vecinos de la red

Física:

Datos representados en un medio físico siendo transportados.

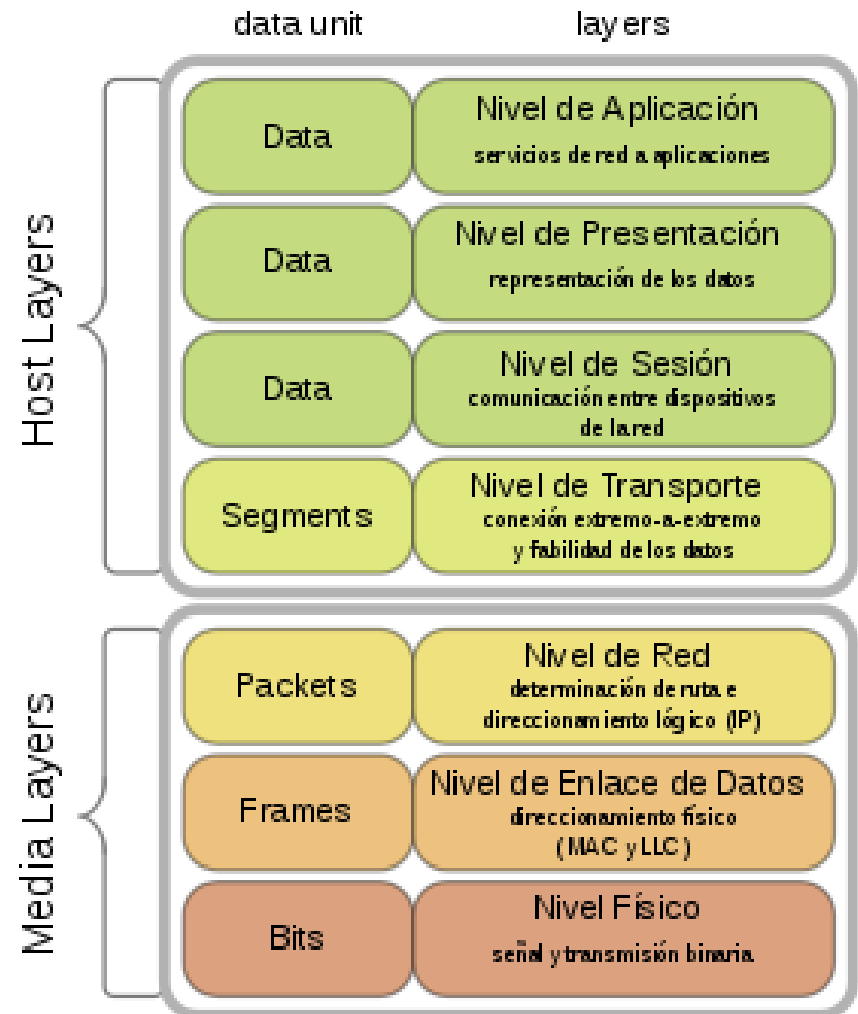
Modelo de referencia ISO-OSI

Presentación

- Permite que las aplicaciones interpreten el significado de los datos, por ejemplo cifrado, compresión, o conversaciones específicas.

Sesión

- Sincronización, checkpointing, recuperación de intercambio de datos.



Mensajes, segmentos, datagramas y tramas

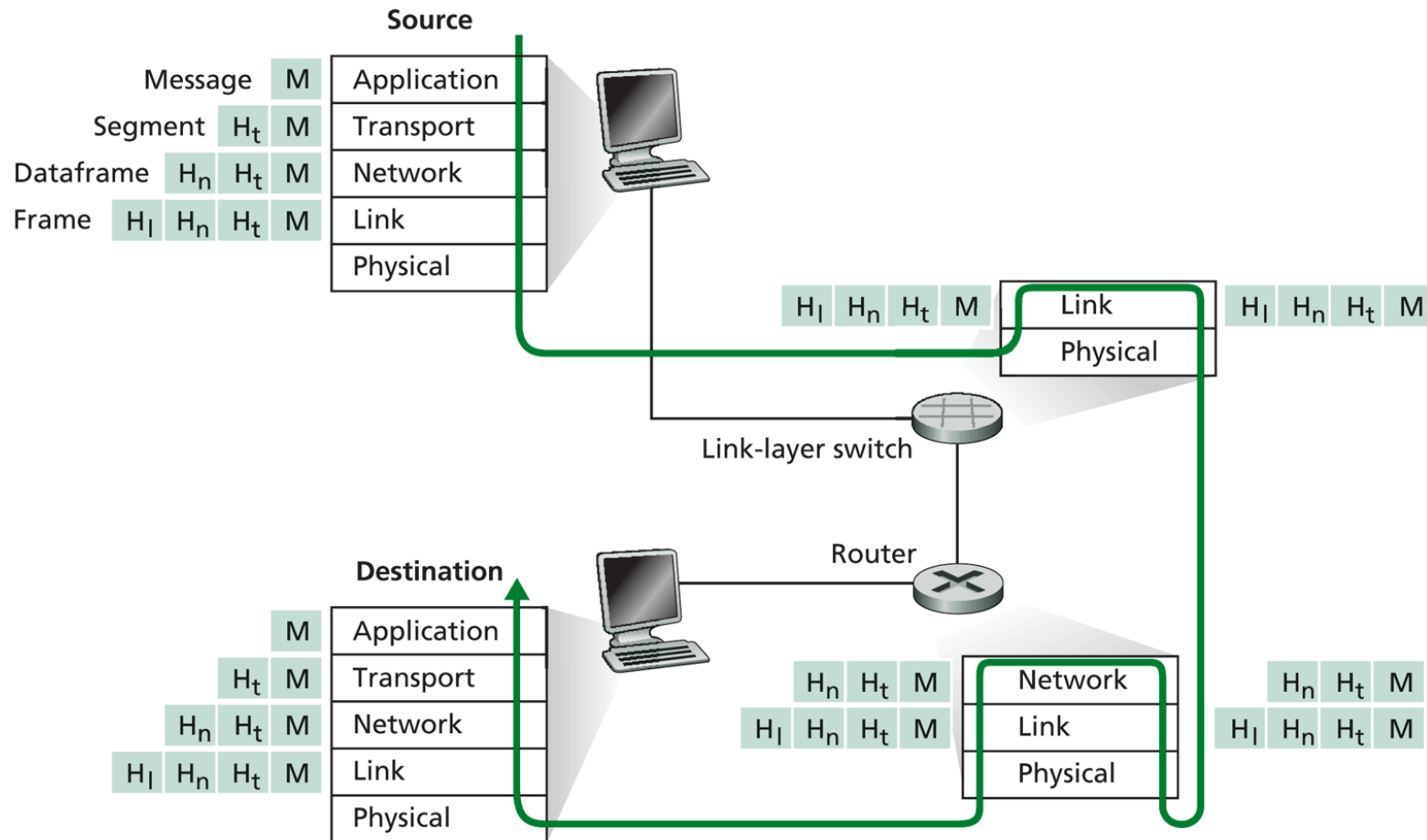
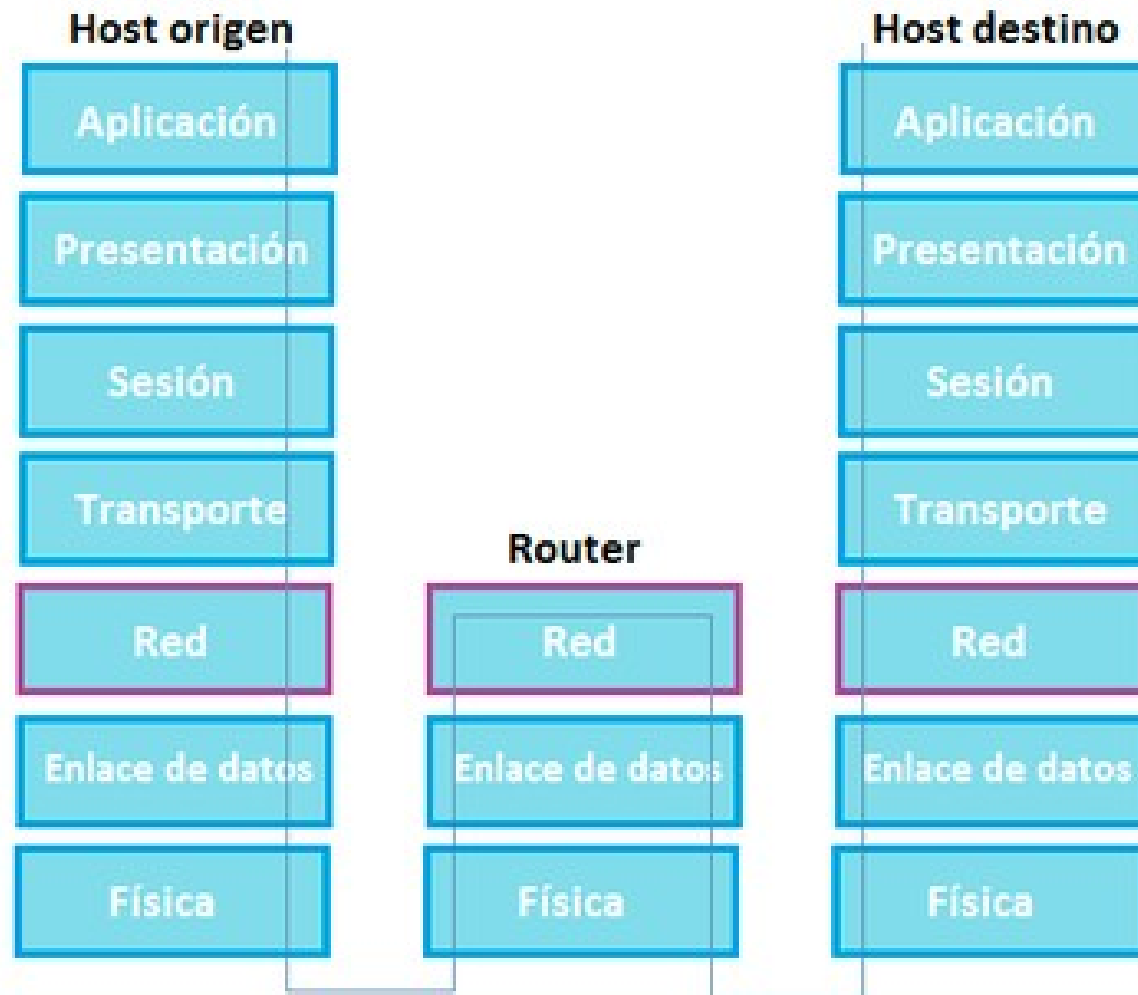
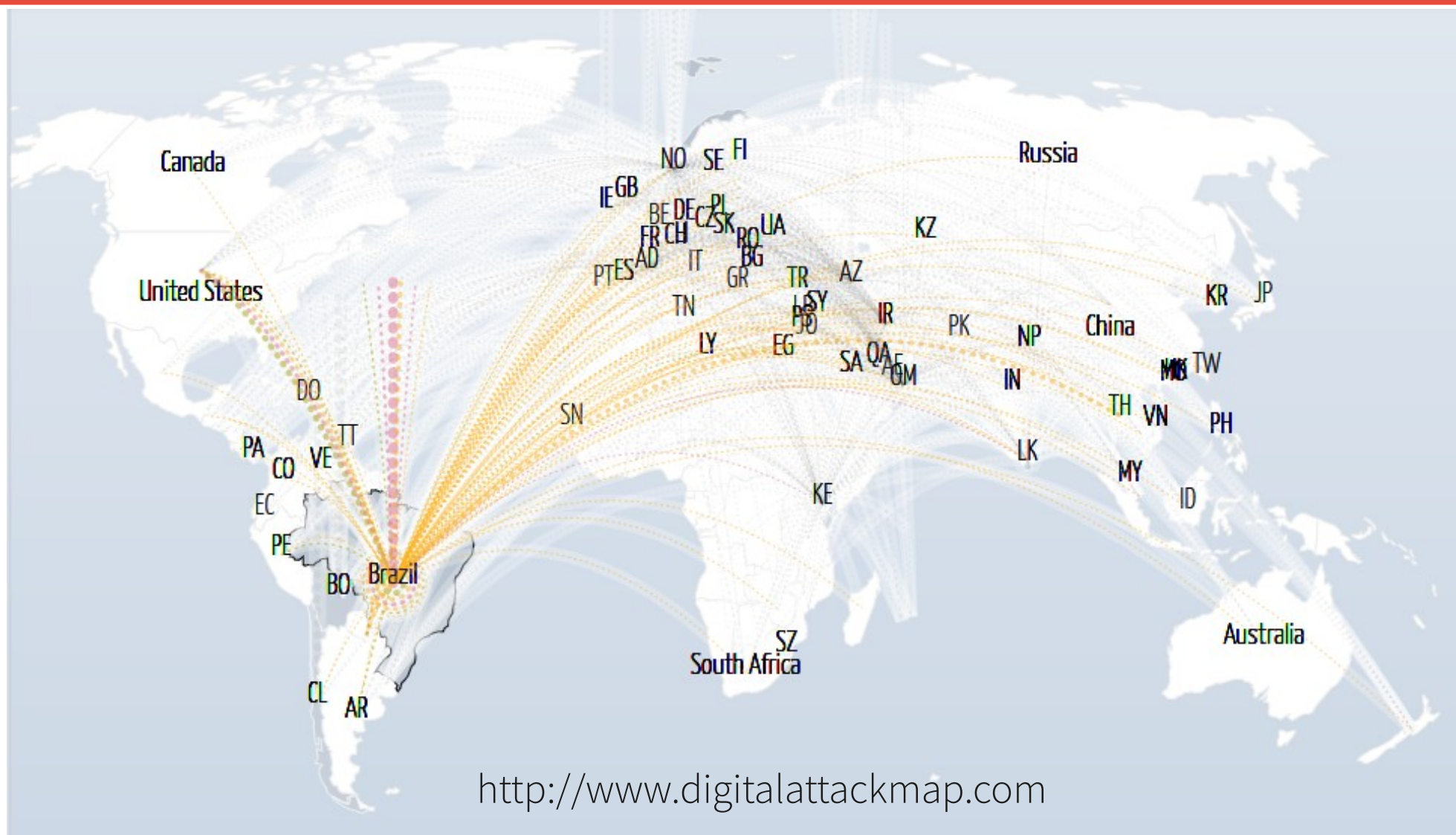


Figure 1.18 ♦ Hosts, routers, and link-layer switches; each contains a different set of layers, reflecting their differences in functionality

Router en capa de red



Seguridad en redes



Seguridad en redes

El campo de la seguridad en redes trata de:

- ¿cómo se pueden atacar las redes de computadoras?
- ¿Cómo se pueden defender las redes de estos ataques?
- ¿Cómo diseñar arquitecturas inmunes a ataques?

La internet no fue diseñada originalmente pensando en la seguridad

- Visión original: “Grupo de usuarios confiables conectados a una red transparente”
- Se realizan actualizaciones en los protocolos

Es posible insertar “malware” en los hosts via Internet

- **Malware:** virus, worms, troyanos
- **Spyware:** Puede grabar secuencias de teclados, sitios web visitados, etc, y subir la información a un sitio recolector.
- Los host's infectados pueden asociarse a una “**botnet**”, usada para ataques de span y **DDOS**.
- El “Malware” suele auto-replicarse: buscar nuevas víctimas desde el host infectado.

Es posible insertar “malware” en los hosts via Internet

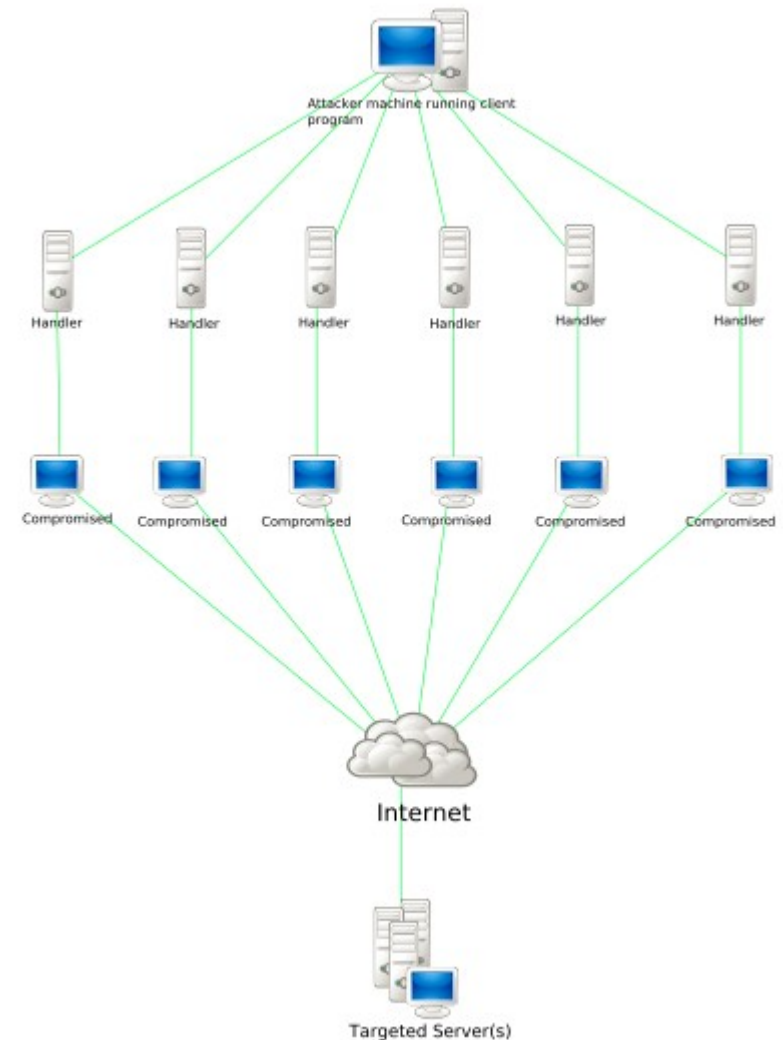
- **Troyano**: malware invasor oculto en software útil.
- **Virus**: Infección por ejecución activa de un objeto recibido.
auto-replicante: se propaga hacia otros hosts.
- **Worm**: Infección por recepción pasiva de un objeto que se auto ejecuta
auto-replicante.

Seguridad en redes

Es posible atacar servidores e infraestructura de red

- Denial of service (DdoS):

Atacantes, usando grandes cantidades de conexiones que saturan los recursos de una víctima.

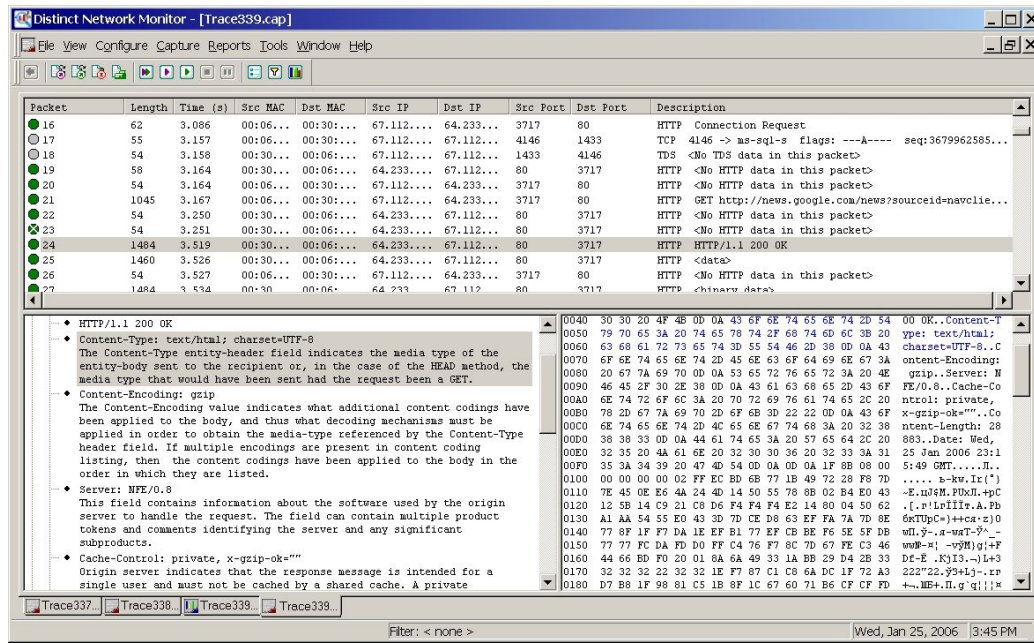


Seguridad en redes

Packet sniffing

Medio de broadcast (Ethernet compartida, red inalámbrica)

Interfaz de red promiscua lee/almacena todos los paquetes

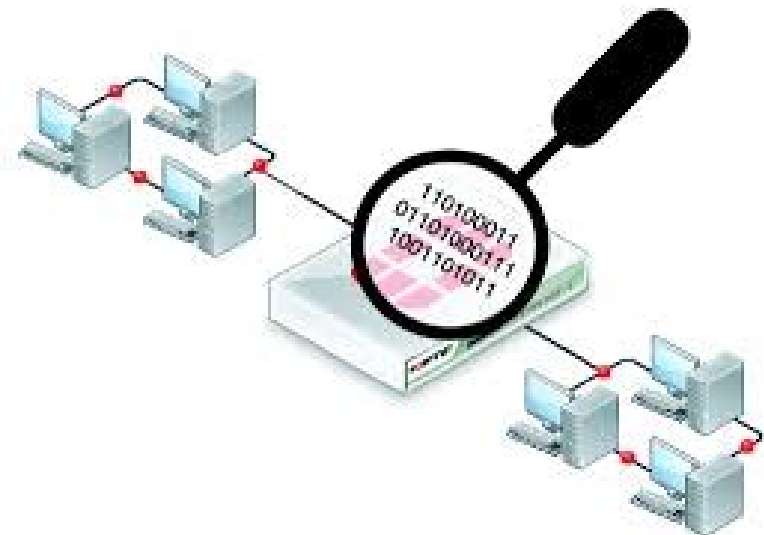


The screenshot shows the Distinct Network Monitor interface with a packet capture of an HTTP transaction. The packet list table is as follows:

Packet	Length	Time (s)	Src MAC	Dst MAC	Src IP	Dst IP	Src Port	Dst Port	Description
16	62	3.086	00:06...	00:30:...	67.112...	64.233...	3717	80	HTTP Connection Request
17	55	3.157	00:06...	00:30:...	67.112...	67.112...	4146	1433	TCP 4146 -> 80 [RST] Seq=3679962585...
18	54	3.158	00:06...	00:06:...	67.112...	67.112...	1433	4146	TDS <No TDS data in this packet>
19	58	3.164	00:06...	00:06:...	64.233...	67.112...	80	3717	HTTP <No HTTP data in this packet>
20	54	3.164	00:06...	00:06:...	67.112...	64.233...	3717	80	HTTP <No HTTP data in this packet>
21	1045	3.167	00:06...	00:30:...	67.112...	64.233...	3717	80	HTTP GET http://news.google.com/news?sourceid=navclie...
22	54	3.250	00:06...	00:06:...	64.233...	67.112...	80	3717	HTTP <No HTTP data in this packet>
23	54	3.251	00:06...	00:06:...	64.233...	67.112...	80	3717	HTTP <No HTTP data in this packet>
24	1484	3.519	00:06...	00:06:...	64.233...	67.112...	80	3717	HTTP HTTP/1.1 200 OK
25	1460	3.526	00:06...	00:06:...	64.233...	67.112...	80	3717	HTTP <data>
26	54	3.527	00:06...	00:30:...	67.112...	64.233...	3717	80	HTTP <No HTTP data in this packet>
27	1484	3.534	00:06...	00:06:...	64.233...	67.112...	80	3717	HTTP <binary data>

The details pane for packet 24 shows the following information:

- HTTP/1.1 200 OK
- Content-Type: text/html; charset=UTF-8
The Content-Type entity-header field indicates the media type of the entity-body sent to the recipient or, in the case of the HEAD method, the media type that would have been sent had the request been a GET.
- Content-Encoding: gzip
The Content-Encoding value indicates what additional content codings have been applied to the body, and thus what decoding mechanisms must be applied in order to obtain the media-type referenced by the Content-Type header field. If multiple encodings are present in content coding listing, then the content codings have been applied to the body in the order in which they are listed.
- Server: NFE/0.8
This field contains information about the software used by the origin server to handle the request. The field can contain multiple product tokens and comments identifying the server and any significant subproducts.
- Cache-Control: private, x-gzip-ok=""
Origin server indicates that the response message is intended for a single user and must not be cached by a shared cache. A private



Seguridad en redes

IP Spoofing

- Enviar paquetes con dirección de origen falso

