

Módulo 01

Introducción a las Redes de Computadoras (Pt. 3)



Redes de Computadoras
Depto. de Cs. e Ing. de la Comp.
Universidad Nacional del Sur



Copyright

- Copyright © 2010-2024 A. G. Stankevicius
- Se asegura la libertad para copiar, distribuir y modificar este documento de acuerdo a los términos de la **GNU Free Documentation License**, versión 1.2 o cualquiera posterior publicada por la Free Software Foundation, sin secciones invariantes ni textos de cubierta delantera o trasera
- Una copia de esta licencia está siempre disponible en la página <http://www.gnu.org/copyleft/fdl.html>
- La versión transparente de este documento puede ser obtenida de la siguiente dirección:

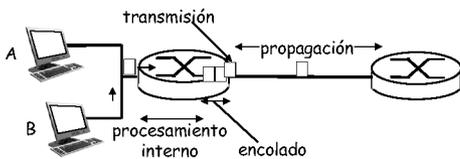
<http://cs.uns.edu.ar/~ags/teaching>

Contenidos

- ¿Qué es internet?
- Concepto de protocolo
- Frontera y núcleo de una red
- Conmutación de circuitos y de paquetes
- Latencia y ancho de banda
- Organización jerárquica de internet
- Modelos de referencia **ISO/OSI** y **TCP/IP**
- La red bajo constante amenaza

Origen de los retardos

- Los retardos surgen como producto de tener que atravesar los nodos y enlaces de la red
- Existen cuatro fuentes de retardo en los paquetes que atraviesan a un cierto nodo:
 - Procesamiento interno
 - Encolado
 - Transmisión
 - Propagación



Origen de los retardos

- Procesamiento interno:
 - Verificar la integridad del paquete (**CRC**, paridad, etc.)
 - Determinar por cuál de las salidas debe ser enviado
- Encolado:
 - Tiempo a la espera de que se libere un determinado enlace de salida
 - Está directamente relacionado al nivel de saturación del router

Origen de los retardos

- Transmisión:
 - Sea R el ancho de banda del enlace (medido en b/s) y L el largo del paquete (en bits); el tiempo de transmisión que toma enviar el paquete por el enlace se calcula como L/R (en s)
- Propagación:
 - Sea d el largo del enlace físico (medido en m) y s el tiempo de propagación de una señal en ese medio físico (en m/s); el tiempo de propagación se calcula como d/s (en s)

El amigo está on fire...

You
¿me podría resumir las fuentes de retardo en las que ocurre un paquete al atravesar un router?

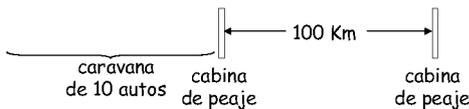
ChatGPT
Cuando un paquete atraviesa un router, puede experimentar varios tipos de retardo, que incluyen:

- Retardo de encolamiento (Queueing delay):** Ocurre cuando el paquete debe esperar en la cola del router antes de ser transmitido. Este retardo depende de la cantidad de tráfico en el router y la política de encolamiento utilizada.
- Retardo de procesamiento (Processing delay):** Se produce mientras el router examina el encabezado del paquete para tomar decisiones de enrutamiento y reenvío. Este retardo varía según la complejidad del enrutamiento y las funciones adicionales del router, como la inspección de seguridad o la redirección de direcciones de red.
- Retardo de transmisión (Transmission delay):** Es el tiempo necesario para transmitir físicamente los bits del paquete a través de la interfaz del router. Depende de la longitud del paquete y la velocidad de transmisión de la interfaz.
- Retardo de propagación (Propagation delay):** Es el tiempo que tardan los bits del paquete en viajar desde el router de origen hasta el router de destino. Depende de la distancia física entre los routers y la velocidad de propagación del medio de transmisión (generalmente fibra óptica o cable de cobre).
- Retardo de almacenamiento y reenvío (Store-and-forward delay):** Este retardo se produce cuando el router recibe todo el paquete antes de retransmitirlo. Depende del tamaño del paquete y la velocidad de enlace del router.
- Retardo de jitter (Jitter delay):** Se refiere a la variación en el retardo de la llegada de los paquetes. El jitter puede afectar la calidad de las aplicaciones sensibles al tiempo, como la transmisión de voz y video.

Estos son algunos de los principales tipos de retardo que un paquete puede experimentar al atravesar un router. La suma de estos retardos determina el tiempo total que lleva que un paquete pase por el router, lo que puede afectar la eficiencia y la calidad de servicio en la red.

Una "car analogy"

• Tratemos de visualizarlo con un ejemplo:



- Cada auto viaja a **100 Km/h**
- Cada auto toma **12s** en pagar el peaje
- Por las dudas: autos = bits, caravana = paquete

• ¿Cuánto tarda en llegar la caravana a la segunda cabina de peaje?

Una "car analogy"

• Ajustemos un poco el ejemplo para hacerlo más parecido al caso de una red de computadoras:



- Cada auto viaja ahora a **1000 Km/h**
 - Cada auto toma ahora **1m** en pagar el peaje
- ¿Llegan autos a la segunda cabina mientras todavía quedan autos saliendo de la primera?

Retardo al atravesar nodos

$$d_{nodo} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

- d_{proc} tiempo de procesamiento interno, típicamente un par de microsegundos
- d_{queue} tiempo de encolado, depende de la congestión
- d_{trans} tiempo de transmisión, L/R es bien pequeño para los enlaces de alta velocidad
- d_{prop} es el tiempo de propagación, puede ser pocos microsegundos o cientos de milisegundos



Retardo de encolado

- Sea R el ancho de banda de un cierto enlace (medido en b/s), L el largo de un paquete (en bits) y a la cantidad promedio de paquetes que llegan a un cierto nodo por segundo
- Denominaremos intensidad de tráfico al cociente La/R
 - $La/R \approx 0$: retardo promedio bajo
 - $La/R \rightarrow 1$: el retardo incrementa
 - $La/R > 1$: llega más trabajo que el puedo atender, el retardo puede llegar a ser ∞ !



$La/R \approx 0$



$La/R > 1$



Traceroute

- ¿En qué nivel estarán los retardos reales tomados de internet?
- El programa traceroute nos permite averiguar exactamente eso:
 - Enviá tres paquetes a cada router en el camino entre la computadora origen y un destino suministrado
 - Cada router contesta al emisor lo más rápido posible
 - El emisor mide el tiempo en recibir la respuesta



Traceroute

```
#> traceroute -I www.uni-muenchen.de
```

tres intentos de medición por cada nodo

```
traceroute to www.uni-muenchen.de [141.84.149.211], 30 hops max, 40 byte packets
 1 1-191-245-190.fibertel.com.ar (190.245.191.1)  8.061 ms  7.908 ms  7.810 ms
 2 * * *
 3 * * *
 4 * * *
 5 69-165-89-200.fibertel.com.ar (200.89.165.69)  21.547 ms  22.109 ms  22.058 ms
 6 * * *
 7 * * *
 8 101-165-89-200.fibertel.com.ar (200.89.165.101)  19.096 ms  39.075 ms  20.069 ms
 9 rab-hornos1-tg7-4.prima.net.ar (200.42.42.69)  35.265 ms  21.581 ms  18.675 ms
10 200-42-42-113.dup.prima.net.ar (200.42.42.113)  19.721 ms  19.524 ms  19.695 ms
11 * * *
12 tengigabithernet4-1.ar3.EZE1.gblx.net (64.214.130.253)  21.728 ms  21.681 ms  21.581 ms
13 64.213.78.238 (64.213.78.238)  234.752 ms  234.910 ms  234.869 ms
14 xr-gar1-te2-2.x-win.dfn.de (188.1.145.54)  242.791 ms  243.863 ms  243.901 ms
15 kr-lrz-muenchen2.x-win.dfn.de (188.1.37.90)  243.774 ms  243.682 ms  243.579 ms
16 vl-3010.csr1-kw5.lrz-muenchen.de (129.187.0.150)  243.261 ms  243.662 ms *
17 vl-3005.csr1-0g2.lrz-muenchen.de (129.187.0.146)  240.788 ms  241.109 ms  243.486 ms
18 141.84.44.211 [141.84.44.211]  243.560 ms  243.507 ms  243.734 ms
```

* indica que el router no contesta o que se perdió el paquete

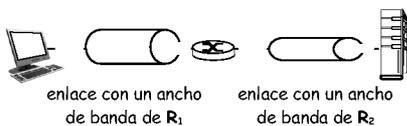
¿qué habrá pasado acá?

Origen de las pérdidas

- Al igual que los retardos, las pérdidas de paquetes tienen diversos orígenes:
 - Al llegar a un router saturado (es decir, con su buffer lleno), el paquete es simplemente descartado
 - El paquete que fue descartado puede ser retransmitido por el último router atravesado, por la computadora de origen, o bien no ser retransmitido
- ¿Por qué un router saturado descarta los nuevos paquetes? ¿El router no debería hacer el intento de colaborar con el emisor?

Desempeño

- Existen dos nociones de desempeño que resulta interesante tener en cuenta:
 - Desempeño instantáneo: el desempeño observado en un determinado instante de tiempo
 - Desempeño promedio: el desempeño observado a lo largo de un período de tiempo



Desempeño

- ¿Cuál será el desempeño promedio si $R_1 > R_2$?



- ¿Y caso contrario, si $R_1 < R_2$?



- Podemos concluir que el desempeño promedio va a depender del ancho de banda del enlace más precario

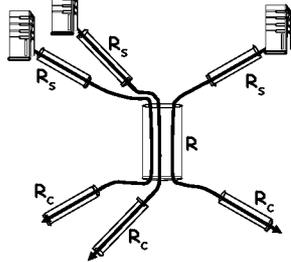
Desempeño

- Desempeño más realista:

→ Por conexión,
 $\min(R_c, R_s, R / 10)$

→ En la práctica, R_c o
a lo sumo R_s suelen
ser el cuello de botella

→ Rara vez el problema
radica en R



10 conexiones comparte (ecuánimemente) el cuello de botella del núcleo de R bits por segundo

Software de la red

- Pensemos por un momento en el problema que debe resolver el software de la red:

→ Tiene que asegurar la comunicación entre todas las computadoras en la frontera de la red

→ Esos datos tienen que atravesar múltiples enlaces y nodos al cruzar el núcleo de la red

→ El camino entre dos computadoras no necesariamente es único ni estático a lo largo del tiempo

→ Las partes del mensaje (los paquetes) puede llegar fuera orden o no llegar directamente

Software de la red

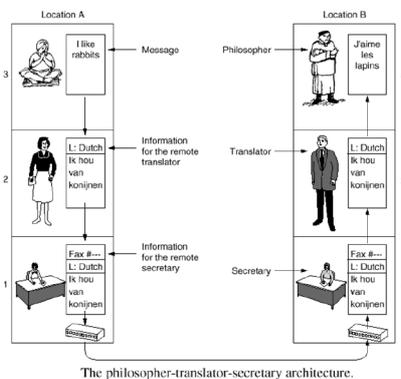
- Se puede afirmar que el problema a resolver es posiblemente uno de los más difíciles que nos podamos enfrentar
- Evidentemente tendremos que hacer uso de alguna técnica de alto nivel que nos permita acotar la complejidad de este problema
 - Naturalmente, deseamos que la solución sea de alta calidad y en la medida de lo posible eficiente
- La propuesta elegida fue atacar este problema haciendo uso de una arquitectura en capas

Un problema complejo

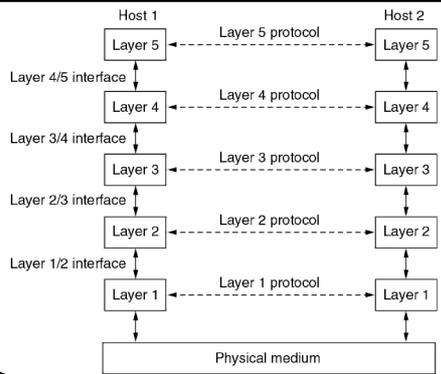
- La existencia de una estructura explícita permite identificar relaciones útiles entre las distintas partes del sistema
- El contar con un modelo de referencia posibilita la participación activa de todos los interesados
- La modularización que aportan las capas facilita el mantenimiento y la actualización del sistema
 - Los cambios en la implementación de los servicios de una capa no afecta a las restantes

Una analogía

- Comunicación entre filósofos:
 - El holandés puede cambiarse por el esperanto
 - En lugar de fax puede usarse email



Arquitectura de red



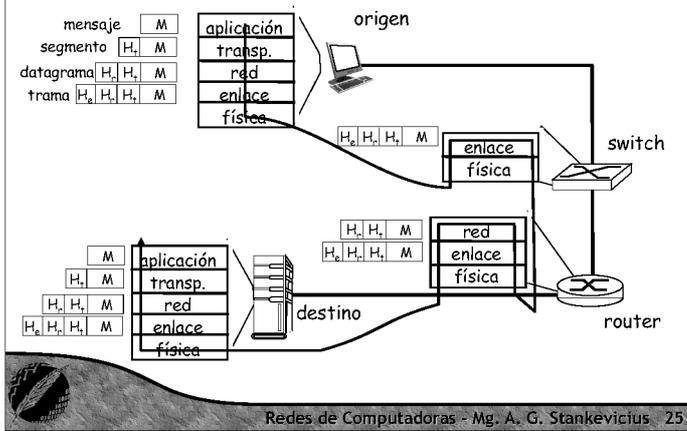
Desafíos de diseño

- En cada capa se debe resolver:
 - Un mecanismo para identificar de forma unívoca tanto al emisor como al receptor
 - Determinar la forma de transferencia (ya sea unidireccional, half-duplex o full-duplex)
 - Fijar una política de control de errores (esto es, elegir el nivel de detección y de corrección deseado)
 - Tomar una decisión acerca de cómo se ordenan y secuencian los mensajes

Desafíos de diseño

- Continúa:
 - Decidir si es necesario implementar control de flujo y/o mecanismos de gestión de la congestión
 - Fijar el tamaño de los mensajes, lo cual implica a su vez fijar el mecanismo de desarmado y rearmado de los mensajes de las capas superiores
 - Definir, si corresponde, el mecanismo de multiplexado y de demultiplexado a ser usado
 - Resolver cómo enrutar los mensajes
 - Analizar qué medidas de seguridad son necesarias

Encapsulado de mensajes



Servicios y protocolos



- ¿Qué relación existe entre un protocolo y los servicios provistos por esa capa?
- ¿Y con los provisto por la inmediata inferior?

Servicios y protocolos

- La especificación del servicio define qué operaciones está dispuesta a prestar una cierta capa a sus clientes
 - Cabe señalar que nada dice respecto de cómo serán implementadas esas operaciones
- La especificación de un protocolo, en contraste, es un conjunto de reglas que gobierna el formato y el significado de los mensajes intercambiados entre los pares de una capa
- Es decir, iel protocolo implementa al servicio!

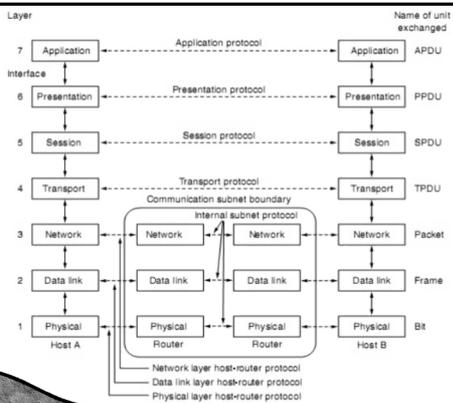
El modelo ISO/OSI

- La **ISO** (International Organization for Standardization) propuso allá por la década del 70' un estándar internacional para mejorar la interoperabilidad de las primeras redes de computadoras
- El modelo propuesto, llamado **OSI** (Open System Interconnect) consiste de dos partes:
 - Un modelo de referencia de siete capas
 - Un conjunto de protocolos para cada una de capas

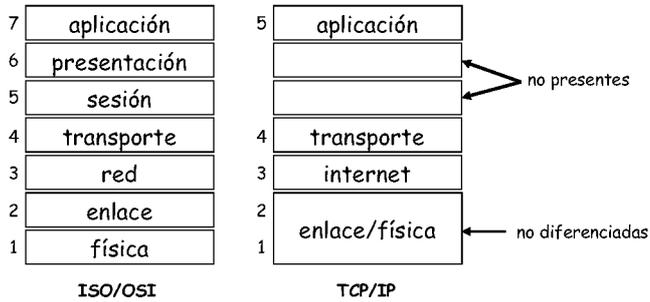
El modelo ISO/OSI

7	aplicación	aplicaciones de red (email, web, etc.)
6	presentación	formateado, encriptado y compresión de datos
5	sesión	inicialización y gestión de conversaciones de punta a punta
4	transporte	envío punta a punta de mensajes
3	red	transmisión punta a punta de paquetes
2	enlace	transmisión de paquetes sobre un dado enlace
1	física	codificación de bits

Protocolos del modelo OSI



El modelo TCP/IP



¿Qué pasó con este modelo?

- El modelo no distingue con claridad los conceptos de servicio, interfaz y protocolo
- El modelo no es genérico y no sirve para describir ningún otro conjunto de protocolos
- El modelo no distingue entre la capa física y la de enlace (es más, ni siquiera las menciona)
- Sólo los protocolos **TCP** e **IP** fueron cuidadosamente pensados e implementados (el resto fue definido de manera más ad-hoc)

OSI vs. TCP/IP

- El modelo **OSI** fue diseñado antes que sus protocolos
 - No favorece ningún conjunto de protocolos en particular (ni siquiera los propios)
 - Los diseñadores no tenían mucha experiencia previa
- Los protocolos del modelo **TCP/IP** se diseñaron e implementaron antes que su modelo de referencia
 - Excelente implementación, disponible desde un primer momento (además de ser libre y gratuita)

Seguridad en redes

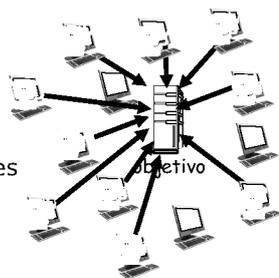
- El campo de la seguridad en redes abarca diferentes facetas:
 - De qué forma pueden atacar mi red de computadoras
 - De qué forma me puedo defender ante esos ataques
 - Cómo diseñar una arquitectura de red que sea resiliente a los ataques
- Lamentablemente internet no fue diseñada con la seguridad en mente
 - Los primeros usuarios... ise conocían todos entre sí!

Inyección de malware

- Internet es un vector de ataque a través del cual un malhechor puede inyectarnos malware
 - Viruses: programas adosados a otros, auto-replicante, que ganan el control de la máquina al recibir y ejecutar un huésped infectado
 - Worms: programas independiente, auto-replicante, que ganan el control de la máquina explotando vulnerabilidades
- El malware de tipo spyware puede registrar y reportar todas las acciones de los usuarios

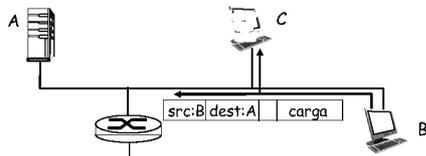
Denegación de servicio

- El ataque de denegación de servicio consiste en sobrecargar con tráfico espurio un determinado objetivo
1. Elegir el objetivo
 2. Tomar control de múltiples nodos (por caso, via un worm)
 3. Enviar multitud de mensajes a la vez y de diversas fuentes al mismo destino



Sniffing de paquetes

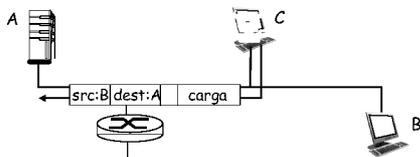
- Los enlaces de tipo difusión posibilitan un tipo peligroso de ataque llamado sniffing
- Un adaptador en modo promiscuo tiene acceso a la totalidad de los paquetes que por él pasen



la herramienta wireshark que usaremos en la práctica hace precisamente esto

Spoofing de IP

- Otro ataque especialmente funesto es el spoofing o engaño de IP
- Un atacante se hace pasar por otro, simplemente cambiando la identidad de origen



al final de la materia retomaremos este candente tópico

¿Preguntas?
