# 

Profesor:   
Miguel Torrealba

Estudiantes:

David Diaz

Alan Argotte

Mauricio Fragachán

Ian García

José Revete

Jesús Gutierrez

Ángel Valero

Redes de Computadoras

**Planificación**

|  |  |  |
| --- | --- | --- |
| Evaluación | Fecha | Ponderación |
| Parcial 35% | Semana 5 | 35% |
| Parcial 35% | Semana 8 | 35% |
| Laboratorios (2) 5% c/u | Semana 12 | 10% |
| Trabajo final de investigación y desarollo | Todo el trimestre | 20% |

Para contacto con el profesor:

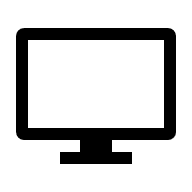
Oficina ???

FE1 ???

migueltorrealbasanchez@gmail.com

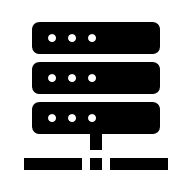
mtorrealba@usb.ve

**Elementos gráficos**



Cliente

Router



Servidor

**Índice**

1. [Clase 1. Título](#Clase_1)

**Capítulo 1. Redes de computadoras y el Internet**

**Definición de Internet**

El Internet es una red de dispositivos de computación conectados entre sí por un propósito común. A los medios a través de los cuales se conectan los llamamos *links de comunicación* y *switches de paquetes*. Existen diversos tipos de links de comunicación, cada uno con distintas *tasas de transmisión ()*. Similarmente, existen distintos tipos de switches de paquetes, al cual reconocemos como el más distintivo al *router*.

A través de links de comunicación son enviados *paquetes*. Todo dato es dividido en distintos segmentos y a cada uno se le añade una pieza adicional de información -un encabezado, o *header*-. A esta estructura de datos la conocemos como paquete. En el Internet, todo paquete que es enviado desde un dispositivo de computación debe seguir un camino o *ruta* hacia el dispositivo destino.

Adicionalmente, los dispositivos de computación acceden al Internet a través de *Internet Service Providers (ISPs)*, que son a su vez redes de otros dispositivos conectados con links de comunicación y switches de paquetes. Estos ISPs son organizados jerárquicamente. ISPs de jerarquía inferior se conectan entre si y estos, a su vez, se conectan a un ISP de jerarquía superior, que se conecta a otros de la misma jerarquía. Independientemente de su jerarquía, los ISPs siguen el *protocolo de Internet (IP*) y ciertos estándares propios.

Respecto a IP, todo dispositivo computacional en el Internet ejecuta protocolos. Estos protocolos contronal el envío y recibimiento de información. Los más importantes son IP y *Transmission Control Protocol* (TCP) y son conocidos colectivamente como TCP/IP.

Toda solución a problemas de diseño del Internet son documentados en *Requests for Comments* (RFCs). Estos documentos conforman los estándares del Internet y son desarrollados por el *Internet Engineering Task Force* (IETF).

El Internet también se puede definir como una infraestructura que provee servicios a aplicaciones. Con aplicaciones nos referimos a toda pieza de código fuente que involucra el intercambio de datos entre diferentes dispositivos o sistemas computacionales. A estas aplicaciones también se les conoce como *aplicaciones distribuidas*. Estas aplicaciones deben cumplir ciertos requisitos para poder utilizar el Internet como medio de comunicación. Asimismo, los dispositivos o sistemas computacionales -a los que nos referiremos simplemente como computadoras-, deben tener una interfaz para poder conectarse al Internet. A dicha interfaz la conocemos como *interfaz de socket.*

Finalmente, en el Internet las computadoras usan protocolos. Cada uno de estos protocolos cumplen un fin distinto, pero todos tienen el objetivo de permitir la comunicación entre las computadoras. Podemos definir un protocolo como *el formato y el orden de mensajes intercambiados entre dos o más entidades comunicativas y las acciones tomadas en la transmisión o recepción de un mensaje u otro evento*. De forma vulgar y simple, podemos definir a un protocolo como una serie de condicionales if-then que determinen las acciones a tomar por una entidad en función del valor de un mensaje.

**Redes de acceso y medios de transmisión**

En el Internet, llaman hosts a las computadoras conectadas a ella. Esto es debido a que *hostean* aplicaciones ejecutándose constantemente. Y podemos clasificar los hosts en dos categorías: los clientes y los servidores. Por experiencia, uno entiende que los servidores son sistemas computarizados poderosos que proveen los servicios asociados al Internet.

Hacemos un par de definiciones antes de comenzar a hablar de los medios de transmisión a través de los cuales las computadoras se conectan al Internet. Primero, definimos a las *redes de acceso* como la red de computadoras conectadas al *router borde*. Un router borde es el primer router alcanzado por un paquete en su camino. Es decir, uno puede verlo como la primera parada que toma un mensaje enviado por una computadora desde una red a otra computadora.

A continuación se procede a explicar los medios a través de los cuales las redes de acceso se conectan al Internet:

* Redes Hogar (Home Access): esencialmente, las redes hogares se conectan al Internet a través de la infraestructura ya ofrecida por la compañía telefónica local (telco). La red hogar se conecta a un router que a su vez está conectado a un splitter. Al splitter también está conectado el teléfono. El splitter se encarga de enviar las señales separadas entrantes a la red telefónica. Una vez en la red telefónica, son interceptadas por un dispositivo llamado *digital subscriber line Access multiplexer* (DSLAM) que actúa como un router y que vuelve a separar la señal entrante de acuerdo con su origen: si viene del teléfono, es enviado a la red telefónica; si viene de una computadora, es enviado al Internet. A este medio se le conoce como *digital subscriber line* (DSL). También distinguimos *cable internet Access* como un medio de las redes hogares para conectarse al Internet a través de la red de televisión. Funciona de forma similar a DSL.

Internet

Red telefónica

Router

Computadora

Teléfono

DSLAM

1 Esquema de DSL

Otro medio más mediante el cual las redes hogares se pueden conectar al Internet es a través de *fiber to the home* (FTTH, o simplemente fibra óptica). A través de la oficina de la compañía telefónica (CO), distintas redes hogares se conectan a una sola fibra que llega al CO y que solo se separa al momento de que alcanza una distancia mínima de cada hogar con el fin de crear fibras específicas para cada hogar.

* Redes empresariales: las computadoras se conectan al router de borde a través de *redes de área local* (local area networks, LAN). La tecnología usada para conectar las computadoras en el LAN es Ethernet Ethernet hace uso de switches y cables de Ethernet.

**El núcleo del Internet y métodos de transmisión de mensajes.**

Llamamos núcleo del Internet al conjunto de switches de paquetes y links de comunicación que unen a las distintas redes de acceso. Las computadoras transmiten mensajes entre sí en el Internet. Un mensaje es información formateada, por lo que teóricamente puede ser lo que uno quiera -imágenes, vídeos, texto, audio… Y existen diversas maneras de transmitir estos mensajes desde una computadora origen a una computadora destino. Una consiste en enviar paquetes; la otra, en establecimiento de sesiones de comunicación.

* Store-and-forward (packet switching)

Una computadora origen quiere enviar a una computadora destino un mensaje dividido en paquetes de bytes cada uno sobre un camino de links de comunicación con switches de paquetes intercalados, donde cada link tiene una tasa de transmisión de bytes por segundo. Store-and-forward consiste, como su nombre indica, en que un switch de paquete almacena el paquete recibido en su puerto de entrada y no lo envía a su puerto de salida con destino a hasta que haya recibido el paquete en su totalidad.

A

Router

B

En general, enviar un paquete de bytes sobre un camino consistente de links con switches de paquetes entre ellos, toma , donde es la tasa de transmisión de bytes por segundo.

Habíamos mencionado los puertos de entrada y de salida de un switch de paquetes. En estos puertos de entrada y salida funcionan como buffers. En estos buffers hay unas colas que almacenan los paquetes. Cuando estas colas están llenas y el switch recibe un paquete, éste o un paquete en el buffer es perdido, ocurriendo así el fenómeno llamado *pérdida de paquetes*. También, consecuentemente, ocurre el *retraso de cola*, que es el tiempo que debe esperar un paquete para ser retransmitido desde el puerto de salida.

* Multiplexing (circuit switching)

Respecto al establecimiento de sesiones, también llamado *circuit switching*, éste consiste en la reserva de una fracción de los recursos disponibles en la red (link de comunicación, switch de paquete y tasa de transmisión de datos del link) para establecer una conexión entre el par de computadoras y .

Existen dos formas de aplicar multiplexing a una red: dividiendo frecuencias (frecuency-division, FDM) o dividiendo tiempo (time-division, TDM). En FDM, el ancho de banda de las frecuencias en un link es dividida en distintas bandas de la misma frecuencia y cada uno está dedicada para una sesión. En TDM, el tiempo se divide en frames de tiempo y cada frame se divide en lotes. Por cada lote, se dedican los recursos de la red para permitir la comunicación entre un par de computadoras y .

A

Router

B

lote

En TDM, a lo largo del tiempo, se crea una unidad de tiempo llamada frame. Ese frame tiene, a su vez, varios lotes o slots. Cada uno de esos slots es a su vez un intervalo de tiempo reservado para la comunicación entre un par de computadoras. Es decir, que durante el slot son reservados los recursos de la red para permitir esta comunicación.

**Jerarquía de ISPs**

El Internet es una red de redes conectadas entre sí. Para recapitular, sabemos que las redes de acceso logran conectarse a Internet a través de ISPs (el primer ISP con el que se conectan es llamado ISP de acceso). Para crear esta red de redes, los ISPs de acceso podrían conectarse entre sí -tarea que resulta cara y complicada. Esto es resuelto creando un ISP global al que todos los ISPs de acceso se conectan. A esta relación la llamamos relación de cliente-proveedor, donde existen ISPs clientes que usan la condición global de un ISP proveedor para conectarse con otros ISPs.

Aquí podemos observar cómo se crea una jerarquía de dos niveles: los ISPs de acceso y el ISP global. En la vida real, existen más niveles en la jerarquía, pues agregamos a los ISPs regionales en esta jerarquía. Los ISPs regionales tienen una cobertura mayor que los ISPs de acceso, por lo cual estos últimos deciden conectarse a estos ISPs regionales. Pero también pueden existir ISPs suprarregionales a los cuales los ISPs regionales a su vez se conectan. Al mismo tiempo pueden existir más de un ISP global. Así es cómo podemos describir el Internet: una red de redes organizada jerárquicamente con ISPs de coberturas diferentes conectados entre sí.

Tier 1 ISP

Access ISP

Tier 2 ISP

Tier 2 ISP

Access ISP

Access ISP

Access ISP

Tier 2 ISP

Tier 1 ISP

Peering

Multi-homing

2 Red de ISPs con instancias de multi-homing y peering. Multi-homing ocurre cuando un ISP cliente se conecta a más de un ISP proveedor; peering, cuando dos ISPs del mismo nivel en la jerarquía se conectan entre sí sin costo alguno

IXP

Tier ISP

Tier ISP

Tier ISP

3 ISPs conectados a un Internet Exchange Point (IXP), a través del cual ISPs en distintos niveles de la jerarquía pueden hacer peering

Provider ISP

Router

PoP

Customer ISP

4 Ilustración de la interfaz con la cual los ISPs clientes se conectan a los ISPs proveedores. Esta interfaz se llama Point of Presence y se trata de un grupo de routers

**Análisis del retraso y los cuellos de botella en redes basados en conmutación de paquetes (packet-switched networks)**

* Retraso de procesamiento, *processing delay*

Es el tiempo que toma un *nodo* (es decir, un router) en examinar la cabecera de un paquete, determinar hacia qué puerto de salida debe dirigirse para acercarlo a su destino y examinar la integridad del paquete (es decir, checar errores a nivel de bits en el paquete).

* Retraso de cola, *queuing delay*

Tiempo de espera que experimenta el paquete en una cola para ser transmitido hacia el link.

Debemos estudiar con un poco más de cuidado este tipo de retraso (jaja), pues varía de paquete a paquete y de la caracterización de la tasa con la que los paquetes llegan a la cola (¿los paquetes llegan poco a poco en intervalos de tiempo, o llegan varios paquetes en ráfaga?).

**Intensidad del tráfico**

Sea la tasa promedio de paquetes que llegan a la cola, bits el tamaño de los paquetes que llegan y la tasa de transmisión del link. Definimos la intensidad del tráfico, , como

Podemos interpretarla como la tasa de bits que entran sobre la tasa de bits que salen. Luego, es evidente que nos podemos hacer las siguientes preguntas: ¿qué ocurre si ? ¿Y si ?

Caso

El retraso de cola se hace considerablemente grande y debe ser considerado en el sistema

Caso

Como la intensidad del tráfico no es significativa, realmente impacta sobre el retraso de cola la naturaleza de la llegada de los paquetes. O sea, si vienen en intervalos de tiempo o en ráfagas.

Supongamos que los paquetes son todos de bits y que la tasa de transmisión del link es . Luego un paquete sale de la cola cada segundos. Y que un paquete llega a la cola cada segundos.

Si los paquetes llegan en intervalos de tiempo, entonces ninguno de ellos experimenta retraso de cola, pues para el i-esimo paquete que llega a la cola, en el tiempo que llega a la cola es el tiempo que requiere el paquete que llegó antes en ser transmitido sobre el link.

Si los paquetes llegan en ráfagas, supongamos entonces que llegan paquetes cada segundos. El primer paquete no tiene retraso de cola; el segundo, tiene un retraso de segundos… En general, el n-esimo paquete tiene un retraso de cola de segundos.

* Retraso de transmisión, *transmission delay*

Tiempo que tardan todos los bits de un paquete en ser transmitidos hacia un link desde un router. O sea, sea un paquete de bits y un link con una tasa de transmisión de , es el tiempo que tarda un paquete en ser transmitido hacia el link desde el router.

* Retraso de propagación, *propagation delay*

Después de que un paquete es transmitido hacia el link desde un router, ahora debe llegar físicamente hacia el siguiente router o computadora destino. La velocidad de propagación de un link depende físicamente de sus propiedades, pero en general uno calcula el retraso de propagación como la distancia entre dos nodos sobre la velocidad de propagación del medio. O sea, el tiempo que tarda un bit recorrer una distancia con una velocidad de propagación .

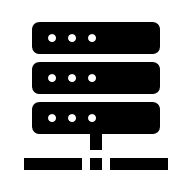
* Retraso end-to-end

Supongamos que el retraso de cola no es considerable en los nodos en la ruta de un paquete de bits sobre links con una tasa de transmisión . Además, que en cada nodo, incluyendo la computadora de origen, tiene un tiempo de procesamiento , que el tiempo de transmisión es y que el tiempo de propagación es . Luego, definimos el retraso end-to-end con la siguiente ecuación:

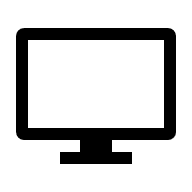
**Throughput o Rendimiento**

Es la razón de datos **recibidos** por un host, digamos , desde un host . puede recibir cualquier tipo de datos. Por ejemplo, podría recibir un archivo con determinado peso en bits. Llamamos **rendimiento promedio** de una transferencia de datos a la cantidad de bits recibidas sobre un periodo de tiempo . Para ilustrar este concepto, imagine que tarda segundos en recibir en su totalidad el archivo de peso ; luego, el rendimiento promedio de la transferencia del archivo es bits por segundo. Similarmente, llamamos **rendimiento instantáneo** en un instante de tiempo a la tasa de datos que recibe por segundo.

**Cálculo del rendimiento en redes de computadoras**



Servidor



Cliente

Router

Supongamos que un cliente solicita a un servidor un archivo de tamaño . El servidor comienza la transmisión del archivo a una tasa . Los paquetes llegan al router, que comienza a transmitir los datos al enlace hacia el cliente con una tasa . El cliente descarga tan pronto el archivo como el router logra empujar los datos al link.

Si la tasa de transmisión servidor-router es menor que la de router-cliente, entonces cuando un paquete llegue al router en y sea transmitido del router al cliente en , tarda más la transmisión de datos en el enlace servidor-router.

Luego, el cliente descarga tantos paquetes por segundo como .

Por lo tanto, el rendimiento cliente-servidor del archivo es

Análogo

Si se quiere, podemos calcular también cuánto tiempo tarda el archivo de peso en ser transmitido hacia el cliente. Es consecuencia lógica que el rendimiento viene dado por (al cual se le llama enlace cuello de botella). Luego,

Es aproximadamente el tiempo que tarda el archivo de peso en ser transmitido hacia el cliente.

**Capas de protocolos y el servicio de modelos**

Utilizamos el modelo de servicios para explicar cómo funciona la red, sintetizando su complejidad en módulos. Para explicar estos módulos, nos centramos en los servicios que se ofrecen entre sí a partir de los protocolos y estándares -he ahí porque se llama *modelo de servicios*. Sin embargo, tratando de explicar el Internet, nos damos cuenta de que los servicios ofrecidos por un módulo dependen de aquellos ofrecidos por otro. Es decir, existe una dependencia “hacia abajo” entre los módulos y , donde depende del servicio ofrecido por . He aquí el modelo de capas: las capas o módulos organizados en forma de pila, con las capas inferiores ofreciendo servicios a las capas superiores.

Aplicación

Transporte

Red

Enlace

Físico

5 Ilustración del módelo de servicios por capas del Internet. La i-esima capa ofrece servicios a la i+1-esima capa. A esta pila se le conoce como la pila de protocolos de Internet

Este modelo es solamente conceptual. En la vida real existen protocolos que uno puede asociar a determinada capa, pero que ejecutan servicios asociados a capas inferiores o superiores.

**Capa de aplicación**

En esta capa residen las aplicaciones distribuidas y los protocolos de aplicación. Computadoras utilizan los protocolos de esta capa para intercambiar paquetes de información entre sí. A estos paquetes se les conoce como *mensajes*.

**Capa de transporte**

Capa de red que transporte mensajes entre los endpoints de una aplicación. A los paquetes de información generados en esta capa se les conoce como *segmentos*.

**Capa de red**

Capa responsable de trasladar paquetes generados en ella, conocidos como *datagramas*, entre hosts. Supuestamente, en esta capa es determinado el camino que debe seguir un paquete para llegar a su destino.

**Capa de enlace**

Capa responsable de enrutar un datagrama entre cualquier par de routers entre su origen y destino. Entre router y router, estos datagramas se convierten en *frames*.

**Capa física**

Capa responsable de mover los frames entre los componentes de una red, bit a bit.

**Encapsulación**

Los dispositivos que existen en el Internet implementan varias capas de la pila de protocolos que expusimos anteriormente. Algunos implementan más capas; otras, menos. Un concepto importante en el Internet es el de *encapsulación*. Esto es, como fue sugerido en la descripción de las capas anteriormente, un proceso mediante el cual agregamos más información a un paquete de datos a medida que transversa las distintas capas. Un mensaje se convierte en un datagrama; un datagrama, en un frame y un frame es enviado bit a bit a través de un link. Por cada capa, el dispositivo *encapsula* el mensaje original, agregando más información.

En cada dispositivo de red a la que llega un paquete, este paquete recorre hacia arriba cada capa del modelo y, una vez procesado en la capa más superior, transversa hacia abajo la capa para acercarse a su destino o es procesado inmediatamente por la computadora destino. Supuestamente, este paso adicional -el de recorrer las capas hacia arriba- es necesario para el dispositivo receptor del frame. Con las añadiduras que fueron agregadas en el mensaje, el dispositivo receptor logra determinar hacia dónde debe enviarlo.

**Tipos de ataque a las redes hoy en día**

* **Malware oculto entre los datos descargados desde el Internet**. El malware se replica a sí mismo: una vez que infecta un host, busca infectar a otro. Un malware también puede incluir un host en una red de bots, una *botnet*, que soporta ataques DOS y envío de spam.
* **Ataques a los servidores e infraestructura de red**. Un conjunto extenso de amenazas de red es conocido como ataque DOS o *denial-of-service*, donde dispositivos de red, hosts o redes en sí se hacen inutilizables por sus usuarios legítimos. Los ataques DOS se clasifican en *ataques a vulnerabilidades (vulnerability attacks)*, *inundación de ancho de banda (bandwidth flooding)* e *inundación de conexión* *(connection flooding)*.

Un ataque a vulnerabilidades consiste en escribir mensajes maliciosos a aplicaciones vulnerables. Si una secuencia correcta de mensajes es enviada al host de la aplicación, puede detener el servicio que ofrece o crashear al host.

Una inundación de bando de ancha consiste en enviar un gran número de paquetes hacia un host. El atacante envía tantos paquetes que bloquea el enlace de la red de acceso, evitando que paquetes de usuarios legítimos alcancen al servidor

Una inundación de conexión consiste en crear un gran número de conexiones TCP entre el atacante y el host.

* **Detección de paquetes**. A través de una pieza de software un atacante puede crear una copia de paquetes enviados en una red para analizar si contienen información confidencial como contraseñas, mensajes privados, entre otros.
* **Atacantes pueden crear paquetes falsos**. Un paquete falso no es más que un paquete creado por un atacante con información hecha a mano sobre su origen, contenido y destino. Al proceso de crear paquetes y enviarlos al Internet con una dirección falsa de origen se le conoce como *IP spoofing*