Redes I

Resumen Primera Parte

Emiliano Salvatori

Agosto 2019

1. Clase 1

¿Qué es una Red? Una Red de Computadoras es un grupo un grupo de de computadoras/dispositivos interconectados. El conjunto (computadoras, software de red, medios y dispositivos de interconexión) forma un sistema de comunicación. Cuyo **objetivo principal** es el de compartir recursos (dispositivos, información, servicios).

¿Qué es internet?: es una red de computadoras que interconecta millones de dispositivos de cómputo, denominados Hosts. Los host están interconectados mediante Enlaces de Comunicación, los cuales pueden ser: fibra, cobre, radio, satélite. Existen también dentro de esta red, dispositivos que tienen la tarea de reenviar paquetes y son los Routers/Switches. La gestión de Internet se realiza mediante conmutación paquetes.

Las aplicaciones de usuario, se ejecutan en los sistemas terminales y no en los routers.

Protocolo: se define como un conjunto de reglas que establece:

- El formato y el orden de mensajes entre entidades de la red.
- Las acciones tomadas al transmitir o recibir mensajes.

En internet las entidades que desean comunicarse deben ejecutar el mismo protocolo (al igual que dos personas que se quieran comunicar entre si, deben hablar un mismo lenguaje).

Todas las actividades en internet están gobernada por protocolos. Algunos ejemplos de protocolos son: HTTP, SMTP, FTP, IP, TCP, UDP, PPP, Ethernet, Wifi.

Cada protocolo se ejecuta en distintas capas, en el modelo OSI, por ejemplo:

- **Capa de Aplicación**: Se ejecutan los protocolos SSH, DNS, FTP, SMTP, HTTP, DHCP, y otros.
- **Capa de Transporte**: Se ejecutan TCP, UDP, ICMP, FCP, y otros.
- **Capa de Internet**: Se ejecutan IP, ICMP, IPSEC, y otros.
- **Capa de Red**: ARP, Ethernet, Wifi, entre otros.

2. Clase 2

Componentes de la Red

Frontera de la red: dispositivos que estan dentro de una red, como pueden ser: hosts, aplicaciones, o Redes de acceso. Los hosts pueden ser tanto pcs, como celulares, camaras webs, Gps, es decir, todo dispositivo que pueda correr aplicaciones como servicios webs, mail, chats, etc.

Redes de acceso: Red formada por nodos de tipo routers. Todos los nodos interconectados se denominan nucleo de red. Red local formada por varios dispositivos. Si se quiere que tenga acceso a internet, se debe llegar a las demas redes, es decir a un nodo que de acceso a internet. Es como se conectan la red a internet, se conecta la red al resto del nucleo. Por ejemplo, cuando se conecta una computadora mediante cable. Puede que exista una red aislada sin conexión a internet, pero para que se conecte a internet será necesario que esta red se comunique con un nodo de acceso.

Nucleo de la red: todos los disipotitivos que interconectan los hosts: ruters, switchs, etc. Se denominan a los nodos interconectados de la red, es lo que se puede ver como la malla de routers interconectados en alguna imagen satelital. Los datos se transfieren a través de la red de dos formas:

- **Conmutación de circuitos**: Es un circuito dedicado por cada "llamada", la cual al establecerse una comunicación se reservan recursos de la misma y se dedica exclusivamente a los host en comunicación.

- **Conmutación de paquetes**: Son datos enviados a través de la red en bloques discretos. Es así como se comunican la gran mayoría de programas que corren en la Capa de Aplicaciones.

Recordar que también existen redes que no estan conectados a internet, sino interconectados con sus propios sistemas mediante redes internas: por ejemplo la red de Carrefour. A esta red se denomina intranet.

Diferencia entre LAN e Internet: LAN confinada a un lugar físico reducido. Se puede tener un red de área local distribuida en todo el mundo; puede ser utilizada toda la infrastructura de internet. Se puede tener una intranet a lo largo de todo el mundo, no interconectada con internet, sino simplemente interconectada con su propia red interna. PREGUNTAR

¿Qué es lo que uno paga cuando accede a internet?

Para conectarse a internet es necesario conectarse a un nodo que permita la conectividad a la red de redes. Los proveedores de internet permiten realizar esto. Por lo tanto, se cobra el acceso, pero no la navegación.

¿Cómo se hace para conecar a un nodo disponible?
Se requieren de 2 cosas:

- El nodo en sí mismo.
- Tener la infraestructura para poder conectarme al nodo.

2.1. ISP

Hay empresas que generan nodos, invierten en infrastructura y brindan el servicio de conección al nodo: empresas denominadas **ISP**. Lo que cobran es el enlace de un hogar hasta el nodo y el ancho de banda que uno contrate, que vendría a ser como una especie de "peaje".

El ancho de banda es algo que se contrata e incide en el precio, ¿por que? Por los gastos que debe destinar la empresa por otorgar esos recursos. Cuanto mas alto es el servicio que se contrata, más es la inversión que la empresa debe destinar a otorgarlos.

Ancho de subida y bajada: el servicio NO todas las veces es simétrico. Esto es porque en algunos servicios se requiere que sea asimetrico y en otros no, dependiendo del negocio que se tenga en mente para consumir ese servicio. Por ejemplo una corporación que tiene una pagina web que requiere mucha banda de subida, para que se conecten muchos usuarios. En cambio si es para consumo hogareño en los años 90 sólo se requiería que tenga mucho ancho de bajada, ya que no se solía subir contenido a la red, sino simplemente descargar. Este tipo de servicio era el ADS cantidad de información, Hoy en día no es tan asimetrico por el uso de las redes sociales, streaming online, donde el ancho de banda si requiere que sea asimetrico.

2.2. Infraestructura para internet

Cuando se fue haciendo cada vez más necesario brindar el servicio de internet, surgió el siguiente interrogante: ¿Cómo se puede conectar a Internet? Se debería basar en una infraestructura ya establecida, por eso se eligió la telefónica. Se usaba esa infraestructura de tendido telefónico, pero había que transformar la información para que viaje a través un medio utilizado para voz, se debía transformar un medio de voz a otro que permita la tranmisión de paquetes (señales) de ahí viene el modem.

Los primeros Modems fueron bastante rudimentarios por lo que transmitía en la misma frecuencia que la voz y en el mismo canal. Por lo que NO se podía hablar y establecer una comunicación de red (conectar a internet) al mismo tiempo. Modem permitía bajar 56kb. No se podía estar siempre .ºnline.es decir que esté siempre conectado a internet, se cobraba como una llamada telefónica cada vez que se conectaba; Para ello se establecían tarifas dependiendo el horario de uso. Luego surgió la **banda ancha** donde el servicio permitía estar todo el tiempo conectado, por lo que no se paga por esa característica, sino por el ancho de banda que se contrata, que se le asigna al usuario. Como por ejemplo el celular que esta todo el tiempo conectado a internet. Si se cobrara por la conexión sería un costo muy alto.

Se comienza a saturar la línea telefónica por lo que en 1998 se utiliza otro sistema. Se pensó no tranmitir en la misma frecuencia, por lo que se separó el rango de voz por un lado y la de datos por otro lado. Se tenía Tres canales: voz, subida de datos y bajada de datos. Ahora si permite estar todo el tiempo conectado. Lo que permite también incrementar la velocidad de transpaso de información. Pero es aún asimétrico. La voz sigue siendo analógica, hasta hoy en día, es decir que no se transporta en datos como los paquetes de internet. Los datos se digitalizan desde que son trasmitidos desde el host.

Fibra optica: son altas las velocidades, se puede hablar por teleféno sin interrupción. El medio por el que se transmite se denomina çable par trenzadoz tiene limitaciones por la cantidad de los datos que puede transmitir. Si se tiene una empresa donde no llegue el cable, la misma puede pagar el sanjeo y la infraestructura que se requiere para el tendido, etc y las empresas proveedoras dan el servicio. En campos muy alejados se utilizan

antenas; es decir: fibra optica hasta el nodo más cercano y desde ahí antena. Se taza por ancho de banda, no por usuarios.

Junto con la Fibra optica se provee el servicio denominado *Tripe Play* que vendría a ser: telefonia, internet y cable. Fibertel y Movistar da este servicio.

Cable coaxial: era un tipo de cable que se utilizaba para transmitir señales de canal, y ya que se tenía la infraestructura tendida y dadas sus características, se pensó un sistema para poder brindar internet. Infraestructura de cable para brindar internet. Se desarrolló la fibra optica la cual tiene mayor capacidad, pero es más cara, debido a que su tendido y su mantenimiento; es más complicado el tendido del cable, se debe realizar por debajo de la tierra, se requiere mucha infraestructura para manternerlo. Su capacidad hoy en día está casi saturada, por lo que se está ofreciendo fibra óptica. El cambio de coaxial a fibra óptica no es instantáneo según el profesor debido a un tema de costos y de seguir amortizando el tendido coaxial; "mientras dure el coaxial, se seguirá utilizando ese".

HFC: es un hibrido entre cable coaxial y fibra optica. Los nodos se interneconectan por fibra optica pero el cable que llega hasta la casa del usuario o empresa se hace mediante cable coaxial.

2.3. División de la parte física

En el cable Coaxial viajan muchas frecuencias superpuestas pero discriminándose,por los canales en los que viaja. Cada usuario utiliza cierta cantidad de canales según lo que paga. Por ejemplo, cuando un usuario tiene contratado 10 megas tiene más canales que uno que tiene 3. A la entrada de cada hogar se instala un objeto que diferencia las distintas frecuencias tanto para telvisión, servidores, computadora, etc. Si se paga internet pero no cable, en los canales dedicados al cable no se transmite nada, lo que se hace es poner un filtro de frecuencia para que no pase el cable. Fibertel no sabe cuando el cable está siendo utilizado de forma pirata, sirviéndose del único medio para saberlo el cual es un técnico, pero sí es posible que sepa cuando se está conectado a internet de forma ilegal por la transferencia de datos; cuando se utiliza el canal del cable como sigue transmitiendo entonces no se puede establecer si existen datos transfiriéndose o no, pero cuando se conecta a internet al haber transporte de datos esto indica a la empresa si se está utilizando por los paquetes transmitidos. ADSL no es compartido, va directo a la central, el HFC si es compartido entre todos los usuarios (si está correctamente dimensionada tiene mayor conexión).

El acceso en instituciones grandes se realiza mediante una conexión al nodo donde se conectan varios dispositivos, como por ejemplo en la UNAJ. Todos los dispositivos están interconectados denominandose *red LAN*. Cuando se tiene una empresa, que quiere tener mayor velocidad, privacidad, etc, es posible tener un cable de fibra óptica hasta el nodo de la empresa servidora/proveedora. Para ello existe servicios corporativos exclusivos para empresas que pueden costear esos precios.

2.4. Tipos de redes

Redes de acceso inalámbrico: se require un access point (router wifi), cuando se conecta a eso se conecta a internet simpre que tenga un punto de acceso.

Red de area amplia (WAN): redes de acceso que cubren áreas grandes, como por ejemplo el área de telefonia celular. Cuando me conecto al paquete de datos, se conecta al area de red de area amplia. Cuando habilita wifi, habilita la red inalambrica.

Como anotación una red *Wimax* permite un acceso a internet donde se esté (calle u hogar) como si fuera una red de accceso de area amplia pero por wifi, pero para los usuarios que paguen el servicio.

WiMAX, siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas), es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,5 a 5,8 GHz y puede tener una cobertura hasta de 70 km. Es una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio. El estándar que define esta tecnología es el IEEE 802.16 MAN. Una de sus ventajas es dar servicios de banda ancha en zonas donde el despliegue de cable o fibra por la baja densidad de población presenta unos costos por usuario muy elevados (zonas rurales). [1]

WAM (sacado de internet): Una red de área amplia o Wide Area Network (WAN) se usa para vincular sistemas de redes más pequeñas. Las redes que deben conectarse están muy separadas en este caso. Por ejemplo, conectar las redes de área local (LAN) de servidores, ordenadores e impresoras de los distintos campus de una universidad.

Los WAN existen en diferentes tamaños. Esto abarca desde conexiones entre diferentes departamentos del ayuntamiento hasta la conexión de una estación base para controlar una red 4G nacional. Incluso cuando la comunicación se realiza de forma intercontinental, se hace a través de WAN. Por ejemplo, de esta manera, una

[1] https://es.wikipedia.org/wiki/WiMAX

empresa española puede ejecutar su sistema de gestión documental o ERP en un servidor dentro de la misma WAN en los Estados Unidos. [2]

Red de area reducida (LAN): servicio para comunicar poca cantidad de usuarios en un area reducida. Una red de área local o LAN (por las siglas en inglés de Local Area Network) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio. [3]

En las Redes caseras el modem adapta la señal al cable coaxial con el cable de red (explicado mas arriba). El modem negocia con la central a la hora de conectarse a internet, en qué frecuencia estará transmitiendo. También se requiere un router para comunicar la red de area local (para conectar varias computadoras) y la conexión entre la conexión del proveedor. Si en vez del router pongo una computadora, esta se conecta directamnete con la la red externa y se visualiza como una única conexicón. Pero si se quiere comunicar muchos dispositivos y varios usuarios se requiere otro tipo de conexión donde intervienen los siguientes elementos:

- Modem.
- Ruter.
- Switches.
- Access point.

La estructura en épocas anteriores era la siguiente:

- Como primer paso lo que primero entra en el hogar sería un cable coaxial (en el caso más generalizado). Esto sería la Red número 1 del exterior.
- A partir del cable proveniente desde el exterior se conecta a un router el cual provee UNA sola conexión para un Host (Red número 2 del interior).
- Para poder conectar varias computadoras con este tipo de instalación era necesario instalar un switch o centro de estrella a varios host. Como se puede ver, la conexión que proveía el ISP de nivel 3 era para una red doméstica y el Router establecía la conexión entre 2 redes (la que provenía del exterior y la que proviene del interior de la casa). El switch es una boca que tiene varios canales para establecer conexiones cableadas (como el reverso del modem hogareño).
- Algunos conectores estrella venían provistos de un Access Point el cual permitía establecer conexiones de tipo wifi.

Con las tecnologías de hoy, las empresas vieron que desarrollar en una misma unidad los 4 componentes juntos era mucho más rentable y se tenía mayor control de las conexiones establecidas. Los modems de ahora vienen con Modem, Route, switch y un access point todo integrado. Antes sólo venía el modem y sólo un acceso para un host, para establecer más conexiones eso se compraba un router que venía con switch y con un access point (pero era más económico construir todo en uno), pero su configuración era responsabilidad del usuario, ya que la empresa proveía conexión para una sola computadora.

2.5. Organización de Internet a nivel mundial

Los que generan los nodos de interconecxión son los ISP. Todas las redes son iguales pero los ISP NO, tienen 3 niveles:

- **ISP nivel 1**: generan nodos de interconexión y se conectan entre si. Por ejemplo que cada ISP ponga nodos para conectar entre países. Los enlaces para ello debe tener mucha infraestructura, mucha inversión; conectan muchas regiones muy distantes. Conectan continentes. Le brindan enlaces a los otros agentes que se conocen como ISP nivel 2.
- **ISP nivel 2**: son los encargados de distribuir conectividad en otras areas más chicas que la ISP 1, por ejemplo distrubuyendo conexión entre provincias (son regiones más chicas que un país). Tienden conexiones de fibras y también satelitales. Ejemplo de algunas empresas de ISP 2: Telecom (Telefonica), Telmex (Claro). Hay que tener en cuenta que algunas empresas como Telecom en algunos países trabaja como ISP 2 y en otros países como ISP 1.
- **ISP nivel 3 (ISP locales)**: son las empresas que toman los nodos que están en las ciudades/proinvicias y las distribuyen a usuarios finales. Los ISP 3 también estar interconctadas entre ellas (como los ISP 1 y 2). Ejemplo de algunas empresas de IPS 3: Fibertel, Speedy, Telecentro, Claro. (casi siempre dueños de ISP2).

[2] https://www.ticportal.es/glosario-tic/wan-red-area-amplia
[3] https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local

Hay que tener en cuenta que en Argentina por lo menos, entre distintas empresas se contratan servicios entre ellas, por ejemplo ¿para qué tender 2 cableadas en una misma zona? Se contrata el servicio de ese tendido a la empresa propietaria y listo; por lo que no existe competencia entre empresas para poder mejorar el servicio de cara al usuario.

Arsat: Es una empresa estatal de ISP nivel 2 cuya conectividad la brinda mediante satelites que proveen enlaces. Si Argentina no los tuvieran deberían de contratar ese servicio a otas empresas, con los satelites también se vendían a otros países el servicio (Paraguay, Bolivia, Chile). Al ser del Estado, se dedicaba a tirar enlaces que no eran necesarios como medio para obtener ganancias pero si otorgaban como calidad de vida en otras ciudades como país federal.

Arsat llega hasta la entrada de un determinado pueblo por ejemplo y debe haber un operador que luego la distrubuya. A diferencia de otros ISP 2 que no son del Estado, estos pueden tender su infraestructura donde le conviene, donde sepa que va a obtener ganancia. Algunas corporaciones grandes contatan servicios directamente con el ISP 2 y no a traves de la Empresas de tipo 3.

2.6. El modelo de capas de Internet

El modelo de capas empleado para entender Internet, para poder abarcarlo y comprenderlo se denomina TCP/IP. Las capas es un modelo para entender la red física, es un marco teórico para que los individuos puedan hacer el sistema lo mas versátil posible. Se requiere una estructura para poder establecer la relación entre ellas, para ello se requiere la modularización. Cada capa se comunica con la misma capa indpendientemente de las demás. Este modelo ayuda tanto para los usuarios, estudiantes, empresarios, y demás personas.

Modelo OSI: modelo de referencia general de comunicación y más completo. Pero en la jerga siempre se utiliza el modelo de 5 capas explicado en las filminas. Modelo OSI es de referencia. El TCP/IP pero se aplica a algo real que son las redes de datos y está basado en el OSI.

Si no se siguieran estos modelos sucedería lo que antes, donde cada fabricante hacía su propia red y para interconectarse era basante difícil; en cambio si se toma como modelo de TCP/IP es más fácil de relacionarla.

1. Capa de Aplicación
2. Capa de Transporte
3. Capa de Red
4. Capa de Enlace de datos
5. Capa física.

Cada uno ofrece determinados servicios dependiendo la capa. El ejemplo provisto por la cátedra es la de un servicio de avión: Para poder abordar el problema se puede hacer más fácil dividiéndolo en capas. Cuando se compra el pasaje por ejemplo se determina en determinada capa, las maletas para otra capa, la pista de despegue y navegación lo administra otra capa, y así sucesivamente.

Otra característica a tener en cuenta es que cada capa es transparente para todas las demas, cada capa no se entera de otras cuestiones ajenas a la propia capa; se trata de que si se modifica algo que pertenece a una capa no modificar todas las demas.

Se puede preguntar porqué 5 capas y no más. En caso por ejemplo que se tengan 100 capas, se dividen muchos problemas chicos no lleva a ninguna solución. Tener pocas capas quita el principio de dividir el problema, 5 son las que terminan balanceando el problema entre dividir y entender; además de que ese número fue establecido luego de varios estudios llevados a cabo por décadas, por lo que tiene un origen científico.

Lo que realizado por cada capa

Capa Aplicación: es la capa donde residen las aplicacione y sus protocolos. Ejemplo: el Skype de un host que se comunica con otro Skype de otro host. Skype no piensa en las otras capas, sólo en comunicarse con el otro usuario. Los protocolos más famosos son: FTP para transmitir archivos, el protocolo especifica cómo proceder cada vez que se envía un archivo; SMTP de correo, cuando se tansmite mediante ese protocolo no se transmite de forma arbitraria, sino como se especifica. Es por ello que se puede enviar mail entre distintos servidores como Yahoo y Gmail, porque ambos se comunican de la misma manera, con las mismas reglas.

Protocolo HTTP es el que va a enmarcar cómo se deben presentar las páginas webs, cómo se deben presentar las imágenes, el cuerpo que debe tener la página, qué pasa si me trato de conectar y la página está caída, etc. Muchas veces se utilizan dos protocolos al mismo tiempo como por ejemplo en *webmail* SMTP (quien levanta los mails) con HTTP (para ver la página web). Los paquetes acá se denominan mensajes, que son los que la capa transmitirá.

Capa transporte: es la capa encargada de la forma en como se transportan los mensajes. La capa provee dos tipos de Servicio: *Orientado a conexión(TCP) y servicio sin conexión (UDP)*. Los protocolos tienen determinada relación, dependiendo el servicio que la capa aplicación quiere dar; por ejemplo si la aplicación quiere enviar streaming utilizaría UDP, pero en cambio si quiere utilizar mensajes puede utilizar TCP. Notar que es la misma aplicación enviando datos mediante distintos protocolos según el servicio que se quiera brindar.

Capa Red: esta capa tiene como objetivo el ruteo de fuentes a destino. El Protocolo más conocido es el IP que es de enrutamiento. Aquí los los paquetes se llaman datagramas.

¿Qué es lo que hace esta capa? Asegurarse que los paquetes sigan una determinada ruta para que lleguen a destino. Se realiza una ponderación por el camino más corto que tiene en cuenta la cantidad de nodos por los que va a pasar : cantidad de saltos que se pueda tener. Se debe generar un protocolo que se estime la cantidad de saltos que debe hacer. Es lo que se hace en la capa de red, es parte de lo que hace el protocolo IP; dentro del protocolo IP hay varios algoritmos que pueden determinar este tipo de caminos.

Capa Enlace: esta capa se encarga de la transferencia de los paquetes de la capa de red entre nodos vecinos. En la de enlace lo que hace es establecer el enlace entre los nodos del camino establecido por la capa de Red. La independicia de capas sirve par que en caso de que se cambie un enlace por ejemplo en el camino, no importa para la capa de red, solo le es pertinente para la de enlace. Aqui los paquetes se llaman tramas. Protocolos propios de esta capa: PPP, Ethernet, Wifi

Dispositivos por capas

Cada dispositivo puede procesar cierta capa, por ejemplo el modem que es de capa física no puede correr un protocolo de enlace.

Los dispositivos de la capa de abajo NO pueden interpretar los de arriba, pero los de arriba SI pueden interpretar los de abajo suyo (Se puede ver mejor los hardwars que soportan según la capa donde opere en la filmina). Porque la información debe pasar por esas capas y por lo tanto lo debe saber interpretar.

Transferencia de datos mediante las distintas capas

¿Cómo se hace para correr los procotoclos y que cada capa cumpla su objetivo? La primer capa toma el dato que quiere mandar, por ejemplo una palabra, por ejemplo, el dato es "Hola". La capa de aplicación le agrega un encabezado donde se determina algo para ser interpretada en la capa de aplicación del destinatario, como por ejemplo el destinatario al que se quiere enviar, su mail, el tipo de mensaje, etc. Le agrega su encabezado y se la pasa a la capa de transporte, ésta lo toma y entiede el mensaje "Holaƶ el encabezado de la capa de aplicación como si fueran datos, por lo que para esta capa todo lo proveniente de la de aplicación es dato, acto seguido lo que hace es agregarle su propio encabezado. Con ello se asegura la independencia de datos entre capas. Cada capa agrega su encabezado y toma como dato todos los encabezados de la capa inferior.

La capa física sólo entiende de ceros y unos. No le importa absolutamente nada, no distingue paquetes, lo único que hace es convertir todo eso de datos en señales. El switch sólo lee datos de capa de enlace por ejemplo. En cambio el router si puede trabajar sobre los encabezados de capa 3.

A la inversa llega el mensaje completo y cada capa le va sacando su propio encabezado para su propia capa, hasta que llegue hasta la capa de aplicación.

2.7. Clasificación de Red por cobertura

1. **LAN**: red de cobertura local (oficina).
2. **MAN**: red metropolitana.
3. **WAM**: cobertura de area amplia
4. **SAN**: redes de storgage, para almacenamiento
5. **PAN**: red que se requiere estar enfrente com la red de Bluetthoot

La red de distrubución geográfica no tiene mucho sentido. Por ejemplo la red de la UNAJ según los libros sería una MAN pero si se ve desde la organización se tomaría como como red LAN.

2.8. Entidades encargadas de los Protocolos

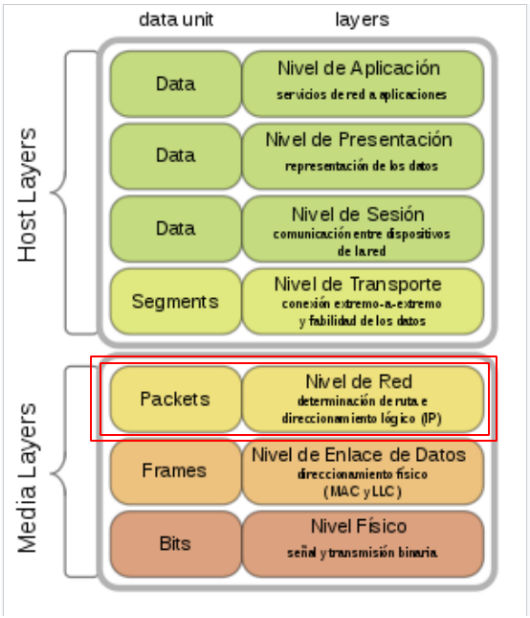
¿Quién se encarga de actualizar y hacer protocolos? Organizaciones desentralizadas, que sacan los protocolos y los organizaciones que fabrican hardware y sofrware se adaptan a ellos. Por ejemplo: ISOC, IAB, IETF (aplicar protocolos al corto plazo), IRTF (investigar los protocolos a largo plazo). IANA, encagarda de la asignaciones de recursos con respecto a las direcciones IP. Lo que hace es venderle segmentos enormes a los ISP nivel 1 que

a su vez particiona esas direciones y vende subdireciones más pequeñas a los ISP nivel 2, y asi hasta llegar al hogar.

DNS: Mantiene una tabla con la relación entre las direcciones de dominio con las direcciones IP. Cada vez que se conecta a una página web, se comunica con un DNS, este le devulve a través de un protocolo la dirección que 32 bits.

Clase nº 3: Capa de Red

Funciones claves



En esta capa, la unidad de datos se denomina: *Paquetes*.

La función de la capa de red : *es transportar paquetes desde un host emisor a un host receptor.* ¿Quiénes son los encargados de realizar este transporte de paquetes? El router a través de dos funciones claves:

- **Ruteo/Enrutamiento/Routing**: Determina una ruta de una punta a la otra, desde origen a destino. La capa de red tiene que determinar la ruta o camino que deben seguir los paquetes a medida que fluyen de un emisor a un receptor. Los algoritmos que calculan estas rutas se conocen como algoritmos de enrutamiento. Un algoritmo de enrutamiento debe determinar, por ejemplo, la ruta por la que fluirán los paquetes para ir de un Host situado en la ciudad/pais A, hasta otro situado en la ciudad/país B.
- **Reenvio/Forwarding**: Tiene que ver con lo anerior, es mover paquetes desde una entrada del router a la salida del mismo. Cuando un paquete llega al enlace de entrada de un router, éste tiene que pasar el paquete al enlace de salida apropiado.

Un paralelismo con lo anterior se puede poner cuando un usuario quiere realizar un viaje en auto por el país. Decidir la ruta que se tomará para llegar a determinada provincia desde la casa del usuario sería el *enrutamiento*. En cambio, llegado a una ciudad (que sería para el ejemplo como ser un router), decidir por qué calle tomar para dar con la ruta que me llevará al próximo pueblo sería el *reenvío*.

El reenvío hace referencia a la acción local que realiza un router al transferir un paquete desde una interfaz de un enlace de entrada a una interfaz del enlace de salida apropiada. El enrutamiento hace referencia al proceso que realiza la red en conjunto para determinar las rutas terminal a terminal que los paquetes siguen desde el origen al destino.

Para saber la mejor ruta los ruters corren algoritmos que van a determinar la mejor ruta para ir de un host a otro, una vez que terimna el algoritmo gnera una tabla de reenvio, esa tabla está conformada como si fuera un algoritmo de Dijkstra. Evalúa dándole determinado peso entre routers.

Todo router tiene una tabla de reenvío. Un router reenvía un paquete examinando el valor de un campo de la cabecera del paquete entrante y utilizando después ese valor para indexarlo dentro de la tabla de reenvío del router. El resultado de la tabla de reenvío indica a cuál de las interfaces del enlace de salida del router será reenviado el paquete. Dependiendo del protocolo de la capa de red, este valor de la cabecera del paquete podría ser la dirección de destino del paquete o una indicación de la conexión a la que pertenece el paquete

Una vez que el router pasa el paquete a otro, se olvida del paquete que envió. Si cada router corre el mismo algoritmo proporcionado por el protocolo que se ejecute,todos llegan a la misma conclusión de que la mejor ruta es una, y en base a ello es que se genera la tabla de reenvío; la problemática es que todos corran el mismo algoritmo y saber cuál usar.

Cada ruter corre el algoritmo, genera la tabla, determina la mejor ruta, envía los paquetes; los algoritmos se corren cada determinado tiempo, para que se actualice la tabla de ruteo; y todo esto se denomina *Ruteo dinámico*. *Ruteo estático*: es cuando se define vía hardware por dónde debe salir un paquete determinado.

En general lo que estiman a la hora de proveer una mejor ruta para los paquetes es la cantidad de nodos que hay en la red para generar la mejor ruta, evalúa la menor cantidad de saltos. Todo esto se conceptualiza mediante la teoría de grafos.

La ponderación de las aristas existentes a lo largo de una ruta es multidimensional, es decir que se tienen en consideración varias variables de distinta naturaleza, por eso que generalmente se simplifica por la cantidad de saltos que debe hacer el paquete.

Redes de Circuitos Virtuales y de Datagramas

La capa de transporte de Internet proporciona a cada aplicación la posibilidad de elegir entre dos servicios: UDP, un servicio sin conexión; o TCP, un servicio orientado a la conexión. De forma similar, la Capa de Red también puede proporcionar un servicio sin conexión o un servicio con conexión. Estos servicios de la Capa de Red con y sin conexión son paralelos en muchos sentidos a los servicios de la capa de transporte orientados a la conexión y sin conexión.

En las principales arquitecturas de redes de computadoras utilizadas hasta la fecha (Internet, ATM, frame relay, etc.), la capa de red proporciona bien un servicio sin conexión host a host o un servicio orientado a la conexión host a host, pero no ambos. Las redes de computadoras que sólo proporcionan un servicio de conexión en la capa de red se cono cen como **Redes de Circuitos Virtuales (VC)**; las redes que sólo proporcionan un servicio sin conexión en la capa de red se denominan **redes de datagramas**.

Redes de Circuitos Virtuales: es como realizar una llamada entre dos host. Esta conexión reserva recursos como si fuera una conexión telefónica. Hasta que no se corte la conexión entro los dos hosts, no cede los recursos que se adquirieron para la realización de la llamada.

Fases identificables en una comunicación de tipo VC.

- Establecimiento de la llamada.
- Transferencia de datos.
- Finalización de la llamada.

Luego:

- Cada paquete lleva un identificador del VC (no dirección de máquina destino).
- Cada router en el camino de fuente a destino mantiene el "estado" por cada conexión que pasa por él.
- Enlace y recursos del router (ancho de banda, buffers) pueden ser asignados al VC.

Por el contrario las **Redes Datagramas** (que es el que utiliza internet), a medidia que los paquetes van llegando, se envían. Un paquete puede enviarse por una for Esta no dice que no vaya a mostrar un paquete asincrónico, esto se ordenan en otra capa. En una Red de Datagramas, cada vez que un sistema terminal desea enviar un paquete marca el paquete con la dirección del sistema terminal de destino y luego introduce el paquete en la red. Esto se hace sin configurar ningún circuito virtual. Los routers de una red de datagramas no mantienen ninguna información de estado acerca de los circuitos virtuales (¡porque no existe ningún circuito virtual!).

A diferencia de las redes de VC, en las redes de Datagramas:

- Tx pone dirección dirección destino destino en la cabecera del datagrama.
- No hay estado mantenido en cada router por cada conexión.
- Los paquetes se reenvían usando la dirección del Host de destino.
- Los datagramas pueden ser transmitidos por diferentes

Se implementa en Internet Red de Datagramas, por una cuestión de uso y costumbre de la población, no significa que en un futuro se modifique la arquitectura a VC.

Como nota de color **QuS** es calidad de servicio, la cual es más fácil poder brindarla en servicios como VC que en Red de Datagramas ya que para la primera se reserva recurso para ofrecer una mínmia calidad. ¿Cómo se hace para brindar cierta calidad de servicio en Redes de datagramas que en VC? Es más fácil con VC. Como

en Datagramas los paquetes van por cualquier parte, es difícil reservar recurso, es difícil articularloas. Hoy en día esto no está implementado. Esto siempre está implementado en la capa de Red.

En algunas arquitecturas de redes, la capa de red cumple otra función decisiva que es la de *establecer una conexión virtual* pero esto es sólo en las **Redes de Circuitos Virtuales (VC)**.

Se establece un circuito y el canal será el mismo mientras se esté conectado. No se evalua todo el tiempo la tabla, sino que se mantiene la misma tabla mientras se mantenga la llamada.

En los circuitos virtuales, al comienzo de la sesión se establece una ruta única entre las ETD (entidades terminales de datos) o los host extremos. A partir de aquí, todos los paquetes enviados entre estas entidades seguirán la misma ruta. Las dos formas de establecer la transmisión mediante circuitos virtuales son los circuitos virtuales conmutados(SVC) y los circuitos virtuales permanentes(PVC).

2.8.1. Circuitos Virtuales conmutados(SVC)

Los circuitos virtuales conmutados (SVC) por lo general se crean ex profeso y de forma dinámica para cada llamada o conexión, y se desconectan cuando la sesión o llamada es terminada. Un ejemplo de circuito virtual conmutado es la red telefónica tradicional así como los enlaces ISDN. Se utilizan principalmente en situaciones donde las transmisiones son esporádicas.En terminología ATM esto se conoce como conexión virtual conmutada. Se crea un circuito virtual cuando se necesita y existe sólo durante la duración del intercambio específico.

2.8.2. Circuitos Virtuales Permanente(SVC)

én se puede establecer un circuito virtual permanente (PVC) a fin de proporcionar un circuito dedicado entre dos puntos. Un PVC es un circuito virtual establecido para uso repetido por parte de los mismos equipos de transmisión. El circuito está reservado a una serie de usuarios y nadie más puede hacer uso de él. Una característica especial que en el SVC no se daba es que si dos usuarios solicitan una conexión, siempre obtienen la misma ruta.

Red de circuitos virtuales: esto es en red. No distingue entre si se está comunicando por UDP o TCP. En la capa de transporte depende del protocolo, se comunica entre aplicaciones, En la capa de transporte SI tiene en cuenta si transporta UPD o en TCP, todo es a nivel procesos.

Los dispositivos finales los que saben si hay que retransmitir o no. Para la capa de RED le es indistinto, no está metido en el protocolo, sólo envía paquetes. En internet la Capa de Red trabaja SIN conexión (a diferencia de las Redes de circuitos virtuales), es decir que cuando se establece una conexión entre dos hosts, no se reservan recursos. Se diagrama de esta manera debido a la cantidad de usuarios y dispositivos conectados. Si esto fuera CON conexión, cada rotur deberá de decidir por la ida y vuelta depaquetes, por si hay que retransmitir o no, le pone mucha más complejidad que hace más densa el transporte. Por eso es prefierile que traminta sin conexión.

2.9. Modelos de Servicio de Red

Consideremos ahora algunos de los posibles servicios que podría proporcionar la capa de red. En el host emisor, cuando la capa de transporte pasa un paquete a la capa de red, entre los servicios específicos que la capa de red podría proporcionar se incluyen:

- **Entrega garantizada**: Este servicio garantiza que el paquete terminará por llegar a su destino.
- **Entrega garantizada con retardo limitado**: Este servicio no sólo garantiza la entrega del paquete, sino que dicha entrega tendrá un límite de retardo especificado de host a host (por ejemplo, de 100 milisegundos).

Además, a un flujo de paquetes entre un origen y un destino dados podrían ofrecérsele los siguientes servicios:

- **Entrega de los paquetes en orden**: Este servicio garantiza que los paquetes llegan al des tino en el orden en que fueron enviados.
- **Ancho de banda mínimo garantizado**: Este servicio de la capa de red emula el comportamiento de un enlace de transmisión con una velocidad de bit específica (por ejemplo, de 1 Mbps) entre los hosts emisor y receptor (incluso aunque la ruta terminal a terminal real pueda atravesar varios enlaces físicos). Mientras que el host emisor transmita los bits (como parte de los paquetes) a una velocidad inferior a la velocidad de bit especificada, no se perderá ningún paquete y todos los paquetes llegarán dentro de un intervalo de retardo host a host pre-especificado (por ejemplo, en 40 milisegundos.)
- **Fluctuación máxima garantizada**: Este servicio garantiza que el intervalo de tiempo transcurrido entre la transmisión de dos paquetes sucesivos en el emisor es igual al intervalo de

CBR en ATM: El objetivo del servicio CBR es conceptualmente simple: proporcionar un flujo de paquetes (conocido como celdas en la terminología ATM) mediante un conducto virtual cuyas propiedades son las mismas que si existiera un enlace de transmisión de ancho de banda fijo dedicado entre los hosts emisor y receptor. Con el servicio CBR, un flujo de celdas ATM se transporta a través de la red de tal forma que se garantiza que el retardo terminal a terminal de una celda, la variabilidad del retardo terminal a terminal de una celda (es decir, el jitter o fluctuación entre celdas) y la fracción de celdas que se pierden o que se entregan tarde sean todos ellos menores que una serie de valores previamente especificados. El host emisor y la red ATM acuerdan estos valores cuando la conexión CBR se establece por primera vez.

ABR en ATM: Como con el modelo de servicio de Internet, las celdas se pueden perder con un servicio ABR. Sin embargo, a diferencia de Internet, las celdas no se pueden reordenar (aunque pueden perderse) y está garantizada la velocidad mínima de transmisión de celda (MCR, Mínimum Cell transmission Rate) de una conexión utilizando el servicio ABR. Si la red tiene los suficientes recursos libres en un instante determinado, un emisor también puede ser capaz de enviar con éxito cel das a una velocidad mayor que la mínima (MCR).

Se debe recordar que ATM da garantías de ancho de banda, de que no haya pérdidas en los paquetes y la indicación de congestión interna, pero **NO es la arquitectura utilizada en Internet** en la Capa de Red.

En la Capa de Red se puede implementar un protocolo de tipo UDP o de tipo TCP pero esto va en conjunto con su arquitectura, no es algo que se pueda modificar como lo hace la Capa de Transporte.

Cuando un paquete se transmite desde un origen a un destino pasa a través de una serie de routers. Cada uno de estos routers utiliza la dirección de destino del paquete para reenviar dicho paquete. Específicamente, cada router tiene una tabla de reenvío que asigna direcciones de destino a interfaces de enlace; cuando un paquete llega a un router, éste utiliza la dirección de destino del paquete para buscar la interfaz del enlace de salida apropiado en la tabla de reenvío. Después, el router reenvía intencionadamente el paquete a esa interfaz del enlace de salida.

2.10. Arquitectura de Routers

Dos funciones claves de routers:

- Correr algoritmos/protocolos de ruteo (RIP, OSPF, BGP), cada protocolo ejecuta su propoo algoritmo.
- Re-envío de datagramas desde enlaces de entrada a salida. No existe un router entrada o salida, en realidad pueden ser bidireccinales, se dice entrada y salida sólo por un tema de comprension.

Para el exámen del router se diagrama un esquema general de las distintas partes operante:

- **Puerto de Entrada** : El puerto de entrada realiza varias funciones. Lleva a cabo las funciones de la capa física consistentes en la terminación de un enlace físico de entrada a un router. Realiza las funciones de la capa de enlace de datos necesarias para interoperar con las funciones de la capa de enlace de datos en el lado remoto del enlace de entrada. También realiza una función de búsqueda y reenvío (el recuadro más a la derecha del puerto de entrada y el recuadro más a la izquierda del puerto de salida) de modo que un paquete reenviado dentro del entramado de conmutación del router emerge en el puerto de salida apropiado. Los paquetes de control (por ejemplo, paquetes que transportan la información del protocolo de enrutamiento) son reenviados desde un puerto de entrada al procesador de enrutamiento. En la práctica, suelen agruparse varios puertos en una única tarjeta de línea dentro del router. Depende el protocolo de la capa de enlace puede correr determinado servicios de la capa de enlace. Acá es donde según el protocolo puede corregir errores. Sirve como un filtro de error desde la entrada, para que no pase al router. En caso de que llegue un error se descarta desde el principo y no permite que pase a las subsiguientes partes del router.
- **Entramado de Conmutación**: Entramado de conmutación. El entramado de conmutación conecta los puertos de entrada del router a sus puertos de salida. Este entramado de conmutación está completamente contenido dentro del router. La Conmutación de paquetes: via memoria por bus del sistema. La rapidez del bus se mide según el ancho de bus que tenga, que se mide por megaherz. YA NO SE USA. Lo que se utiliza es el *Via bus*: un bus compartido, no puede habe más de un paquete por bus, de lo contrario se complica. De qué depende de que sea rápido o no un router, dependiendo de dónde se coloque, no es lo mismo un router un ISP nivel 2 que para una corporación. Conmutación via red de interconexión: Tipo crossbar: Todas las conexiones en simulanea. Se puede mandar multiples paquetes al mismo tiempo por lo que es más rápido y más eficiente. Pero también depende de lo que quiera manejar, para una empresa es muchísimo, si es para un ISP 1 quizás es poco.
- **Procesador de enrutamiento**: Procesador de enrutamiento. El procesador de enrutamiento ejecuta los protocolos de enrutamiento, mantiene la información de enrutamiento y las tablas de reenvío y realiza funciones de gestión de red dentro del router.

- **Puertos de Salida**:Un puerto de salida almacena los paquetes que le han sido reenviados a través del entramado de conmutación y los transmite al enlace de salida. Así, el puerto de salida lleva a cabo la función inversa de la capa física y de la capa de enlace de datos que el puerto de entrada. Cuando un enlace es bidireccional (es decir, transporta tráfico en ambas direcciones), un puerto de salida del enlace normalmente estará emparejado con otro puerto de entrada de dicho enlace en la misma tarjeta de línea.

- **Buffer**: pone los paquetes en una cola a medida que llegan. Dada la dirección destino del datagrama, se obtiene el puerto de salida usando la tabla de re-envío de la memoria del puerto de entrada. El Objetivo es que el procesamiento se realice en el puerto de entrada a la velocidad de la línea. Esto quiere decir que necesita que sea continuo, dinámico, antes de que llegue, posicionar la línea para enviarlo. Se puede ver la linea como un carril de un tren, y al tren como la ráfaga de paquetes a enviar, antes de ser enviado por determinado carril (línea) es necesario que evaluar el destino del tren (paquetes) y modificar los carriles según sea que vayan.

Se formará cola si los datagramas llegan más rápido que la tasa de re-envío de la estructura de switches. Esto quiere decir que el conmutar la vía por donde saldrán los paquetes si es mas lento que lo que entra, se comienza a encolar, por loque se tiene dos posiblidads o buffers muy grandes, o muy chicos. Lo que se tiene que tener en cuenta es dimensionar bien el buffer,

Conmutación via red de interconexión: Tipo crossbar, todas las conexiones en simulanea. Se puede mandar multiples paquetes al mismo tiempo por lo que es más rápido y más eficiente. Pero también depende de lo que quiera manejar, para una empresa es muchísimo, si es para un ISP 1 quizás es poco.

Tabla de Reenvio: La tabla de reenvío es el producto de accionar los algoritmos de Capa de Red en cada Router. Se generan a través de dos campos que contiene la dirección destino y las interfaz por la que se enviará el paquete en caso de coincidir la dirección de envío con el de la cabecera del paquete. Las direcciones posibles son 2^32 bits, por lo que se obtienen mas de millones de 4 mil millones de entradas; cantidad imposible de mantener una tabla y que cada router por cada paquete tenga que recorrer esas millones de direcciones para saber hacia dónde debe enviar la información. Por lo que se implementa de una manera más sencilla. Cada Router, dependiendo el nivel al que pertenezca (router ISP 1, 2 o 3) manejará distintos rangos de direcciones. Si el paquete recibido tiene una dirección comprendida entre un rango y otro, se enviará por la interfaz 1, si está comprendido entre otro rango, se enviará por 2,etc.

Dependiendo del nivel del ISP seran los rangos que manejará la tabla del router. El paquete va pasando por routers que tienen distintos rangos, desde los rangos más generales (ISP 1) hasta más locales (ISP 3).

Por ejemplo: Si se quiere enviar un paquete de datos a Australia, lo que se hace al despachar el paquete es mirar el bloque más significativo de la dirección destino, lo que hace que se rediriga a un router que tiene conexión con otro continente (ISP 1), una vez que el paquete llega allí, se vuelve a analizar el paquete evaluando su rango, en caso de estar ya en Australia, entonces lo toma un Router ISP 2, el cual lo vuelve a lanzar a la zona geográfica perteneciente a ese rango para que lo tome otro router ISP 1 que lo envía a una zona más localizada, como puede ser una conexión hogareña.

En el siguiente ejemplo se puede ver cómo dependiendo de los últimos 3 dígitos, se envía a una interfaz o a otra.

- 11001000 00010111 00011**000** : Se envía hacia la interfaz nº 1

- 11001000 00010111 00011**001** : Se envía hacia la interfaz nº 2. Ver que a partir del rango 001 se envía a esta interfaz.

- 11001000 00010111 00011000: Por ejemplo, el siguiente es un rango y no una dirección ya que falta el último octeto

Pregunta: ¿por qué no mantiene la misma cabera que se entregó? La capa de enlace se encarga de enviar de host a host, por lo que el enlace pueden llegar a cambiar, y cambian los protocolos, pero desde elpunto de visa de la Capa de Red, al ruter no le importa, lo envia igual.

¿Por qué se necesita un buffer en la entrada y en la salida? Es por el cambio de velocidad de transmisión, es para balancear los paquetes. Puede haber mayor capacidad de procesamiento pero en la salida puede existir menor capacidad de velocidad de envío en el enlace.

Encolamiento en puerto de entrada: Ver la problemática que hay con el paquete rojo (Filmina nº 34) para un lugar determinado, si hay muchos rojos para una misma salida y una entrada quiere enviar a esa misma salida un paquete rojo, lo detiene y se encolan no sólo el rojo sino el verde también.

Para ello se implementan lo que se denomina como *Políticas de descarte y envío*:

- **Primero que llega primero que envía**: Colas podnderadas equitativas, se distribuya mejor el gráfico entre medio. Se reparte el gráfico.

- **Descarte al ingresar a la cola**: El que se queda fuera, se descarta. Otra forma, RED: a deerminados paquetes se marcan para eliminarlo, ¡¿con qué criterio? Bueno se hace una ponderación para cada uno de los usuarios si es que procesa muchos paquees y otro usuario se envía 1 paquete , para que no quede afuera este último usuario lo que se hace es eliimnar los paquetes marcados previamente para el usuario A.

3. Clase nº 4

3.1. Repaso clase nº 3

Objetivo de la capa de Red:

- Transportar segmntos de un lado a otro. Función principal: conectar un host a otro. Realizar una comunicación entre host, lo hace a traves del routeo y el reenvío.
- Ruteo: determinar la mejor ruta para llegar de host a host
- Reenvio: mover los paquetes de un enlace a un enlace.

Internet se utiliza la red de datagrama. NO se basa en una ruta fija, sino que la ruta varía, y los paquetes puden tomar distintas rutas sin importar el orden en que lleguen; de la organización y sincronización de los paquetes se encarga otra capa. La red virtual determinaba una conexión establecida y fija y se asemeja a la del teléfono.

3.2. Esquema de IP en TCP/IP

El protocolo que más se usa es el IP, es el más importante en la capa de red, por el nombre del modelo. Cada protocolo es independiente a las anteriores capas, sin embargo IP obtiene información de otras capas para mejor sus servicio, aún así trata de ser lo más indpendiente posible.

En la tabla de reenvío de los routers, las direcciones que la componen están basadas en el protocolo IP.

3.3. Formato del datagrama

Cada capa le agrega un encabezado y encapsula todo lo demás, proveniente de otra capa como un dato más. Y cada capa le pone su propio encabezado, en este caso el de red.

El *Encabezado de Red* se puede ubicar en la filmina nº 5. Lo que se denomina como *Data* en la estructura del datagrama, es información que proviene de las demás capas.

- **HaeadLen / Longitud de Cabecera**: Puesto que un datagrama IPv4 puede contener un número varia ble de opciones (las que se incluyen en la cabecera del datagrama IPv4), estos 4 bits son necesarios para determinar dónde comienzan realmente los datos del datagrama IP. La mayoría de los datagramas IP no contienen opciones, por lo que el datagrama IP típico tiene una cabecera de 20 bytes.
- **Tipo de servicio**: Los bits del tipo de servicio (TOS, Type of service) se incluyeron en la cabecera de IPv4 con el fin de poder diferenciar entre distintos tipos de datagramas IP (por ejemplo, datagramas que requieran en particular un bajo retardo, una alta tasa de transferencia o una entrega fiable). Por ejemplo, puede resultar útil diferenciar datagramas en tiempo real (como los utilizados en aplicaciones de telefonía IP) del tráfico que no es en tiempo real (como por ejemplo el tráfico FTP). El nivel específico de servicio que se proporcione es una política que determinará el administrador del router.
- **Longitud del datagrama**: Es la longitud total del datagrama IP (la cabecera más lo datos) en bytes. Puesto que este campo tiene una longitud de 16 bits, el tamaño máximo teórico del datagrama IP es de 65.535 bytes. Sin embargo, los datagramas rara vez tienen una longitud mayor de 1.500 bytes.
- **Fragmentación del datagrama**: La capa de red determina la ruta y es el encargado de fragmentar el datagrama, en función de los MTU de los enlaces. Básicamente, Un datagrama se convierte en varios. Se debe saber cómo fragmentarlo. Acá no hace faltan que lleguen seguidos los datagramas fragmentados. Cada uno es un datagrama individual. También puede que al haber mas MTU puede tomar 3 datagramas y juntarlos en uno. Si se cambia el tipo de medio, el cable por ejemplo se modifica el MTU y por lo tanto esta capa permite diversificar y adaptarse a la red.
- **Tiempo de vida**: El campo Tiempo de vida (TTL, Time-To-Live) se incluye con el fin de garantizar que los datagramas no estarán eternamente en circulación a través de la red (debido, por ejemplo, a un bucle de enrutamiento de larga duración). Este campo se decrementa en una unidad cada vez que un router procesa un datagrama. Si el campo TTL alcanza el valor 0, el datagrama tiene que ser descartado.

- **Protocolo**: Este campo sólo se emplea cuando un datagrama IP alcanza su destino final. El valor de este campo indica el protocolo específico de la capa de transporte al que se pasarán los datos contenidos en ese datagrama IP. Observe que el número de protocolo especificado en el datagrama IP desempeña un papel análogo al del campo que almacena el número de puerto de un segmento de la capa de transporte. El número de protocolo es el elemento que enlaza las capas de red y de transporte, mientras que el número de puerto es el componente que enlaza las capas de transporte y de aplicación.

- **Suma de comprobación de cabecera**: La suma de comprobación de cabecera ayuda a los routers a detectar errores de bit en un datagrama IP recibido. Esta suma de comprobación se calcula tratando cada pareja de 2 bytes de la cabecera como un número y sumando dichos números utilizando aritmética de complemento a 1. Un router calcula la suma de comprobación de cabecera para cada datagrama IP recibido y detecta una condición de error si la suma de comprobación incluida en la cabecera del datagrama no coincide con la suma de comprobación calculada.

- **Direcciones IP de origen y de destino**: Cuando un origen crea un datagrama, inserta su dirección IP en el campo de dirección IP de origen e inserta la dirección del destino final en el campo de dirección IP de destino. A menudo el host de origen determina la dirección de destino mediante una búsqueda DNS. Las direcciones son de tipo IP. Para una mejor lectura humana se separan en 4 octetos y se traducen a números decimales. Cada octeto puede ir desde un rango de 0 a 255:

  $$0/255{,}0/255{,}0/255{,}0/255$$

  Con esto se puede saber cuántos dispositivos conctados: $2^{32} = 4,294,967,296$ .7 mil millones de personas existen en el mundo, pero sólo 4 millones de dispositivos se permiten conectar a internet, sin tener ambiguedad, según el rango de direcciones IP.

- **Opciones**: El campo de opciones permite ampliar una cabecera IP. La idea original era que las opciones de cabecera rara vez se emplearan: de ahí la decisión de ahorrar recur sos no incluyendo la información de los campos opcionales en la cabecera de todos los datagramas. Sin embargo, la mera existencia de opciones complica las cosas, ya que las cabeceras de datagrama pueden tener una longitud variable, por lo que no puede determi narse a priori dónde comenzará el campo de datos. Además, dado que algunos datagramas pueden requerir el procesamiento de opciones y otros no, la cantidad de tiempo necesario para procesar un datagrama IP en un router puede variar enormemente. Por estas razones las *Opciones* fueron quitadas de la cabecera de IPv6.

- **Datos (carga útil)**: En la mayoría de las circunstancias, el campo de datos del datagrama IP contiene el segmento de la capa de transporte (TCP o UDP) que va a entregarse al destino. Sin embargo, el campo de datos puede transportar otros tipos de datos.

Se debe recordar si o sí se enviarán 40 bytes de encabezado por paquete. Por lo tanto es ineficiente si se envían muchos paquetes con pocos datos.

Ejemplo de división de Datagramas

Si se tiene un MTU de 1500 y se quiere transportar un paquete de 4000 ¿Cuál sería la longitud de cada datagrama?.

Se generan 3 paquetes: Cada uno tiene un encabezado de 20 bytes, más la cantidad de datos que se deben dividir (es decir: 1500 + 1500 + 1000). Recordar que se tiene 20 bytes de encabezado IP por cada nuevo datagrama que se fragmente.

Flag: un bit que identifica si hay mas segmentos para ensamblar o no. Si el campo Flag se encuentra 1 significa que faltan llegar datagramas.

Offset: Campo que permite reconstruir los datagramas fragmentados indicando la posición en un buffer. Ejemplo:

Se quiere transmitir un archivo de 4000 bytes mediante una red que tiene 1500 de MTU. Se divide en 3 datagramas y en cada uno de ellos se indica en el offset hasta dónde llega el dato que contiene.

- **Offset**: 3980

- **Offset**: 2960

- **Offset**: 1480. Se debe tener en cuenta que 20 bytes son para la cabecera. Si se generan dos paquetes de más serán 40 bytes que irán "de más".

- **Offset**: 0. Desde acá se comienza a reenzamblar el datagrama. El offset se encuentra en cero por lo tanto el router sabe que a partir de este datagrama será necesario reensamblar, por lo que lo coloca al comienzo del buffer. Con el campo **Longitud del datagrama** le es posible al router poder desde dónde empieza y dónde termina el datagrama fragmentado, permite que se reenzamble. Quien reensambla los paquetes **NO** son los routers de red sino los *sistemas terminales*.

Problema: *Un destino de una red IP recibe varios fragmentos de tamaño 444, otro de 444 y otro de 253 bytes. ¿Qué se puede decir respecto del MTU más pequeño de la ruta?.*

Se puede decir que el MTU de la ruta será de 444. Ya que se puede ver que es el límite de dos paquetes, mientras que el de 253 es el restante. El tamaño *original* del datagrama es la suma de:

$$(444 + 444 + 253) - 40 = 1101$$

Se debe recordar que se resta 40 porque son dos datagramas de más que se crearon por la desfragmentación dada por el MTU de 444 bytes.

Direccionamiento IP

Interfaz: límite entre el host y el enlace físico; o entre el router y cualquiera de sus enlaces. Vinculación del medio al dispositivo. Computadora tiene interfaz que está dada por el adapardor de red, que me conecta con el canal y se genera una intefraz, un servidor puede tener más de una interfaz. El router tiene más de una interfaz. Puesto que la tarea de un router consiste en recibir un datagrama por un enlace y reenviarlo a algún otro enlace, un router necesariamente está conectado a dos o más enlaces. El límite entre el router y cualquiera de sus enlaces también se conoce como interfaz.

La direccion IP está asociada a la *interfaz*. El router no tiene una dirección, tiene 3 direcciones diferentes. Esta dirección está en la interfaz, dividido 4 grupos de 8 bits. En la filmina nº 11 por ejemplo, el Router conecta 3 redes.

La dirección IP se puede dividir en dos partes:

1. **Net Id**: Bits más significativos (los que están más a la izquierda). Dirección de una subred. 223.1.1 (es lo mas significativo en la filmina) 223.1.2 el de la derecha.

2. **Host Id**: dispositivo de esa red .1, .2 (es lo menos significativo en la filmina)

Subred: dispositivos que tienen el misma Net Id, si esta es diferente, se está en otra red, en otra LAN , por lo tanto se tiene que comunicar utilizando otro router.

¿Cómo se hace para identificar una sub red de otra? Una forma es ver el router y ver qué dispositivos están de un lado y del otro. Cada una de esas islas pertenecen a una subred. Dentro de la misma red por mas que no haya internet, se van a poder comunicar.

Un router requiere saber cuál es el NetId y el HostId. Para eso hay un subnúmero denomina máscara d subred, es un número que permite identifiar el Net y el hostId. Lo que hace es poner en 1 los bits más significativos y pone en 0 los menos. El NetId termina en 1 y el HostId en 0.

Por ejemplo:

$$223, 1, 1, 2/24$$

En la anterior dirección iP, se simboliza con 24 para indicar que se quedan con los primeros 24byts más significativos.

Ejemplo:

223.1.1.2/24 ¿cuál es la dirección de red? La misma sería el NetId pero y con todos los ceros por detrás:

- **NetId**: Dirección de Red, resultaría 223.1.1.0

- **HostID**: 2/24

Otro ejemplo:

223.1.1.4/24: La dirección de Red sería 223.1.1.0

255.255.255.0: Mascara tiene todos 1 donde tiene el NetId y ceros en el HostID. Esto es la forma que tiene de identificar Si se hace una AND entre la dirección IP y la máscara y así se puede obtener de forma rápida el hostId y el NetId.

Otro Ejemplo:

223.1.1.128/25 Es una dirección de red porque el último octal termina en cero, por lo que sería: 223.1.1.10000000/25. Hay que pensarlo en binario siempre, por más que el número esté escrito en decimal. Hay que pensarlo entre la máscara y el final de la dirección terminada en ceros (que puede ser en binario o en decimal).

223.1.1.128/28 La misma es una dirección de red porque el último octal termina en 0.

División en las direcciones IP

Antes de que se adoptara el enrutamiento CIDR, la parte de red de una dirección IP estaba restringida a longitudes de 8, 16 o 24 bits, un esquema de direccionamiento conocido como direccionamiento con clases, ya que las subredes con direcciones de 8, 16 y 24 bits se conocían, respectivamente, como redes de clase A, B y C.

- **Clase A** : subnet :/8, lo que daría: 2^8 redes diferentes de 2^{24} host
- **Clase B** : subnet :/16
- **Clase C** : subnet :/24, lo que daría: 2^{24} redes diferentes de 2^8 host

Por ejemplo: 192.168.1.1 se puede decir que es una Red Clase C.
Las subdivisiones entre clases ya han quedado obsoletas. Porque ahora con la máscara de red se puede definir la cantidad de bits que se puden rservar para los host y cuántos para las redes.
Direcciones que se reservan de entre las clases de A, B, C. ¿Por qué?

- Al comienzo se pensó que cada máquina debía tener una dirección única en el planeta. Esto no es necesario porque si se tienen maquinas conectadas en red pero sin internet, entoncs no hace falta que las direcciones sean unicas.
- Para este propósito se reservó una subred de cada clase para crear redes privadas.

Máscara de subRed

Las mismas se pueden simbolizar de distintas maneras:

- 255.255.255.[Binario]
- 255.255.255.[10000000]
- 255.255.255.[128]: lo que daría 2^{25} redes de 2^7 host

Por ejemplo: 223.1.1.2/26
Significaría: 255.255.255.[11000000]
Existe otro tipo de dirección IP, la dirección de difusión o de *Broadcasting*: 255.255.255.255. Cuando un host envía un datagrama cuya dirección de destino es 255.255.255.255, el mensaje se entrega a todos los hosts existentes en la misma subred. Opcionalmente, los routers también reenvían el mensaje a las subredes vecinas (aunque habitualmente no lo hacen).
Dirección de broadcast:

- Directed Broadcast: la última (unos)
- Ej: 172.16.255.255, 192.168.1.255
- Limited Broadcast: (all ones)
- 255.255.255.255
- Este host, cuando aún no tiene a
- Mascara: 223.1.1.0
- Broadcast: 223.1.1.255

Tipo de conexiones

- **Unicast**: destino a un host/interfaz en particular, son las más comunes. Ej: 172.16.4.21
- **Broadcast**: destino a todos los hosts en una red. Ej: 255.255.255.255. Se manda un paquete a todos los host, por inundación se dice
- **Multicast**: destinada a un grupo de hosts en una red o varias redes.
- **Anycast**: destinada al primero que resuelva. IPv4 no hay casos especiales. Ejemplo en filmina 19.

Las direcciones con las que se conectan fuera de internet es una direccion pública. La interna o la hogareña es la de 192.168.1.1, pero la pública es otra
Ip reservadas que no son para hosts: 127.0.0.1 este numero se manda cuando se hace alución a su propia dirección. Cuando la aplicación no puede resolver una dirección y quiere hacer alución a su propia dirección, manda esa.

Estrategias para aumentar las conexiones

Existieron dos estrategias para ampliar el número de dispositivos a conectarse a internet:

1. Flexibilizar el tamaño de subredes: Direccionamiento CIDR.
2. Permitir el uso de internet de redes privadas a través del uso Nat. Muchas máquinas conectadas en red hogareñas, todas ellas salen con la misma dirección pública en internet. Se procede con el protocolo NAT.

3.3.1. CIDR

CIDR: Classless InterDomain Routing

- Porción de dirección de la red (subred) se hace de tamaño arbitrario
- Formato de dirección: a.b.c.d/x, donde X es el # de bits de la dirección de sub-red.

Por ejemplo:
200.1.17.128/25: $2^6 - 2$ direcciones IP posibles, ya que se le restan 2 porque : la de red y la de broadcast
Un host ¿cómo obtiene su dirección de IP? Se puede cambiar forzdamente pero de la forma interna y la máscara de red. ¿quien maneja las direcciones públicas? Los ISP. Dependen del servicio que uno contrate, tendrá determinada dirección pública.
DHCP: protocolo que asigna directamente de forma automática a los host que se conecten. Es un servicio determinado, eso lo asigna un servicio, que lo tiene contratado sl proveedor de internet. Este servicio viene implementado en el proveedor, es un servidor dinámico, que un host se conecta y el servidor le asigna una dirección. Es dinámico porque cambia según los host se conectan y se desconctan.
Cuando se pone un ruter en el medio, se genera una nueva LAN, pero se conectan de forma externa con una contraseña determinada.
¿Cómo se obtiene las direcciones públicas? Las tiene los ISP, compran bloques de direcciones, con los bits más significativos. ISP's block 11001000 00010111 00010000 00000000 que sería: 200.23.16.0/20
DNS: servidor que asigna un nombre de donminoi a una dirección IP donde está el host donde está almacenada. El servidor físico puede cambiar de direccion IP, pero el DNS la modifica dinámicamente y para nosotros los humanos es transparente.

3.3.2. NAT

Direcciones no alcanzan, direcciones privadas y acceden a internet y no pudieron. Salen con una misma red. una sola red para conectarse a una red exerior, ISP no se tiene que dar varias direcciones para todos los hots, sino una sola para toda la red que se quiere conectar.
Para saber información pública de la red por la que se está saliendo se puede visitar: *whatismyip.org*. También permite generar mucha información acerca de la red que se está utilizando.
¿Cómo se hace para salir a internet desde una red de computadoras?
Cada host que se quiere comunicar a internet, un host tiene que comunicar a otro que está afuera envia el paquete a la dirección: *Puerta de enlace* predeterminada: 10.0.0.4; si una computadora se quiere comunicar dentro de su propia red lo hace sin problema, pero si se quiere comunicar con otra que NO esté, lo tiene que enviar a 10.0.0.4 que lo envía el router, que es el único que pude hacer eso de salir públicamente a inernet.
El paquete cuando sale de adentro hacia afuera, el protocolo lo que hace es cambiar la dirección de puerta de enlace y le pone la pública (118.76.29.7), viaja ese paquete por la red como si fuera esa red una solo host.
Cando el paquete vuelve viene con nombre destino la pública, y el router la modifica por la interna.
¿Cómo sabe cuando vuelve el paquete a qué host tiene que darselo?
Mediante lo que se conoce como *Código de puerto*, el cual es un número, cuando vuelve la respuesta a través de ese número de puerto, sabe a qué host tiene que enviarle ese paquete. El router lo que hace es mantener una tabla con esos números de Código de Puerto y las direcciones de host de cada una de las máquinas. Por ejemplo: el Puerto 8080 sirve para las páginas internet.
El Router tiene un propio servidor de HCP para la red pública, cuando se conecta un nuevo host lo que hace es asignar automáticamente una dirección privada.
www.google.com.ar:200 si se escribe en la barra del navegador la anterior consulta, lo que hace es consultar al servidor de google donde está hospedada la página mediante el código del puerto 200 (que seguro el servidor lo tendrá configurado como cerrado)

4. Clase nº 5

4.1. Protocolo NAT

Lo que hace es ejecutarse en el ruter, cada dispositivo que se quiera conectar en el exterior, cambia la dirección privada para hacerla pública. La reemplaza por su inteface de salida, la dirección de fuente tiene la pública. Cuando el paquete vuelve el roter vuelve a transformar la dirección pública en privada. ¿Cómo sabe qué máquina tiene que entregar el paquete? Por el puerto que escucha para distintas aplicaciones. Si es por ejemplo una página web, sería puerto 80. Puerto es distinto para cada una de las máquinas que están en la red. Si varias computadoras hacen una petición̈a a la misma web, lo que sucede es que por cada paquete tendrá el número de puerto que tiene cada una de las máquinas, que son distintas. También se pueden reservar puertos para diferentes máquinas.

Campo de puerto: 16 bits, número reservado: 8080 por ejemplo para web. Tiene un máximo 65000 usuarios en una sola LAN (no es posible que supere esto).

Los ruters son de capa 3 solamente, por lo que viola el argumento de extremo a extremo, ya que es una función que no debería de cumplir el ruter. Sería ideal que no la cumpla el ruter; con la nueva versión 6 IP va a contemplar mayor rango de direciones para no hacer nateo (NAT) de direcciones. Recordar que el "nateo" de direcciones es debido al incremento de dispositivos conectados a internet. Ello hace que los ruters que estarían dedicados a otra cosa, tengan que realizar otros trabajos para poder salvar la problematica de las pocas direcciones IP públicas.

4.1.1. ICMP

ICMP: Informe de errores y señalización de routers (cómo es que se comunican los ruters entre si). La sigla ICMP significa Internet Control Message Protocol. El protocolo IP no es fiable, porque no ofrece garantías. El grueso de los errores no lo corrigue la capa de red.

Lo que hace este protocolo es:

- Protocolo IP no es fiable, los datagramas IP pueden perderse o llegar defectuosos a su destino.
- ICMP informa al origen si hubo algún error en la entrega del mensaje.
- Informa errores y mensajes de control.
- Informa sobre errores pero no toma decisiones sobre estos Mensaje ICMP
- Los mensajes ICMP se encapsulan como parte del área de datos del protocolo IP:v

Se envían datagramas de control, como ejemplo cuando se realiza un ping a una dirección ip, sirve a la red para saber el estado de conexión de determinado host. Esto lo utiliza también el browser de internet cuando no se puede conectar.

Un ejemplo de este tipo de errores es *Red destino inalcanzable*: Quiere decir que el router ese no está respondiendo, es problema de toda la red. También se pueden hacer ping a las computadoras que están en la misma red. Que es distinto a *Host destino inalcanzable*: la máquina no está activa pero la red funciona correctamente.

Hay mensajes que sirven para comunicar los rotuers entre si, como ser:

- Anuncio de router
- Descubrimiento de rout

Otro error es el de **Cabecera IP errónea** el cual significa que tiene un header checksum, sólo de la cabecera, si da mal entonces ICMP anuncia esto.

IPV6

Este nuevo protocolo es una versión nº 6 que vendría a reemplazar la versión nº 4.

Una de las características que tiene IPv6, es aumentar el espacio de direcciones, es la motivación inicial. También permite cambiar el encabezado para agilizar el envío y el recibo; y también se modifica el encabezado para facilitar QoS (Quality of Service): para poder darle mayor prioridad dependiendo del paquete, si proviene de una aplicación de streming o de llamada tendrá por ejemplo más prioridad que un pedido de una soliciud de página web por ejemplo.

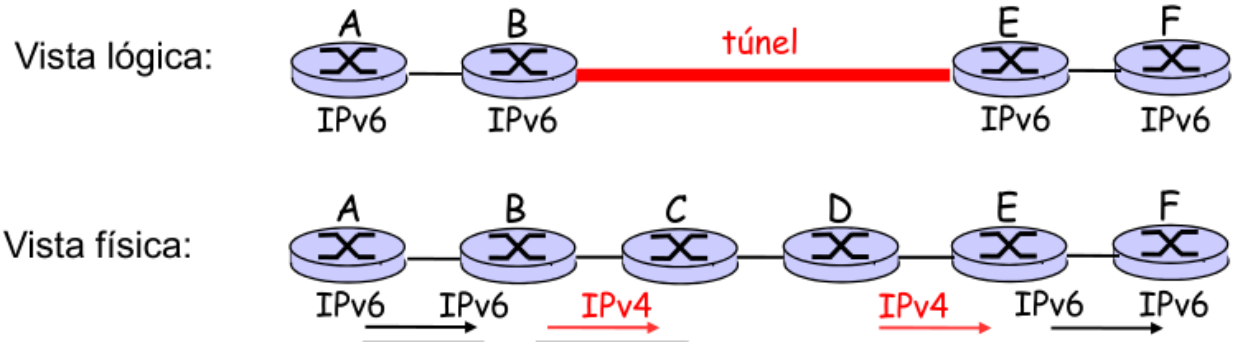
Algunas modificaciones:

- El nuevo protocolo evita el Nateo (utlizar el protocolo NAT).

- El encabezado se duplicó en tamaño, la fragmentación no está permitida.
- Permite direcciones anycast.
- Se elimina el campo de opciones.
- Y hay una nueva versión ICMP para que labure con este protocolo. Disminuyendo de esta forma considerablemente el reenvío IP dentro de la red.
- Checksum: eliminada enteramente para reducir tiempo de procesamiento en cada router al ser redundante, ya está en capa de transporte y de enlace (Ethernet).
- Se elimina la linea de fragmentación, más espacio para la dirección de origen y destino.

Tunelización

¿Cómo sabe el dispositivo receptor del datagrama si es IPv4 o IPv6? Lo que se denomina **tunelización**, los ruters laburan con IPV6, pero también acepta el IPv4, esto se hace mediante el *tunelling*. Es necesario ir *implementando de a poco* aquellos ruters que soportan IPv6, no se puede implementar de un día para el otro.



El ruter B a C (el cual no admite IPv6),el encabezado de v6 lo guarda en la sección de datos y le manda una cabecera para que C lo pueda entender. En su interfaz el ruter B implementa tanto la versión 4 como la 6, y cuando transmite a C es a través de versión 4, lo recibe E que sabe que el campo de vesión es 6, entonces sabe que el campo de datos está el encabezado del protocolo 6, descarta el encabezado del 4 y toma el de 6.

La tunelización lo que hace es modificar el encabezado para que lo pueda entender un versión de 4. Esto es posible porque los ruters saben mediante el NETId si se utiliza una versión o la otra.

Clase nº 5

Protocolos de Ruteo

Los ruters, corren algoritmos de ruteo, los cuales consisten en endeterminar buenas rutas a través de los ruters, desde los emisores hasta los receptores. Los caminos desde una computadora a otra, son muchos. El algoritmo se corre cada cierto tiempo, el tiempo lo determina el protocolo que se está corriendo.

El algoritmo determina la mejor ruta y a partir de ahí genera la tabla de re-envío. Determina internamente desde qué interfaz del router se enviará un paquete una vez que llegue. Los paquetes de datagrama NO siguen una ruta definida, a difrencia de ATM, que se reserva recursos entre un punto y al otro y cada paquete pasa siempre por los mismos enlaces.

Cada ruter debe determinar la ruta óptima. Para poder hacerlo, requiere ponderar los enlaces, y para ello se utilizan grafos. Un grafo consiste en un conjunto de nodos y aristas que conectan otros nodos. En los modelos de grafo se denomina:

- **G**: una función.
- **N**: Un conjunto de nodos.
- **E**: Aristas, que figurarían ser enlaces físicos.

Ponderar el costo de cada arista, de una conexión, dependerá de muchas cosas. Por lo que será una *ponderación multidimensiaonal*, porque se tiene magnitudes distintas, y todo ello debe ser medible ¿cómo se puede pensar que una ruta/enlace es mejor que la otra? Se debe determinar de alguna forma, se debe tener un *Costo*. El Costo se encuentra determinado por:

- Longitud física del enlace.

- Velocidad del enlace.
- Costo monetario asociado.

Una vez que el rotuer ya calculó la tabla, dispone la interfaz por la que saldrán los paquetes, este llega y lo manda sin la necesidad de seguirlo, lo patea para determinada interfaz y listo.

Los otros ruters también deben haber corrido el algoritmo y llegado al mismo tiempo al mismo resultado. Cada ruter debe conectarse con los demás ruters. Los enlaces son bidireccionales, es decir, que por un mismo enlace pueden salir paquetes, como también entrar. Pero en los ISP los enlaces son asimetricos, por ejemplo el ancho de subida y bajda, no tiene el mismo ancho de banda de ida que de vuelta, pero de esto se desentiende, no se contempla para el modelo a analizar.

El Costo de dos nodos que no están conectados entre si, es decir, que NO son vecinos, se considera en un principio como infinito. Se denomina *nodos Vecinos* si es que hay un enlace que los una. Costo total es la suma total de nodos que pasen por el medio del camino elegido.

Clasificación de los Algoritmos de ruteo

Pueden existir de dos tipos:

- **Algoritmos de Ruteo Globales**: Cada roter debe conocer a todos los ruters de forma directa, es decir que los consulta. Se va a valer de la info de todos los nodos y enlaces que hay en la red. Se denominan Algoritmos de Estado de Enlace, y son centralizados. Se basa en el conocimiento global y completo de la red (conectividad y costos de los enlaces). Se Requiere que el algoritmo adquiera esta información antes de realizar el cálculo
- **Algoritmos de Ruteo Decentralizados**: Solo va a saber el costo que tiene hacia sus vecions y de los que NO son vecinos, se calcula el costo teniendo en cuenta lo que sus vecinos le dicen de los otros vecinos pero no los consulta él mismo, sino que se basa en información de la demás red de otras. La información se propaga entre ruters vecinos.
- **Estaticos**: Se usan cuando se tiene un conjunto de nodos que no varían mucho en el tiempo, ni en cantidad ni en calidad. Las rutas cambian muy lentamente con el tiempo.
- **Dinamicos**: es cuando se ve modificado el tráfico o la topología de la red se modifica, y por lo tanto, se modifica a su vez, la ponderación. Se está ejecutando todo el tiempo. Son más suceptibles a problemas, porque las rutas cambian muy rápido.

Algoritmo de Dijkstra

Es un algritmo **global**, porque se saben todos los costos. Se logra bajo difusión de estado de enlace, es decir,que manda paquetes que se interrogan entre ellos. Cada uno reporta su estado. Todos los nodos tienen la misma información, por lo que todos sabrán en un momento dado cuál será la mejor ruta para llegar de un lado a otro.

Tabla de reenvío debe saber por dónde mandar o calcular los caminos posibles entre ditintos host. Para cada iteración, y se descrubren mayores rutas mejores, entoncs se actualiza la ponderación de las aristas. En la inicilización, pondera la arista entre sus vecinos, y en los demás que no son vecions, es decir que no tiene aristas conecadas, es infinito; luego en las otras iteraciones va descubriendo van ia ir sumando las ponderaciones de los distintos caminos.

Este algoritmo lo que genera es la tabla de reenvío. En las filminas, lo que se explica es por dónde tiene que salir el paquete para llegar a deteminardo lugar, por qué interfaz debe salir. El algoritmo de Dijkstra es de orden cuadrático, si se agregan 10 ruters, debe hacer 100 operaciones, para conocer toda la topología,por lo que se vuelve más costoso.

Clase nº 6

Repaso de la Clase nº 5

Capa de Red

- Protocolo principal : ip, icmp.
- Tareas: ruteo y reenvío.
- Objetivo: determinar la mejor ruta de host a host.

Para generar esto requiere protocolos, que utilizan diferentes algoritmos. Se utilizan los grafos y se clasifican en dos grupos:

- **Globales**: Cada Router conoce toda la topología de la red.
- **Decentralizado**: Cada Router conoce sólo los vecinos y se tiene información de los demás nodos, en función de la información que le llega de sus vecinos.

Recordar que cada nodo tendrá su propia tabla. El Orden del algoritmo de Dijkstra es cuadrático, por lo que si se duplican los nodos, se cuadriplican la cantidades de cuentas.

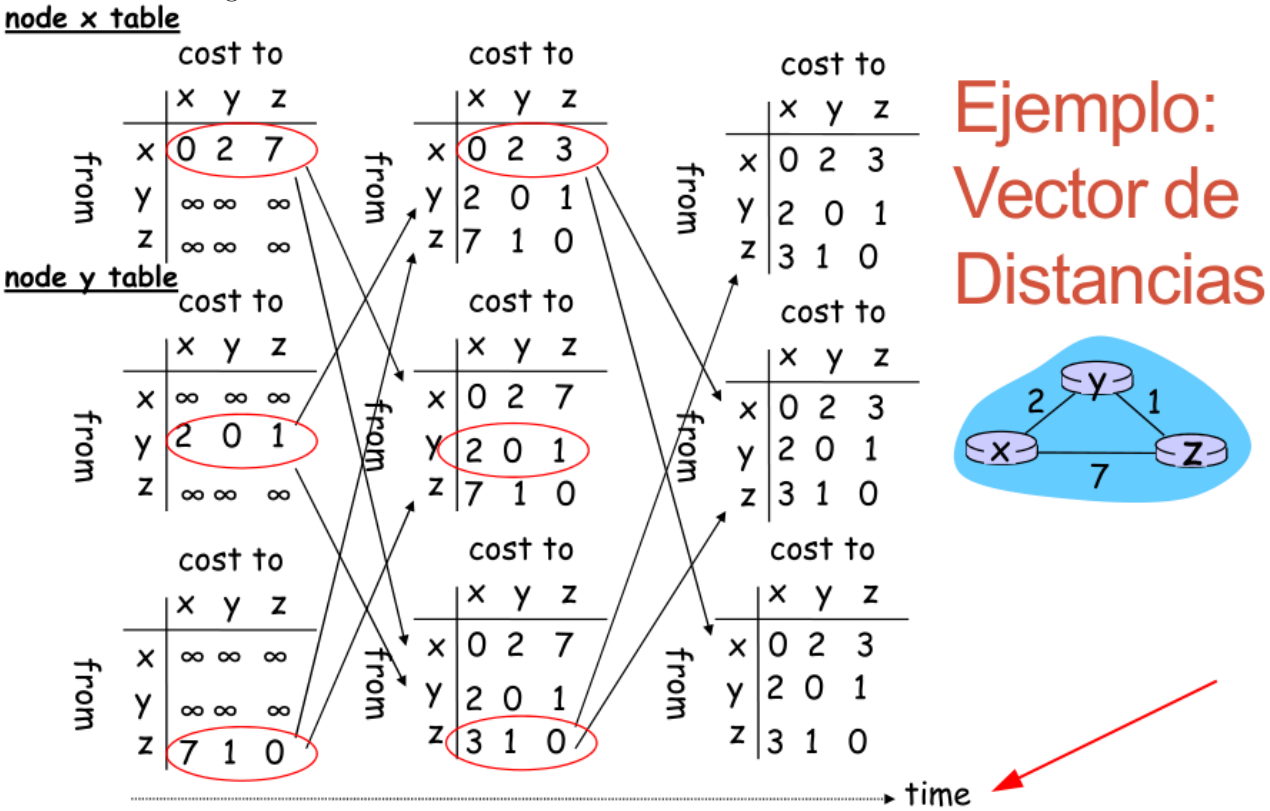
4.2. Algoritmo de Vector Distancia

Vector distancia, es de tipo **distribuido** por lo que no conoce los demas routers que NO son sus vecions, sólo conoce los nodos vecinos. Calcula la distancia de los demás (que no son vecinos), mediante lo que le indican sus allegados.

Es de tipo Iterativo: se corre el algoritmo hasta que no haya mas información para intercambiar. Es por iteraciones, en cada iteración se comparte la info entre vecinos, cuantas más veces se corra, mayor información (El vecino informa de sus vecinos y esos vecinos informan a los demás, etc). Lo bueno es que no tienen que estar sincronizados, si no hay cambios entonces el algoritmos converge a la ruta de minimo costo.

Se tiene en una conexión horizontal: El nodo H, A y B. H tendrá como vecino a A. Si H contiene un protocolo que corre un algoritmo de Vector Distancia, entonces la información que tenga H de A será directa, es decir, que podrá calcularlo sin problemas. Pongamos por ejemplo un Costo de 5. Ahora, para conocer a B, será mediante lo que le informe A de B. Entre A y B puede haber millones de nodos, pero para H es lo mismo.

Cada nodo calcula el costo hacia los vecions, los que no son vecinos le pone infinito en una primera instancia. Esto lo guarda como vectores, lo envía a los vecinos y los vecinos generan nuevamente esta información y la vuelven a enviar. Y así va recopilando información. En la filmina 29 de la Clase 5 se puede ver cómo es que se comunican los vectores generados mediante 3 iteraciones.



¿Cómo repsonde este algoritmo frente a la cambio en los costos? Si hay tráfico por ejemplo, se le asigna otro valor, Se actualiza la información de ruteo, se actualiza los propios vectores distancia, se lo comunican a los vecinos, y se hace todo el algoritmo. Lo que tiene este algoritmo es que sigue: "Buenas noticias viajan rápido, pero las malas viajan lento"

Cuando aumenta el costo entre host, se complica el algoritmo [filmina 35] El problema que tiene es que se actualiza desde x a Y = 6, pero el problema que tiene ahí es que Z actualiza con la información de Y, esto se prolonga en las iteraciones y se vuelve un problema. Lo que no se está dando cuenta Y es que todo está pasando a través de él, y no tiene en cuenta que los host vecinos pasarán por él. Este proceso se repite 44 veces,

y ahí recien comienza a cambiar el camino, porque evalua el paso de 44 con respecto al otro costo (también mal calculado de por ejemplo 45) por lo que será más beneficioso ir por 44.

En el ejemplo del comienzo entre los nodos horizontales H, A y B, si entre A y B, la conexión se cae, A tiene la tabla anterior, por lo que sabe que para llegar a B, pude enviarlo a H y H lo envía a B mediante A + B, Entonces A lo que hace entre infinito A/B y A/H/B (un número menor) se lo envía a H, H lo ataja y como la única manera que tiene de llegar a B es mediante A, lo vuelve a enviar a A, y así se reenvían entre H y A.

Ruteo Jerárquico

Ruteo Jerárquico: Se agrupan los ruters de cada red en lo que se denomina *Región Autónoma*. Cada ISP controla determinados routers que denominann reginoes autónomas.

Dos tipos de ruteos:

- **Interno**: (intra), si me tengo que conectar dentro de mi sistema autónomo. Cada administrador maneja un sistema autónomo, si es que se quiere monitorear la densidad de tráfico por ejemplo.
- **Extero**: (inter) se comunica entre los sistemas autónomos.

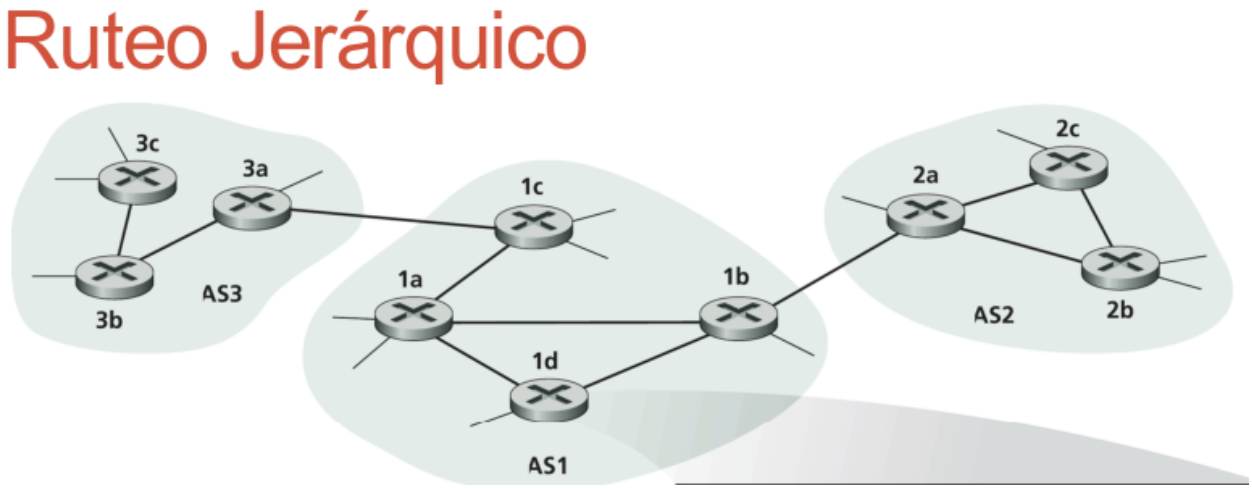
Esta diferencia lo que permite es que manejar mejor la performance para generar mejores rutas, y no generar tablas enormes. Cada Sistema Autónomo (AS) se maneja como un sólo ruter, vista desde otro AS.

Red plana: todos los nodos de forma jerárquica, son iguales. El problema es que esto no pasa en la vida real. No se podrían almacenar en una tabla de ruteo, porque sería una tabla enorme. Cada red puede querer controlar el ruteo de la forma que se quiera.

Dentro de un Sistema Autónomo se debe tener el mismo protocolo de ruteo. El **Router de frontera/borde/gateway**, es el que comunica distintos sistemas autónomos. El tema es cómo llegar a ese router de borde (frontera). Lo que hace un router si le llega una dirección que no sea propia de su red, es enviar directamente el paquete a la puerta de enlace.

Puerta de enalce predeterminada: dirección que me saca de mi propia red. Cualquier paquete que NO esté dentro de mi red, se considera que está afuera, y para ello se envía directamente a la puerta de enlace predeterminada.

El problema es cuando se tienen varios ruters de frontera, que comunica diferentes AS. Para ello requiere correr dos protocolos: uno que corre entre los sistemas autónoms y otro intra (que es adentro). En la filmina 42 una cosa es enviarla en 1b y otra es 1c. ¿Cómo sabe? Bueno, para eso corren protocolos denominado *inter-as*.



Se puede complejizar aún más cuando se tienen más AS todos interconectados, es decir, multiple elección entre múltiples AS.

Cuando se tienen otros AS, se deben hacer cálculos para saber el mejor camino para llegar por ejemplo, a AS4, si es mediante AS2 o AS3. Para solucionar esto, y para no complejizarlo, lo que se hace es calcular dentro de AS1 si es mejor 1c o 1b, se elige la menos costosa y se envía ahí y el otro AS lo resolverá de la misma forma.

Protocolos de Ruteo Intra-AS

Protocolos de ruteo Internos a los AS más comunes:

- **RIP**: Routing Information Protocol (vector-distancia)
- **OSPF**: Open Shortest Path First (Estado de enlace - Dijkstra)

- **IGRP**: Interior Gateway Routing Protocol (propietario de Cisco). Optimizado para los productos CISCO, NO es de código abierto.

Routing Information Protocol(RIP):
La distancia no pondera los enlaces sino que el camino más corto será el que tenga menos saltos. Intercambia avisos entre vecinos cada 30 segundos (aviso RIP). En cada aviso puede listar entre 25 redes destino dentro del mismo AS. Existe un maximo de 15 saltos, 15 saltos es demasiado para todo Internet, y esto viene configurado dentro del mensaje.
Open Shortest Path First (OSPF):
Es de código abierto. Utiliza el algoritmo de estado de enlace.

- Se difunden paquetes de estado de enlace.
- Se crea un mapa de la topología en cada nodo.
- Las rutas se calculan usando el algoritmo de Dijkstra.
- Avisos OSPF transportan una entrada por cada router vecino.
- Avisos son difundidos al sistema autónomo entero (vía inundación: Avisa a travez de inundación, mediante la dirección de broadcast)
- Permite hasta tener 3 mejores caminos, a diferencia de RIP que sólo contempla 1.

Protocolos de Ruteo Inter-AS

Border Gateway Protocol(GBP)

- BGP (Border Gateway Protocol): Estándar por defecto
- BGP provee a cada AS un medio para:
  1. Obtener la información de alcanzabilidad de una subred desde sus AS¿s vecinos.
  2. Propaga la información de alcanzabilidad a todos los routers internos al AS.
  3. Determina rutas ¿buenas¿ a subredes basados en información de alcanzabilidad y políticas.
- Permite a una subred dar aviso de su existencia al resto de internet.

Es a travéz de los puertos que saben los ruters para comunicarse entre routers.

5. Clase nº 7

5.1. Repaso de Capa de Red

Lo que se vio: modelos de capas y capa de enlace
Capa de Red: conectar host con otros, que paquetes lleguen de un lado a otro, través de un *ruteo y reenvío*.
Cómo se determinan esas rutas: mediante algoritmos. Estos pueden ser:

- **Globales**: se denominan todos los nodos conocen a todos los otros nodos, todos los demas enlaces
- **Vector distancia**: cada nodo conoce a sus vecinos, y conoce las trayectorias estimando según la información que les dan los demas.

Protocolos principales, los host tienen que estar identificaods, numerados, mediante el protocolo TCP/IP.

5.2. Capa de Enlace

Terminología:

- **Nodos**: ruters, y los dispositivos en el medio: switch, access point, que conecte cualquier enlace (el enlace es la comunicación que conectan dos nodos adyacentes). Hosts, routers y swiches.
- **Enlaces**: puede ser tanto cableado como inalámbrico. Switch conecta varias computadoras, NO es un ruter. El Switch genera una red local, se puden intercomunicar entre los host de la misma red. Si se conecta un swtich con otro, no funciona, para conectar dos redes se requiere un ruter. Pueden ser:
  1. Enlaces cableados

2. Enlaces inalámbricos

- **Trama (o frame)**: es el paquete de la capa de enlace, que encapsula a los datagramas. Si se tienen dos tipos de enlace, el protocolo EN CAPA DE ENLACE serán distintos. La capa de red le da lo mismo, no se da cuenta de este enlace.

Los servicios que otorga la Capa de Enlace son:

- Detección y corrección de errores.
- Compartición de canales broadcast: acceso múltiple.
- Direccionamiento de la capa enlace.
- Transferencia de datos confiable y control de flujo.
- Descripción e implementación de varias tecnología.

Canales broadcast: canales compartidos por varios usuarios. Acceso múltiple hacia varios usuarios. Se requieren dos tipos de direccionamiento. En esta capa,el Emisor y Receptor son dos interfaces (nodos) que se tengan, y ya no es un host y otro host en esta capa.

Direfencia entre capa de red y de enlace:

- En la capa de red conecta dos host, el de enalce es nodo a nodo.
- El objetivo es asegurarse de que la información llegue de un nodo a otro.

¿Por qué se requiere la capa de enlace? *Porque varían los tipos de enlace*, porque se puede tener un cable, de un nodo a nodo, luego se pude tener un access point con conexión wifi, inalambrica.

Cada enlace va a tener un protocolo a nivel enlace, si está mal el paquete entre nodos, hace que no se propague entre toda la red, sino que se determine entre nodo a nodo. Para ello se ampara en una comprobación de errores. Esto sucede ya que si sólo la comprobación de errores existiría en capa de Red, los que evaluarían el error serían los host de los extremos, por lo que a cada error, pedirían retransmitir todo el paquete, inundando la red de retransmisiones. Para evitar ello, es que se implementa un control sobre la Capa de Enlace, para que no se propaguen paquetes de forma inecesaria.

La capa de Enlace garantiza el transporte del datagrama a través del enlace sin errores (Entre nodos adyacentes). Se utiliza en enlaces con altas tasas de error. Se evita de llenar los paquetes con errores en toda la red. Se corrige a nivel enlace; el nivel de errores es más robusto a nivel en este nivel; la capa de enlace es la que contiene mayores controles sobre los posibles errores en los datagramas, sumado a los controles de errores que ejecutan las otras capas genera que se tenga pocos errores en general.

5.3. Protocolos de Capa de Enlace

Ejemplos de protocolos de capa de enlace son:

- Ethernet.
- LAN inalámbricas 802.11 (WiFi)
- Token ring: no se utiliza para internet.
- PPP.

Cada protocolo provee servicios distintos. Recordar que la transferencia de datos en capa de red NO es confiable, a nivel capa de red, NO es confiable, quiere decir que a la capa de red no le importa si se pierden paquetes, quizás otra capa si le importa. Es por ello que todo funciona bien, por la independencia de tarea.

Accesos al Enlace: Protocolos MAC. ¿Para que se necesitan estos? porque quizás los medios están compartidos, se requiere que alguien los arbitre. El bus de datos es compartido por ejemplo, no es dedicado, quien arbitra es el bus de control, a través de las señales de control lo controla el microprocesador. Esto es una anoalogía por lo que se requiere un estado de Enlace.

Dirección Mac: identifica fuente y destino. Diferentes a las direcciones IP; se requieren direcciones MAc para identificar cada enlace. A nivel la capa de red la dirección de destion y origen son la misma a travez de toda la red. A nivel capa de Enlace, la dirección de destino y origen son para cada enlace, se requieren para saber de qué punto de enlace sale y hasta dónde debe llegar.

Servicios que otorga la Capa de Enlace

Control de Flujo:

- Capacidad limitada de almacenamiento en buffer de los nodos: Evita que el nodo se sature. Cuando se comienza a inundar el buffer, lo que hace es disminuir el tránsito de datagramas entre nodos.
- Proporciona un mecanismo de control de flujo para evitar que el nodo emisor abrume al nodo.

Detección de errores: Detección de errores de bit, causados por atenuación de señal y ruido.

- Pide al transmisor retransmisión o descartar la trama: dependiendo de si es TCP o UDP, si es TCP, trata de retransmitir, si es UDP, lo deja pasar.
- Es más sofisticada que la proporcionada por la capa de transporte y red: se corregían determinados errores, pero en esta capa la detección de errores es muchísimo más robusta.
- Se implementa en hardware: Es sumamemte rápido, porque se genera mediante control electrónico y no a nivel software. El problema es que el control electrónico es más rápido que el software.

Mediante una secuencia de bits, se puede determinar si hubo error. Existen códigos que permiten determinar en dónde está el error, el problema es que requieren *bits de redundancia*, son necesarios para saber en qué bit se produce el error (diferencia con la detección de errores vista en arquitectura, que sólo detecta si hay error pero NO en qué bit).

Para saber en qué lugar hubo un error, se requieren bits de redundancia, y eso se transfiere a más bits en la transmisión, el problema de ello es que la tasa efectiva decrece a medida que se agregan más bits en el envío. Los bits de redundancia permiten determinar mejor la comunicación.

Una analogía puede llegar a ser cuando se deletrea una palabra en una charla telefónica, y se indica A, de Andres, B de Barco, siendo en este caso los bits de redundancia "ndresz .ªrco". Esto se agregan más o no dependiendo del enlace en el que se transmita, por ejemplo si es fibra opptica, se utiliza otro protocolo que utiliza menos bits de redundancia, lo mismo que cuando el enlace es inalámbrico, se utilizará otro protocolo que utilice más bist de redundancia, dado que el medio es más propenso de tener mayores errores.

Tipos de transmisiones: **Semi-duplex y full-duplex**

- **Full-duplex**: los nodos de ambos extremos transmiten paquetes al mismo tiempo. Es decir que en el enlace, se puede transmitir ida y vuelta al mismo tiempo.
- **Semi-duplex**: los nodos no terminan de transmitir y recibir al mismo tiempo. El canal es bidireccional, pero se requiere que cuando se hable uno, el otro no. Como los teléfonos Nextel.

Adpatadores de Red

Cada interface tiene un dispositivo denominado **Adpatador de Red**. El protocolo depende del Adaptador de Red (dispositivo lógico y físico). La diferencia física entre un adaptador de etehernet por ejemplo, y el access point es que uno utiliza rj45 y el otro utliza una antena. La capa de enlace es implementada mayoritariamente en un adaptador de red (NIC). Por ejemplo una Tarjetas Ethernet ó 802.11 (WiFi), el adaptador ya está implementado onboard, es decir que por ejemplo el conector rj45 ya viene quemada en la placa. Es el Adaptador de red, el que permite transmitir en los enlaces. Recordar que el Adaptador es semi autónomo, porque labura en hardware y trabaja en capa de enlace y en capa física.

El Adaptador de Red actúa desde el lado **transmisor** realizando lo siguiente:

- Encapsula el datagrama en una trama.
- Agrega bits de chequeo de errores, control de flujo, etc.
- Transmite la trama al enlace.

El Adaptador de Red actúa desde el lado **transmisor** realizando lo siguiente:

- Recibe la trama y extrae el datagrama.
- Busca errores, control de flujo, etc
- El adaptador es semi-autónomo

Técnicas para la detección de errores

Comprobación de paridad: bit de paridad. Lo que hace el transmisor es poner un bit más y pone un bit para que la cantidad de 1 sea par o no. Cuando llega del otro lado, si hay un error un 1 se convierte en un 0 en caso de error. Por lo que habrá un 1 de más, por lo que no es par. El que cuenta es el receptor. Si existen dos errores, el bit de paridad no lo detectará. El algoritmo matricial NO interesa. Sólo detecta errores impares.

Suma de comprobación (cheksum): Hay un campo de checksum en datagrama IPv4, que permite tener un checksum para saber si hay errores en la cabecera. Se agarran grupos de 16 bits, que no se sabe la info que transportan, y se interpreta como un número de 16 bits, por ejemplo se toman 3 grupos de 16 bits cada uno, donde el primero es el número "21", los otros 16, dan "7" y los otros "5", por lo que se suma y se pone el "33" en binario. El receptor agarra los 3 números de 16, los convierte a un número como hizo el transmisor, los suma de nuevo, y si da un número distinto a "33", pide retransmisión. Si hay overflow, lo deja pasar. La probabilidad que se pase un error es muy baja, cuanto más larga la cadena la probabilidad es mucho más baja de que pase un error.

Características:

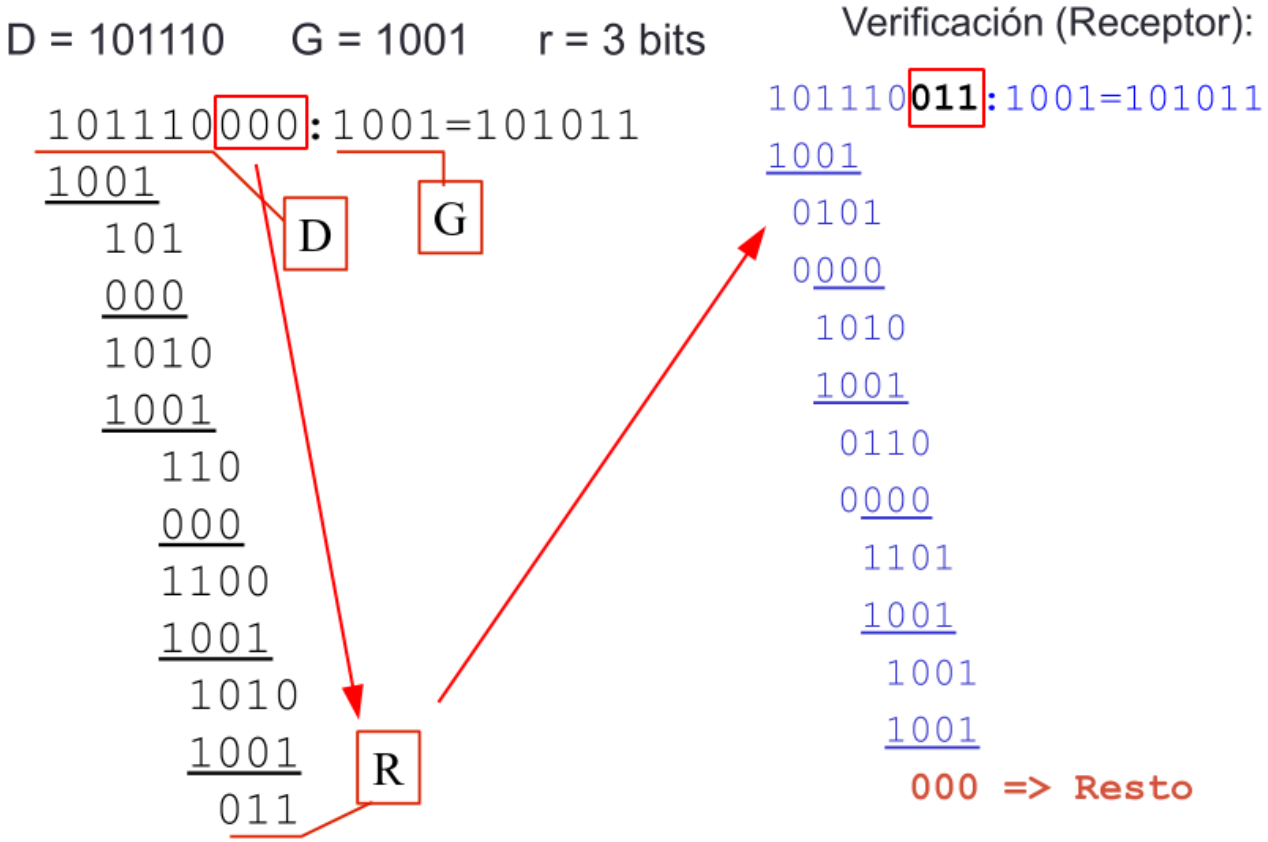
- Requiere poca sobrecarga de bits.
- Pero tiene una protección relativamente débil.

Código de redundancia cíclica (CRC): Funciona en base a polinomios. Se tratan los bits de datos como coeficientes de polinomios, polinomio generador:

$$G = 101 = 1 * X^2 + 0 * X^1 + 1 * X^0$$

Se tienen coeficiente entre ceros y unos. Se elige un patrón generador al azar, que el más significativo tiene que ser 1. En el caso anterior, 101 el bit más significativo es 1 y el valor es $2 + 1 = 3$, R + 1. R = resto.

Cada el receptor divide el número divisible por el generador, si hay error entonces el resto será distinto de 0. A la cadena enviada se le concatena un número divisible por el generador. El polinomio generador lo sabe tanto el emisor como el receptor. Cuanto más grande es el generador, se le tiene que agregar más bit de número divisible. Si el resto de la división es otra cosa que no sea cero, entonces es error. Cuanto mas grande el polinomio generador, menor probabilidad de errores pero mas bits requeridos para generar la divisisón, por lo que se vuelve más pesado el datagrama a enviar.



Se completa el Dato con cero atrás, se divide por el polinomio generador, se obtiene el resto y al resultado se le agrega el resto y ese es el número que se envía. Dependiendo del resto, se sabe dónde está el error.

Protocolos de Acceso múltiple

Punto-a-apunto:

- Acceso discado usando Point-to-Point Protocol (PPP)
- Enlaces punto-a-punto entre switch Ethernet y host (computadora)

Broaddcast (cable o medio compartido):

- Múltiples nodos emisores y receptores conectados a un único enlace.
- Ethernet y redes LAN inalámbricas son ejemplos de acceso múltiple.
- Flujo de subida en HFC (Hybrid Fiber Coax).

Colisiones/Interferencia: Pueden haber dos o más transmisiones simultáneas en distintos nodos por lo que habría una Interferencia. Se Esto se conoce como colisión si un nodo recibe dos o más señales al mismo tiempo.

Protocolos de acceso múltiple:

- Algoritmo distribuido que determina cómo los nodos comparten el canal, es decir determina cuándo un nodo puede transmitir.
- Son los mensajes para ponerse de acuerdo sobre cómo compartir el mismo canal.

Se tiene un ideal a seguir para poder implementar un protocolo y se denomina **Protocolo de Acceso Múltiple Ideal**

- Cuando un nodo quiere transmitir, éste puede enviar a tasa R.
- Cuando M nodos quieren transmitir, cada uno puede enviar en promedio a una tasa R/M
- Completamente descentralizado:
  1. No hay nodo especial para coordinar transmisiones.
  2. No hay sincronización de reloj o ranuras.
- Protocolo simple, de modo que no sea costos.

En internet se tiene un medio desentralizado, donde no hay uno quién defina o arbitre quién transmite o no. Por ende lo tiene internalizado cada nodo. Cada nodo va a querer transmitir al máximo de la tasa R. Cuando se mete otro, entonces la tasa será de R/2. Por lo tanto será R/M (este es un ideal que no existe, lo mejor posible que se quiera). Debe ser fácil y que no sea costoso.

Protocolos Mac, 3 clases:

- **Canal subidivido**: particinar el canal y cada usuario se le da un espacio dentor de ese canal. Se divida el canal en varios pedazos. Asigna pedazos al nodo a su uso exclusivo. El punto dos anterior, se puede salvar, pero no cumple con el primer punto de l acceso Múltiple ideal [filmina 21].
- **Acceso Aleatorio**: canal no es dividido, no se divide el canal, ocurre colicciones, todos tranmiten a lo más alto de su tasa. CUmple el punto 1 pero no del dos [filmina 21]
- **Toma de turnos**: de alguna manera busca lo mejor de los anteriores dos, cuando se quiera transmitir se le da más prioridad a uno o más, se le da más tiempo de transmisión a quien quiera transmitir más cantidad de datos.

Canal Subdividido

TDMA (multiplexación por división en el tiempo): Se accesde al canal por rondas, se tienen 4 usuarios por lo que el tiempo se divide en 4 ranuras, Si uno solo quiere transmitir, como la división ya está establecida en 4 lo que hará es que el rango será de R/N, sólo podrá tranmitir a la tasa más efectiva el 4to de tiempo. Las ranuras no usadas no se aprovechan. Se limita la tasa de transferencia a R/N para todos los nodos. Y cada nodo siempre tiene que esperar su turno para transmitir.

FDMA: Se divide el espectro en bandas de frecuencias. Todos transmiten en cualquier momento, pero a una tasa reducida, si se tiene 4 usuarios con 10 mb, cada uno transmitirá 10/4, por lo que es lo mismo al anterior. Los canales de televisión se transmite así. Cada uno transmite a un rango de frencuencia asignada. La Banda de frecuencia de transmisión no usada no es aprovechada. Las ventajas y desventajas se asimilan al protocolo anterior,TDMA.

Acceso Aleatorio

Si dos nodos transmiten hay una colisión y se retransmitirá hasta que pase el dato. Se transmitirá luego de determinado tiempo, porque si se retransmite a la misma cantidad de tiempo, entonces de nuevo habrá colisión, por lo que se quiere que sea aleatorio, pero tampoco TAN aleatorio, porque sino sería ineficiente, ya que estarían esperando demasiado tiempo cuando se podría utilizar el canal en menos tiempo. Ejemplos de estos protocolos son:

- ALOHA ranurado.
- ALOHA.
- CSMA, CSMA/CD, CSMA/CA (CSMA: Carrier Sense Multiple Access - Acceso múltiple por sondeo de portadora).

ALOHA Ranurado: Se envían tramas de todos los usuarios, de igual tamaño. El tiempo es dividio en ranuras, y las mismas las pueden ser utilizados por cualquier usuarios. Si solo un usuario quiere transmitir, entonces utiliza todas las ranuras, por lo que transmite a tasa R (cumple el punto 1). En este caso, Ranura significa, espacio de tiempo. Si hay 3 usuarios, entonces habrá colisión, esperaran determinadas ranuras de forma aleatoria, no es tiempo, son ranuras. Si hay colisión, el nodo retransmite la trama en cada ranura siguiente con la probabilidad P hasta que la transmisión sea exitosa. El problema acá es que cuanto mayor cantidad de usuarios es menos eficiente. La eficiencia para el usuario es de 9 ranuras, en cambio implementarlo en el anterior protocolo daría 3 (por ser 3 los usuarios), acá se transmitió a 1/9 bits por segundo. La cantidad de Ranuras para poder transmitir se determina de forma aleatorioa.

Ventajas

- Un único nodo activo puede transmitir continuamente a tasa máxima del canal. El punto 1 se cumple.
- Altamente descentralizado.

Desventajas

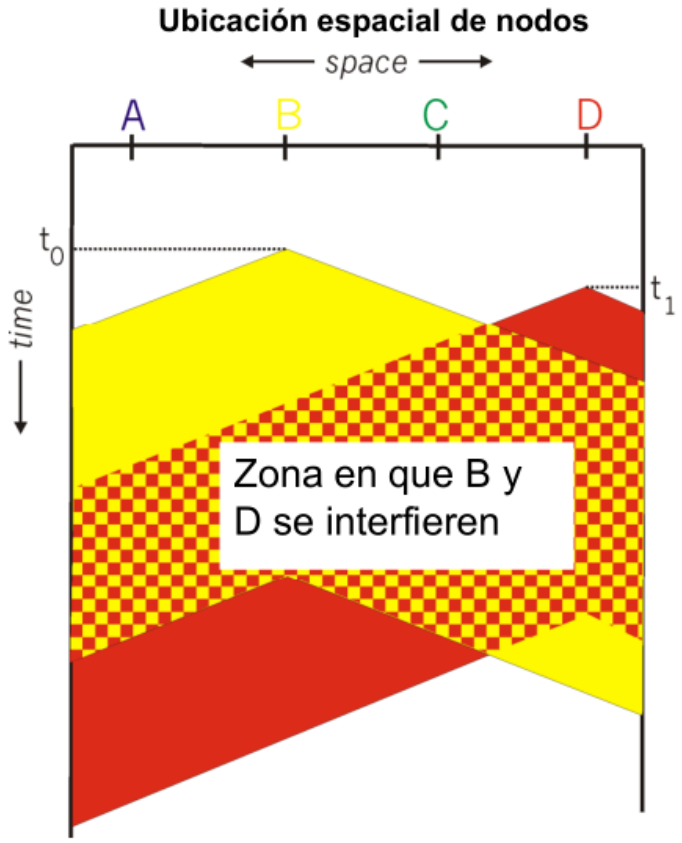
- Colisiones, las ranuras se desperdician.
- Ranuras no ocupadas.
- Nodos podrían detectar la colisión en menor tiempo que el de transmitir un paquete.
- Requiere la sincronización de todos los nodos.

Eficiencia: fracción (a largo plazo) de uso exitoso de ranuras cuando hay muchos nodos y cada uno tiene muchas trama para enviar. Se obtiene un 0.37 de tasa de transmisión. Cuando son pocos usuariosa quizás sea necesario que los datos sean transmitidos con otros protocolos, pero cuando se tienen muchísimos más se podría utilizar Aloha Ranurado. Parece que sea 0.37 sea poco, pero cuando son miles de usuarios transmitiendo, el porcentaje es alto. En promoedio será 37 %.

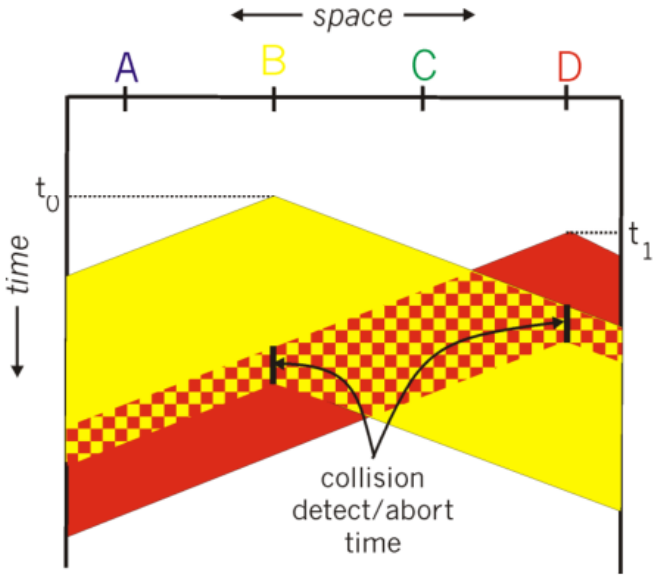
Aloha Puro (no ranurado):

Es más simple, no hay sincronización, porque no se divide en ranuras fijas. Cada uno transmite en el momento que quiera. Se puede llegar a tener doble colisión, se puede colisionar en distintos puntos, tanto al comienzo como al final. La eficiencia es la mitad del aloha ranurado.

CSMA: Cada usuario que quiera transmitir sondea el canal antes de tranmisitir, lo sondea realizando una medición. Posterga la transmisión un tiempo aleatorio, en caso de detectar que hay otros transmitiendo. Puede haber colisión porque cuando se detecta que no hay nadie, comienza a transmitir, pero hubo otro que también luego de un tiempo muy reducido, comienza a transmitir. Se puede ver que comienzan a transmitir en una distancia de tiempo muy corta, pero hay interferencia cuando se superponen.



CSMA/CD (con deteccion de colisiones): Cuando encuentra que hay colisiones, entonces deja de transmitir. Puede pasar con varios usuarios, dejan de transmitir los dos los que haya, lo que permite es que se reduce el mal uso del canal. [En la filmina 35 se ven las colisiones]



En la práctica:

- Fácil en LANs cableadas: se mide la potencia de la señal, se compara señales transmitidas con recibidas.
- Difícil LANs inalámbricas: receptor es apagado mientras se transmiten. El emisor y receptor están en la misma antena y se va alternando.

Toma de Turnos

Busca lo mejor de los Protocolos de Compartición de Canal y Acceso Aleatorio.
Nodo maestro:

- Invita a nodos esclavos a transmitir en turnos.
- Limita la cantidad de tramas que pueden transmitir dichos nodos.
- Detecta si un nodo dejo de transmitir.

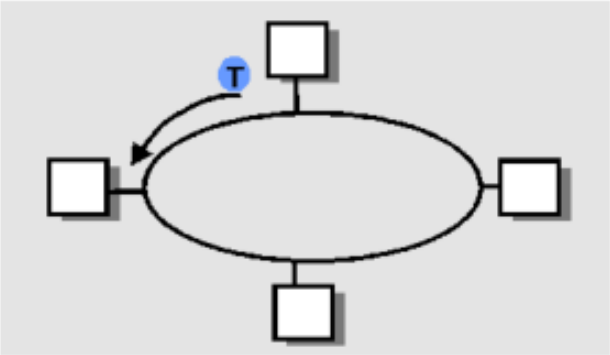
Ventajas:

- Elimina colisiones y particiones vacías.
- Mejora eficiencia.

Desventajas:

- Retardo de sondeo.
- Latencia.
- Punto único de falla (maestro).

Token: paquete que tiene un encabezado, y con datos a transmitir. Es el único dato que se puede transmitir por el canal. Cuando se quiere comunicar lo que se hace es solicitar el token, cuando se apropia un host, lo carga, y el token circula. Sólo pasa eso cuando el token está vacío, que se indica con un flag. Se utilizaba con algunas arquitecturas viejas.



Clase nº 8 - Final de teoría

Repaso de la clase pasada

Capa de enlace: sirve para transportar de nodo a nodo la información. Está encargada de corregir el grueso de los errores. Los Enlaces pueden ser compartidos o dedicados. **Compartidos**: los protocolos que se ejecutan en ellos, se ponene de acuerdo cómo compartir el medio. La forma de hacerlo es:

- Partir el canal en varios usuarios. A través de frecuencia, por tiempo. Ventajas: cada usuario tiene asignado un pedazo de canal. Contra: tasa máxima será la tasa del canal dividido la cantidad de usuarios que haya en el canal.
- Transmitir todos en el mismo canal. Cuando hay colisión, se debe retrasmitir, el cómo recuperarse de esa colisión depende del protocolo.

Direccionamiento de la Capa de Enlace

Como se sabe en la Capa de Red existen dos direcciones para poder transportar los datos entre hosts: dirección de origen y de destino.

En la Capa de Enlace se conectarán dos interfaces, esas direcciones para cada enlace conocen como **Direcciones MAC**. Son Direcciones de 48 bits, a diferencia de las IP que son de las 32.

Las direcciones MAc son Utilizadas para conducir un datagrama de una interfaz a otra interfaz físicamente conectada. Las Dirección MAC se encuentran grabada en la ROM de la tarjeta adaptadora, no es jerarquico, pero es portable porque se conserva la dirección por estar en la ROM. Por lo que se puede mover una tarjeta de una LAN a la otra, sin sufrir modificaciones en la dirección MAC. Los fabricantes de hardware son los que

compran grandes porciones de direcciones que ponen en sus productos. Anécdota: Mother a una pc de escritorio, se le ponen una placa de red se anula la que está en el mother.

Dentro de una red LAN, se conectan generalmente mediante direcciones MAC. Cada tarjeta tiene una dirección MAC, todo siempre a nivel de red local. Porque en esta red no hace falta identificar hostID ni tampoco NetID. Las direcciones lucen como números en hexagesimal, pero tanto las IP como las MAc recordar que son binarios. Las direcciones MAC se dividen en 6 grupos, lo que se hace es interpretarlo en Hexa: 1A = 0001 — 1010 en binario

Dirección de Broadcast: FF-FF-FF-FF-FF-FF = todos uno, o en IP 255.255.255.255

Dentro de la LAN se debe saber si o si la dirección MAC. Si no se sabe la MAC de destino, ¿cómo se hace para averiguar sabiendo la IP? ¿Cómo se sabe la IP? La IP a priori siempre se debe conecer, porque es la máquina con la que me quiero comunicar, se debe saber que se quiere comunicar con alguien. De alguna forma la IP es la dirección lógica (de fantasía se podría decir), y la MAC es la dirección física, donde está ese host.

Ahora bien ¿cual es esa dirección MAC? Para eso hay un protocolo **ARP**, el cual establece que cada router tiene una tabla que tiene mapeado la dirección MAC con la IP. En la tabla se encuentran los Campos IP, MAC, y un campo denominado TTL (es un tiempo de refresco de la tabla ARP), ya que se puede cambiar a la computador la placa de red (con lo cual queda la IP) o cambiar la IP por temas de administración y queda la MAC.

La Capa de Red comunica dos host y la de Enlace dos nodos. Dirección origen y destino en la Capa de Red son iguales a lo largo de toda la red. Pero en la Capa de Enlace se va modificando a lo largo de la red, ya que las direcciones origen es de un enlace de un router a otro, va cambiando la dirección por donde tiene que ir, la IP siempre se mantiene. En una LAN siempre es necesario conocer la MAC, mediante el protocolo ARP, es como se conoce o se descubre esa dirección.

¿Cómo se hace para actualizar la tabla?

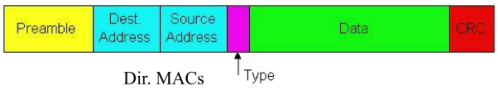
A quiere enviar un datagrama a B, y la dirección MAC de B no está en tabla ARP de A.

A envía un mensaje mediante difusión(broadcast), el cual es un paquete que en su dirección destino MAC lleva una consulta ARP, (recordar que la dirección de Broadcast son todos uno), lo reciben todos los host de area local. Consulta a todos, para el host que no es, lo descarta, cuando le llega a B, como es la misma dirección IP de B, entonces responde a la dirección MAC de origien (de A) con lo que tiene su tabla, que es la MAC y la IP. B le envía a A su dirección MAC.

El protocolo ARP es plug-and-play: cuando se conecta un host, automáticamente se genera la tabla ARP. Los nodos crean sus tablas de ARP sin intervención de la administradores.

Ethernet

El esquema de una trama vía Ethernet es el siguiente:



Prambulo: el patrón utilizado. Usado para sincronizar la frecuencia de reloj del receptor. El receptor recibe bits, pero cómo sabe dónde comienza y dónde termina un bit. Si se envían muchos ceros, el valor de tensión es siempre la misma, ¿cómo se sabe si es 3 o 4 bits enviados o la cantidad que sea? Se tiene "detección por flancos"por eso es que se envía esto. Es para marcar el tiempo.

Si el adaptador recibe una trama con dirección destino propia o dirección de broadcast (por ejemplo un paquete ARP), éste pasa los datos de la trama al protocolo de Capa de Red, de otro modo, el adaptador descarta la trama.

Tipo: indica el protocolo superior, casi siempre es IP. Pero hay otras arquitecturas que utilizan otros protocolos.

CRC: chequeado en receptor, si un error es detectado, la trama es simplemente descarta.

Servicios Ethernet

Sin conexión y No confiable:

- Flujo de datagramas pasado a la capa de red puede tener vacíos por tramas descartada.
- Los vacíos son llenados si la aplicación está usando TCP.
- Si la aplicación está usando UDP entonces va a contener vacíos en la secuencia de datos recibidos.

Utiliza CSMA/CD.

- Sin ranuras.
- Sensa por portadora ¿ el adaptador no transmite si otro adaptador lo está haciendo).
- Detecta Colisiones ¿ adaptador transmisor aborta cuando éste detecta que otro adaptador está transmitiendo.
- Acceso Aleatorio Antes de intentar una retransmisión el adaptador espera un tiempo aleatorio.

CSMA/CD de Ethernet

CSMA/CD: ¿Cómo se genera esa espera aleatoria? Se denomina Backoff Exponencial.
Objetivo: estimar la carga actual. Si la carga es alta, la espera aleatoria será mayor.

Si alguien esá transmitiendo por un canal, cada vez que quiero transmitir empeora la situación de los demas, por lo que se empeora tambien la situación de uno. Si hay mucha espera, no tiene que ser muy largo el tiempo ; es una cuestión estadística el tiempo que se espera para transmitir de nuevo. Se tira la moneda, si sale 0 se retransmite al instante, si sale 1 entonces se espera 512 períodos de bits. Si hay interrupción, puede ser ahora en vez de 0 o 1 es 0, 1 2, 3, se espera otros 512. El K se va agrandando para que sea menos probable que vuelva a estar en 0. "Backoff" significa retirarse, de forma exponencial.

Los 512 dependen del procesamiento de transmisión, por lo que si es tiene más o menos transmisión cambia ese valor. Esto mismo se utiliza también en los procesadores.

Da la impresión de que conviene tener un canal subdividido, pero en el peor de los casos se tiene muchísimas colisiones o más, elige K de en un rango que va desde 0,1,2,3,4,... hasta 1023. Si cae en 1023, que sería en el peor de los casos, se espera 50 milisegundos, que no es mucho el tiempo que se debe esperar.

$$K * 512 = X$$

$$X * 1023 = tEspera$$

El tiempo de espera está en el orden del retardo de nodos. Con lo cual el sistema es muy eficiente, aún cuando haya muchas colisiones.

Topología Estrella

En los 90 se utilizaba la topología BUS. Comunicaba a través de un medio compartido, complementamente compartido. NO es muy versatil, ya que había que cortar el cable si se quería conectar otra máquina, y volver a reconectar todo de nuevo, por lo que se perdía mucha calidad de transmisión.

A medida que se escala, y que las computadoras se vuelven menos costosas, que hay necesidad de agregar más computadoras, fue naciendo el centro de estrella. El primero fue el HUB, dispositivo sin inteligencia que lo único que hace es una vinculación física entre uno y otro host, no procesa direcciones MAC. Lo que hacía es distribuir la información para todos vía inundación de canal, es decir mediante Broadcast, sin importar si tenía las direcciones de origen y destino, lo retransmite para todos.

Pero es muy ineficiente porque inunda toda la red. Se tenía un problema de seguridad, ya que a todas les llegaba toda la información, por lo que estas conexiones eran muy vulnerables. El HUB aumenta la probabilidad de colisiones. Recordar que el HUB es de la Capa Física. Se desarrolla un dispositivo conocido como Switch, que tiene la psibildiad de intercambiar canales entre otros.

Switches

Características de los Switches:

- Dispositivo de capa enlace de dato:
  - Almacena y re-envía tramas Ethernet.
  - Examina encabezados de tramas y re-envía basado en dirección MAC.
  - Cuando debe re-enviar una trama utiliza CSMA/CD

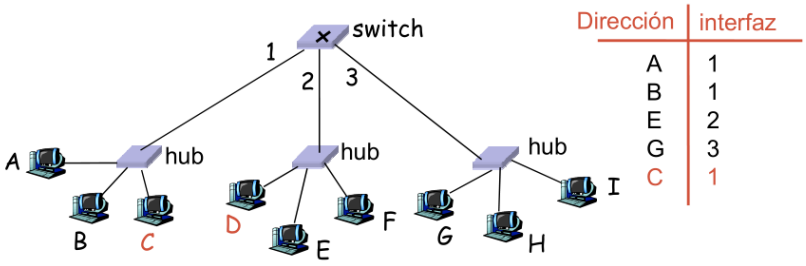
  Transparente:
  - Hosts no notan la presencia de switches

  Plug-and-play (aprenden solos):
  - Switches no requieren ser configurados. Aprenden solos.
  - Divide la subred en segmentos de LAN (para efectos de colisiones, por ejemplo)

Filtra paquetes:

- Tramas de un mismo segmento de LAN no son re-enviados a los otros segmentos.
- Los segmentos pasan a ser dominios de colisión separados.

Cada Switch tiene una tabla de conmutación. La tabla es lo que aprende ni bien se conecta a la red.



D transmite primero al HUB, el HUB no lo encuentra entonces lo envía a switch, como en su tabla el switch no lo encuentra, lo que hace es enviarlo a todos, lo inunda. Cuando recibe D un paquete de C, entonces D lo envía al HUB, lo envía a D, E, F, el HUB lo envía al switch y eso hace que el switch se agregue a D en su tabla.

A medida que los paquetes pasan por el Switch, va aprendiendo dónde está cada host. Cuando se conecta todo en su tabla está en 0. [Esto se toma en el parcial]

El Switch evita colisiones cuanto más conozca la red, ya cuando el Switch tiene sus tablas ARP que viajan directamente de host a host, pero si hubiese en vez de un Switch un HUB, entonces habría má colisiones ya que está todo el tiempo transmitiendo mediante broadcast, por lo que inunda la red. Desde el punto d vista del tráfico, la eficiencia de la red disminuye mucho.

Aislamiento de tráfico

El HUB tiene un Dominio de Colisión muy amplio. Retransmite a todos lados, hace que se colisione todo con todos. Pero con el swithc al filtrar paquetes, aisla el Dominio de Colisión, porque por cada transmisión tiene la posibiliad de aprender la topología de la red.

No es del todo aislado, las tablas ARP siempre se regeneran por lo que los paquetes distribuidos Broadcast siguen existiendo, pero sólo cuando no está completa o generada la tabla ARP.

Switches de acceso dedicado:

- Switch con muchas interfaces
- Cada host tiene conexión directa al switch
- No hay colisiones; full duplex.

Diseño de Redes Institucionales

Es complejo, hay mucha bibliografía al respecto. Cosas a tener en cuenta: Las colisiones dependen de los Usuarios a conectar. Conviene separar las computadoras por oficinas, conectados por Switch, y todos esos Swtich conectados a un Swtich CORE. Dentro de este Core se suele conectar servidores. Hay que tener en cuenta que la conexión del Core siempre debe ser mejor que las demás, ya que conecta para todos.

Existen 3 niveles de Switch depende del tamaño de la corporación. Swithc de nivel 3: rompe el principio de que es un dispositivo de Capa 2, pero si puede rutear por direcciones IP, no necesite actualzar la tabla ARP. Si se quiere comunicar internet hacia afuera, se debe tener en cuenta que debe poner un Router. En la filmina está mal puesto el HUB, es porque la filmina es vieja, podría ir bien los Switch.

Se debe saber lo que es un HUB de un Switch. Cómo divide los dominios de colisiones.

Switches vs. Routers

- Ambos son dispositivos de almacenamiento y re-envío
  - Routers son dispositivos de capa de red (examinan encabezados de capa de red)
  - Switches son dispositivos de capa enlace de datos.
- Routers mantienen tablas de ruteo, implementan los algoritmos de ruteo.
- Switches mantienen las tablas de switches, implementan filtrado y algoritmos de aprendizaje.

Resumen comparativo

	Hubs	Switches	Routers
Aisla tráfico	No	Si	Si
Plug & play	Si	Si	No
Ruteo óptimo	No	No	Si

Lo que se puede ver en el gráfico es que los Switches no reconoce las direcciones IP, sólo trabaja con direcciones MAC. El router si entiende de la Capa nº 3, de Red, es decir que trabaja con direcciones IP.