Redes I

Resumen Primera Parte

Emiliano Salvatori

Agosto 2019

1. Clase 2

1.1. Partes de la red

Frontera de la red: dispositivos que estan dentor de una red en si mismo. **Nucleo**: todos los disipotitivos que interconectan los hosts: ruters, etc.

La gestión de Internet se realiza mediante conmutación paquetes.

Red de acceso: Red formada por nodos de tipo rouers. 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: se denomina los nodos interconectados de la red.

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 luar físico reducido. Se puede tener un red de area 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 con simplemente interconectada con su propia red interna. PREGUNTAR

1.2. ¿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

1.3. ISP

Hay empresas que generan nodos, inviernetn 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 "pegaje".

El ancho de banda es algo que se contrata e incide en el precio, ¿por que? Por los destinos 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 es simetrico muchas veces. Esto es porque en algunos servicios se requiere que sea asimetrico y en otros servicios no, dependiendo del negocio que se tenga en mente para consumir ese servicio. Por ejemplo si se tiene una corporación que tiene una pagina web que se necesita 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. 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.

1.4. Infraestructura para internet

La problemática cuando se fue haciendo cada vez más necesario brindar el servicio de internet fue: ¿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 mediante 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 horairo de uso. Luego surgió lo denominado **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 .ºn". 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 trenzadoτ 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 mediante antenas; es decir: fibra optica hasta el nodo más cercano y desde ahí antena. Se taza por ancho de banda, no por usuarios.

Fibra optica Tripe Play = 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: 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 se produce un cambio instantáneo según el profesor por 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.

1.5. División de la parte física

En el cable Coaxial viajan muchas frecuancias superpuetas pero se pueden discriminar 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 es que lo vea 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 puedeestablecer existen datos transfiriéndose o no, pero cuando se conecta a internet hay transporte de datos por lo que se sabe si existen datos 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 si 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.

1.6. 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 mucho araea, como por ejemplo el area 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 para los usuarios que paguen el servicio, pero por wifi.

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]

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 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 SÓLO 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.

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

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.

1.7. 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 qeu cada ISP ponga nodos para conectar entre países. Los enlaces para ello debe ser 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).

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 brindan 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.

1.8. 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 usuarios.

Modelo OSI: modelo de referencia general de comunicación y más completo. Pero en la jerga siempre se utiliza el modelo de 5 capas explicado anterior. 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. Antes cada fabricante hacía su propia red y para interconectarse era basante difícil, si se toma como modelo de TCP/IP es más fácil de relacionarla. El modelo consta de los siguientes estratos:

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 mcuhos 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.

Modelo OSI: modelo de referencia general de comunicación y más completo. Pero en la jerga siempre se utiliza el modelo de 5 capas explicado anterior. Modelo OSI es de referencia. El TCP/IP 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.

1.9. 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 transferrir archivos, el protocolo especifica 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. 2 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 dar.

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

1.10. 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.

1.11. 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 lo que 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, estalo toma y entiede el mensaje "Holaτ el encabezado de la capa de aplicación

como si fueran datos, por lo que para esta capa todo lo de la 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.

1.12. 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.

1.13. 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.

2. Clase nº 3: Capa de Red

2.1. Funciones claves

La función de la capa de red es por tanto tremendamente simple: transporta paquetes desde un host emisor a un host receptor. En la realización de esta tarea podemos identificar dos importantes funciones de la capa de red:

¿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 agarrar 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 des tino.

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 Dikstra. 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 es que todos corran el mismo algoritmo y 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 por hardware y por dónde salir no determinado por los algorítmos de Red.

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.

2.2. 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, una 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 cómo se hace 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).

2.2.1. 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.

2.2.2. 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.

2.3. 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.

2.4. 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 petición 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 tipo de Aumentar el espacio de direcciones, es la motivación inicial. También permite cambiar el encabezado para agilizar el envío y el recibo, y también Cambiar encabezado para facilitar QoSk: 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. El nuevo IP Evita el Nateo (utlizar el protocolo NAT). El encabezado se duplicó, la fragmentación no está permitida. Permite direcciones anycast: Se elimina el checksum. Se elimina el campo de opciones. Y hay ua nuvea versión ICMP para que labure con este protocolo. iderablemente 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).