**RESUMEN REDES DE INFORMACION 1er Parcial**

**UNIDAD N°1: ARQUITECTURA DE REDES**

Clase 12 de Marzo

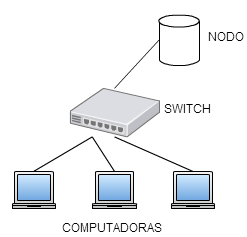
**Red:** Conjunto de dispositivos interconectados, que pueden estar cercanos o no.

**Red Informática:** Se utiliza para compartir recursos e intercambiar información. En este tipo de red el emisor y el receptor están cerca.

**Red de Telecomunicaciones:** Es una red donde el emisor y el receptor están muy lejos.

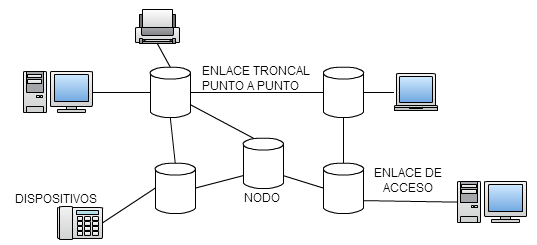
|  |  |
| --- | --- |
| **VENTAJAS** | **DESVENTAJAS** |
| * Compartir recursos * Rapidez de comunicación * Seguridad * Administración centralizada (Los datos se almacenan en un servidor central y se puede controlar el acceso a los mismos) * Teletrabajo (Trabajo desde mi casa) * Disponibilidad * Tolerancia a fallos * Movilidad | * Costo de implementación (es inicial, solo se hace una vez) * Seguridad (naturalmente no son seguras, hay que implementarla y hacerlo bien) * Costo de mantenimiento |

**Componentes de una LAN:** Componentes necesarios para instalar una red en una empresa.

* Estaciones de trabajo y servidores.
* Dispositivos de interconexión (Switch, Router, HUB, Access Point)
* Medios de conexión (UTP, Coaxil, Fibra óptica, Aire, conectores, etc.)
* NIC (Network Interface Card o tarjeta/placa de red)
* Protocolos de conmutación
* Recursos compartidos
* Sistemas operativos de red (Los que se instalan en las estaciones de trabajos y servidores)
* Aplicaciones

**Componentes de una WAN:**

* Nodos: Cumplen la función de encaminar los paquetes (decidir por qué enlace sale la trama)
* Enlaces: Son lo que une los dispositivos
  + Troncales: Son los que van de nodo a nodo
  + De acceso: permiten interconectar el dispositivo hacia la red wan
* Dispositivos de interconexión (Terminales, hosts)
* Protocolos de comunicación: Estos son distintos a los de la red LAN (Frame Relay, red telefónica, ATM, etc)



**Clasificación de las redes:**

1. **Según el área de cobertura:**
   * PAN (Personal Area Network): Un ejemplo sería una red que se puede establecer entre la pc y un teléfono celular
   * LAN (Local Area Network): Tiene un área de cobertura relativamente chica , hasta un kilómetro puede ser mas o menos no es algo estricto. Son propietarias, es decir que pertenecen a una organización, y solo pueden acceder las personas o empleados que pertenezcan a esa organización. La velocidad de acceso es alta con respecto a las WAN,
   * MAN (Metropolitan Area Network): Son redes que salen de la empresa y abarcan una ciudad, lo mas común es que se implementen con un “anillo” de fibra óptica (como por ejemplo EPEC) otro ejemplo puede ser la red de TV Cable.
   * WAN (Wide Area Network): Pueden abarcar un país o un continente, son propietarias pero de uso público (pago), es decir que se puede contratar para tener acceso. La velocidad de transmisión es más lenta que las LAN, ya que es de telecomunicación (los dispositivos están alejados).
2. **Según la tecnología de transmisión:**
   * Redes de difusión (Broadcast): En general las redes LAN son de difusión, por ejemplo un punto de acceso wireless, difunde el mensaje a todos los dispositivos conectados, y sólo la maquina que le corresponde acepta dicho mensaje.
   * Redes Punto a Punto: Supongamos un switch y varias pc conectadas, cuando una maquina le quiere enviar un mensaje a otra, el switch se fija la dirección de destino y si la tiene conmuta y une el camino entre dichas máquinas, lo que se conoce como conexión punto a punto.

Clase 19 de Marzo

**Clasificación de las redes (Continuación):**

**3) Según la direccionalidad de los datos:** clasifica a las redes según la dirección en la que se mueven los datos, es decir, según vayan hacia un lado o hacia el otro:

* **Simplex:** en estas redes la información es transmitida en un único sentido o dirección, es decir, va y no vuelve. Vamos a tener un origen y uno o muchos destinos. Por ej: una radio, hay una emisora y los receptores no pueden transmitir.
* **Semiduplex:** también conocidas como half-duplex. En este caso puedo transmitir información en ambos sentidos pero no de manera simultánea (al mismo tiempo). Por ej: los handies.
* **Dúplex:** también conocidas como full-dúplex. En este caso puedo transmitir información en ambos sentidos de manera simultánea. Por ej: la telefonía.

**4) Según la topología física:** clasifica a las redes según como están conectados físicamente los dispositivos entre sí:

* **Anillo:** puede ser de anillo simple o doble. Se usa para redes MAN
* **Estrella:** es la que se usa cuando tenes un swith o hub donde están conectadas las maquinas.
* **Bus:** es un canal principal donde se van conectando los distintos dispositivos. Por ej: red de cable.
* **Malla:** es cuando se conectan todos los dispositivos entre sí. Tendremos enlaces para una malla completa. Tiene enlaces redundantes.

**5) Según la tecnología de implementación:** clasifica a las redes según como se va a comunicar un dispositivo que está en un extremo con otro dispositivo que está en otro extremo de la red. Se usa para redes WAN.

* **Conmutación de circuitos:** es la que implementa la red de telefonía convencional. Presenta la característica de tener 3 fases: establecimiento de llamada, transferencia de datos, y finalización de la llamada. En el establecimiento de la llamada se va abriendo el *circuito*, es decir se va formando el camino por donde van a viajar los datos. Antes de poder establecerse la llamada o conexión definitivamente, debe aceptarse la llamada (el receptor debe levantar el tubo); cuando esto ocurra la aceptación de la llamada volverá hasta el emisor por el mismo camino físico por el cual llegó, y en el momento en que el emisor recibe ésta aceptación es cuando queda establecida la conexión. A partir de este momento comienza la transferencia de datos que se da de manera dúplex, es decir que la transferencia se da en ambos sentidos y de manera simultánea. La transferencia de datos termina cuando alguien finaliza la llamada. Este último paso es importante ya que al momento de establecer la llamada se reserva ancho de banda para poder enviar los datos, y el mismo deja de utilizarse únicamente al momento de finalizar la llamada.

Es importante recalcar que todos los datos viajan por el mismo camino físico.

*Ventajas:* *garantiza la calidad de servicio*: como se reserva un ancho de banda, es decir cómo se reserva un camino para la conexión, los datos llegan instantáneamente ya que la única demora que tengo es el tiempo de propagación de la señal (que se propaga muy rápido, tiene bajo retardo). Por lo tanto se me garantiza una alta velocidad para transmitir los datos.

*La información no llega desordenada.*

*Desventaja:* *No es tolerante a fallas o fiable:* esto quiere decir que si se cae un nodo se corta la comunicación porque se pierden todos los enlaces establecidos que pasan por ese nodo, lo que implica que haya que establecerse nuevamente la conexión.

* **Conmutación de paquetes:** presenta la característica de que la información que quiero enviar es dividida en trozos llamados *paquetes*. Cada uno de estos paquetes puede viajar por un camino diferente si el enlace o camino por el cual los envío está muy ocupado, por lo tanto cada uno deberá tener la dirección de origen y la dirección de destino para que sean autónomos e independientes y puedan llegar todos al mismo destino. Como los paquetes pueden tomar distintos caminos puede ocurrir que lleguen desordenados al destino (algo que no sucede en la conmutación de circuito ya que la información llega toda junta por un mismo camino físico).

Aquí no hay establecimiento de la comunicación como ocurría en la conmutación de circuitos

*Ventaja:* si se cae un nodo solamente se pierden los paquetes que estén en ese momento en la memoria de ese nodo (el resto sigue su camino), es decir que no se corta la transmisión sino que solamente tengo que reenviar los paquetes que se perdieron. Se llaman nodos de almacenamiento reenvió, ya que los paquetes llegan al dispositivo (un router) donde se almacenan momentáneamente en memorias (buffers), hasta que el dispositivo tiene tiempo de procesar esos paquetes y encaminarlos por los distintos enlaces.

*Desventajas:* *transmisión de datos más lenta:* esto se debe a que cada paquete que llega al dispositivo del nodo (router) tiene que ser reencaminado.

*Puede que los datos lleguen desordenados.*

* **Retransmisión de tramas (frame relay) NO LO VAMOS A VER:** es un hibrido (mezcla) entre la conmutación de paquetes y la conmutación de circuitos, sacando lo mejor de cada uno. Consiste en transmitir paquetes (que en frame relay reciben el nombre de tramas) todos por un mismo camino físico, es decir dividido a la información en trozos o tramas (conmutación de paquetes) que son enviadas por un circuito o camino virtual (conmutación de circuitos). Los datos llegan ordenados.

*Ventaja: Rapidez:* los switch lo único que hacen es recibir una trama y conmutarla. La conmutación a nivel de trama (capa 2 del modelo OSI: Enlace) es mucha más rápida que la conmutación de paquetes (capa 3 del modelo OSI: Red).

*Desventaja: no es fiable:* si se cae un switch o nodo se pierde la comunicación, pero no hay que retransmitir todos los paquetes, sino solo aquellos que no llegaron a ser enviados

* **Conmutación de celdas:** ATM (modo de transferencia asíncrono)

Los datos que se van a transmitir se dividen en trozos muy pequeños llamados celdas todos del mismo tamaño (celda= 53 bytes). Estas celdas tienen un tamaño muy pequeño si las comparamos con una trama Ethernet que tiene un tamaño de 1500 bytes. La idea de trabajar con tamaños tan pequeños para celda es que es mucho más rápido conmutar trozos pequeños que grandes. La conmutación se da a nivel de hardware.

**6) Según el ancho de banda:** está relacionado con la cantidad de información que se transfiere por unidad de tiempo.

* **Banda angosta:** las redes de telefonía o la primera generación de celulares son de banda angosta
* **Banda ancha:** las redes que transmiten imágenes como la red de tv por cable o también la tercer generación de celulares es de banda ancha.

**ARQUITECTURA TCP/IP:**

Esta arquitectura utiliza la conmutación de paquetes para la transmisión de datos. Nace a partir de lo que se conoce como DARPA net (Agencia de Proyectos de Investigación Avanzados para la Defensa). DARPA fue un proyecto militar de los Estados Unidos.

Protocolo: es un estándar que sirve para ponerse de acuerdo entre los distintos dispositivos que se van a comunicar sobre cuál será el significado o interpretación que tendrá una trama de bits (formato de una trama). Es un software que interpreta los bits siempre de la misma forma, que previamente fue instalado en ambos dispositivos que participan de la comunicación. Por ej: al receptor únicamente le llegan unos y ceros, entonces por medio de un protocolo se le dice cómo interpretarlos: los primeros 48 bits son de la dirección origen, los segundos 48 bits son de la dirección destino (es el formato de trama).

TCP/IP es una pila de protocolos (muchos) que trabajan de manera conjunta. TCP significa Transmission Control Protocol – Protocolo de Control de Transmisión, mientras que IP significa Internet Protocol – Protocolo de Interred. Si bien esta arquitectura consta de una pila de protocolos como antes dijimos, recibe este nombre debido a que estos dos protocolos son los más importantes.

**Objetivos:**

* **Conectividad permanente:** con esto se busca que si se cae un nodo a través del cual se está estableciendo una comunicación la misma no se pierda, esto implica que los paquetes que se transmiten tomaran otro camino físico para llegar al destino (conmutación de paquetes)
* **Independiente del hardware y del sistema operativo:** debe poder implementarse sin importar el hardware o el sistema operativo que se esté ejecutando en ese hardware.
* **Transmitir todo tipo de información:** permite transmitir archivos de texto, videos, música, etc.

**Comparación del modelo TCP/IP con el modelo OSI**:

**Modelo TCP/IP: Modelo OSI:**



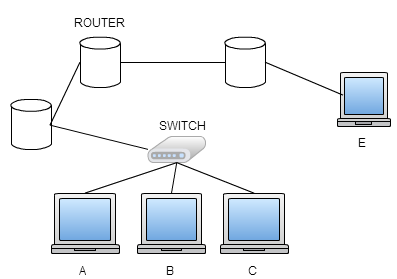
El modelo TCP/IP tiene 4 capas o niveles en comparación con el modelo OSI que tiene 7. La capa de Aplicación de TCP/IP incluye las capas de Aplicación, Presentación y Sesión del modelo OSI ya que no es necesario hacer una subdivisión para esas capas. La capa de presentación está referida a como se van a representar los datos (en código aski, en código bcdic, etc.).

La capa de transporte es la misma para ambos modelos, al igual que la capa de red en donde lo único que cambia es el nombre.

La arquitectura TCP/IP define los protocolos desde la capa de Interred hacia arriba, desde esta capa para abajo (Host a red) no define nada ya que es independiente del hardware y el sistema operativo. La capa de Host a red (también llamada capa de enlace) abarca las dos primeras capas del modelo OSI: Enlace y Física.

Las unidades en que trabaja cada capa, en el modelo OSI, se denominan PDU (unidad de datos de protocolo). En el modelo TCP/IP estas unidades cambian, a nivel de la capa de aplicación hablamos de *datos* (archivo de texto, imagen, voz, etc), en la capa de transporte se habla de *segmentos*, a nivel Interred hacemos referencia a los *paquetes*, mientras que en la capa de Host a red a nivel de enlace utilizamos las tramas y a nivel físico hablamos de bits.

* **Host a red:** la función de esta capa es transferir datos entre maquinas que pertenecen al mismo segmento o enlace.

****

Para poder transferir datos entre dos maquinas necesito tener alguna dirección para que el switch sepa a qué maquina le envío los datos (o trama propiamente dicho), en el caso de que queramos comunicar la maquina A con la C esta dirección seria la MAC, si quisiera comunicar la maquina A con la E utilizaría el IP lo que me haría trabajar en la siguiente capa y no en esta debido a que aquí solo se trabaja entre dispositivos del mismo segmento.

* **Interred:** la función de esta capa es intercambiar datos entre maquinas que pertenecen a segmentos distintos, es decir que están distantes entre ellas. En este caso hacemos lo que se llama telecomunicación (comunicación a distancia).

Esta capa tiene 3 funciones: Direccionamiento, Encaminamiento y Control de congestión.

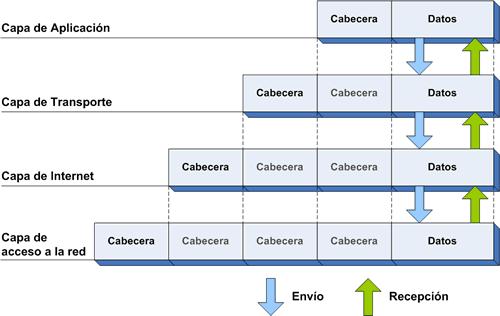
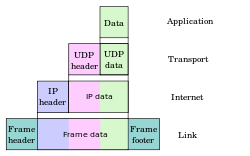
**Características del protocolo IP (Internet Protocol – Protocolo de Interred):**

Este protocolo se implementa sobre la conmutación de paquetes. Presenta las siguientes características:

* *No orientado a conexión:*significa que cada paquete se transmite de manera independiente y no se establece una conexión entre los extremos como si sucede en la conmutación de circuitos, ya que dijimos que se implementa sobre una conmutación de paquetes únicamente. La información se divide en paquetes los cuales son enviados al router que se encargará de fijarse cual es la dirección de destino (IP en este caso) y en base a tablas decide por qué enlace envía ese paquete.
* *No fiable:*este protocolo intenta que los datos lleguen a destino, pero no garantiza que los mismos lleguen, es decir que los datos pueden perderse en el camino.
* *Direccionamiento:*para tener conectividad en internet necesito tener una IP donde comunicarme, es decir una dirección que sea única e irrepetible (análogamente con la comunicación telefónica que se necesita tener un número de teléfono único e irrepetible)
* *Encaminamiento:*cada vez que llega un paquete el router lo encamina en función de la IP de destino.
* *Control de congestión:* consiste decidir por cual camino van a ser enviados los datos evitando seleccionar un camino donde haya mucho tráfico. Está relacionado con la calidad de servicio, la cual implica que los datos lleguen rápido al otro extremo (por ejemplo cuando transmito en tiempo real).

**Encapsulamiento:** para enviar datos a través de una red los mismos son pasados a la capa inferior, en donde se le agrega un encabezado. Esto se debe a que cada capa habla un idioma distinto por utilizar distintos protocolos, entonces los datos que llegan a una capa deben ser encapsulados, lo que implica que se les agrega un header (encabezado) del protocolo en el cual estoy trabajando. El encapsulamiento se da a medida que los datos bajan por las distintas capas

**Desencapsulamiento:** Es el proceso inverso al encapsulamiento. El router recibe un conjunto de bits a los cuales debe desencapsular, lo que implica que debe conformar o recomponer la trama, esto es: toma la trama y elimina de la misma el encabezado. De esta manera se queda únicamente con la parte de datos de la trama, los cuales dentro tienen un encabezado de paquete (el IP) que es el que le interesa al router por ser un dispositivo de capa 3 (que trabaja con paquetes). Luego busca la dirección de destino, consulta una tabla y encamina.

** **

* **Transporte:** esta capa tiene como función conectar dispositivos extremo a extremo. Esta conexión es una conexión lógica, no física. Además, tiene dos funciones bien definidas por lo que utiliza dos protocolos que son el TCP y el UDP para implementarlas. Las funciones a las que antes hacíamos referencia son: Orientada a conexión y No orientada a conexión.

Otra funcionalidad que presenta esta capa es la de segmentación de datos.

**Características del protocolo TCP (Transmition Control Protocol - Protocolo de Control de Transmisión):**

Este protocolo se utiliza para la transferencia de todo tipo de datos como las transacciones bancarias, envíos de mail, etc.

* *Orientado a conexión:* Si quiero comunicarme con un dispositivo que está muy ocupado y le envío los datos, ese dispositivo no tendrá lugar en su buffer para almacenar todos los segmentos que le voy a transferir. Entonces, para garantizar que el dispositivo va a procesar todos los segmentos que le envío, antes de enviarlos le consulto si está preparado para recibir los datos, de manera que reserve lugar en el buffer para almacenar todos los datos que le voy a enviar. Es por este motivo que decimos que es una conexión lógica y no física, ya que me conecto con el dispositivo para asegurarme que va a recibir todos los datos, pero luego esos datos o segmentos pueden viajar por caminos físicos distintos, lo que no me garantiza que los segmentos lleguen ordenandos al destino.
* *Fiable:* Me garantiza que todos los datos que son enviados van a llegar a destino, no puedo garantizar que me lleguen ordenandos, pero una vez que todos los datos llegan la capa de transporte los reordena antes de pasarlos a la capa de aplicación. Para asegurar que todos los datos fueron entregados se utiliza un acuse de recibo, que funciona de la siguiente manera: cuando el receptor recibe todos los segmentos le avisa al emisor dicha situación mandándole un mensaje, de esta manera el emisor sabe que toda la información llego bien. Supongamos el caso de que después de un tiempo el emisor no recibe el acuse de recibo por parte receptor, entonces el emisor interpreta eso como que los paquetes no llegaron al destino y por lo tanto los retransmite. La fiabilidad también contempla lo que se conoce como integridad de datos, que garantiza que la información o datos que se envía no va a ser alterada por nadie ni nada en el camino que recorre; esto se logra aplicando un código de integridad en el origen y luego volviendo a aplicarlo en el destino, si dan el mismo resultado significa que los datos no sufrieron ningún cambio, si da incorrecto debe retransmitirse los paquetes necesarios.
* Es más lento que el protocolo UDP.

**Características de UDP (User Datagram Protocol – Protocolo de Datagrama de Usuario):** Este protocolo se utiliza para las transmisiones en vivo o tiempo real de audio o video, porque no me garantiza que los datos lleguen pero me brinda mucha velocidad.

* *No orientado a conexión*
* *No fiable:* no me interesa garantizar que todos los datos enviados lleguen a destino.
* Es muy rápido.

Proceso de encapsulamiento en la capa de transporte:

Como sabemos, la comunicación entre capas es adyacente y por lo tanto, para el encapsulamiento, la capa de transporte recibirá los datos de la capa de aplicación. Como las capas hablan en distintos idiomas por tener protocolos diferentes, será necesario encapsular los datos que recibe la capa de transporte. Para ello, lo que se hace es tomar los datos tal cual llegan de la capa de aplicación, guardarlos en un campo datos, y agregarle un encabezado del protocolo en el cual este trabajando en la capa actual. Por tratarse de la capa de transporte, los protocolos que se utilizan son TCP o UDP

Otra funcionalidad importante de la capa de transporte es la de *segmentación de los datos:* Partimos del hecho de que en la capa de transporte hablamos de segmentos, y esto implica dividir los datos en trozos de un determinado tamaño a los que se le agrega un encabezado.

* **Aplicación:** Hace referencia a aplicaciones de red NO de escritorio, es decir hablamos de aplicaciones que me permiten transferir datos. Se utilizan los siguientes protocolos:
* *HTTP:* Hiper Text Transfer Protocol – Protocolo de Transferencia Hiper Texto. Se utiliza para transferir páginas Web. Este protocolo está montado (implementado) sobre TCP.
* *FTP:* File Transfer Protocol – Protocolo de Transferencia de Archivos. Se utiliza para transferir archivos. Este protocolo está montado (implementado) sobre TCP.

Clase 26 de Marzo

* *SMTP:* Simple Mail Transfer Protocol – Protocolo Simple de Transferencia de Mail. Se utiliza para la transferencia de correo, fue el primero que se uso para dicha función. También se conoce como protocolo de entrega porque entrega correos desde las maquinas al servidor de correo, y a su vez entre servidores. Este protocolo está montado (implementado) sobre TCP. Se llama simple porque originalmente permitía transmitir únicamente código aski.
* *SNMP:* Simple Network Management Protocol – Protocolo Simple de Gestión de Red. Se utiliza para administrar o gestionar redes, generalmente se usa en redes chicas (10 o 20 dispositivos) donde se pueden administrar manualmente los dispositivos. Sirve para ver si funcionan correctamente todos los dispositivos de mi red (pc, impresora, switch, antena, cámara web, etc.). este protocolo está montado sobre UDP porque la idea de la gestión es que se consuman pocos recursos de red, y el protocolo TCP consume muchos recursos.
* *RTP:* Real-Time Transfer Protocol – Protocolo para Transferencia en Tiempo Real. Se utiliza para la transferencia en tiempo real. Puede montarse sobre TCP y UDP, pero generalmente se lo utiliza con UDP (porque es más rápido).
* *DNS:* Domain Name System – Sistema de Nombre de Dominio. Se utiliza para traducir las direcciones de dominio en direcciones IP, esto es así porque es seria muy difícil recordar las direcciones IP de las computadoras a las cuales nos conectamos, entonces se ideo darle un nombre de dominio a ese sitio o pc (cualquier nombre de una página web) que esté vinculado a una IP. Además, cumple la función de ser una base de datos distribuida a nivel mundial, porque contiene todas las direcciones IP. Esta montado sobre UDP.

**INTERNET:**

Es una red de redes. En un comienzo las empresas formaban su propia red LAN, pero en un momento surgió la necesidad de conectar esas redes y es allí donde surge internet. ¿Quién es dueño de internet? Es de todos y no es de nadie, es decir la usamos todos, somos todos participes de ella, pero existe un backbound o columna vertebral de internet.

**Evolución:**

Nace en Estados Unidos como una necesidad del departamento de defensa que necesitaba garantizar conectividad todo el tiempo para su red (que era una red telefónica), entonces a partir de esto se funda la DARPA –Agencia de Proyectos de Investigación Avanzada para la Defensa-. Esta organización firma convenios con universidades para que investiguen sobre la conmutación de paquetes, y de esta manera se logra que las universidades se interconecten entre sí (inclusive a través de dispositivos diferentes), dando origen a lo que se conoce como DARPANET, que es una red de DARPA que estaba conformada por las redes de todas las universidades que habían firmado el convenio antes mencionado con ARPA. Aquellas universidades que querían conectarse a la red DARPA y no habían firmado el acuerdo no podían hacerlo, es por este motivo que se da comienzo a la NSFNET –National Sciense Fundation o Fundación Nacional de la Ciencia- para integrar a esta gente que quedo fuera.

A partir de estas dos grandes redes, como necesidad de unión de ambas, nace lo que hoy en día conocemos como INTERNET. En el comienzo internet simplemente se utilizaba por muy poca gente y para mandar algún archivo o mail, pero hoy en día es una herramienta que contiene una cantidad inmensurable de integrantes que tuvo un crecimiento muy grande debido a la Worl Wide Web que surgió en Europa. La WWW surge como una necesidad de intercambiar documentos y paginas en HTML, de manera que las personas puedan intercambiar documentos por más que se encuentren en distintos países. En este entonces, todos los enlaces eran de 56k, que eran provistos por las redes telefónicas a las que se contrataba para poder tener el servicio de internet.

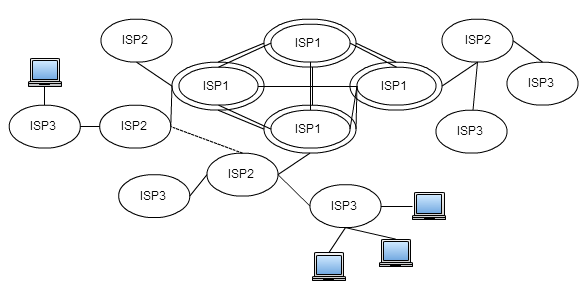
**Servicios básicos:**

Los servicios básicos que originalmente brindaba internet se ejecutan en la capa de aplicación y son los siguientes:

* Correo electrónico
* Transferencia de archivos
* Grupos de noticias: si me interesa algún tema en particular me inscribo a un grupo y recibo información sobre ese tema.
* Ejecución remota: me permite ejecutar comandos en otros dispositivos. Se usa para configurar, o administrar otros dispositivos.

**Arquitectura:**

Jerárquicamente Internet está organizada de la siguiente manera:



ISP: Internet Service Provider – Proveedor de Servicio de Internet

ISP1: proveedor de servicio de internet nivel 1

ISP2: proveedor de servicio de internet de nivel 2

ISP3: También se lo conoce como ISPLocal. Es el proveedor de servicios de internet de nivel 3 al que se conectan los usuarios.

Las grandes empresas de telecomunicaciones se conectan entre sí con enlaces de muy alto ancho de banda y forman lo que se llama el backbound (columna vertebral) de Internet, en donde hay enlaces redundantes (marcados con doble línea en la grafica) para garantizar que si se cae uno no se pierde la conexión. Estos proveedores de servicio de Internet (ISP1) crearon y son dueños de grandes instalaciones o redes conectadas mediante fibra óptica, que se las conoce como redes de transito que brindan conectividad al resto de proveedores de servicio de internet. Una pc de un usuario nunca se va a conectar a una red de transito, porque su función no es brindarle servicio a usuarios comunes sino a grandes proveedores de servicio de internet (los ISP2).

Los ISP2 son empresas que pagan a los ISP1 por el uso de los servicios del backbound. A su vez, estos les cobraran por sus servicios a los proveedores de servicio de internet ISP3. Por su parte, los ISP3 les cobran a los usuarios comunes por acceder al servicio de internet.

Si un usuario que está conectado a un ISP3 quiere conectarse con otro usuario que está conectado con otro ISP3, debería trasladarse o moverse a través de toda la red para poder lograrlo. Para evitar esto se utiliza lo que se llama conexión entre pares (peer to peer), esto significa que los ISP de un mismo nivel se pueden comunicar directamente sin tener que pasar por el resto de los proveedores de servicio.

**Alternativas de conexión a Internet:**

Los distintos tipos o alternativas de acceso a internet que existen son:

* **Modem:** Un modem se conectaba a través de una red telefónica, donde accedíamos a 56Kbytes de velocidad para navegar. Como la computadora transmite digitalmente y la red telefónica lo hace de manera analógica, se utiliza el modem que convierte la señal digital en analógica. Esta velocidad funciona para funcionalidad básica, pero para las transferencias de video o imágenes (que ocupan mucho ancho de banda) no es buena.

La desventaja que presenta este tipo de conexión es que no se podía usar simultáneamente el

Servicio de internet y teléfono, es decir o se transmitía voz o se transmitían datos, pero ambos al mismo tiempo no era posible.

* **ADSL:** Asymmetric Digital Subscriber Line – Línea de Subscripción Asimétrica Digital. Asimétrica significa que el ancho de banda para bajar datos es distinto al ancho de banda para subir datos, el que se utiliza para bajar es mayor que el que se utiliza para subir debido a que los usuario descargan muchas más cosas que las que suben. Esta tecnología está montada sobre la red telefónica, pero la diferencia que presenta con la anterior es que aprovecha el ancho de banda que no se utiliza para la transmisión de voz, lo que hace que el ancho de banda disponible sea mayor. Me permite hablar por teléfono y conectarme a internet simultáneamente. La restricción que presenta es que para utilizar el servicio tengo que estar cerca de la red telefónica (a menos de 5 o 6 kilómetros) y la línea tiene que tener buena calidad para poder brindar una alta tasa de transferencia.
* **Cable-Modem:** Esta tecnología está montada sobre la red de tv por cable, y esto es posible porque utiliza distintas frecuencias para enviar (y recibir) datos y para enviar la señal de cable. La diferencia con la conexión ADSL es que en ella tengo un ancho de banda asignado punto a punto, y en este caso el ancho de banda se comparte entre todos los abonados porque todos están conectados a una topología de red de bus.

**ORGANISMOS INTERNACIONALES DE ESTANDARIZACION:**

Cada empresa manejaba su propia tecnología, entonces mientras se trabajaba de manera aislada esto no presentaba ningún inconveniente, pero si las empresas buscaban interactuar entre esto significaba una limitación ya que no era posible comunicarse a través de equipos de diferentes fabricantes. Es así como surge la idea de *estandarizar* o compatibilizar, para poder lograr la comunicación entre distintas empresas.

**Ventajas de la estandarización:**

* **Aumenta el mercado:** esto significa que puedo vender mi producto mucho más fácil, debido a que estoy vendiendo algo que le sirve a todos por ser estándar; en definitiva se amplía el mercado.
* **Disminuir los costos:** esto se debe a que puedo fabricar masivamente.
* **Libertad al consumidor:** El consumidor puede elegir al fabricante. esto significa que yo puedo comprar cualquier pc de cualquier fabricante sin tener que “casarme” con una marca determinada. Además permite la interoperabilidad, esto es que se puedan comunicar dos dispositivos de distinta marca.

**Tipos de estándares:**

Hay dos tipos de estándares:

* **De facto o hecho:** es un estándar que surge sin ninguna planificación formal previa, sin que nadie de la orden, sino que es algo que se expande porque es adoptado por la sociedad. Por ejemplo el uso de celulares, o TCP/IP.
* **De jure o por Ley:** en este caso una organización establece un estándar y le da la directiva a una empresa o fabricante de cómo tiene que aplicarla. Por ejemplo: si fabrico tapas hay un estándar que dice que tienen que enroscar hacia la derecha.

**Organizaciones de estandarización:**

* **ITU (Unión Internacional de Telecomunicaciones):** Esta organización está formada por miembros voluntarios de muchos países distintos y por representantes de algunas empresas que venden productos de telecomunicaciones. Esta organizada en ramas según la misión u objetivo que persiga:
* *ITU*
* *ITU-T (Telecomunicaciones):* se encarga de definir normas para las telecomunicaciones de telefonía y comunicación de datos, en especial para las tecnologías WAN. Por ejemplo cual debe ser la disposición de los pines de un conector RJ11.
* *ITU-R (Radiocomunicaciones):* administra la comunicación a través del aire, y lo hace definiendo quien va a transmitir en una banda determinada para evitar que se pisen en las transmisiones. Esta rama determina estas normas y luego la CNC (Comisión Nacional de Comunicaciones) de cada país las implementa, es decir es el organismo que se encarga de controlar que las empresas no transmitan en otra banda de frecuencias que no sea la que le fue asignada.
* *ITU-D (Desarrollo):* se encarga de investigar nuevas tecnologías y desarrollar nuevos estándares.
* **IEEE (Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos):** Esta organización define estándares para las redes LAN. Entre los estándares definidos por esta organización podemos nombrar los 802.3, 802.5 entre otros. Es una organización voluntaria a nivel internacional de profesionales en Ingeniería, y la función que cumplen es organizar conferencias, distribuir revistas e información, etc. Podemos suscribirnos a esta organización para recibir información pagando, no es gratis.
* **ISO (Organización Internacional de Estándares):** esta organización desarrollo el modelo OSI. Es una organización de nivel internacional formada por miembros de todos los países. Se encarga de definir estándares de temas generales, como por ejemplo el enroscado de las tapas de gaseosas, los talles de la ropa, etc. Esta organización esta subdividida en grupos ya que hay que tratar muchos temas de diversas áreas.
* **Internet:**

Es un estándar de facto, ya que todos usamos internet sin que nadie nos obligue a hacerlo.

* *IAB (Consejo de Arquitectura de Internet)*: el objetivo del IAB es guiar por cual camino debe ir desarrollándose internet.
* *Internet Society* – *Sociedad de internet*
* *IETF (Internet Ingenieering Task Force – Fuerza de Tareas de Ingeniería de Internet)*: es un grupo de personas que intenta ver que es lo hace falta a corto plazo para desarrollar en Internet, investigan sobre temas o problemas que deben ser solucionados en poco tiempo.
* *IRTF (Internet Research Task Force – Fuerza de Tareas de Investigación de Internet)*: investigan cosas que podrían desarrollarse para mejorar internet en un largo periodo de tiempo, tienen una visión más a futuro.

¿Cómo trabajan estas organizaciones? Cuando alguien tiene una idea escribe un documento y lo

comparte con todos, todas las personas dan sus opiniones al respecto y si están todos de acuerdo se hace un borrador que se publica. Si todos están de acuerdo en el borrador, recién ahí se le da el formato de ley que se conoce como *RFC (Request For Commments – Solicitud Para Comentarios)*. La RFC es la ley de internet, me dicta las reglas que debo cumplir; son documentos públicos que están en internet a los cuales todos tienen acceso. Los desarrolladores consultan estos documentos para que sus programas o sistemas sean compatibles con las normas establecidas.

Clase 9 de Abril

**CAPAS DE ACCESO EN WAN (Tipos de Redes):**

**Red telefónica:**

La red telefónica es una de las primeras redes de comunicación a nivel mundial, la misma surgió en el año 1880 para la transmisión de voz. En el año 1980 esta red comienza a transmitir vos y datos debido a que ya existía la infraestructura necesaria para hacerlo.

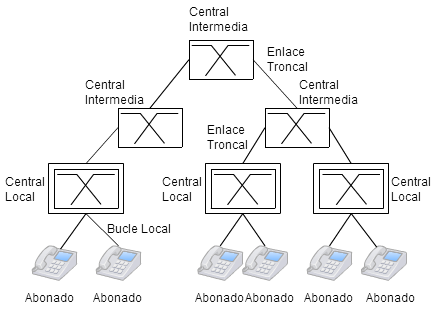
Esta red está montada o implementada sobre una conmutación de circuitos. Las ventajas que esto presenta es que los datos no se desordenan, es decir llegan todos ordenados porque viajan por el mismo camino físico. No hay retardo, debido a que al usuario se le asigna un ancho de banda que es reservado para su uso, lo que garantiza que haya calidad en la comunicación y velocidad para la transferencia de datos, ya que ese ancho de banda no es compartido con otros usuarios sino que es dedicado (de uso único para ese usuario). Las desventajas que presenta es que si deja de funcionar algún nodo intermedio o central telefónica se pierde la comunicación y hay que establecer de nuevo la llamada; esto se debe a que la conmutación de circuitos es orientada a conexión lo que significa que antes de comenzar a transmitir los datos o la voz es necesario establecer una conexión (armar el camino físico por donde se transmitirá) y una vez establecida esta conexión es cuando se transfieren los datos, hasta el momento en que ya no me quiero comunicar mas y se libera esa conexión. Toda la información viaja por el mismo camino físico debido a la conmutación de circuitos.

La forma que tiene esta red de transmitir datos es a través de un modem, usando la tecnología de DialUp (56K de transmisión) XDSL.

Cuando se creó esta red era completamente analógica, pero en la actualidad esta digitalizada casi en su totalidad, la única parte que sigue siendo analógica es el tramo que va desde el abonado o usuario hasta la central local.

**Arquitectura de la Red Telefónica:**

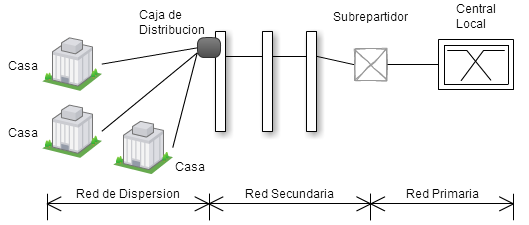
La red telefónica está organizada de la siguiente manera:



La arquitectura de una red telefónica está conformada por los siguientes 5 elementos:

1. **Dispositivos de acceso (Abonados):** Son los dispositivos que permiten acceder o conectarse a la red, es decir usar la red y se llaman abonados. Estos dispositivos puede ser teléfonos, módems y sensores de alarmas. Cada abonado pertenece (está conectado) a una central Local si o si, no pueden no pertenecer a alguna.
2. **Centrales Locales:**
3. **Centrales Intermedias:** También conocidas como centrales de transito. Son centrales que se utilizan para conmutar las llamadas y no tienen abonados conectados directamente.
4. **Bucle local:** Es el enlace que va desde el abonado a la central local. El bucle local es una conexión dedicada, esto significa que ese enlace le pertenece únicamente al abonado y no lo comparte con nadie, por ahí solo viaja su llamada.
5. **Enlaces troncales:** Todos los enlaces que no son locales se los denomina troncales. La diferencia con los bucles locales es que los enlaces troncales unen únicamente centrales, tanto centrales intermedias entre si, como centrales locales con centrales intermedias. Por tal motivo este tipo de enlaces se encuentra únicamente entre centrales, nunca jamás van hacia un abonado; y esto es así porque las centrales necesitan comunicarse entre si de una manera diferente que la manera en que se comunica una central local con un abonado. Los enlaces troncales son de fibra óptica o satelitales y de una altísima velocidad. Además, estos enlaces son compartidos entre todos los abonados (varias llamadas viajan por el mismo enlace), y por tal motivo se utiliza la multiplexación por división de frecuencia, de tiempo y de longitud de onda para que no se superpongan las llamadas.

**Profundizando el bucle local:**



La conexión que va desde el abonado (las casas) hasta la central local se llama bucle local. Este enlace está dividido en tres tramos: el primero de ellos se llama Red Primaria que es el que va desde la central local hasta el primer Subrepartidor. De ese subrepartidor salen cable multipares hasta lo que se llama una caja de distribución que generalmente están ubicadas en los postes de luz, conformando la Red Secundaria. De la caja de distribución salen muchos pares telefónicos hasta las distintas casas, en lo que llamamos la Red de Dispersión. A cada casa llega un solo par telefónico, y si por ejemplo hubiera 20 abonados que salen de la misma caja de distribución esos 20 cables se van a unir y van a formar lo que se llama un cable multipar. Para las empresas de comunicaciones el tramo que va desde la caja de distribución hasta las casas es el más costoso porque es el que más gasto tiene de instalación, y además es el menos utilizado porque es un tramo dedicado que solo le pertenece a un abonado.

**Encaminamiento jerárquico:**

Cada central tiene 10.000 abonados, por ejemplo si tomamos el numero 466XXXX veremos que los primeros 3 dígitos pertenecen o distinguen a una central local en particular, y la combinación de los restantes 4 dígitos me dan los 10.000 abonados que perteneces a esa central. Si yo quiero comunicarme con otra persona que se encuentra conectada a la misma central local que yo, es decir que su número comienza con 466XXXX, lo que hago es transferir el numero con el que me quiero comunicar a la central local, la cual toma el numero e interpreta donde se encuentra esa persona y conmuta (une) la llamada.

En el caso en que yo quiera comunicarme con una persona que pertenece a una central local diferente a la mía, voy a tener que subir desde mi central local hacia una central intermedia de mayor nivel, donde también se encuentre conectada la central local que contiene al abonado con el que me quiero comunicar. Esta central intermedia será la encargada de conmutar la llamada. Recibe el nombre de encaminamiento jerárquico debido a que yo tengo que subir niveles en la jerarquía de centrales para poder comunicarme con otros abonados.

**Señalización:**

Para que los datos que quiero transferir lleguen correctamente es necesario usar Información de control o de señalización. La señalización es información extra que tiene que transferirse para poder establecer, mantener y finalizar llamadas.

Habrá señalización en toda la red, desde nuestra casa hasta la central local (usuario-red, que sería el bucle local) para decirle con quien nos queremos comunicar, desde una central a la otra (red-red), y habrá señalización entre las centrales y el centro de gestión de red. El centro de gestión de red es el lugar donde se administra todas las cuentas de los abonados o usuarios de la red telefónica, es decir es el lugar donde se determina cuanto tiempo llama cada uno, las tarifas por llamar, y los distintos costos que luego se contabilizan para hacer la factura.

La señalización sirve para:

* Tono de llamada (cuando levantamos el tubo).
* Tono de ocupado.
* Tono cuando está llamando.
* Transferir el número que nosotros tecleamos desde nuestro teléfono hasta la central local.
* Para encaminar la llamada entre las centrales: esto significa que se va estableciendo el camino por el cual se va a transferir la voz o datos; y en el caso de que una central no tenga lugar para tomar una llamada busca otra central que se encuentre disponible para hacerlo.
* Para tarifar: esto significa que cuando yo llamo a alguien, mi llamada viaja hacia el teléfono con el cual me quiero comunicar, ese teléfono acepta mi llamada (levanta el tubo) y vuelve la aceptación de la misma por el mismo camino hacia mi teléfono y es ahí cuando comienza a cobrarse la llamada. Cuando se interrumpe la llamada porque alguno de los dos cuelga se le avisa al centro de gestión de red que interrumpa el contador de pulso y que cargue la cantidad de pulsos a la cuenta del usuario que realizo la llamada.
* Para administrar o gestionar la red.
* Para detectar fallas en la red.
* Tono de llamada de espera.
* Buzón de llamadas.
* Identificación de llamada: saber el número de la persona que está llamando.
* Llamadas de conferencias.

**Implementación de la señalización:**

Antes la señalización se implementaba con personas que se encontraban en las centrales, las cuales cuando uno quería realizar una llamada consultaba con quien nos queríamos comunicar y en base a eso conmutaba (unía) la llamada en un tablero estableciendo la conexión entre ambos y permitiendo la comunicación. Es decir la conmutación era manual.

No es la misma la señalización que va desde el abonado a la central local (usuario-red) que la señalización que hay entre centrales (red-red). Por este motivo hay dos tipos de señalización:

* **Intracanal:** Se llama de esta manera debido a que dentro del mismo canal donde se transmiten los datos se transmite también la señalización. Este tipo de señalización se utiliza desde el abonado hacia la central local, es decir en el bucle local, debido a que este tramo es analógico. La señalización en este caso puede ser:
* *En banda:* significa que la información de señalización se transmite dentro del ancho de banda de la voz (4Khz).
* *Fuera de banda:* significa que la información de señalización se transmite fuera de la frecuencia (o ancho de banda) por la cual se transmite la voz.
* **Por canal común:** Esto significa que por un mismo canal viaja información de muchos abonados. Es decir que mientras la información viaja desde el abonado hasta la central local (el bucle local) lo hace intracanal, pero una vez que llega a la central local esta une la señalización de todos los abonados en un solo canal, por ello recibe el nombre de canal común. Este tipo de señalización se utiliza entonces entre centrales.

Como la red telefónica brinda en la actualidad muchas funciones complejas como las antes mencionadas,

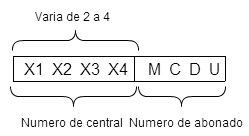
fue necesario separar la señalización de la transferencia de datos. Es por ello que la red telefónica hoy en día está separa en dos redes distintas: una **red de datos** (voz, imagen, etc.) y una **red de señalización**.

El sistema utilizado en la Argentina se llama **Sistema de Señalización Numero 7 (SS7 – Signal System Number 7)**. Este sistema es una pila de protocolos que se implementa sobre conmutación de paquetes y su propósito es ser un sistema de señalización general, esto quiere decir que sirve para muchas cosas y no solo para conversaciones telefónicas. Además, esta estandarizado internacionalmente.

**Plan de numeración:**

Está dividido en dos tipos de llamadas:

* **Llamadas urbanas:** Son las llamadas que se dan entre abonados de una misma localidad. Una llamada urbana está dividida en dos partes: la primera es el número de la central que puede contar con 2, 3 o 4 dígitos, esta variación es producto de las cantidades de centrales locales que haya en la localidad. La segunda parte es el numero del abonado, que los distinguimos por M C D U que representan las unidades de mil, centena, decena y unidad respectivamente. En esta última parte queda demostrado que podemos tener 10.000 abonados por central debido a todas las posibles combinaciones de números entre 0000 y 9999.

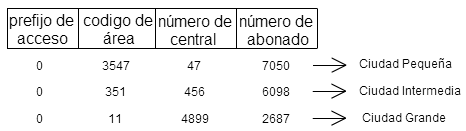
****

El número de central presenta dos restricciones: El primer digito jamás puede ser cero ni uno. No puede ser cero porque este valor es el que se conoce como *prefijo de acceso*, es decir, es el número que discamos cuando queremos hablar con otra localidad. No puede ser uno porque es el número que está destinado a las llamadas de emergencia.

* **Llamadas interurbanas:** Son las llamadas que se dan entre abonados de localidades distintas

Para realizar este tipo de llamadas, nuestro país adopto un *sistema de numeración cerrado* que está formado por 11 dígitos. Un número interurbano está compuesto por cuatro partes: un *prefijo de acceso*, un *código de área*, un *número de central* y un *número de abonado*.

En este tipo de llamada el número de abonado siempre tiene 4 dígitos, mientras que el número de central varia de 2 a 4 dígitos debido a la cantidad de centrales que puede haber de acuerdo al tamaño de la localidad. Las localidades chicas tienen pocas centrales (9), y las ciudades grandes como Buenos Aires tienen muchas centrales (100). A medida que se tiene más centrales, la cantidad de dígitos del código de área va disminuyendo, esto se debe a que hay que respetar la regla del sistema cerrado de numeración de formar 11 dígitos en total para un número. Por lo tanto si tengo más dígitos para los números de centrales, tendré menos para el código de área.



Estos números se denominan *geográficos* porque a partir de ellos podemos ubicar el lugar donde se encuentra una persona debido a la información que proporcionan (código de área). Pero a su vez, también existen números *no geográficos* o de *red inteligente* que son aquellos que utilizan las empresas para atención al público que comienzan con 0800, 0810, 0610; o también aquellos números utilizados para emergencia como el 100, 911,etc. La característica que tienen es que cuando yo llamo a uno de estos números no tengo noción de a qué lugar geográfico estoy llamando.

**ATM (Asynchronous Transfer** **Mode - Modo de Transferencia Asíncrono):**

Es una tecnología de capa 2, es decir que abarca la capa física y la de enlace del modelo osi, mientras que en modelo de TCP/IP se encuentra en la capa de Host a Red. Esta tecnología comenzó a crearse en la década del 80, y sirve para transmitir todo tipo de información (voz, video, datos, correos electrónicos, páginas web, etc.) integrada o sobre una misma red física, a través de servicios diferenciados. Cuando hablamos de servicios diferenciados hacemos referencia a que distingue diferentes tipos de servicios, es decir que en función de lo que quiera transmitir contrato un servicio especifico de ATM para hacerlo. Esta tecnología se utiliza en los troncales de internet y en las redes telefónicas entre centrales.

Las características que presenta son:

* **Implementa conmutación de celdas:** Las celdas son trozos de información muy pequeños todos de longitud fija, del orden de los 53 bytes, de los cuales 5 son de cabecera (información de control o señalización) y 48 son de datos.
* **La conmutación es muy rápida:** El hecho de tener que conmutar trozos de información tan pequeños, y hacerlos a nivel de hardware permite una muy alta velocidad de conmutación. Permite transmitir en velocidad que van desde 155 a 622 MB por segundo, y aun mas rápido.
* **Es orientada a conexión:** Esto significa que todas las celdas van a seguir un mismo camino físico, lo que implica que lleguen todas ordenadas al destino. Si una celda llegara a perderse no se retransmite porque esta no es una característica de ATM. Lo que si puede hacer es detectar errores, y cuando lo hace notifica cual error se encontró.
* **Montada sobre fibra óptica:** ATM puede montarse sobre cualquier medio de transmisión, pero lo más normal es que se implemente en fibra óptica sobre una tecnología que se llama Sonet.
* **Utiliza VCC (Virtual Channel Connection):**
* **Utiliza VPC (Virtual Path Connection):**

Clase 16 de Abril

**CLASES DE SERVICIOS DE ATM**

ATM permite transmitir todo tipo de información integrada, cuando hablamos de todo tipo de información nos referimos a datos, voz, video, trafico web, archivos, etc. Lo que intenta hacer esta tecnología es transmitir cualquier tipo de información sobre una misma red brindando diferentes tipos de servicios. Por ello, en función de lo que se necesite transmitir en la red convendrá elegir un tipo de servicio en particular para esos datos:

**Servicios en tiempo real:**

Estos servicios se utilizan para aplicaciones que son muy sensibles al retardo y a la variabilidad del mismo, como por ejemplo la transmisión en tiempo real de audio y video, y en general todas las aplicaciones que corran sobre UDP. Que sean sensibles al retardo quiere decir que no aceptan o no toleran el retardo, que es el tiempo que pasa entre que se envía la información y se recibe en el destino. La variabilidad del retardo, también conocida como fluctuación o Jitter se da cuando yo transmito algo cada un segundo y en el destino la información no llega cada un segundo sino que los tiempos en los que se va recibiendo la misma varían, es decir que el retardo desde el origen al destino no es siempre el mismo, sino que va variando.

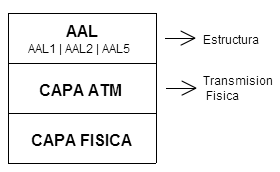
* **CBR (Constant Bit Rate – Tasa de Bit Constante):** Se utiliza para aquellas aplicaciones que son sensibles al retardo (y a la variabilidad del mismo) y además transmiten a un flujo constante. Por ejemplo: audio y video sin comprimir como puede ser telefonía, conferencias, etc. Este servicio me va a garantizar un canal virtual dedicado en la red en donde se me asigna un cierto ancho de banda durante toda la transmisión.
* **RT-VBR (Real-Time Variable bit Rate – Tasa de Bit Variable en Tiempo Real):** Se utiliza para aquellas aplicaciones que son sensibles al retardo (y a la variabilidad del mismo) y que no transmiten un flujo continuo de información, sino que es variable. Por ejemplo: audio y video comprimido. Es decir que no hay un tráfico constante de información sino que se transmite de a ráfagas, pero cuando esto ocurre necesito que llegue rápido.

**Servicios no en tiempo real:**

Estos servicios se utilizan para aplicaciones que no son sensibles al retardo ni a su variación. Estas aplicaciones corren generalmente sobre TCP como por ejemplo: una página Web.

* **NRT-VBR (No Real-Time Variable Bit Rate – Tasa de Bit Variable No en Tiempo Real):** Se utiliza para aquellas aplicaciones que tienen requerimientos de retardo de variabilidad pero que no necesitan tanta urgencia. Por ejemplo: transacciones bancarias, acceso a bases de datos de reservas de vuelos, etc.
* **UBR (Unespecified Bit Rate – Tasa de Bit No Especificada):** la red tiene cierto ancho de banda disponible, es decir cierta cantidad de recursos para brindarle al usuario. Estos recursos van a ser repartidos primero para los que usen el servicio de CBR, en segundo lugar serán repartidos para los usuarios del servicio VBR, y lo que sobre será repartido entre los usuarios de UBR. Es decir que la capacidad de la red que no sea usada por los servicios de CBR y VBR es asignada al servicio UBR. Las aplicaciones que necesitan este tipo de servicio son aquellas que soportan perdida de celdas (es decir que pueden perder celdas), aquellas que no tengan apuro en la transmisión, como por ejemplo: todo el tráfico web que corre sobre TCP. El hecho de que las aplicaciones soporten este tipo de servicio es que si se pierde un paquete o celda, el protocolo TCP se encargara de retransmitirlo para solucionar el problema. También es conocido como *servicio del mejor esfuerzo*, porque intenta entregar la información aunque no lo garantice. No informa si hay congestión.
* **ABR (Available Bit Rate – Tasa de Bit Disponible):** se utiliza para aquellas aplicaciones que necesitan que se les garantice cierto ancho de banda. Por ello, para este servicio se define una tasa mínima de transferencia y una tasa máxima o de pico. Es decir que este servicio me va a garantizar la tasa mínima de transferencia todo el tiempo y además me va a permitir alcanzar la tasa máxima de transferencia cuando los otros usuarios no transmitan (ya que la red está libre).
* **GFR (Garantized Frame Rate – Tasa de Trama Garantizada):** Todos los servicios antes mencionados sirven para conectar usuarios a la red, lo que se conoce como Host. En este caso, este servicio permite conectar una empresa entera, es decir una red entera (conocida como LAN) a la red. Para que esto ocurra, es decir para conectar una LAN a un switch ATM, ya no se conecta como un Host o usuario sino que lo que se hace es conectar la red de la empresa a un router a través de un switch, y de esta manera tengo toda la empresa conectada a la tecnología ATM.

**PILA DE PROTOCOLOS DE ATM:**

****

**Capa AAL (ATM Adaption layer – Capa de Adaptación ATM):**

Permite que diferentes tecnologías puedan acceder a la red ATM. Esta capa es similar a la capa de transporte del modelo TCP/IP debido a que se ejecuta en los extremos de la red, no se ejecuta en los switch de ATM (de capa 2) sino que lo hace en los routers o Host.

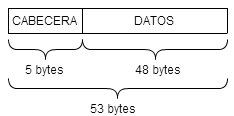
En esta capa se definen los diferentes AAL1, AAL2, AAL3, etc. para brindar los servicios a la red. Cada servicio se brinda a través de un AAL distinto, por ejemplo: AAL1 🡪 CBR, AAL2 🡪 VBR, AAL5 🡪 Trafico IP (Trafico web de los servicios en tiempo real), etc.

*Completar.*

**Capa ATM:** Esta capa sería similar a la capa 2 del modelo OSI (capa de enlace). Se encarga de definir la estructura que va a tener la celda ATM, es decir define como va a estar conformada una celda. En esta capa se ejecutan los switch o conmutadores ATM.

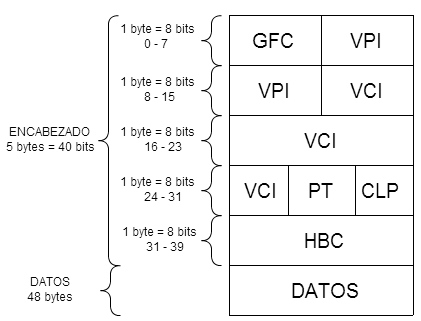
**Capa Física:** Hace referencia a como se transmiten los bits, a nivel de capa 1. Es decir se encarga de determinar la temporización de los bits, cuánto tiempo dura un bit, si se implementa sobre UTP define el voltaje que se va a utilizar para representar un 1 o un 0, si se implementa sobre fibra óptica define el tamaño del pulso, etc. Es decir, define aspectos técnicos de la capa física por la cual va a correr ATM. Si bien puede correr por cualquier medio de transmisión lo normal es que lo haga sobre fibra óptica, debido a las altas velocidades.

**Estructura de una celda ATM:**

Sabemos que todas las celdas son de longitud fija y que tienen 53 bytes, de los cuales 5 son para el encabezado y los 48 restantes para los datos. 

Pero el encabezado de las celdas, que contiene 40 bits (Cada byte posee 8 bits) va a cambiar en función de si son transmitidas del Host al switch o de un switch a otro switch. Podemos definir entonces dos tipos de encabezados de celdas: UNI y NNI.

**UNI (User to Network Interface – Interfaz desde el Usuario a la Red):** Formato de celda desde el usuario a la red.



Formato de cabecera UNI

**NNI (Network to Network Interface – Interfaz entre Redes):** En la imagen anterior representamos gráficamente el formato de una cabecera UNI. Cabe remarcar que el formato de una cabecera NNI es exactamente igual al anterior representado con la única diferencia de que el primer campo de control de flujo (GFC) no aparece y en su lugar los 4 bits son otorgados al campo VPI, llegando a tener en total dicho campo 12 bits disponibles.

**GFC (Generic Flow Control – Control de Flujo Genérico):** La idea de este campo es diferenciar los distintos tipos de flujos, es decir qué tipo de servicio estoy utilizando: si estoy transmitiendo voz, datos, etc. Entonces, a través de los 4 bits que contiene este campo yo voy a diferenciar que tipo de flujo estoy transmitiendo, para poder manejar las prioridades.

Este campo únicamente existe en la interfaz UNI, es decir para las comunicaciones del usuario a la red.

**VPI (Virtual Path Identifier – Identificador de Camino Virtual):** Lo utilizo para saber cómo agrupar varios canales virtuales.

**VCI (Virtual Channel Identifier – Identificador de Canal Virtual):** Se utiliza para encaminar las celdas al usuario correcto cuando llegan al destino.

**CLP (Cell Loss Priority - Prioridad de Perdida de Celda):** Significa que si a los conmutadores se le saturan las memorias o buffer pueden empezar a descartar celdas. Se va a encaminar siempre y cuando haya recursos, si se llegaran a congestionar los buffers de la red ATM las celdas que se van a descartar solamente serán las que tengan en alto este bit, debido a que no es una tasa garantizada.

**HSC (Header Error Correction – Corrección de Error de Cabecera):** ATM en cada salto, es decir de cada switch a switch trata de detectar si hubo un error en la cabecera, y solamente en la cabecera, porque si hubo un error en los datos no le importa debido a que es una tecnología del mejor esfuerzo. Para verificar entonces un error en la cabecera lo hace a través del campo HSC. ¿Por qué hacerlo salto a salto? Debido a que en cada salto puede llegar a cambiar el número de canal virtual. Sabemos que los switch manejan tablas de entrada y tablas de salida, entonces las celdas que llegan a un switch llegan por un numero de puerto determinado pero pueden salir por un numero de puerto diferente.

Si llegara a detectarse un error en alguna cabecera la celda simplemente se descarta.

**PT (Payload type – Tipo de Carga):** Mencionamos anteriormente que ATM puede transmitir video entre usuarios, información de señalización desde el usuario a la red, e información de señalización o de gestión de red entre switches. Ahora bien, ¿Cómo sabe la red si se está transmitiendo información de usuario, de la red o de señalización? Lo sabe gracias al campo Payload Type.

**UNIDAD N°2: CAPA DE INTERRED**

**DIRECCIONAMIENTO:**

**CARACTERISTICAS O FUNCIONES DE LA CAPA INTERRED:**

* Esta capa recibe de la capa superior (capa de transporte) segmentos. A través del protocolo IP va a tomar esos segmentos y los va a encapsular (esto es, agregarle un encabezado) en un paquete o datagrama IP.
* Se encarga de que los paquetes viajen por la red a través de routers. Es decir, encamina los paquetes en función de su dirección IP. Encaminar significa que cuando entra un paquete a un router, este dispositivo lee la dirección IP de destino, consulta las tablas que tiene y toma la decisión de por cual camino va a enviar ese paquete a su destino.
* Direccionamiento: para que dos dispositivos se puedan comunicar a través de internet deben tener asignados una dirección única e irrepetible a nivel global de internet (direcciones publicas). El direccionamiento consiste entonces en asignar y configurar direcciones IP a maquinas y routers.
* Controles de congestión: debido a que el tráfico de la red es a ráfagas (no es un flujo constante), puede que la red se congestione. Existen diferentes técnicas para controlar la congestión, intentando que ingrese un menor flujo a la red (una tasa mas reducida).
* La capa de Interred se implementa a través del protocolo IP. Este protocolo se considera que es lo que mantiene unida a la internet, ya que se ejecuta en los Host, routers, servers, etc. (menos en los Hub y switch). IP significa Internet Protocol o Protocolo Interred (como se llama la capa). Este protocolo es un protocolo, al igual Ethernet, de máximo esfuerzo, esto significa que intenta que los paquetes atraviesen la red y lleguen a su destino sin garantizar nada. Además, este procotolo descarta paquetes, no los retransmite.
* El protocolo IP es no orientado a conexión: cada paquete se encamina de manera independiente, esto significa que si un paquete debía salir por un enlace y ese enlace no está disponible (no interesa el motivo), entonces el router se auto configura y envía ese paquete por otro enlace. Al ir por otro enlace, el paquete puede demorar más o menos en llegar al destino, por lo que los datos puede llegar desordenados al destino. Este protocolo NO ordena los mensajes, el encargado de ordenarlos es el protocolo TCP.

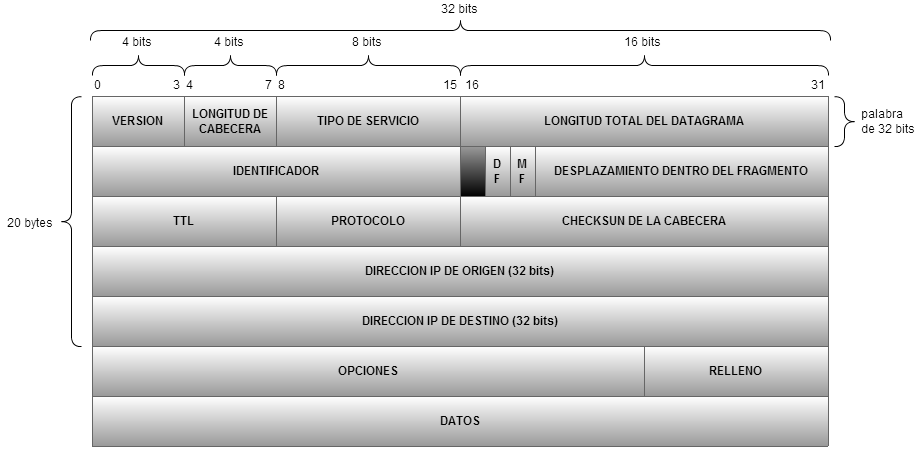
Clase 23 de Abril

**FORMATO DEL DATAGRAMA IPV4 (ENCABEZADO):**

Un protocolo es un estándar que se establece para comunicar dos capas del mismo nivel, es decir que vamos a hablar un mismo idioma; lo más importante es que me permite interpretar una serie de bits. El protocolo IP se encuentra en la capa de Interred, la cual recibe de la capa superior (capa de transporte) un segmento, al que lo va a encapsular (esto es, agregarle un encabezado) y lo va a convertir en un paquete o datagrama.

La IPV4 fue la primera versión del protocolo IP.

Por defecto, un encabezado IPV4 tiene 5 palabras (sin contar la que contiene el campo opciones que casi nunca se usa) de 32 bits cada una, o lo que es igual 4 bytes. Es decir la cabecera del datagrama tiene generalmente 20 bytes (5 palabras x 4 bytes c/u). Sin embargo, el tamaño de la cabecera es variable, esto significa que puede expandirse.



Formato del datagrama IPV4

Analicemos cada uno de sus campos:

**Versión:** En función del valor que tenga este campo, será la interpretación que se le dará a todos los bits que siguen. Es por este motivo, que se encuentra al comienzo del datagrama, porque si estuviera al final del mismo no sabría como interpretar el resto de los bits. En resumen, este campo me dice cual es la versión del protocolo, y para ello utiliza 4 bits (que van del cero al 3). El valor 0100 es el 4 en decimal, por lo que si estamos en presencia de este número en el campo versión sabemos que estamos hablando de un datagrama de IPV4. En cambio, si el valor que se presenta es el 0110 que es el 6 en decimal, podemos afirmar que estamos en presencia de un datagrama IPV6.

**Longitud de la cabecera:** Este campo contiene 4 bits que van del 4 al 7, y me determina cuantas palabras de 32 bits tiene la cabecera. Habíamos mencionado que por default el datagrama de IPV4 contiene 5 palabras, pero también dijimos que la cabecera tiene un tamaño variable, y por lo tanto puede expandirse hasta 15 palabras de 32 bits cada una. Entonces, con los 4 bits que tiene este campo podemos formar los números decimales que van del 0 al 15 para determinar la cantidad de palabras que tiene la cabecera.

Podríamos plantearnos la pregunta: ¿Cómo me doy cuenta si una cabecera es variable o no? Si la cabecera es variable, debe contener un campo Longitud de cabecera.

Es importante determinar la longitud de la cabecera para que el destino pueda saber dónde termina la cabecera y donde comienzan los datos. Si la cabecera es fija no es necesario.

**Tipo de servicio:** Este campo se utiliza para manejar las prioridades de los paquetes, para darles más importancia a algunos sobre otros. Para ello utiliza 8 bits que van del 8 al 15. Por ejemplo, los paquetes de los datos que se envían en tiempo real deben llegar más rápido que los paquetes comunes, por lo tanto tienen una mayor prioridad. Entonces, la forma de hacer que un paquete se encamine más rápido es poniéndole prioridad alta en el campo tipo de servicio, de lo contrario tendrán prioridad mínima.

**Longitud total del datagrama:** Este campo utiliza 16 bits que van del 16 al 31, y me permite saber la longitud de un datagrama, es decir conocer desde donde hasta donde va. Como máximo, el protocolo me permite tener un datagrama o paquete de bits, es decir 64KBytes, aunque en la actualidad se utilizan datagramas de 1,5KBytes debido a que es el tamaño que puede soportar una trama Ethernet.

Es importante determinar la longitud de un datagrama o paquete debido al encapsulado y desencapsulado.

Debemos mencionar que el segundo renglón del datagrama utiliza la fragmentación.

**MTU (Maximum Transfer Unit – Unidad Máxima de Transferencia):** Cada enlace por los que viajan los datos tienen una MTU. Cuando un paquete o datagrama llega a un router, el dispositivo determina porque enlace va a viajar el paquete (que camino va a tomar). Pero antes de largar el paquete por ese enlace, el router debe determinar cuál es la unidad máxima de transferencia que presenta ese enlace. Entonces, si un paquete tiene que atravesar un enlace que no soporte el tamaño que tiene el paquete, el router lo fragmenta antes de lanzarlo por el enlace. Esta fragmentación consiste en tomar el paquete y dividirlo en partes más chicas que no superen la unidad máxima de transferencia del enlace. Entonces, en lugar de enviar un paquete por la red, vamos a enviar muchos fragmentos de ese paquete. Cabe recalcar que lo que se divide no es el datagrama completo sino que solamente se fragmenta la parte de datos, a la que luego se le anexa la cabecera IP.

Luego, el destinatario se encarga de reunir cada una de las partes y las reensambla. Decimos que se encarga de reunirlas debido a que los fragmentos del paquete pueden viajar por caminos distintos.

Paquete antes de la fragmentación: 

Paquete luego de la fragmentación: 

Nota: paquete=datagrama

Un ejemplo que podemos citar es: yo debo enviar por correo 20 hojas, pero en el correo me dicen que el tamaño máximo que puedo enviar es 2 hojas (MTU), por lo tanto armo 10 paquetes de 2 hojas cada uno (los 10 paquetes son la analogía a los fragmentos).

La fragmentación prácticamente no se usa en la actualidad debido a que consume mucho tiempo del router. Esto es así porque generalmente el router lo que hace es: le llega un paquete, ve la dirección de destino, consulta las tablas y encamina. En cambio, si un paquete es muy grande debe dividirlo, agregarle la cabecera, calcular que numero de fragmento es, y encaminar a cada uno de los fragmentos, lo que toma mucho tiempo. Se usa tan poco que IPV6 elimino la fragmentación de su cabecera, es decir que no se implementa la fragmentación en dicho protocolo.

**Identificador:** Todos los paquetes poseen un identificador o ID que los diferencia. Hay que mencionar que todos los fragmentos de un datagrama IP van a tener el mismo identificador debido a que cada vez que se fragmenta un paquete, cada fragmento pasa a ser un paquete independiente y por lo tanto se va a encaminar de manera independiente. Entonces, el destino cuando los recibe de manera desordenada sabe que aquellos paquetes (o fragmentos) que lleguen con el mismo ID pertenecen a mismo paquete que fue fragmentado.

**Bit sin uso:** Hay un bit del datagrama que se dejo sin uso, de reserva, para el caso en el cual el protocolo evolucione y necesite utilizarlo para representar alguna funcionalidad.

**DF (Don´t Fragment - No Fragmentar):** Si el origen quiere que su paquete no sea fragmentado se pone en alto este bit. En caso de que el router no pueda transferir el paquete porque es muy grande (supera el MTU del enlace) y no puede fragmentarlo porque este bit esta en alto, lo que hace es descartar el paquete y le informa al origen dicha situación a través de un protocolo llamado ICMP. Entonces el origen construye paquetes mas pequeños para enviar.

En caso de que este bit se encuentre en cero el router puede fragmentar el paquete si es necesario.

**MF (More Fragment – Mas Fragmentos):** ¿Cómo sabe el destino cuantos fragmentos son los que conforman un paquete? La respuesta es gracias al bit More Fragment. Si este bit esta en alto, es decir es 1, significa que todavía quedan fragmentos por llegar; en cambio si esta en bajo, es decir es 0, significa que ya llegaron al destino todos los fragmentos que conforman un paquete.

Cabe mencionar que cada uno de los fragmentos posee este bit en 1, pero solo el último lo posee en 0. Entonces, supongamos que llega el ultimo fragmento con el bit en cero antes de que hayan llegado el resto de los fragmentos. El destino podría considerar que llegaron todos los fragmentos que conforman el paquete, pero esto en realidad no es asi. Entonces lo que debe hacer el destino es fijarse en el campo desplazamiento dentro del fragmento el valor que posee el fragmento que tiene el bit Mf en cero, que se va a corresponder con la cantidad de fragmentos que hay, y debe ver si concuerda con la cantidad de fragmentos que llegaron. Entonces, si no llegaron todos los fragmentos que conforman el paquete, simplemente sigue esperando a que lleguen. (Chequear lo que está en color)

**Desplazamiento dentro del Fragmento:** Este conjunto de bits me indica cual es el orden que tienen los fragmentos de un paquete, de manera que, cuando llegan todos los fragmentos al destino, este pueda ordenarlos y rearmar el paquete original.

Con los desplazamientos y con el bit MF el destino es capaz de reensamblar o rearmar un paquete que fue fragmentado.

**TTL (Time To Live – Tiempo Para Vivir):** Este campo se utiliza para evitar que un paquete quede dando vueltas eternamente en la red y consuma recursos (ancho de banda, tiempo de router, etc.). Para lograr esto, lo que se hace es asignarle a un paquete al momento en que es transmitido un tiempo de vida determinado. El TTL se cuenta en saltos, donde un salto es cada uno de los routers por los que va pasando un paquete. Entonces, cuando un paquete llega a un router, este le descuenta 1 al tiempo de vida del paquete. Si el campo TTL del paquete llega a cero significa que el tiempo de vida de ese paquete expiro, por lo tanto el router lo descarta y le avisa al origen que el paquete fue descartado por exceder su tiempo de vida. Dicha notificación se hace a través de un protocolo llamado ICMP. Como máximo un paquete podrá tener un TTL de 255, ya que este campo posee 8 bits ( = 256 – el cero).

**Protocolo:** Dijimos anteriormente que el protocolo IP se encuentra en la capa de Interred, y que recibe de su capa superior, la capa de Transporte, un segmento. Dicho segmento es encapsulado (se le agrega un encabezado) para ser convertido a un paquete o datagrama. Ahora bien, este paquete es transmitido a través de distintos enlaces y pasa por distintos routers hasta que llega al destino. Aquí, el paquete debe ser desencapsulado, esto es, se le saca el encabezado IP y se entrega el segmento a la capa superior (capa de transporte). Pero, sabemos que en la capa de transporte hay dos protocolos: el UTP y el UDP, entonces se presenta un interrogante: ¿Como sabe el destino a que protocolo debe ser entregado el segmento? Lo sabe gracias al campo protocolo. Lo que se hace es, al momento de encapsular el segmento y transformarlo en un paquete, se indica en este campo el protocolo al que pertenece dicho segmento (UTP, UDP o también ICMP), de manera que cuando el paquete sea desencapsulado en el destino se chequee cual es el valor del campo y así pueda saber a qué protocolo entregar el segmento.

Este campo protocolo es el que une las capas.

**Checksun de la cabecera:** Es un control de integridad de la cabecera, es decir controla que no se modifique. Debemos remarcar que esto se hace solamente para la cabecera, si se modifican datos no es algo que le importe al protocolo IP debido a que es no fiable y no orientado a conexión.

Esto se logra realizando el cálculo de un algoritmo en el origen, que genera el valor de checksun y lo almacena en dicho campo. La verificación de este campo se hace en cada salto, es decir en cada router por el que pasa el paquete o datagrama. Cuando llega a un router entonces, el router realiza nuevamente el algoritmo para comparar el valor que le da con el valor del campo checksun, es decir que valida que los valores sean los mismos lo que significa que la cabecera no fue modificada (esta integra). Si el router llegara a calcular un valor que no coincida con el del campo checksun del paquete, lo que hace es descartarlo debido a que fue dañado (sufrió una alteración).

Pero además de este cálculo que se realiza cuando llega el paquete al router, existe un segundo cálculo del algoritmo que toma lugar en el dispositivo. Esto se debe a que al pasar por el router, la cabecera del paquete sufre un cambio en sus valores, mas precisamente en el campo TTL donde se le resta 1 al valor del tiempo de vida. Por este motivo, el valor del algoritmo calculado previamente ya no es válido y debe recalcularse y almacenarlo en el campo checksun para que sea chequeado nuevamente en el próximo router por el que pase.

En resumen, el campo checksun se calcula en el origen una vez, y en cada salto dos veces.

**Opciones:** Como su nombre lo indica estas funciones que se pueden agregar son opcionales. Las opciones que puedo utilizar son:

* Indicar si el paquete tiene seguridad, es decir si va cifrado.
* Encaminamiento basado en origen: Significa que yo puedo indicar el camino por el cual quiero que vaya el paquete para llegar al destino, entonces en el campo opciones se ponen las direcciones IP de los routers por los que va a pasar el paquete. Si en algún punto el paquete no pudiera continuar por el camino indicado es descartado.

De la misma manera puede agregarse funcionalidad para indicar por donde quiero que no vaya

un paquete, es decir indicar que camino no debe tomar.

* Time Stamp – Estampa de Tiempo: consiste en configurarle en el campo opciones al paquete la opción de que cada vez que pase por un router, el dispositivo le registre la fecha y la hora en la cual recibió el paquete. Esto se hace con fines estadísticos, para ver cuánto tarda un paquete por un camino determinado y cuanto tarda por otro, de manera de poder decidir por donde conviene que viaje.

**Relleno:** Sabemos que la cabecera cuenta palabras de 32 bits cada una. Supongamos que yo agrego opciones a la cabecera pero que la cantidad de bits utilizados para tal fin no llega a 32 que es el tamaño de una palabra. En ese caso, la solución está en utilizar el relleno para completar la cantidad faltante de bits hasta llegar a los 32 que contiene una palabra. Es importante mencionar que si o si, todas las palabras (en este caso) deben tener 32 bits, debido a que si esto no se cumpliera no sabría cuando termina una palabra y cuando comienza la otra. El relleno consiste en agregar bits 0.

**PARAMETROS DE CONFIGURACION DE UNA PC:**

Para que un dispositivo tenga conectividad a internet es necesario configurarle (en IPV4):

**Dirección IP:** Las computadoras que están en una misma LAN tienen diferentes direcciones de red, ya que estas son jerárquicas y me permiten obtener la ubicación física de una PC. En cambio, la dirección IP puede ser la misma para maquinas que se encuentran dentro de una misma LAN. En el caso en que tengamos maquinas de distintas redes privadas, si o si sus direcciones IP deben ser diferentes.

**Mascara:** Una dirección IP es jerárquica porque necesito saber donde está ubicada físicamente una pc para poder localizarla. Además, está dividida en dos partes: la parte de red y la parte de Host. Dependiendo de la clase que tenga la dirección será la cantidad de bytes que tengamos para la parte de red y para la parte de Host, por ejemplo: Clase A, 1 byte de red y 3 bytes de Host.

Clase B, 2 bytes de red y 2 bytes de Host

Clase C, 3 bytes de red y 1 bytes de Host

La máscara me indica cuantos bits de una dirección IP pertenecen a la parte de Red y cuantos bits pertenecen a la parte de Host. De esta manera se puede identificar a que red pertenece una maquina, haciendo un and booleano entre la dirección IP y la mascara (como resultado me da la dirección de red con algún valor en la parte de red y ceros en la parte de Host).

La máscara se configura sola en función de la dirección IP que tenga la maquina. Su valor puede variar (extenderse o achicarse) para crear subredes.

Configurando los parámetros antes mencionados, es decir la dirección IP y la máscara, únicamente estoy garantizando la conectividad local, dentro de una misma red privada o LAN. Si yo quisiera comunicar una pc que se encuentra en una LAN determinada con otra pc que pertenece a otra red privada debo configurar además:

**Puerta de enlace o Gateway:** Para que una pc de una red privada determinada se comunique con otra pc que se encuentra en otra red privada si o si debe pasar por una puerta de enlace. Esta puerta de enlace tiene una dirección de IP asociada, que generalmente se le asigna la primera o la ultima del rango de Host. La puerta de enlace se encuentra en el router, y se puede tener tantas puertas de enlace como huecos o salidas tenga un router.

Todas las maquinas que pertenecen a una misma LAN tienen la misma mascara, la misma puerta de enlace y diferente dirección IP.

**Direcciones de Servidores DNS:** Es un software que se encarga de convertir o traducir una dirección de dominio (por ej: [www.frc.utn.edu.ar](http://www.frc.utn.edu.ar)) en una dirección IP (por ej: 194.15.1.2). Existen dos DNS: uno primario y otro secundario, por si alguno de los dos falla.

Clase 7 de Mayo

**AGOTAMIENTO DE LAS DIRECCIONES IP:**

Cuando se desarrolló en el año 1980 el protocolo IP se reservó 32 bits para las direcciones IP y se las dividió en clases. La asignación de las direcciones se hizo en base a estas clases, por ejemplo: si una empresa necesitaba conectividad para 50 dispositivos se le asignaba una dirección de clase C. Sabemos que con una dirección de clase C se pueden direccionar 254 Host, debido a que en la clase C tenemos el último byte otorgado a los Host, es decir que hay host disponibles. Es decir que, de los 254 tenemos 204 Host derrochados (que no pueden ser utilizados por ninguna otra empresa) ya que solamente utilizamos las direcciones para 50 dispositivos. Si una empresa necesitaba más de 254 dispositivos, supongamos 1000, se le asignaba una dirección de clase B con la cual se pueden direccionar 65.534 Host (). En este caso se estarían derrochando 64.534 Host. Lo que notamos es que al asignarse las direcciones IP por clases la cantidad de direcciones IP derrochadas fue muy grande. Lo cierto es que en esa época la cantidad de gente que se conectaba a internet era muy poca, y por lo tanto no se cuidaban las direcciones debido a que habían muchas.

A partir de la WWW la cantidad de usuarios en internet creció exponencialmente, entonces la demanda de direcciones comenzó a ser muy grande hasta llegar un momento en el que empezaron a escasear. Aquí las comunidades de internet empezaron a analizar posibles soluciones para esta situación, y terminaron dividiéndose en dos grandes grupos: aquellos que creían que era necesario desarrollar un protocolo nuevo porque de seguir así se agotarían las direcciones en muy poco tiempo, dando nacimiento a IPV6; y aquellos que intentaron aplicar técnicas o parches sobre el protocolo para alargarle la vida, al menos durante un tiempo.

**TECNICAS PARA SOLUCIONAR EL AGOTAMIENTO DE DIRECCIONES IP MOMENTANEAMENTE:**

Estas técnicas buscan cuidar o administrar lo mejor posible las direcciones IP que están escasas. De hecho, ya se han asignado todas las direcciones IP, las últimas que quedaban están ahora en manos de los Servidores de Internet. Por lo tanto, si hoy quiero tener una dirección IP se la tengo que pedir a mi ISP3.

**Direccionamiento privado:** El direccionamiento privado es una de las formas que se aplico para tratar de que siga existiendo el protocolo IPV4. Esta técnica tomo y reservo alguna dirección IP o varias, para las tres clases de direcciones A, B y C.

Clase A: **10**.0.0.0/8 🡪 se reservo 1 dirección IP que va desde la 10.0.0.0 al **10**.255.255.255

Clase B: 172.**16**.0.0/12 🡪 se reservaron 16 direcciones IP que van desde 172.**16**.0.0 al 172.**31**.255.255

Clase C: 192.168.**0**.0/16 🡪 se reservaron 255 direcciones IP que van desde 192.168.**0**.0 al 192.168.**255**.255

El símbolo que vemos luego de cada dirección IP /8, /12. /16 me indica la cantidad de bits que son fijos y no pueden variar. Por ello si notamos para la clase B por ejemplo, tengo 16 direcciones disponibles ya que de los 16 primeros bits (2 primeros bytes) que son utilizados para la parte de red tengo 12 que quedan fijos y únicamente puedo variar 4. Las combinaciones que puedo generar con 4 bits son , y de ahí provienen las 16 direcciones de clase B privadas. Podemos hacer el mismo análisis para la clase A y C. En el caso de esta última notemos que de los 3 bytes que pertenecen a la parte de red, los primeros 16 bits quedan fijos, pudiendo variar los últimos 8 de la parte de red. Las combinaciones que puedo generar con esos 8 bits ().

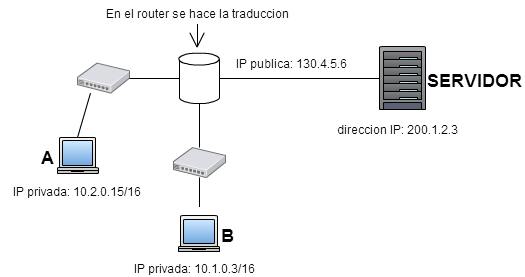
La idea que persigue esta técnica es que dentro de una empresa o red privada se le pueda asignar a las computadoras que formen parte de ella cualquiera de las direcciones privadas que quiera, sin pedirle permiso a ningún proveedor de servicio (únicamente hay que pedir permiso por las direcciones públicas, no por las privadas). En los hogares generalmente se usan las direcciones privadas de la clase C, en las empresas utilizan las direcciones de la clase B y las empresas muy grandes como Coca-Cola o Telecom utilizan la clase A.

¿Qué sucede si una máquina que pertenece a una LAN quiere comunicarse con otra computadora que se encuentra en otra red privada, a través de internet? La computadora no puede comunicarse utilizando la dirección privada que tiene debido a que puede haber otra computadora en el mundo que esté utilizando la misma dirección privada, y como sabemos para comunicarnos a través de internet necesitamos tener una dirección única e irrepetible (dirección pública), es decir que no deben haber dos iguales en el mundo. Por ello la dirección privada que tiene la pc únicamente sirve dentro de la red privada, no hacia afuera.

**NAT (Network Adress Translation - Traducción de direcciones de Red):**

Supongamos que la maquina A se quiere conectar con alguna otra máquina que este dentro de su misma red privada, tranquilamente podría hacerlo utilizando la dirección IP que tiene configurada, ya que es de dominio privado. Ahora, supongamos que en esta ocasión desea comunicarse con un servidor o con una maquina que pertenece a otra LAN. Para lograrlo deberá salir de la red privada y utilizar internet, pero ya no será posible hacerlo utilizando la dirección IP que tiene configurada, sino que deberá usar una dirección IP pública, por lo tanto deberá realizarse una traducción de direcciones.

En el router es el lugar donde se hace la traducción de dirección IP. ¿Qué significa esto? El paquete IP tiene dirección IP de origen y dirección IP de destino. Cuando el paquete sale de la LAN donde está la computadora A, la dirección IP origen (dirección que tiene configurada la computadora) es privada y la dirección IP destino (dirección del servidor) es publica porque se va a comunicar con el server.



IP origen privada= 10.2.0.15/6

IP destino publica= 200.1.2.3

Cuando el paquete llega al router, el dispositivo se encargara de hacer la traducción, para ello va a tomar la dirección IP de origen y la va a reemplazar por una dirección IP pública de manera que el paquete pueda ser entregado a internet, esto es lo que se conoce como traducción de direcciones de red:

*Dirección IP privada de origen= 10.2.0.15/16 🡪 dirección publica= 130.4.5.6*

A partir de aquí, el paquete viajara por internet con dirección de origen y destino pública. Ahora supongamos que el servidor recibió el paquete y emite una respuesta a la computadora A. Cuando el servidor envíe el paquete de respuesta las direcciones se van a invertir, es decir la dirección IP de origen será ahora la del servidor: 200.1.2.3 y la dirección IP destino será la de la computadora A: 130.4.5.6. Cuando el paquete de la respuesta del servidor viaja a través de internet y llega al router, este dispositivo vuelve a transformar la dirección destino (publica en este caso) en la dirección IP privada que tiene la computadora A, de manera que el paquete pueda llegar hasta ella, esto es:

*Dirección IP destino (publica)= 130.4.5.6 🡪 dirección IP privada de la maquina A=10.2.0.15*

¿Cómo sabe el router cual es la dirección IP privada de destino que tiene la maquina A? Lo sabe gracias a que al momento de realizar la traducción cuando envió el mensaje hacia el servidor guardo en una tabla que la maquina la dirección privada de la maquina A es 10.2.0.15 y que fue reemplazada por la dirección IP publica 130.4.5.6.

|  |  |
| --- | --- |
| Privada | Publica |
| 10.2.0.15 | 130.4.5.6 |
| 10.1.0.3 | 130.4.5.6 |

Ahora bien, supongamos que también tenemos conectado al router un switch que pertenece a otra LAN que contiene dispositivos privados. Podríamos también suponer que dentro de la misma red privada donde se encuentra la pc A existen otros dispositivos conectados. Si el router utiliza para salir a internet la misma dirección pública para todos los dispositivos ¿Cómo sabe cuando recibe un paquete con dirección destino 130.4.5.6 hacia cual de las computadoras va dirigido el mensaje, es decir como sabe a qué dirección privada debe transforma la dirección destino? Lo sabe gracias al puerto SOCKET. Un socket es una dupla entre la dirección IP y el puerto. Como nunca jamás dos direcciones van a compartir el mismo puerto del socket, el router almacena en la tabla el número de puerto al que está asociada la dirección, y de esa manera puede identificar a que computadora le corresponde el mensaje.

El problema que tiene esta técnica es que se puede generar un cuello de botella en el router debido al tiempo que tarda en hacer la traducción de las direcciones.

En resumen, esta técnica transforma IP públicas en privadas y viceversa.

**CIDR (Classless Interdomain Routing – Encaminamiento Entre Dominio Sin Clase):**

Al comenzar la clase comentamos que en un comienzo la asignación de direcciones IP públicas se hacía por clase, derrochando de esta manera muchas direcciones que no son utilizadas. A partir del agotamiento de las direcciones IP se decidió que las direcciones que ya fueron asignadas no se tocarían, pero que las pocas que quedaban libres serian asignadas muy cuidadosamente.

 El nuevo método de asignación borra del mapa a la asignación por clases, para dar lugar a la asignación basada en bits. Supongamos que una empresa solicita direcciones públicas para 50 dispositivos, según el método anterior se le hubiera otorgado una dirección de clase C, pero lo que propone este método es darle a la empresa la cantidad de bits potencia de dos que alcancen para direccionar 50 dispositivos. Es decir que se empiezan a fraccionar las direcciones IP.

*Para 50 Host 🡪 direcciones 200.1.2.0/26 🡪 00|000000*

*00|000001*

*00|000010*

*.*

*.*

*00|111111*

Notemos que a la empresa se le asigno una dirección IP de clase C ya que con ella podemos direccionar 254 Host, pero como vemos en el /26 únicamente pueden variar los últimos 6 bits para generar las direcciones. Esto es, los 3 primeros bytes de una dirección de clase C pertenecen a la parte de red, entre ellos suman 24 bits. El ultimo byte pertenece a la parte de Host, pero en lugar de otorgarle los 8 bits que tiene ese byte únicamente le otorgamos 6 bits para que varíe, ya que con esa cantidad de bits puede direccionar la 64 Host que superan la cantidad que el necesita. Si bien esta claro que se produce un derroche de 14 Host, este derroche es mucho menor que si se hubiera utilizado la asignación por clase, donde se hubieran perdido 205 Host.

Supongamos que una empresa necesita conectividad para 500 dispositivos, en lugar de otorgarle una dirección de clase B se le dará dos direcciones de clase C consecutivas, ya que con una dirección de clase C puedo direccionar 254 Hosts, y con dos podrá direccionar 208, logrando de esta manera disminuir la cantidad de Hosts derrochados.

*Para 500 Host 🡪 direcciones: 200.1.****4****.0/23 🡪 0000010 |0.00000000*

*.*

*.*

*0000010|****0****.11111111*

*200.1.****5****.0/23 🡪 0000010|****1****.00000000*

*.*

*0000010|1.11111111*

Como vemos con 9 bits puede generar 512 Host, derrochando únicamente 12.

¿Cómo sé cuántas direcciones de clase C consecutivas debo darle? En función de la cantidad de Hosts, y lo puedo calcular rápido contando la cantidad de bits de la parte de red que tomo y elevándola a la potencia de dos, por ejemplo:

*Para 2000 Host 🡪 direcciones: 200.1.****8****.0/21 🡪 00001|000.00000000*

*.*

*.*

*200.1.****9****.0/21 🡪 00001|001.0000000*

*200.1.****10****.0/21 🡪 00001|010.00000000*

*.*

*200.1.****10****.0/21 🡪 000001|111.00000000*

En este caso vemos que tomamos 3 dígitos de la parte de red, y si los elevamos a potencia de dos obtenemos: . De esta manera vemos que le estamos otorgando 8 direcciones clase C consecutivas que van desde 200.1.8.0 hasta 200.1.15.0

**Encaminamiento más eficiente (mejora de CIDR):**

Las direcciones IP se asignaron sin ninguna lógica, por ejemplo: la dirección 30 se asignó a una empresa de América del Norte, su consecutiva, la dirección 31 se asignó a América del Sur, la 32 a Europa, la 33 a Asia, etc. Cuando las direcciones IP se asignan sin ninguna lógica las tablas de encaminamiento de los routers son muy grandes. Es decir, sabemos que cada vez que llega un paquete a un router, este dispositivo busca en sus tablas y toma la decisión de por dónde va a encaminar o enviar ese paquete. El router sabe por dónde encaminar un paquete gracias a sus tablas. Si el tamaño de estas tablas fuera muy grande, el dispositivo demoraría mucho tiempo en encaminar el paquete, mientras que si el tamaño de las tablas fuera menor el tiempo disminuiría considerablemente.

Pongamos un ejemplo: supongamos que entramos a la facultad y queremos saber a qué aula debemos dirigirnos para tomar clases. Imaginemos que el guardia tiene una lista muy larga con todos los nombres de los alumnos de la facultad y sus respectivas aulas y comienza a buscarnos dentro de la misma para indicarnos a que aula debemos asistir. Esta búsqueda tomaría demasiado tiempo. Ahora imaginemos que en lugar de los alumnos, el guardia tiene en sus tablas un listado mucho más acotado que solamente contiene de los cursos y sus respectivas aulas. Si nosotros le proporcionamos el curso al que vamos, el demoraría mucho menos tiempo en indicarnos cuál es el aula al que tenemos que ir. Es obvio mencionar que en la analogía, el guardia es el router y los alumnos los paquetes.

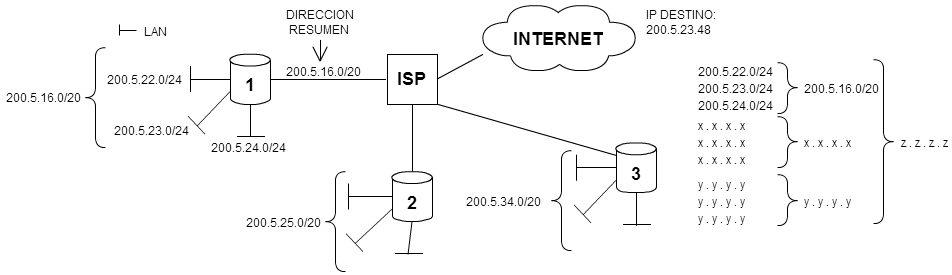
Por lo tanto, las tablas de los routers no contienen todas las direcciones IP de todas las redes que está conectando (símil a tener todos los nombres de alumnos), sino que contienen únicamente las direcciones de red o subred (cursos).

¿Cómo actua el router para encaminar los paquetes? Cuando llega un paquete desde internet, el router toma la dirección IP de destino y va comparando bit a bit contra cada entrada de la tabla de encaminamiento hasta encontrar una coincidencia, y en caso de no encontrarla manda al paquete por una ruta por defecto. ¿Cuántos bits va a comparar? Va a comparar la cantidad de bits de red, porque al router únicamente le interesa identificar a que red pertenece ese paquete.

Como previamente dijimos, si las direcciones IP son asignadas sin ninguna lógica, las tablas de encaminamiento de los routers van a tener muchas entradas, haciendo que la comparación necesaria para el encaminamiento tome mucho más tiempo. Hubiera sido mejor organizar la asignación de direcciones IP geográficamente, de una manera jerárquica, como lo hace la red telefónica con los números de teléfono de sus usuarios. De esta manera se logra un encaminamiento mucho más rápido, ya que cuando la red telefónica recibe una llamada para conmutar, únicamente necesita comparar los primeros dígitos del teléfono, supongamos 011, para saber que debe encaminar hacia Buenos Aires (toma la decisión mucho más rápido).

Por este motivo, se decidió que para que el encaminamiento fuera más rápido, las pocas direcciones que quedan deben ser asignadas de manera geográfica (utilizando el concepto de la red telefónica). A partir de ahora a América del Sur se le asignan todas las direcciones que comienzan con 200 o 201, para Europa las que comienzan con 194 a 195, y de esta manera se fue dividiendo el mundo geográficamente. Entonces cuando a un router le llega un paquete con una dirección IP que comienza con 200 no sigue leyendo el resto de los bits sino que directamente encamina hacia América del Sur. Es asa como el CIDR ayudo a que el encaminamiento sea más eficiente haciendo que los routers tengan menos entradas en las tablas de encaminamiento.

**Resumen de ruta o sumarización (mejora del CIDR):**

****

Supongamos que tenemos la empresa 1, la 2 y la 3. La empresa 1 tendría que enseñarle a su proveedor de servicio que tiene 3 redes: la 200.5.22.0, la 200.5.23.0 y la 200.5.24.0. Por lo tanto el proveedor de servicio debería tener en su tabla de encaminamiento una entrada por cada una de estas redes. Supongamos también, que hay otras dos empresas conectadas a ese servidor que cuentan con tres redes cada una, de manera que en la tabla de encaminamiento del servidor tendríamos 6 entradas más. Si siguiéramos agregando las direcciones de otras redes, esta tabla se volvería muy grande haciendo que la comparación de bits necesaria para el encaminamiento tarde mucho tiempo ya que hay más cantidad de renglones contra los cuales comparar. Para evitar esto podemos hacer un resumen de ruta que consiste en resumir la tabla, esto es minimizar la cantidad de renglones utilizando una dirección IP que abarque al resto de las direcciones. Por consiguiente, cuando el proveedor reciba un paquete con una dirección IP destino determinada, solo necesitara comparar unos pocos bits de las pocas direcciones que tiene en tabla para saber hacia cual empresa encaminar dicho paquete. Es decir, la idea es que pueda distinguir entre una empresa y otra realizando menos comparaciones (porque hay menos entradas en la tabla), y a su vez que la búsqueda de coincidencia se haga comparando bit a bit (para no tener que comparar toda la dirección completa), todo esto por supuesto es busca de disminuir el tiempo de encaminamiento.

Para el ejemplo citado, de las 3 redes que pertenecen a la empresa 1 se utilizara una dirección resumen, para las 3 redes de la empresa 2 otra dirección resumen y lo mismo para las redes de la empresa 3. Así, en lugar de tener 9 entradas en la tabla de encaminamiento, el servidor únicamente tendrá 3 para comparar. A su vez, si todas las direcciones resumen del servidor comienzan con el mismo número (supongamos 200) puede generar una dirección que sea resumen de las anteriores tres para enseñar a internet, de manera que tenga una sola dirección en su tabla de encaminamiento para comparar cuando llegue un paquete.

A continuación calcularemos el resumen de ruta para las direcciones de la empresa 1. Como el primer y el segundo byte de las direcciones coinciden no las vamos a comparar simplemente para disminuir los cálculos, pero en realidad son comparados también:

200.5.**22**.0 🡪 200.5.0001|0110.00000000

200.5.**23**.0 🡪 200.5.0001|0111.00000000

200.5.**24**.0 🡪 200.5.0001|1000.00000000

 Dirección resumen: **200.5.16.0/20** 🡪 200.5.00010000.00000000

16

Como vemos, para generar una dirección resumen lo que debemos hacer es pasar las direcciones a binario y realizar una comparación bit a bit buscando coincidencia. La cantidad de bits que coinciden (de izquierda a derecha) entre todas las direcciones son los valores que no se modifican, y a partir del bit que deja de haber coincidencia trazamos una recta y completamos la dirección con ceros. Luego pasamos la dirección resultante de binario a decimal.

La máscara le dice al router o proveedor cuantos bits debe comparar para buscar coincidencia. Entonces, luego de hacer el resumen de ruta tenemos una dirección que tiene menos bits en la mascara (/20), porque la idea es que el router deba comparar menos bits. Es decir, en lugar de tener tres entradas y tener que comparar 24 bits (/24) por cada entrada, ahora solamente tiene que comparar contra una entrada (la dirección de resumen) y tan solo buscar coincidencia entre los 20 primeros bits.

Supongamos que desde internet ingresa un paquete al proveedor de servicios con dirección IP destino: 200.5.23.48. El proveedor tiene en su tabla de encaminamiento las direcciones resumen de cada una de las empresas, y comienza a comparar (buscar coincidencia) bit a bit entre la dirección que llego contra las direcciones de la tabla. En esa coincidencia va a notar que los primeros bits de la dirección destino coinciden con la dirección resumen de la empresa 1 entonces encamina el paquete hacia el router de dicha empresa. Este router a su vez, contiene como entrada en su tabla de encaminamiento cada una de las direcciones IP de las computadoras de la empresa, entonces comparara nuevamente bit a bit la dirección destino hasta encontrar coincidencia con alguna de las direcciones que tiene en la tabla y encaminara el paquete.

En resumen podemos decir que mientras más cerca estamos del destino más específicas son las entradas en las tablas de los routers, y a medida que nos vamos alejando son más resumidas porque tengo menos bits en la máscara y a su vez menos entradas en la tabla de encaminamiento, lo que hace que el encaminamiento sea más eficiente ya que la comparación se realiza mucho más rápida.

Sabemos que cada clase tiene una máscara por defecto, para la clase C es: 255.255.255. Cuando creamos subredes la máscara por defecto para esta clase es /24 (porque los primeros 24 bits pertenecen a la parte de redes).

Subneting: alargamos la máscara con respecto a la máscara por defecto, creamos mascaras más largas.

Superneting: achicamos la máscara con respecto a la máscara por defecto, creamos máscaras más cortas.

**VLSM (Variable Length Subnet Mask – Mascara de Subred de Longitud Variable):**

Supongamos que hay una empresa que tiene 5 subredes, cada una de las cuales con una cierta cantidad de dispositivos. La cantidad de bits de Host que voy a necesitar para cumplir con los requerimientos de la empresa me lo va a dar la subred que tenga la mayor cantidad de dispositivos. En nuestro caso vemos que el mayor número de Host que tiene una subred es 50, por lo que con 6 bits alcanzaría a cubrir esa necesidad (y todas) ya que con Host disponibles.

Si nosotros aplicáramos subneting, esto es alargar la máscara con respecto a la máscara por defecto, se desperdiciarían una cierta cantidad de direcciones IP: 52 para un caso, 32, 48, 12 y 18 para el resto. Por lo tanto solo se debe usar subneting cuando trabajamos con direcciones privadas, ya que si derrochamos direcciones no hay ningún inconveniente; en cambio si trabajamos con direcciones públicas conviene utilizar VLSM. Notemos también que cuando aplicamos subneting toda la máscara debe ser la misma en la empresa, pero con la tecnología VLSM podemos lograr que la longitud de la máscara sea variable. Es decir que podemos tener diferentes mascaras en función de cuantos Host hagan falta en cada red o subred. Vamos a asignar la cantidad justa de bits para Host en función de la necesidad de cada una de las subredes.

Clase 14 de Mayo

**IPV6**

**Objetivo:**

* **Mayor espacio de direccionamiento:** El gran problema que surgió con IPV4 es que la cantidad de usuarios de internet creció exponencialmente lo que llevo a que se agotaran las direcciones IP disponibles. IPV6 surge para lograr tener una mayor cantidad de direcciones IP públicas.
* IPV6 optimiza el protocolo IPV4, es decir que supera las limitaciones o fallas que tenia. Por ejemplo: lograr un encaminamiento más rápido.
* En IPV6 no nos referimos a direcciones públicas o privadas, sino que hablamos en términos de direcciones globales. Nos importa más el alcance, es decir cuán lejos puedo ir con una dirección IP.

**Objetivos Principales:**

* **Manejar millones de Host:** La cantidad de bits que tiene una dirección IPV6 es 4 veces la de IPV4. Es decir, en IPV4 manejábamos 32 bits y en IPV6 manejamos 128 bits, lo que permite tener una mayor cantidad de direcciones.
* **Reducir el tamaño de las tablas de encaminamiento:** El direccionamiento en IPV6 está organizado geográfica y jerárquicamente, muy parecido al sistema que utiliza la red telefónica. Viendo los primeros bits de una dirección IPV6 puedo encaminar un paquete sin necesidad de tener que leer los 128 bits, lo que agiliza y disminuye el tiempo de encaminamiento.
* **Simplificar el protocolo:** Se intenta de que el procesamiento del protocolo IPV6 sea más rápido. Se reduce la cantidad de campos de la cabecera para que cuando los paquetes lleguen a los routers sean procesados más rápido.
* **Proporcionar mayor seguridad:** La seguridad en IPV4 es opcional mientras que en IPV6 es obligatoria. Se usa un protocolo llamado AXC o IPC
* **Permitir que el protocolo evolucione:** En IPV4 se había dejado un bit libre sin uso en la cabecera para prever un futuro uso o permitir que el protocolo evolucione, de manera que si necesito agregar alguna funcionalidad tengo ese bit libre para ser usado. En IPV6 no se deja ningún bit libre de la cabecera, pero utiliza lo que se conoce como “siguiente cabecera” para permitir que el protocolo se expanda y crezca dándole nuevas funcionalidades sin tener que modificar nada de la cabecera.
* **Permitir que las versiones 4 y 6 coexistan por años:** Cuando comenzaron con el desarrollo de IPV6 fueron conscientes de que no se podía implementar de un día para el otro IPV6. Por lo tanto se generaron estrategias llamadas métodos de transición para permitir que ciertos usuarios ejecuten IPV4 y otros IPV6.

**Características avanzadas de IPV6:**

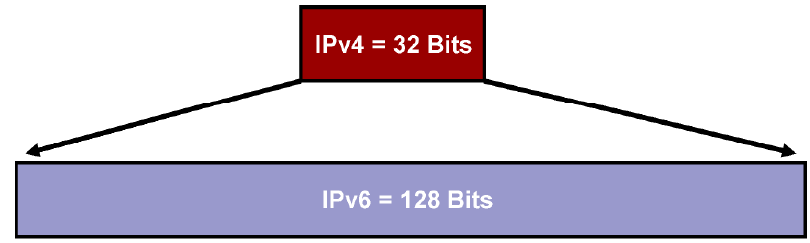
* **Espacio de direccionamiento más grande:** Como mencionamos previamente, en IPV4 se utilizan 32 bits para las direcciones, mientras que en IPV6 la cantidad de bits utilizados es 4 veces más grande, es decir 128 bits. Con esta cantidad de bits se pueden direccionar una cantidad mucho mayor de dispositivos, superando la limitación del agotamiento de direcciones que tiene IPV4.
* **Alcance y flexibilidad global:** Las direcciones IPV6 se caracterizan por tener alcance. Alcance hace referencia a hasta dónde puedo llegar con una dirección IP. Hay direcciones IP que tendrán un alcance de un segmento de la red, otras tendrán alcance a nivel de una empresa y otra tendrán alcance a nivel mundial o internacional. Hay entonces, diferentes tipos de direcciones IP y cada uno tiene un alcance diferente. Las maquinas con IPV4 tenían configurada únicamente una dirección IP, mientras que las maquinas con IPV6 tienen muchas direcciones IP, de acuerdo al uso que quiera tener, con cada una de las direcciones voy a tener un alcance diferente. Es decir que la forma de asignación o configuración de direcciones IP es distinta.
* **Sumarización:** Implementa la sumarización, que consiste en crear un resumen de varias direcciones IP. Esto hace que disminuya el tamaño de las tablas de encaminamiento de los routers.
* **Plug-and-Play (Enchufar y Usar):** Yo enchufo la maquina y automáticamente se autoconfigura una dirección IP. Es decir, la maquina puede averiguar en el router la parte de red de la dirección IP, que aquí se conoce como prefijo de red, y en función de eso configurarse una dirección IP. Por más que no haya router, al momento de encender la maquina, ella se configura automáticamente una dirección IP de alcance local. Una maquina que trabaja con IPV6 tiene siempre por lo menos una dirección IP configurada.

Cada dirección IPV6 maneja “tiempos de vida o valid Time Life”, es decir que cada vez que la

maquina se autoconfigura una dirección IP esa dirección tiene un tiempo de vida. Ese tiempo de vida puede ser infinito en caso de que se esté completamente seguro de que no existe otra dirección IP igual, o puede ser un determinado periodo de tiempo (segundos) donde se examina que no hayan direcciones IP duplicadas (con el mismo número). Si existieran direcciones IP duplicadas entonces la dirección de la maquina es desconfigurada. Es decir, que no puede haber dos direcciones IP iguales en el mismo segmento de red, si en segmentos diferentes.

* **End to end sin NAT (Extremos a Extremo sin NAT):** No existe la traducción de direcciones en IPV6, al contrario de lo que sucedía con IPV4. Aquí se pueden comunicar dos maquinas sin realizar traducción de direcciones alguna, por ello recibe el nombre de *extremo a extremo sin transducción*. Cada máquina con su dirección de IP global se puede comunicar y entablar un dialogo sin necesidad de realizar ninguna traducción, ya que esto es muy lento (utiliza mucho tiempo del router en traducción en lugar de encaminamiento) y se puede producir un cuello de botella en el router. En cambio, IPV4 utiliza el parche de NAT, como necesidad por la limitación del agotamiento de direcciones.
* **Cabecera más simple:** Si bien la cabecera de una dirección IPV6 es más larga porque tiene más bytes, presenta la ventaja de tener menos campos para procesar.
* **Encaminamiento eficiente:** El encaminamiento en IPV6 es más eficiente porque es geográfico. Al dividirse la asignación de las direcciones por área geográfica se permite que el router al leer los primeros bits de una dirección pueda saber hacia dónde tiene que encaminar el paquete, demorando mucho menos tiempo que en IPV4. Con leer la primera parte de una dirección alcanza, no es necesario leer todos los bits. El mundo se dividió geográficamente en 5 zonas.
* **No hay broadcast:** No existe el broadcast en IPV6, es decir que se eliminaron las direcciones de broadcaste 255.255.255.255. Si quiero enviar un paquete IPV6 a un grupo de maquinas lo hago utilizando direcciones multicast (direcciones de grupo). Esto es muy bueno porque los broadcast consumen mucho tiempo de máquina, ya que todas las maquinas que reciben el mensaje deben procesarlo.
* **No hay checksums:** en IPV4 se utiliza un checksum para la cabecera, esto es un control de integridad que se realiza a la cabecera para ver que no se modifico. En IPV6 no se utiliza esta función porque era lento ya que se debe calcular dos veces por cada salto, cuando el paquete llega y cuando el paquete es transferido (porque se le disminuye un tiempo al TTL). Si se desea controlar la integridad que lo haga la capa de arriba (capa de transporte).
* **Cabeceras de extensión:** Implementa cabeceras de extensión para permitir que el protocolo evolucione sin tener que agregar bits a la cabecera
* **Etiquetas de flujo:** Esta funcionalidad todavía no está implementada. La idea que persigue es que cada comunicación entre una maquina y otra sea definida como un flujo distinto de comunicación y sea tratado de una manera especial, algo así como un canal virtual en ATM o un circuito virtual en Frame Relay.

**Gran espacio de direccionamiento:**

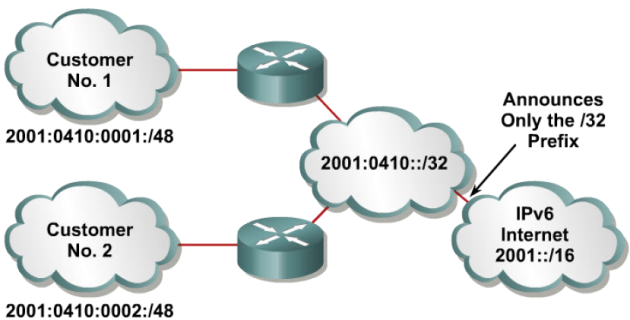
****

IPV4: 32 bits o 4 bytes de longitud = 4.200.000.000 nodos direccionables

IPV6: 128 bits o 16 bytes: cuatros veces los bits de IPV4

5\* direcciones por persona.

**Resumen de ruta o sumarización:**

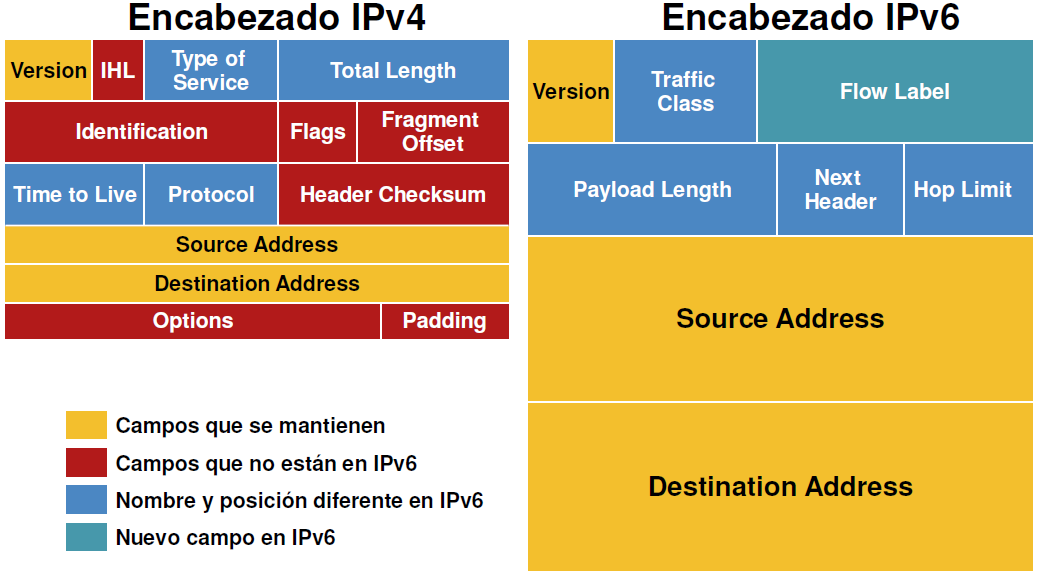
****

Una dirección IPV6 esta expresada en hexadecimal, tiene 8 grupos de 4 dígitos hexadecimales.

Debemos ingresar el concepto de prefijo de red: cuantos bits de la parte de red son importante en la dirección IPV6. En la imagen tenemos dos empresas con direcciones IPV6 asignadas, de las cuales los primeros 48 bits son importantes, es decir que todos los dispositivos de la red van a tener los mismo primeros 48 bits. Esos 48 bits fueron resumidos en 32 bits, de manera que el servidor que trabaja con las dos redes en lugar de tener dos entradas en la tabla de conmutación tiene una sola de 32 bits importantes. Es decir que cuando un paquete llegue a ese servidor, únicamente deberá comparar o buscar coincidencia en los primeros 32 bits que tenga la dirección de destino del paquete, y luego lo conmutara.

De esta manera se produce un encaminamiento más eficiente y escalable, ya que la idea es que la tabla de encaminamiento de los routers tenga la menor cantidad de entradas posibles y tengan que comparar la menor cantidad de bits posibles para efectuar la conmutación más rápidamente. En las tablas de encaminamiento de los routers únicamente hay direcciones de red y de subred, no hay direcciones de Host.

**Comparación del encabezado de IPV4 e IPV6:**

****

Campos que se mantienen: Versión, dirección origen y dirección destino.

El campo versión es muy importante porque en base al valor que tenga se le da significado a todos los bits que siguen. En IPV4 el campo versión comienza con 0100 (4 en binario) y en IPV6 este campo comienza con 0110 (6 en binario).

Campos que desaparecen: Longitud de la cabecera, identificación, banderas, desplazamiento dentro del fragmento, checksum, opciones y relleno.

Si no existe el campo longitud de la cabecera, ¿Qué tamaño tiene la cabecera? El tamaño de la cabecera es fijo, por lo tanto no me es necesario tener el campo longitud de la cabecera.

Todo el segundo renglón del encabezado IPV4, que estaba dedicado a la fragmentación, no se encuentra en el encabezado IPV6, debido a que este protocolo no implementa la fragmentación porque es muy lento para los routers.

Elimina el checksum porque no existe ningún campo en una cabecera IPV6 que valide la integridad del paquete, ya que esto hace que el procesamiento en los routers sea mucho más rápido al no tener que calcular el valor del checksum dos veces por cada salto que dé el paquete.

El campo opciones desaparece, pero esto no significa que en IPV6 no se puedan implementar opciones, sino que se implementan pero de otra manera.

Campo que varia el nombre y posición pero tiene el mismo significado: El campo *tipo de servicio* de IPV4 que era para manejar prioridades ahora se llama *Clase de Trafico*¸ este campo sigue permitiéndome distinguir entre un paquete importante de uno no tan importante.

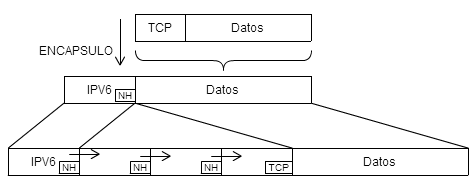
El campo *Total Length o Longitud Total de la cabecera* ahora se denomina *Payload Lengtho Longitud de carga útil.* En IPV4 este campo incluía la longitud de la cabecera, algo que no ocurre en IPV6, donde simplemente mide la longitud de la carga o datos ya que el tamaño de la cabecera es fijo.

El campo *TTL* ahora se denomina *Limite de Salto*. Este campo sigue utilizándose para contar la cantidad de saltos que puede dar un paquete, es decir la cantidad de routers por lo que puede pasar. Se usa sobre todo para impedir que un paquete quede dando vueltas eternamente en la red mientras consume recursos.

El campo *Protocolo* se usa para saber al momento de encapsular un segmento que protocolo entrego el paquete de la capa de transporte a la de Interred, de manera que cuando ese paquete se desencapsule sea entregado al mismo protocolo. Los protocolos de la capa transporte pueden ser el UTP o el UDP, y ese valor es guardado en el campo protocolo. El campo protocolo es el punto de unión entre todas las capas. En IPV6 este campo se llama *Próxima Cabecera o Next Header*, porque la forma que tiene IPV6 de expandirse es agregando cabeceras. Entonces, al realizar en el encapsulado del segmento que nos pasa la capa de transporte, en el campo Next Header de la cabecera IPV6 guardamos cual es el protocolo que utiliza ese segmento en la capa superior.

Supongamos que queremos agregar lo que se conoce como una *Cabecera de Extensión* para expandir el paquete. En este caso, el campo Next Header de la cabecera va a apuntar hacia otra cabecera, que a su vez puede apuntar hacia otra cabecera, y así sucesivamente según la cantidad de cabeceras que queramos agregar para ampliar el paquete. La ultima cabecera que agregamos es la que va a guardar en el campo Next Header, no el valor a la próxima cabecera (porque ya no hay mas), sino que guardara cual es el protocolo que utiliza el segmente encapsulado en la capa de transporte.

De esta manera IPV6 permite que el protocolo evoluciones sin tener que modificar la cabecera. Si queremos agregar funcionalidad simplemente tenemos que agregar una cabecera de extensión. Debemos mencionar, y como la imagen corrobora, que las cabeceras de extensión se colocan entre la/s cabecera/s original y la parte de datos del paquete



Campo nuevo: Etiqueta de flujo, se utiliza para distinguir una comunicación de otra. Todavía no está implementado.

¿Qué cabecera es más grande? La cabecera de IPV6 es más grande, el doble exactamente, que la de IPV4. La cabecera de IPV4 tiene 5 renglones o palabras de 4 bytes cada uno, es decir que en total tiene 20 bytes. Mientras que la cabecera de IPV6 posee los dos primeros renglones o palabras de 32 bits y los últimos dos, que representan la dirección origen y la dirección destino, tienen 128 bits cada uno (16 bytes), es decir que se podrían ver como 4 renglones o palabras de 4 bytes cada uno. La cabecera IPV6 presentaría entonces 10 renglones o palabras de 4 bytes cada uno, dando un total de 40 bytes.

En resumen, en tamaño la cabecera de IPV6 es más grande que la de IPV4, a pesar de que tiene menos campos. De todas maneras, al tener menos campos se procesa más rápido. Es mas larga debido a las direcciones IPV6 que tienen 4 veces el tamaño de una dirección IPV4.

**Representación de la dirección IP:**

Una dirección IPV6 se representa: **X:X:X:X:X:X:X:X** donde X es un campo hexadecimal de 16 bits. Como tiene muchos bits, la forma más corta de expresarla es en un formato hexadecimal. Para representar la dirección IPV6 usamos 8 grupos de 4 dígitos hexadecimales cada uno, es decir de que cada grupo tiene 16 bits. La cantidad de bits por grupo multiplicada por la cantidad de grupos me da el tamaño de la dirección, esto es16x8 = 128 bits. Cada grupo es separado por **:** a diferencia de una dirección de IPV4 que se separaba con un solo punto.

Existen **métodos de compresión** para las direcciones IPV6, que me permitan escribirlas de una forma más resumida:

Los primeros ceros de un campo de una dirección IPV6 son opcionales, es decir que pueden omitirse, por ejemplo: 

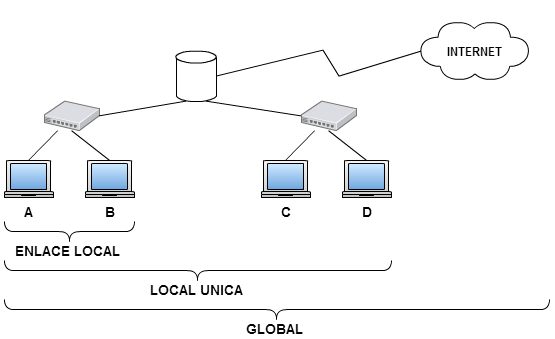
Además, si hay grupos sucesivos o consecutivos que tengan todos ceros, pueden ser eliminados y en su lugar los representamos por **::.** Esta optimización solamente puede hacerse una vez en una dirección debido a que la forma que tiene el protocolo de calcular cuantas grupos de ceros fueron reemplazados por :: es contar la cantidad de grupos sin reemplazar y restársela a ocho. El valor que da esa diferencia me indica cuantos grupos de ceros fueron reemplazados. Por lo tanto, si yo tengo ese reemplazo más de dos veces, no puedo determinar cuántos grupos de cero hay en un reemplazo y cuantos en el otro. Por ejemplo:



**Modelo de direccionamiento de IPV6:**

Las direcciones IPV6 se asignan a las interfaces, no a las maquinas como si sucedía con IPV4. Lo que se denomina interfaz de una maquina es la placa de red. De hecho una maquina en IPV6 se llama nodo, y un nodo puede tener muchas interfaces y cada interfaz a su vez puede tener muchas direcciones IPV6. Es decir que cualquier maquina tiene muchas direcciones IPV6, debido a que cada dirección tiene un **alcance** definido.

Es decir, en una maquina IPV4 yo por más que cambie 20 veces la dirección IP siempre me recuerda la ultima que configure, a menos que tenga muchas interfaces. En cambio en una maquina IPV6, por más que tenga una sola interfaz puedo tener muchas direcciones IPV6 configuradas. Y esto se debe al alcance de las direcciones.



Con una dirección IPV6 voy a tener **alcance local o local link**, esto significa que la maquina con esa dirección IP solamente se va a poder comunicar con las maquinas de ese segmento de red. Una dirección de enlace local es la que se autoconfigura en la maquina, y solamente me permite comunicarme con otra máquina que se encuentre en el mismo segmento o enlace de red, es decir que esté conectada al mismo switch. Por ejemplo las maquinas C y D o A y B podrían comunicarse a través de una dirección IPV6 de enlace. Estas direcciones comienzan con FE80

Si quiero comunicar la maquina A con la maquina C que se encuentra en otro segmento, bajo otro switch debo utilizar otra dirección IPV6 que se llama **Local Única** que tiene alcance a nivel de la empresa. Estas direcciones comienzan con FC.

Si la maquina A quiere comunicarse con una maquina que esta fuera de la red de la empresa, en la otra punta de internet, deberá utilizar una dirección IPV6 de **Alcance global.** Estas direcciones empiezan con 2.

Como vemos, la diferencia que se presenta es que en IPV4 hablamos en términos de direcciones públicas o privadas mientras que en IPV6 se pierde ese concepto y en su lugar nos referimos al alcance de las direcciones.



Otra característica que presenta IPV6 es que las direcciones tienen tiempo de vida, que puede ser: tentativo, preferido o valido.

**Tipos de direcciones IPV6:**

Hay tres tipos de direcciones IPV6:

* **Unicast (uno a uno):** Se usan para las comunicaciones de una maquina a otra. Por ejemplo una comunicación cliente-servidor. Es una dirección para una sola interfaz.
* **Multicast (uno a muchos):** Cuando una maquina se comunica con un grupo de maquinas. Estas direcciones comienzan con FF.
* **Anycast (uno al más cercano):** En IPV4 no se permite que dos dispositivos estén configurados con las misma IP, salvo que sean direcciones privadas y estén en distintas empresas, pero dentro de una misma empresa no pueden haber dos maquinas que tengan la misma IP. En IPV6 esto si puede ocurrir, y para ello se usan las direcciones Anycast. Con estas direcciones se le entrega el paquete a la dirección que este más cercana a mí maquina. Es decir, una misma dirección IP puede estar configurada en distintas partes de la empresa, si yo emitiera un paquete desde mi maquina con dirección destino de Anycast (que está configurada en varias maquinas), el router le va a entregar el paquete a la maquina más cercana que tenga esa dirección configurada, al resto no. Los routers saben que tan lejos esta una maquina. Estas direcciones sirven para hacer balanceo de carga.

Por ejemplo: imaginemos que quiero entregar un trabajo a algún profesor de redes (que hay

muchos). Entonces nosotros le damos el trabajo a la secretaria y ella al que primero vea le entrega el trabajo.

**Tipos de direcciones IPV6 Unicast:**

Pueden ser:

* **Global:** seria como una dirección publica de IPV4, tiene alcance mundial. Estas direcciones empiezan con 2.
* **Local de enlace:** estas direcciones comienzan con FE80. Tiene un alcance local
* **Local de sitio (en desuso)**
* **Local Única (ULA):** estas direcciones tienen alcance a nivel de empresa.
* **IPV4 Compatible (en desuso)**
* **IPV4 Mapeada:** significa meter una dirección IPV4 adentro de los 128 bits de una dirección IPV6.

**Prefijos de tipos de direcciones IPV6:**

****

No especificada: cuando una maquina arranca puede que no tenga ninguna dirección IP configurada, y en ese caso se autoconfigura la ::/128. Esta dirección en IPV4 es reservada y nunca la puede tener configurada una maquina. Esta dirección se conoce como “Este Host o This Host”.

Loopback: Esta dirección tiene 127 bits en 0 y el último bit en 1. El /128 es el prefijo que me indica que esa cantidad de bits tienen que tener el valor que se indica, no puedo cambiar ningún bit de esos. En IPV4 se reservo toda una red clase A entera, toda la 127.0.0.0 como dirección de Loopback. En IPV6 solo hay una dirección de loopback la ::1.

Multicast: los primeros 8 bits tienen que ser 1. Empieza con FF.

Unicast Local de enlace: esta dirección se autoconfigura. Comienza con FE80, los primeros 10 bits son fijos.

ULA: seria como una dirección privada de IPV4 ya que abarca únicamente el entorno de la empresa. Estas direcciones comienzan con FC.

Global: estas direcciones tienen alcance global. Comienzan con 2, los primeros tres bits del primer grupo son fijos y deben valer 001.

IPV4 Mapeada: Yo puedo poner una dirección IPV4 dentro de una dirección IPV6 agregándole FFFF al comienzo y a continuación la dirección IPV4. Tiene /128 porque no puede variar ya que son direcciones únicas.

Prefijo de documentación: se reservaron direcciones para enviar documentación.

**Direcciones Globales Unicast:**



Una dirección IPV6 se divide en dos partes: la primera mitad hace referencia a la parte de red y la otra mitad a la parte de Host. La diferencia con IPV4 está en que la parte de red ahora se llama *prefijo de red* y la parte de host es conocida como *ID d Interfaz*. Esto es fijo e inamovible, siempre habrá 64 bits para identificar a la red y 64 bits para la interfaz.

Los 64 bits de la parte de prefijo de red tienen una lógica que está estructurada, esto es tiene una jerarquía. Como sabemos son direcciones globales y por lo tanto comienzan con 001 (2 en decimal). Luego viene lo que se conoce como *prefijo de enrutamiento global* que está dividido geográficamente para poder encaminar más rápido. Con respecto a los 64 bits de la parte de interfaz podemos mencionar que siempre comienzan con 16 bits de *ID de subred*, esto significa que cada empresa siempre va a contar con subredes, cada una de las cuales puede tener dispositivos.

**Prefijos de IPV6:**

Es importante mencionar que no se utilizan mascaras de subred en IPV6, sino que se utilizan prefijos de red. Un prefijo está compuesto por una / y un numero, que me indica que la cantidad de bits señalada con ese número identifican al prefijo de red, y el resto de los bits identifican a la interfaz.

**Registros Regionales de Internet (RIRs):**

El mundo se dividió geográficamente en 5 partes.