**Listas de control de acceso**

Las listas de control de acceso nos permiten llevar a cabo el **control del tráfico** sobre paquetes que circulan en la red utilizando **direccionamiento origen o fuente y direccionamiento destino.**

Adicionalmente cuando hablamos del protocolo TCP que se comunica a través de puertos utilizando las primitivas para el intercambio de segmentos TCP o UDP utilizando los puertos.

El día de hoy los ejercicios preparados he diseñado unos ejercicios para trabajar con direccionamiento **IP utilizando máscaras y ACLs estándar**, las más básicas.

**Vamos a recordar las capas del modelo OSI,**

La capa de **enlace de datos** es la primer capa que interactúa con un esquema de direccionamiento. En la capa de enlace de datos el esquema de direccionamiento que se utiliza es la dirección MAC compuesta por 48 bits en un formato hexadecimal. Toda trama o frame requiere de un direccionamiento **MAC origen y un direccionamiento MAC destino**.

Una vez que la trama sale del dominio de un **Swith** y va hacia **un router** la trama se convierte en un paquete. Los paquetes utilizan un direccionamiento de **capa 3 de red**: IP. Y se utilizan la dirección IP origen y la dirección IP destino.

Todos los servicios del protocolo de la **capa de transporte** **TCP** son orientados a conexión, que requiere establecer la conexión entre un origen y un destino. Un ejemplo es el protocolo de comunicaciones **ssh, telnet, FTP.** Estos protocolos trabajan con sesiones, es decir, con una conexión. Los servicios orientados a conexión consumen más recursos que los servicios orientados a no conexión.

Por el otro lado, los servicios del protocolo **UDP** son orientados a no conexión, no garantizan el intercambio de información exitosa entre un origen y un destino. No se establece un circuito. Los protocolos que utilizan servicios orientados a no conexión son por ejemplo **DHCP**, **TFTP y SNMP** (Correo electrónico)

En la capa de enlace de datos se manejan como unidades de datos de protocolo: **tramas**, en la capa de red **paquetes** y en la capa de transporte se manejan **segmentos**, segmentos de tipo **TCP** y **UDP**. Y para distinguirlos se utilizan los puertos. Los puertos más conocidos, que podemos utilizar son:.

* 80: http (Utilizando el protocolo de comunicaciones web)
* 22: ssh
* 20, 21: FTP (corresponde con el servicio FTP)

Supongamos que queremos comunicar un **cliente a un servidor** utilizando el protocolo **web**, el proceso sería el siguiente:

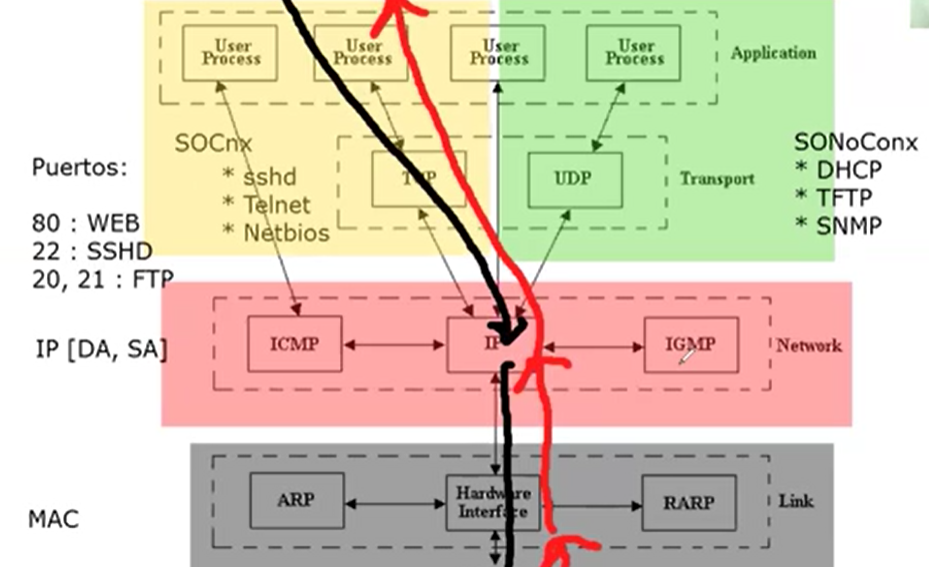
Para que la información pueda fluir sale de la petición de la aplicación:

* Utiliza el servicio TCP
* Se agregan los encabezados del direccionamiento IP
* Se agregan los encabezados MAC

Viaja por el medio físico se da la comunicación

Cuando la información viene de regreso se valida la MAC, luego se valida la dirección IP.

En la capa 3 al subir a la capa 4, se tiene que decidir si es un servicio orientado a conexión o no conexión. Si es orientado a conexión utilizará el puerto 80.



En la capa 3 al subir a la capa 4, se tiene que decidir si es un servicio orientado a conexión o no conexión. **EN la capa 4 podemos discernir si permitimos o negamos el tráfico** al aplicar listas de control de acceso utilizando los **puertos**.

Hay una lista muy grande de puertos, son **65 535 puertos**. Y algunos puertos ya están declarados como estandarizados.

20 y 21 corresponden con FTP

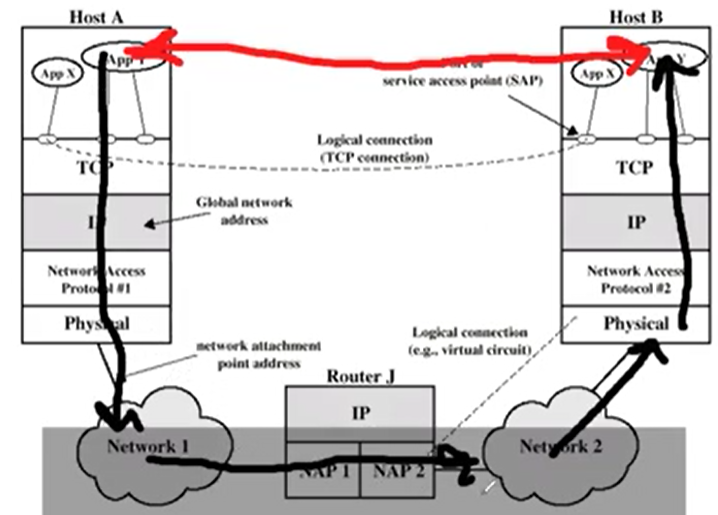
23 telnet

80 http

Las comunicaciones donde **un origen se quieren comunicar con un destino** **de una aplicación “y” a una aplicación “y” la comunicación lógica** fluye en ese sentido y la **comunicación física** en otro

La comunicación en rojo es lógica, y la comunicación en negro es física.

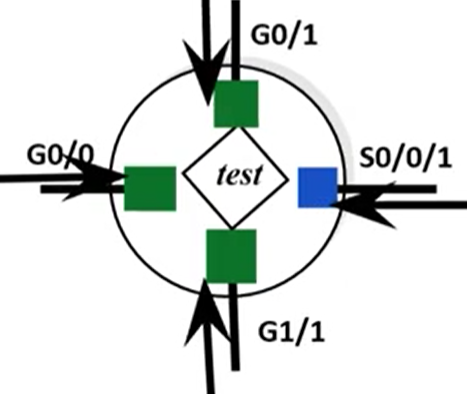
**Los filtros para permitir o bloquear algún tipo de tráfico se instalan o aplican en los routers, en el direccionamiento IP.**



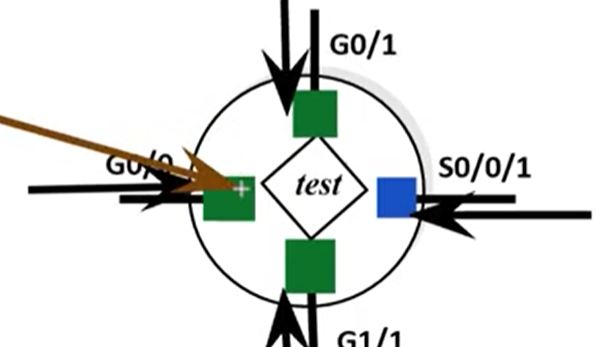
Las listas de control de acceso se utilizan para:

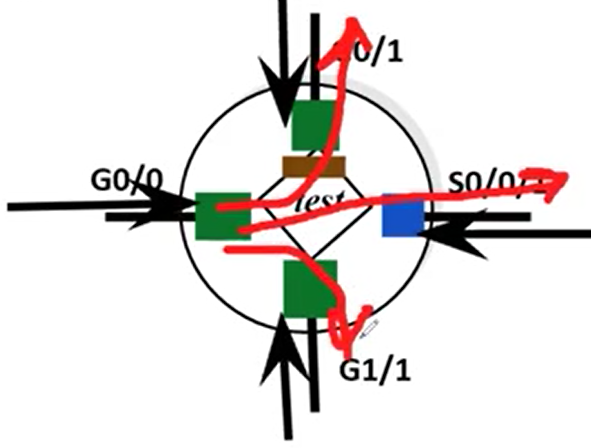
* **Limitar el tráfico de la red e incrementar el desempeño de la misma.** Como cuando segmentamos el tráfico en homeoffice y entretenimiento, podemos configurar para que el tráfico de los segmentos no entre a una sección no permitida.
* **Suministrar mecanismos de control de flujo.** A un servidor algunos puedan entrar algunos equipos y otros no (concursos de programación: jueces y alumnos). Otro ejemplo son las impresoras no todos pueden imprimir en todas la impresoras.
* **Necesidad de controles básicos de seguridad.** Las acciones permitir o negar el tráfico.
* **Bloquear algún tipo de tráfico.** Puedo bloquear el tráfico de un equipo en particular o de un bloque o segmento en particular.

En un router tengo interfaces distintas (gigabit ethernet y seriales. Los **puertos tienen canales de recepción y de transmisión**. Los puertos reciben datos de la red.

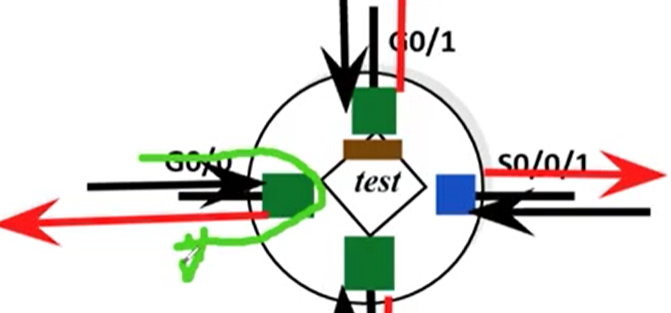


Para un paquete que llega por la interface g0/0. El router toma la decisión de qué hacer con ese paquete que acaba de llegar. En ese momento el paquete es analizado y tiene la posibilidad de salir por la interface g0/1, por la g1/1 o por la s0/0/1. Todas las interfaces pueden sacar tráfico para alcanzar su destino final.





Pero hay una regla, **tráfico que llega por una inteface jamás puede ser regresado por la misma interface o no puede salir por la misma interface.** Con las subinterfaces es distinto llega con la subinterface 10 y sale por subinteface 20, eso sí está permitido.



Para el control de flujo se debe analizar la **fuente y el destino**.

Después de ver **el video** ya se tuvo un primer acercamiento con las listas de control de acceso.

A las listas de control de acceso también se les puede identificar con un nombre, como en la práctica del laboratorio.

* Las **listas estándar** son utilizadas para filtrar el tráfico con base en la **dirección IP fuente** de donde viene.
* Las **listas extendidas** son utilizadas para filtrar el tráfico con base en la **dirección IP fuente, dirección destino, tipo de protocolo e inclusive el puerto** que se puede utilizar.

Para trabajar con las listas de control de acceso se utiliza una **máscara comodín (wildcard mask).**

Esta máscara comodín se identifica como un **complemento de la máscara de Subneteo (complemento de 255).**

El wildcard mask es el complemento de la máscara de Subneteo.

**Estas wildcard mask se utilizan para permitir o bloquear el tráfico**

Las **listas de control estándar son del 1 – 99**, lo que significa que se va a filtrar el tráfico con base en la **dirección IP fuente. Solo se permite ejecutar una de dos acciones : permitir o negar.**

Después viene la dirección IP fuente que se verifica y la máscara comodín.

Las listas de control de acceso se **ejecutan de arriba abajo y de izquierda a derecha verificando los contenidos.**

**Las listas de control de acceso no tienen ningún efecto hasta que no son asignadas a una interface.**

Hasta que la interface tiene asociada una lista de control de acceso, la acción de permitir o negar el tráfico toma acción.

Hay que acceder a la interface.

Luego poner el comando **ip access-group número de la lista**, la acción de entrada o de salida, solo una acción.

**Una interface puede tener dos listas de acceso, una lista asociada a la entrada y otra lista asociada a la acción de salida.**

**Aplicar la lista de acceso a la interface**