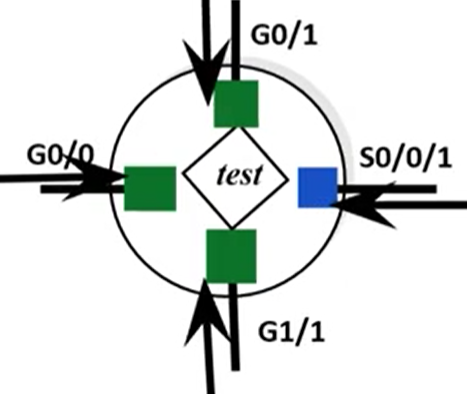
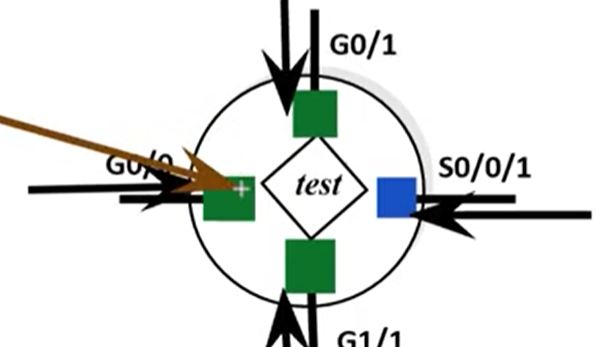
**Listas de control de acceso**

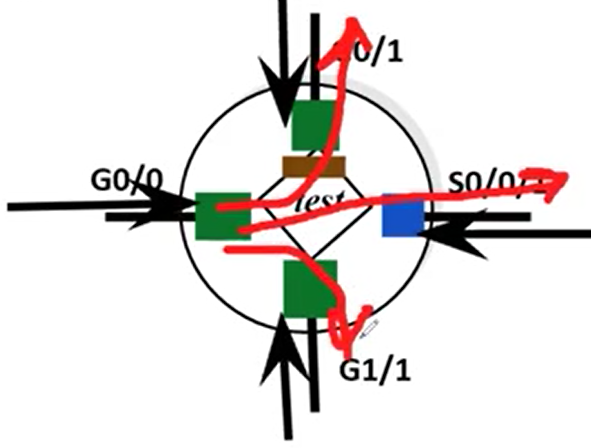
Las listas de control de acceso nos permiten llevar a cabo el **control del tráfico** sobre paquetes que circulan en la red utilizando **direccionamiento origen o fuente y direccionamiento destino.**

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.

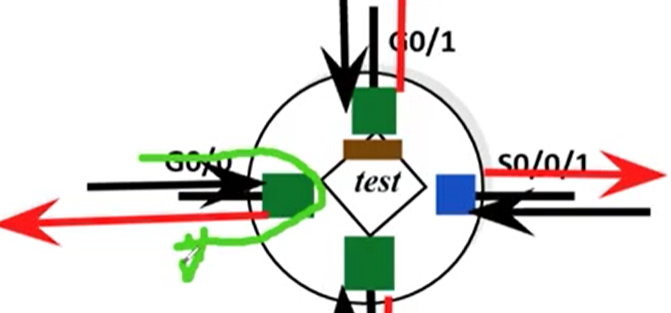


Para un paquete que llega por la interface g0/0. El router toma la decisión de qué hacer con ese paquete que acaba de llegar. En ese momento el paquete es analizado y tiene la posibilidad de salir por la interface g0/1, por la g1/1 o por la s0/0/1. Todas las interfaces pueden sacar tráfico para alcanzar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