**Listas de acceso extendida**

**Breve repaso de listas de control de acceso.**

**Hoy vamos a trabajar con listas de control de acceso extendidas y las aplicaremos para poder limitar el tráfico de un protocolo en particular como web, ftp, icmp (para bloquear la posibilidad de recibir pings).**

**Recordemos que el protocolo TCP/IP está compuesto por dos capas:**

**La capa de red o 3 donde se da la comunicación de paquetes y se utiliza el protocolo IP. El protocolo IP requiere de dos elementos para poder comunicarse: IP ORIGEN E IP DESTINO**

**La capa de red da servicio a la capa de transporte, que se subdivide en dos protocolos, uno de ellos orientado a conexión y otro de ellos orientado a no conexión. El intercambio de información se da utilizando segmentos. Tenemos segmentos TCP orientados a conexión y segmentos UDP orientados a no conexión. Ambos requieren de un mecanismo para poder identificar con quién se están comunicando. En la capa 4 lo que se utiliza son los puertos.**

**Tenemos 2 a la 16 puertos**

**0 – 1023 puertos completamente estandarizados o fijos para algún tipo de aplicaciones.**

**80 Protocolo web**

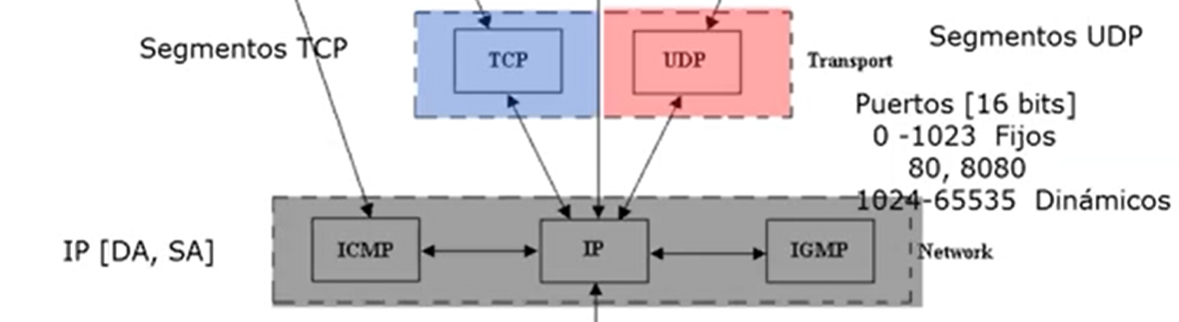
**22 SSH**

**23 Telnet**

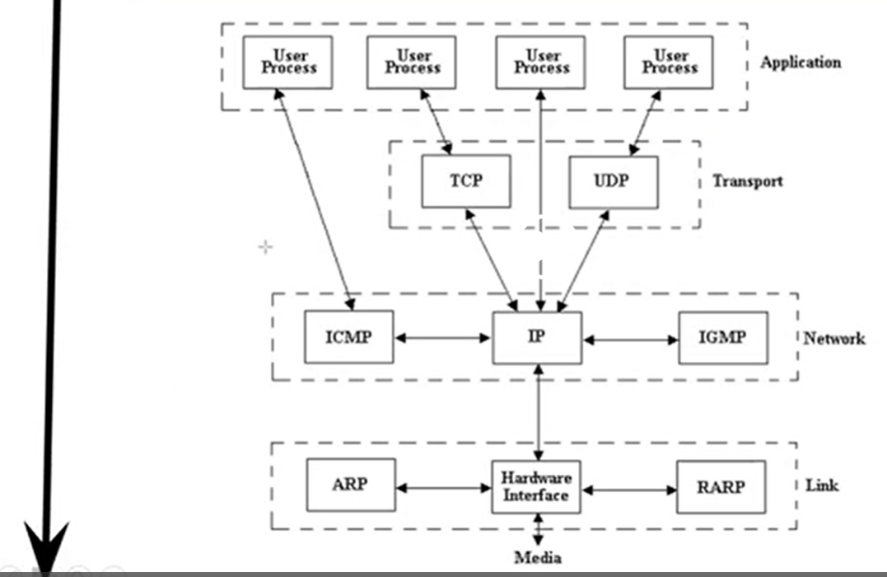
**1024 – 65535 son puertos dinámicos.**

**Nuestra computadora cada que desea comunicarse con una aplicación (FTP, WEB, ETC) genera localmente un puerto dinámico que se genera de manera aleatoria arriba de 1024.**

**La capa de transporte.**

****

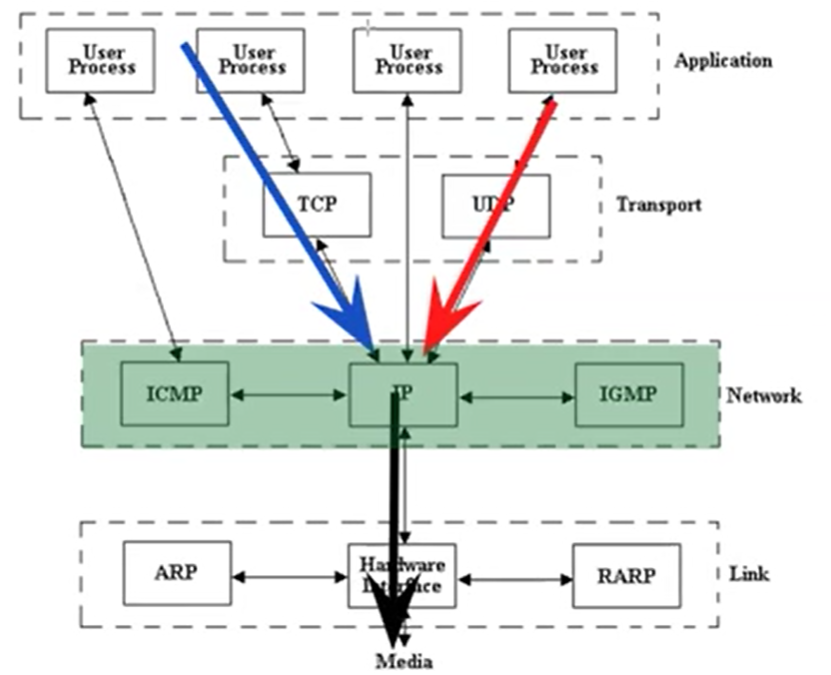
El flujo de información va de las capas superiores a las capas inferiores, hasta la capa física que inyecta los bits en el medio



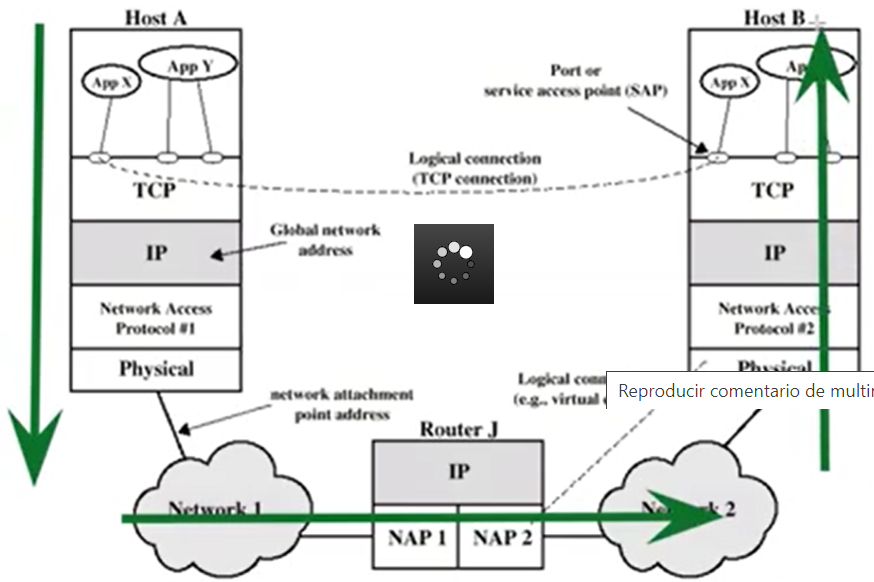
Toda la comunicación que fluye de los servicios orientados a conexión y no conexión se comunica con la capa 3 donde el protocolo IP va a entrar en acción. La capa 3 es la que se encarga de pasar la información a la capa física. Sin la capa 3 no se podría dar la comunicación de las capas superiores 4, 5, 6 y 7 con las capas inferiores. La capa 3 es la que soporta el intercambio de información de un extremo a otro.

**Cuando utilizamos listas de control acceso estándar estamos trabajando con la capa # 3**

**Cuando utilizamos listas de control acceso extendidas estamos trabajando con la capa # 3 o en la capa #4.**



El flujo de la información va en ese sentido de capa superior a inferior, pasa a través de la red y finalmente llega a su destino.



Las listas de acceso extendidas hacen un filtrado más granular o detallado y podemos bloquear protocolos como http, ftp etc.

Vamos a filtrar fuente y destino utilizando las máscaras comodín.

Estaremos utilizando dos máscaras de CISCO

Any permite o niega todo tipo de tráfico.

Host permite filtrar para una única dirección ip.

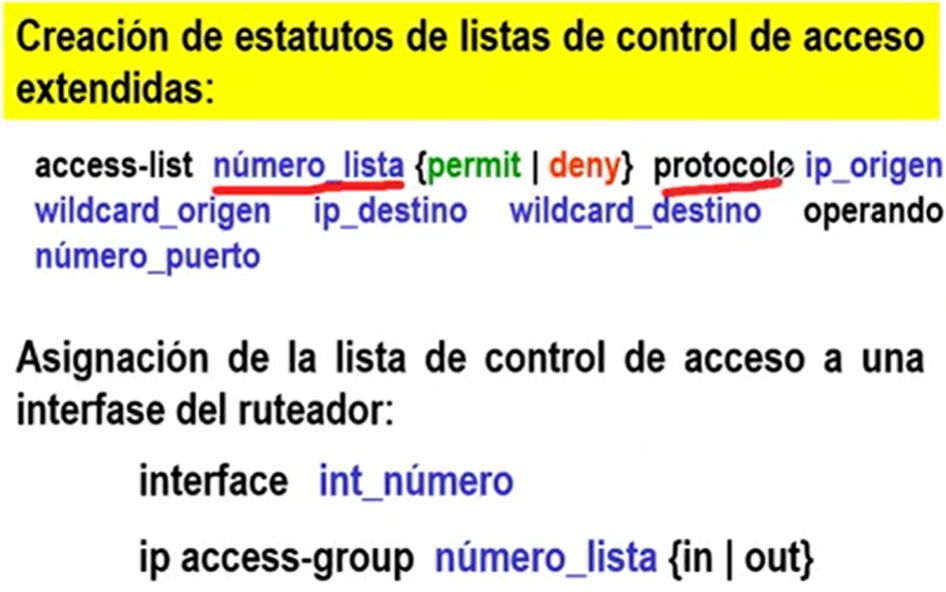
En las listas de acceso extendidas.

El número de lista va entre 100 y 199

La acción de permitir o negar se le va a aplicar exactamente a un protocolo en la capa 4.

Las ips origen y destino

Operando que es opcional como los primeros dos caracteres de la palabra en ingles equal (eq) o más grande que.



La lista de acceso tiene efectp hasta que se asigne a un interface.