

TC 2022

Interconexión de redes

## Listas de control de acceso

Tecnológico de Monterrey, Campus Querétaro

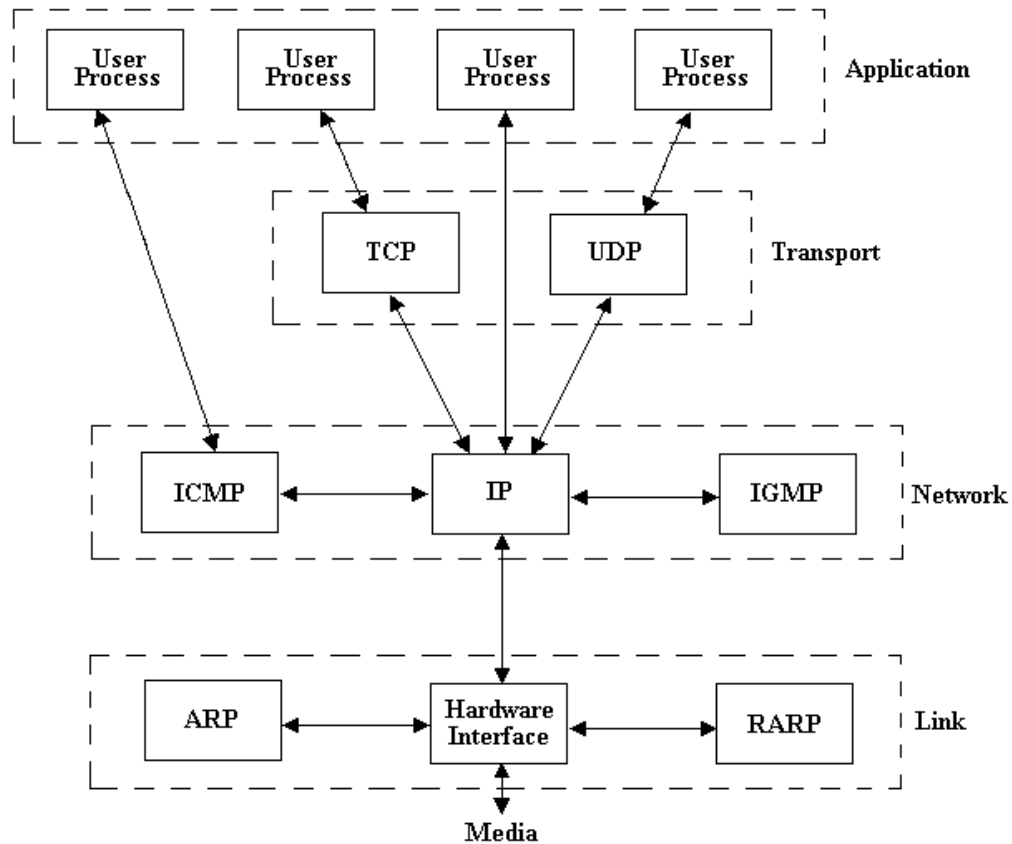


# Objetivos de esta sesión

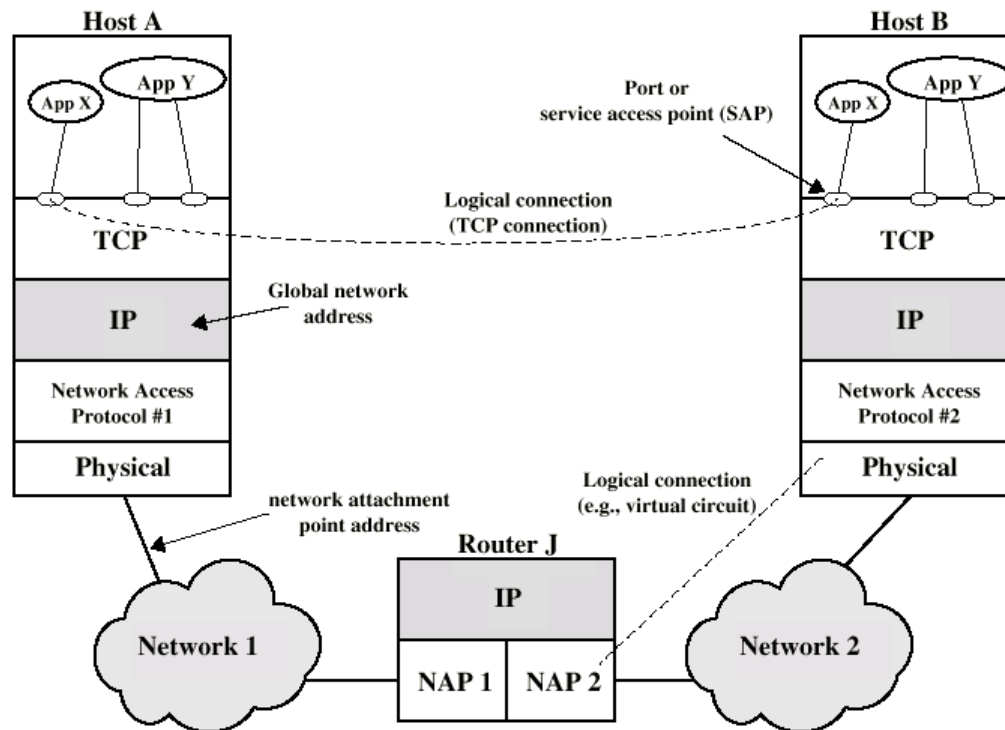


**Estudiar** el conjunto de protocolos **TCP/IP** y  
**diseñar** listas de control de acceso (**ACL's**) en los  
ruteadores **CISCO**.

# Protocollo TCP/IP



# Protocollo TCP/IP



# Servicios del protocolo TCP/IP

## Servicios orientados a conexión:

En este tipo de servicios existe un circuito lógico entre el emisor y el receptor que proporciona gran calidad en la entrega de datos, confiable y libre de errores.

## Servicios orientados a no conexión:

En este tipo de servicios los paquetes (capa 3) insertados siguen distintas rutas, no es confiable.

# Puertos del protocolo TCP/IP

Los programas de aplicación que utilizan los servicios del protocolo **TCP/IP** necesitan de una identificación lógica para poder comunicarse entre si.

<b>20, 21</b>	<b>FTP</b>
<b>22</b>	<b>SSH</b>
<b>23</b>	<b>Telnet</b>
<b>53</b>	<b>DNS</b>
<b>69</b>	<b>TFTP</b>
<b>80</b>	<b>HTTP</b>
<b>161</b>	<b>SNMP</b>
<b>443</b>	<b>HTTPS</b>

# Listas de control de acceso

Una lista de acceso es un conjunto de acciones le indican al router la acción que debe tomar para cada paquete que entra al router : **permitir** o **negar** el flujo del tráfico.

La acción que el router toma sobre cada paquete puede estar basada en la **dirección IP del origen, la dirección IP del destino, el protocolo o el puerto utilizado.**

Las listas de control de acceso permiten establecer un nivel de seguridad básico dentro del router.

# Listas de control de acceso

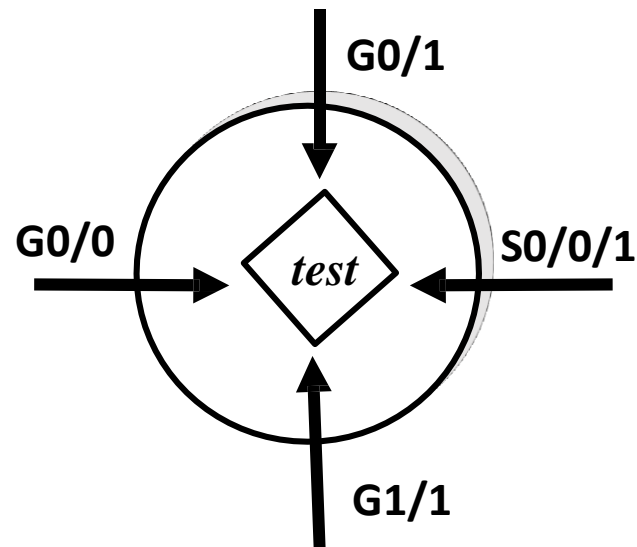
**Las Listas de Control de Acceso se utilizan para:**

- Limitar el tráfico de la red e incrementar su desempeño.
- Suministrar mecanismos de control de flujo.
- Establecer controles básicos de seguridad.
- Bloquear algún tipo de tráfico.



# ¿Cómo trabajan las Listas de control de acceso?

Cuando un router cuenta con listas de control de acceso todo el tráfico que pasa por el router es analizado antes de continuar su camino.



# Listas de control de acceso

Ver con atención el siguiente video (14 minutos):

<https://www.youtube.com/watch?v=4PPUvRj2PvM>



# Listas de control de acceso

Para el protocolo TCP/IP existen dos tipos :

## Lista estándar:

- Bloquea o permite el tráfico con base en la **dirección fuente**.
- Bloquea o permite todo un protocolo de comunicaciones.
- Se identifican por un número entero en el intervalo [1..99]

## Lista extendida:

- Bloquea o permite el tráfico con base a la **dirección fuente, dirección destino, tipo de protocolo** y un **puerto** en particular.
- Bloquea o permite un subconjunto de un protocolo de comunicaciones.
- Se identifican por un número entero en el intervalo [100..199]

# Wildcard de IP para listas de acceso

**0** : Verifica el valor del bit correspondiente.

**1** : Ignora el significado del bit.

**any** : Es una **wildcard** cuyo significado toma efecto para cualquier IP.

<b>0.0.0.0</b>	<b>255.255.255.255</b>
<b>dirección</b>	<b>wildcard mask</b>

El **1** en el wildcard mask ignora el significado del bit, por lo tanto esta máscara comodín permite cualquier IP.

**host** : Es una **wildcard** cuyo significado toma efecto sobre una única IP.

<b>A.B.C.D</b>	<b>0.0.0.0</b>
<b>dirección</b>	<b>wildcard mask</b>

El **0** en el wildcard mask verifica el significado del bit, por lo tanto, esta máscara comodín, hace un match exacto con la dirección IP.

# Comandos para crear listas de control de acceso estándar

Creación de estatutos de listas de control de acceso estándar:

```
access-list número_lista {permit | deny} IP_Origen wildcard
```

Asignación de la lista de control de acceso a una interfaz del ruteador:

```
interface int_número
```

```
ip access-group número_lista {in | out}
```

# Comandos para crear listas de control de acceso extendidas

**Creación de estatutos de listas de control de acceso extendidas:**

```
access-list número_lista {permit | deny} protocolo ip_origen  
wildcard_origen ip_destino wildcard_destino operando  
número_puerto
```

**Asignación de la lista de control de acceso a una interfaz del ruteador:**

```
interface int_número  
  
ip access-group número_lista {in | out}
```