*2 de Octubre de 2024*

Redes de Teleinformática II - Práctico 6

*Nombre:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

**Tema:**

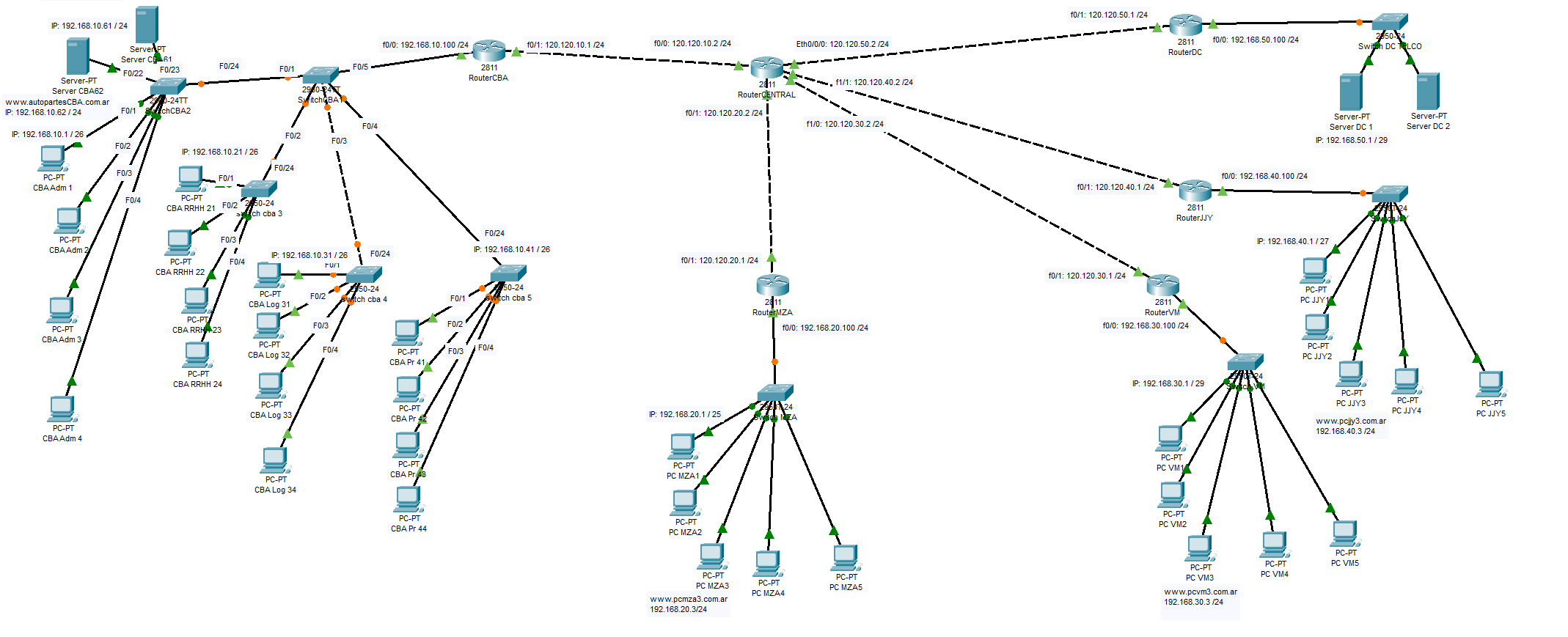
* ACL
* Permitir y denegar tráfico entre dos hosts
* Permitir y denegar tráfico entre dos redes

**Objetivo de la clase:**

* Crear Access Lists para permitir o denegar el tráfico entre hosts y redes. Usaremos el packet tracer para tal fin

**Actividad:**

**Diagrama de red:**

****

**Lista de accesos ACL**

**Funcionamiento de las ACL**

Para explicar el funcionamiento utilizaremos el software Cisco IOS.

El orden de las sentencias ACL es importante .

* Cuando el router está decidiendo si se envía o bloquea un paquete, el IOS prueba el paquete, verifica si cumple o no cada sentencia de condición, en el orden en que se crearon las sentencias.
* Una vez que se verifica que existe una coincidencia, no se siguen verificando otras sentencias de condición.

Por lo tanto, Cisco IOS verifica si los paquetes cumplen cada sentencia de condición de arriba hacia abajo, en orden. Cuando se encuentra una coincidencia, se ejecuta la acción de aceptar o rechazar y ya no se continúa comprobando otras ACL.

Por ejemplo, si una ACL permite todo el tráfico y está ubicada en la parte superior de la lista, ya no se verifica ninguna sentencia que esté por debajo.

Si no hay coincidencia con ninguna de las ACL existentes en el extremo de la lista se coloca por defecto una sentencia implícita deny any (denegar cualquiera). Y, aunque la línea deny any no sea visible sí que está ahí y no permitirá que ningún paquete que no coincida con alguna de las ACL anteriores sea aceptado. Se puede añadir de forma explícita para 'verla' escrita y tener esa tranquilidad.

Veamos el proceso completo:

1. Cuando entra una trama a través de una interfaz, el router verifica si la dirección de capa 2 (MAC) concuerda o si es una trama de broadcast.
2. Si se acepta la dirección de la trama, la información de la trama se elimina y el router busca una ACL en la interfaz entrante.
3. Si existe una ACL se comprueba si el paquete cumple las condiciones de la lista.
4. Si el paquete cumple las condiciones, se ejecuta la acción de aceptar o rechazar el paquete.
5. Si se acepta el paquete en la interfaz, se compara con las entradas de la tabla de enrutamiento para determinar la interfaz destino y conmutarlo a aquella interfaz. Luego el router verifica si la interfaz destino tiene una ACL.
6. Si existe una ACL, se compara el paquete con las sentencias de la lista y si el paquete concuerda con una sentencia, se acepta o rechaza el paquete según se indique.
7. Si no hay ACL o se acepta el paquete, el paquete se encapsula en el nuevo protocolo de capa 2 y se envía por la interfaz hacia el dispositivo siguiente.

* **wild-mask**: indica con 0 el bit a evaluar y con 1 indica que el bit correspondiente se ignora. Por ejemplo, si queremos indicar un único host 192.168.1.1 especifico: 192.168.1.1 con wild-mask 0.0.0.0 y si queremos especificar toda la red clase C correspondiente lo hacemos con 192.168.1.0 y wild-mask 0.0.0.255.

En los routers podemos permitir o denegar el acceso a determinadas IP address, determinadas redes, determinados protocolos con el fin de dar un nivel de seguridad a la red.

¿qué significa poner un wild-card **0.0.0.255** ?

Significa que la dirección de origen va a compararse cada bit que le indique el wild-card, es decir 0 le indicará que compare los 8 primeros bits de la dirección, luego el 0 siguiente le indica que compare los segundos ocho bits de la dirección y el tercer 0 le indica que compare los terceros 8 bits de la dirección y 255 le indica que NO compare los últimos 8 bits de la dirección.

**Actividad práctica:**

Realice los siguientes ejercicios en su red:

* **Permisos de Host a Host**

Vamos a corroborar que todos los hosts se comuniquen entre si mediante el comando Ping.

ACL Host to Host:

* El Host cuya IP address es la 192.168.20.1 no debe ver el host cuya IP es la 192.168.10.1
* El host cuya IP address es la 192.168.30.1 no debe ver el host cuya IP es la 192.168.10.1
* El host cuya IP address es la 192.168.20.4 no debe ver el host cuya IP es la 192.168.30.2
* El host cuya IP address es la 192.168.30.3 no debe ver el Host cuya IP es la 192.168.20.1

¿Cómo configuramos estos permisos y denegaciones?

1. Elegimos el router en que vamos a crear el Access List ACL.
2. Definimos todos los posibles caminos que puede hacer el paquete que enviaría el host de origen al destino para definir si el ACL va a estar asignado a la entrada o salida de la interfaz a la que asignaremos esa lista de acceso.
3. Ingresamos al router y realizamos dos pasos para poner a funcionar el ACL:

**Primer paso:**

Cargar la lista de acceso con los siguientes comandos:

**Router(config)#** [access-list numACL] [permit|deny] [protocolo] [origen del paquete] [mascara-fuente] [destino del paquete] [mascara-destino]

**Access-list:** es el comando para iniciar el ACL

**numACL:** es el número de ACL

**Permit/Deny:** es la orden que se cumplirá si al realizar la comparación entre el paquete que ingresa al router y las dos condiciones que le definí se cumplen

**Protocolo:** es el protocolo que se va a considerar para la comparación

**Origen del paquete:** es la IP address de origen que se va a comparar con la IP address de origen del paquete que ingreso

**Máscara-fuente:** es la máscara que define con 0 (cero) hasta donde se va a comparar con el IP address de origen del paquete que ingresó

**Destino del paquete:** es la IP address de destino que se va a comparar con la Ip address de destino del paquete que ingresó

**Máscara destino:** Es la máscara que define con 0 (cero) hasta donde se va a comparar con el IP address de destino del paquete que ingresó.

Ejemplo:

ROUTER MZA(config)#access-list 100 deny ip 192.168.20.1 0.0.0.0 192.168.10.1 0.0.0.0

ROUTER MZA(config)#access-list 100 permit ip any any

ROUTER MZA(config)#exit

ROUTER MZA#wr

**Segundo paso:**

Ingresar a la interfaz elegida, asociar la lista de acceso que creamos a la interfaz y definir el sentido de tráfico es decir si IN ingresa o si OUT sale de la interfaz.

*ROUTER MZA(config)#interface fastEthernet 0/0*

Una vez que ingresé a la interfaz debo agregar el comando:

*ROUTER MZA(config-if)#ip access-group 100 in*

**Ip access-group**: es el commando que le dice a la interfáz que aplique el access list que previamente escribí

**100**: es el número de ACL

**IN/OUT**: con este commando le estoy diciendo al router que solo aplique el access list 100 a los paquetes que ingresan/egresan a/de la interfáz.

Una vez aplicado los comandos:

1. Comprobamos si la restricción se realiza exitosamente.
2. Comprobemos que la PC pueda ver las otras computadoras de la red.

* **Permisos de Host a Red**

Ahora vamos a denegar el acceso de un determinado host a una determinada red:

Veamos algunos ejemplos:

* Host: **192.168.10.2** denegado a la red **192.168.30.0**

Ingrese al modo de configuración:

Config t

*access-list 101 deny ip host 192.168.10.2 192.168.30.0 0.0.0.255*

*access-list 101 permit ip any any*

Ingrese a la interfáz sobre la que se va a aplicar el ACL:

*interface FastEthernet x/x*

*ip access-group 101 in*

* Host: **192.168.10.4** denegado a la red **192.168.20.0**

*access-list 102 deny ip host 192.168.10.4 192.168.20.0 0.0.0.255*

*access-list 102 permit ip any any*

*interface FastEthernet x/x* (aqui debe definer el número de la interfáz sobre la que va a aplicar el ACL)

*ip access-group 101 in*

Ahora vamos a permitir el acceso de un determinado host a una determinada red:

* Permitir que solo el el Host **192.168.10.4** pueda acceder a la red **192.168.30.0**

*access-list 102 permit ip host 192.168.10.4 192.168.30.0 0.0.0.255*

*access-list 102 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255*

*access-list 102 permit ip any any*

*interface FastEthernet X/X*

*ip access-group 102 in*

* Permitir que solo el host **192.168.30.3** pueda acceder a la red **192.168.20.0**

access-list 103 permit ip host 192.168.30.3 192.168.20.0 0.0.0.255

access-list 103 deny ip any any

*interface FastEthernet X/X* (es la interfaz sobre la que voy a aplicar el ACL)

*ip access-group 103 in*

**Síntesis de pasos para configurar los ACL:**

1. Definimos el camino que realizará el paquete para ir de ese origen a esa red de destino
2. Definimos el router
3. Definimos la interfaz que tendrá asociada el ACL y si se aplicará para el tráfico de entrada o salida

1 . Creamos una nueva lista de acceso

*Router#*

*Router#config t*

*Router(config)#*

*Router(config)# access-list 102 permit/deny ip (IP del Host) 0.0.0.0 (IP de la RED) 0.0.0.255*

*Router(config)# access-list 102 permit/deny IP ANY ANY*

*Router#*

2. Ingresamos a la interfaz elegida

*Router(config)#interface fastethernet x/x*

*Router(config-if)#*

3.Asociamos la lista de acceso que creamos para que lo aplique al tráfico que sale de ella o entra a ella:

*Router(config-if)#IP Access-group 102 in/out*

Comprobamos si las restricciones y los permisos se realizan exitosamente.

* **Permisos de red a red**
* Vamos a denegar el acceso de la red JJY a la red VM.

*Router(config)#access-list 103 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255*

*Router(config)#access-list 103 permit ip any any*

*Router(config)#exit*

*Router#wr*

Luego asignamos a la interfaz que elegimos esta ACL

*Router(config)#interface fx/x*

*Router(config-if)#*

*Router(config-if)# IP Access-group 103 in/out*

*Router(config)#exit*

*Router#wr*

**ACLs extendidas**

Las ACL extendidas filtran paquetes IP según:

* Direcciones IP de origen y destino
* Puertos TCP y UDP de origen y destino
* Tipo de protocolo (IP, ICMP, UDP, TCP o número de puerto de protocolo).

Las ACLs extendidas usan un número dentro del intervalo del 100 al 199.

Al final de la sentencia de la ACL extendida se puede especificar, opcionalmente, el número de puerto de protocolo **TCP o UDP** para el que se aplica la sentencia:

20 y 21: datos y programa FTP

23: Telnet

25: SMTP

53: DNS

69: TFTP

80: HTTP

**Definir ACL extendida, sintaxis:**

**Router(config)#** [access-list numACL] [permit|deny] [protocolo] [fuente] [mascara-fuente] [destino] [mascara-destino] [operador] [**operando**]

]

**protocolo**: IP, TCP, UDP, ICMP, GRE, IGRP

**fuente | destino:** Identificadores de direcciones origen y destino

**mascara-fuente | mascara-destino:** Máscaras de wildcard

**operador:** lt, gt, eq, neq ( menor, mayor, igual, no igual)

**operando:** número de puerto

**Respecto a los protocolos:**

* Sólo se puede especificar una ACL por protocolo y por interfaz.
* Si ACL es entrante, se comprueba al recibir el paquete.
* Si ACL es saliente, se comprueba después de recibir y enrutar el paquete a la interfaz saliente.
* **Permisos para permitir o denegar ciertos puertos en TCP**

Vamos a denegar el acceso a ciertos puertos TCP que provienen de una determinada IP y que van a una determinada IP.

El ejemplo será:

La 192.168.20.1 no puede ingresar al server 192.168.10.9 usando la aplicación Telnet (port 23)

*Router(config)#access-list 104 deny tcp 192.168.20.1 0.0.0.0 192.168.10.9 0.0.0.0 eq 23*

*Router(config)#access-list 104 permit ip any any*

*Router(config)#interface f0/0*

*Router(config-if)#ip access-group 104 out*

*Router(config-if)#exit*