

Redes de Teleinformática II - Práctico 6

Nombre: Santiago Vietto

Tema:

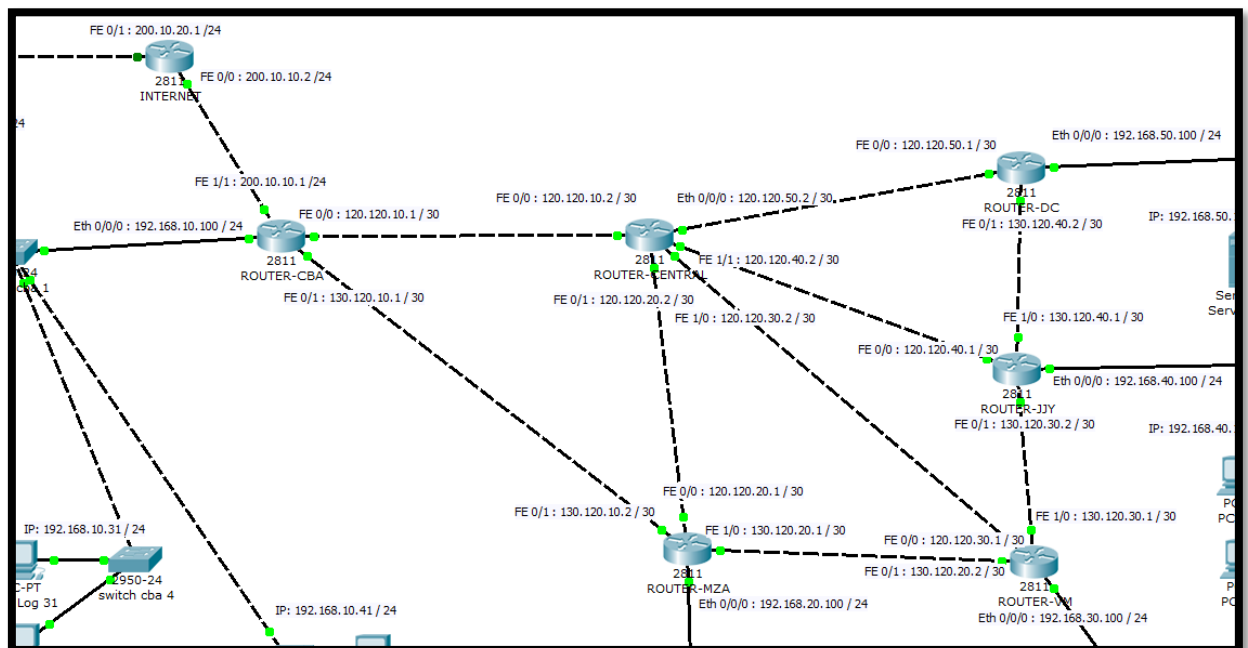
- ACL
- Permitir y denegar tráfico entre dos hosts
- Permitir y denegar tráfico entre dos redes

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:



1)_ Como primera medida, tenemos que agregar un camino adicional entre los routers, el mismo empieza desde CBA, MZA, VM, DC hasta JJY. Para ello debe anunciar las redes adicionales al OSPF mediante los comandos:

Ej:

```
ROUTER-CBA(config)#router ospf XXX
ROUTER-CBA(config-router)#network 220.120.10.1 0.0.0.3 area XXX
ROUTER-CBA(config-router)#exit
ROUTER-CBA(config)#exit
ROUTER-CBA#wr
```

_ Vamos a crear una nueva red entre Cordoba y Mendoza, luego entre Mendoza y Villa Mercedes y así sucesivamente. Como primera medida lo que hacemos es habilitar las interfaces de los routers que se ven en la red que creamos. A esto lo podemos hacer antes o después de colocar las IPs. A continuación habilitamos la interfaz de Cordoba, y lo mismo hacemos con la de Mendoza, y así sucesivamente con las que se conectan una con la otra.

```
ROUTER-CBA>ena
Password:
ROUTER-CBA#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-CBA(config)#interface fastEthernet 1/0
ROUTER-CBA(config-if)#no shutdown

ROUTER-CBA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up
exit
ROUTER-CBA(config)#exit
ROUTER-CBA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-CBA#
```

_ Luego lo que hacemos es en la nueva interfaz del router de Cordoba que usamos añadimos una nueva IP, y lo mismo para la interfaz que se conecta del router de Mendoza. A continuación configuramos la IP del router de Cordoba:

```
ROUTER-CBA>ena
Password:
ROUTER-CBA#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-CBA(config)#interface fastEthernet 1/0
ROUTER-CBA(config-if)#ip address 220.120.10.1 255.255.255.252
^
% Invalid input detected at '^' marker.

ROUTER-CBA(config-if)#ip address 220.120.10.1 255.255.255.252
ROUTER-CBA(config-if)#exit
ROUTER-CBA(config)#exit
ROUTER-CBA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-CBA#
```

_ De igual forma configuramos la IP del router de Mendoza:

```
ROUTER-MZA>ena
ROUTER-MZA#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-MZA(config)#interface fastEthernet 0/1
ROUTER-MZA(config-if)#ip address 220.120.120.10.2 255.255.255.252
^
% Invalid input detected at '^' marker.

ROUTER-MZA(config-if)#ip address 220.120.10.2 255.255.255.252
ROUTER-MZA(config-if)#exit
ROUTER-MZA(config)#exit
ROUTER-MZA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-MZA#
```

_ Ahora procedemos a crear las rutas dinamicas OSPF entre ambos. A continuacion observamos la configuracion para el router de Cordoba:

```
ROUTER-CBA>ena
Password:
ROUTER-CBA#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-CBA(config)#router ospf 1
ROUTER-CBA(config-router)#network 220.120.10.0 0.0.0.3 area 0
ROUTER-CBA(config-router)#exit
ROUTER-CBA(config)#exit
ROUTER-CBA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-CBA#
```

_ En el caso de Mendoza, una de sus networks va a ser también 220.120.10.0 ya que comparte con Cordoba, y de Mendoza a Villa Mercedes van a compartir la 220.120.20.0, y así sucesivamente. Realizamos esta misma configuración para los demás routers con sus determinadas redes.

Nota: en cada Router agregar la red que corresponde para que el OSPF tenga todas las redes declaradas.

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 específico, 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.

Wild-card 0.0.0.255: si ponemos este, 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.

Permisos de Host a Host:

1)_ Vamos a corroborar que todos los hosts se comuniquen entre si mediante el comando Ping. ACL Host to Host, tenemos que configurar los siguientes:

A)_ El Host cuya IP address es la 192.168.20.1 no debe ver el host cuya IP es la 192.168.10.1. Es decir, los paquetes que se envíen desde la IP 192.168.20.1 no pueden llegar o no pueden ser recibidos por 192.168.10.1, ya que justamente no esta viendo esa IP.

B)_ El host cuya IP address es la 192.168.30.1 no debe ver el host cuya IP es la 192.168.10.1

C)_ El host cuya IP address es la 192.168.20.4 no debe ver el host cuya IP es la 192.168.30.2

D)_ El host cuya IP address es la 192.168.30.3 no debe ver el Host cuya IP es la 192.168.20.1

_ Elegimos el router en que vamos a crear el Access List ACL. 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. Ingresamos al router y realizamos dos pasos para poner a funcionar el ACL:

Primer paso: vamos a cargar la lista de acceso con los siguientes comandos:

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

```
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
```

_ El numero 100 puede repetirse en distintos routers, ya que la configuración es distinta, pero no se puede repetir en un mismo router, como por ejemplo en el de Mendoza en el que tenemos dos configuraciones, por lo tanto, una puede ser 100 y la otra 101, y asi sucesivamente.

Segundo paso: de allí vamos a ingresar a la interfaz elegida, luego vamos a asociar la lista de acceso que creamos a esta interfaz y le vamos a decir que la aplique al tráfico que sale de ella o entre a ella

```
ROUTER MZA(config)#interface fastEthernet 0/0
ROUTER MZA(config-if)#ip access-group 100 in
ROUTER MZA(config-if)#exit
```

- In: desde la red o host de origen a la interfaz de la red de origen.
- Out: desde la interfaz de la red de destino a la red o host de destino.

A)_ Teniendo en cuenta los pasos anteriores, luego de ver los distintos caminos, elegimos el sentido de la ruta, que en este caso es del router de Mendoza al de Cordoba. Y se eligió como router el router de Mendoza y la interfaz es la que sale a la red, que en este caso es 192.168.20.100. Pudimos haber elegido el router de Cordoba en donde la interfaz a configurar en ese caso seria 192.168.10.100. Entonces, nos posicionamos en el router de Mendoza y hacemos la siguiente configuración:



```
ROUTER-MZA>
ROUTER-MZA>ena
ROUTER-MZA#config t
Enter configuration commands, one per line. End with CNTL/Z.
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 permit ip any any
^
% Invalid input detected at '^' marker.

ROUTER-MZA(config)#access-list 100 permit ip any any
ROUTER-MZA(config)#exit
ROUTER-MZA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-MZA#
```

_ Una vez que negamos el tráfico, procedemos a asignar la interfaz. En este caso al haber elegido la que entra desde el router de Mendoza, la asignamos In, y si hubiésemos elegido la de Cordoba que apunta a su red, tendríamos que colocar out. A continuación, vemos la configuración:

```
ROUTER-MZA>ena
ROUTER-MZA#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-MZA(config)#interface Ethernet 0/0/0
ROUTER-MZA(config-if)#ip access-group 100 in
ROUTER-MZA(config-if)#exit
ROUTER-MZA(config)#exit
ROUTER-MZA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-MZA#
```

_ Para probar que la configuración fue correcta, hacemos un ping desde la PC de Mendoza a la de Cordoba y vemos que la conexión es fallida:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC MZA 1	CBAAdm 1	ICMP		0.000	N	0	(edit)	



```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.20.100: Destination host unreachable.
Reply from 192.168.20.100: Destination host unreachable.
Reply from 192.168.20.100: Destination host unreachable.
Reply from 192.168.20.100: Destination host unreachable.

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

_ Posteriormente hacemos ping desde la PC de Mendoza hacia otras PC de la red y vemos que la conexión es exitosa:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC MZA 1	CBAAdm 2	ICMP		0.000	N	0	(edit)	

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=126
Reply from 192.168.10.2: bytes=32 time=2ms TTL=126
Reply from 192.168.10.2: bytes=32 time=26ms TTL=126
Reply from 192.168.10.2: bytes=32 time=4ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 26ms, Average = 8ms
```

_ Para los incisos B, C y D, hacemos exactamente el mismo procedimiento. En donde si hacemos sh run, podremos ver las configuraciones en cada router, como por ejemplo vemos las denegaciones que asignamos en el router de Mendoza, pero la interfaz solo va a tener establecida una sola de ellas, en este caso o la 100 o la 101:

```
access-list 100 deny ip host 192.168.20.1 host 192.168.10.1
access-list 100 permit ip any any
access-list 101 deny ip host 192.168.20.4 host 192.168.30.2
access-list 101 permit ip any any
!
```

Permisos de Host a Red: ahora vamos a denegar el acceso de un determinado host a una determinada red:

A)_ Host: **192.168.10.2** denegado a la red **192.168.30.0**. En este caso la IP siguiente no se puede comunicar con ninguna PC de la red de Villa Mercedes.

```
access-list 100 deny ip 192.168.10.2 0.0.0.0 192.168.30.0 0.0.0.255
access-list 100 permit ip any any
```

```
interface FastEthernet x/x
ip access-group 100 in
```

B)_ Host: **192.168.10.4** denegado a la red **192.168.20.0**

```
access-list 101 deny ip 192.168.10.4 0.0.0.0 192.168.20.0 0.0.0.255
access-list 101 permit ip any any
```

```
interface FastEthernet x/x
ip access-group 101 in
```

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

C)_ Permitir que solo el Host **192.168.10.4** pueda acceder a la red **192.168.30.0**. En este caso únicamente la PC 4 de Cordoba se puede comunicar con la red de Villa Mercedes (con cualquier PC), pero cualquier otra PC de Cordoba no puede.

```
access-list 102 permit ip 192.168.10.4 0.0.0.0 192.168.30.0 0.0.0.255
access-list 102 deny ip any any
```

```
interface FastEthernet X/X
ip access-group 102 in
```

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

```
access-list 102 permit ip 192.168.30.3 0.0.0.0 192.168.20.0 0.0.0.255
access-list 102 deny ip any any
```

```
interface FastEthernet X/X (es la interfaz sobre la que voy a aplicar el ACL)
ip access-group 103 in
```

_ Vamos a comenzar por negar las PC a las redes:







A)_ Luego de ver todos los caminos, y elegir el sentido de la red, procedemos a realizar la siguiente configuración, tomando como router el de Cordoba:

```
ROUTER-CBA>ena
Password:
ROUTER-CBA#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-CBA(config)#access-list 100 deny ip 192.168.10.2 0.0.0.0 192.168.30.0 0.0.0.255
ROUTER-CBA(config)#access-list 100 permit ip any any
ROUTER-CBA(config)#exit
ROUTER-CBA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-CBA#
```

_ Una vez que negamos el tráfico, procedemos a asignar la interfaz. En este caso al haber elegido la que entra desde el router de Cordoba, la asignamos In, y si hubiésemos elegido el de Villa Mercedes que apunta a su red, tendríamos que colocar out. A continuación, vemos la configuración:

```
ROUTER-CBA>ena
Password:
ROUTER-CBA#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-CBA(config)#interface Ethernet 0/0/0
ROUTER-CBA(config-if)#ip access-group 100 in
ROUTER-CBA(config-if)#exit
ROUTER-CBA(config)#exit
ROUTER-CBA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-CBA#
```


_ Para probar que la configuración fue correcta, hacemos un ping desde la PC de Cordoba a cualquiera de Villa Mercedes, y vemos que la conexión es fallida:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	CBAAdm 2	PC VM 1	ICMP		0.000	N	0	(edit)	
	Failed	CBAAdm 2	PC VM 2	ICMP		0.000	N	1	(edit)	
	Failed	CBAAdm 2	PC VM 3	ICMP		0.000	N	2	(edit)	

```
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),



C:\>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

_ Si hacemos ping desde otra PC de Cordoba a la red de Villa Mercedes, verificamos que la conexión es exitosa:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	CBAAdm 1	PC VM 1	ICMP		0.000	N	0	(edit)	

```
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<lms TTL=125
Reply from 192.168.30.1: bytes=32 time<lms TTL=125
Reply from 192.168.30.1: bytes=32 time<lms TTL=125
Reply from 192.168.30.1: bytes=32 time<lms TTL=125

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

_ Para el inciso B, realizamos exactamente los mismos pasos de configuración. Y ahora procedemos a permitir el acceso de ciertas PC a toda una red, negándole el acceso a todas las otras PC.







C)_ Luego de ver todos los caminos, y elegir el sentido de la red, procedemos a realizar la siguiente configuración, tomando como router el de Cordoba:

```
ROUTER-CBA>ena
Password:
ROUTER-CBA#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-CBA(config)#access-list 102 permit ip 192.168.10.4 0.0.0.0 192.168.30.0 0.0.0.255
ROUTER-CBA(config)#access-list 102 deny ip any any
ROUTER-CBA(config)#exit
ROUTER-CBA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-CBA#
```

_ Una vez que permitimos el tráfico, procedemos a asignar la interfaz. En este caso al haber elegido la que entra desde el router de Cordoba, la asignamos In, y si hubiésemos elegido el de Villa Mercedes que apunta a su red, tendríamos que colocar out. A continuación, vemos la configuración:

```
ROUTER-CBA#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-CBA(config)#interface Ethernet 0/0/0
ROUTER-CBA(config-if)#ip access-group 102 in
ROUTER-CBA(config-if)#exit
ROUTER-CBA(config)#exit
ROUTER-CBA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-CBA#
```

_ Para probar que la configuración fue correcta, hacemos un ping desde la PC de Cordoba a cualquiera de Villa Mercedes, y vemos que la conexión es exitosa:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	CBAAdm 4	PC VM 1	ICMP		0.000	N	0	(edit)	
	Successful	CBAAdm 4	PC VM 2	ICMP		0.000	N	1	(edit)	
	Successful	CBAAdm 4	PC VM 3	ICMP		0.000	N	2	(edit)	





```
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=125
Reply from 192.168.30.1: bytes=32 time=2ms TTL=125
Reply from 192.168.30.1: bytes=32 time=2ms TTL=125
Reply from 192.168.30.1: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

_ Si hacemos ping desde cualquier otra PC de Cordoba a la red de Villa Mercedes, verificamos que la conexión es fallida:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	CBAAdm 1	PC VM 1	ICMP		0.000	N	0	(edit)	
	Failed	CBAAdm 5	PC VM 7	ICMP		0.000	N	1	(edit)	

```
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 192.168.30.7

Pinging 192.168.30.7 with 32 bytes of data:

Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.
Reply from 192.168.10.100: Destination host unreachable.

Ping statistics for 192.168.30.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

_ Si hacemos sh run, podremos ver las configuraciones en cada router, como por ejemplo vemos las denegaciones y permisos que asignamos en el router de Cordoba, pero la interfaz solo va a tener establecida una sola de ellas, en este caso o la 100, la 101, o la 102:

```
access-list 100 deny ip host 192.168.10.2 192.168.30.0 0.0.0.255
access-list 100 permit ip any any
access-list 101 deny ip host 192.168.10.4 192.168.20.0 0.0.0.255
access-list 101 permit ip any any
access-list 102 permit ip host 192.168.10.4 192.168.30.0 0.0.0.255
access-list 102 deny ip any any
!
```

_ Para el inciso D, realizamos exactamente los mismos pasos de configuración.

Repaso: entonces, de forma general 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

_ 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#
```

_ Ingresamos a la interfaz elegida:

```
Router(config)#interface fastEthernet x/x
Router(config-if)#
```

_ 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
```







_ Entonces, despues de ver todos los caminos, y elegir el sentido de la red, procedemos a realizar la siguiente configuración, tomando como router el de Jujuy:

```
ROUTER-JJY>ena
ROUTER-JJY#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-JJY(config)#access-list 103 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
ROUTER-JJY(config)#access-list 103 permit ip any any
ROUTER-JJY(config)#exit
ROUTER-JJY#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-JJY#
```

_ Una vez que negamos el tráfico, procedemos a asignar la interfaz. En este caso al haber elegido la que entra desde el router de Jujuy, la asignamos In, y si hubiésemos elegido el de Villa Mercedes que apunta a su red, tendríamos que colocar out. A continuación, vemos la configuración:

```
ROUTER-JJY>ena
ROUTER-JJY#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-JJY(config)#interface Ethernet 0/0/0
ROUTER-JJY(config-if)#ip access-group 103 in
ROUTER-JJY(config-if)#exit
ROUTER-JJY(config)#exit
ROUTER-JJY#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-JJY#
```

_ Para probar que la configuración fue correcta, hacemos un ping desde cualquier PC de Jujuy a cualquiera de Villa Mercedes, y vemos que la conexión es fallida:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC JJY 1	PC VM 2	ICMP		0.000	N	0	(edit)	
	Failed	PC JJY 5	PC VM 1	ICMP		0.000	N	1	(edit)	
	Failed	PC JJY 10	PC VM 7	ICMP		0.000	N	2	(edit)	

```
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.40.100: Destination host unreachable.
Reply from 192.168.40.100: Destination host unreachable.
Reply from 192.168.40.100: Destination host unreachable.
Reply from 192.168.40.100: Destination host unreachable.

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.40.100: Destination host unreachable.
Reply from 192.168.40.100: Destination host unreachable.
Reply from 192.168.40.100: Destination host unreachable.
Reply from 192.168.40.100: Destination host unreachable.

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 192.168.30.7

Pinging 192.168.30.7 with 32 bytes of data:

Reply from 192.168.40.100: Destination host unreachable.
Reply from 192.168.40.100: Destination host unreachable.
Reply from 192.168.40.100: Destination host unreachable.
Reply from 192.168.40.100: Destination host unreachable.

Ping statistics for 192.168.30.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

fuelle | destino: Identificadores de direcciones origen y destino

mascara-fuelle | 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):

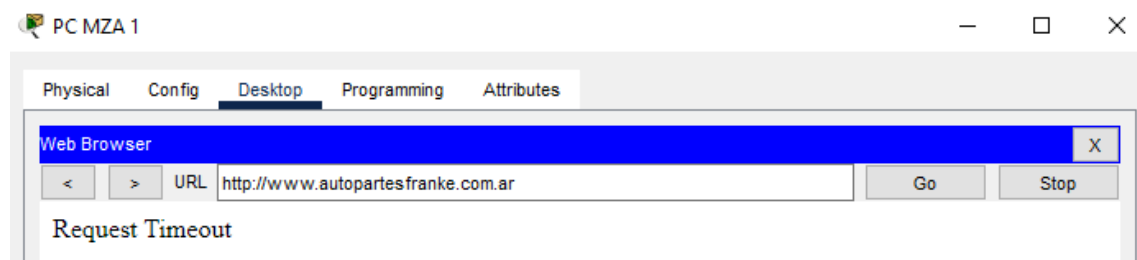
```
Router(config)#access-list 104 deny tcp 192.168.20.1 0.0.0.0 192.168.10.9
0.0.0.0 eq 23
```

```
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
```

_ Para hacer una prueba hacemos que la 192.168.20.1 no puede ingresar al server 192.168.10.62 usando la aplicación http (port 80). En este caso lo haremos en el router de Cordoba:

```
ROUTER-MZA>ena
ROUTER-MZA#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-MZA(config)#access-list 104 deny tcp 192.168.20.1 0.0.0.0 192.168.10.62 0.0.0.0 eq 80
ROUTER-MZA(config)#access-list 104 permit tcp any any
ROUTER-MZA(config)#access-list 104 permit ip any any
ROUTER-MZA(config)#interface Ethernet 0/0/0
ROUTER-MZA(config-if)#ip access-group 104 in
ROUTER-MZA(config-if)#exit
ROUTER-MZA(config)#exit
ROUTER-MZA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-MZA#
```

_ Es importante aclarar aca que primero debemos permitir el ip y luego el tcp, cosa que en la configuracion de la interfaz quede solo la del ip any any.



Extra

1)_ Ahora lo que hacemos es que por ejemplo 8 PCs de Jujuy no puedan ver a toda la red de Mendoza, y permitir que el resto de PCs de Jujuy si puedan:

Access-list 100 deny ip 192.168.10.0 0.0.0.7 192.168.20.0 0.0.0.255

Access-list 100 deny ip 192.168.10.8 0.0.0.0 192.168.20.0 0.0.0.255

Access-list 100 permit ip any any

```
ROUTER-JJY>ena
ROUTER-JJY#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-JJY(config)#access-list 100 deny ip 192.168.40.0 0.0.0.7 162.168.20.0 0.0.0.255
ROUTER-JJY(config)#access-list 100 deny ip 192.168.40.8 0.0.0.0 162.168.20.0 0.0.0.255
ROUTER-JJY(config)#access-list 100 permit ip any any
ROUTER-JJY(config)#interface Ethernet 0/0/0
ROUTER-JJY(config-if)#ip access-group 100 in
ROUTER-JJY(config-if)#exit
ROUTER-JJY(config)#exit
ROUTER-JJY#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-JJY#
```

_ Si mandamus un ping de cualquier PC de la 1 a la 8 de Jujuy a cualquiera de Mendoza, no podran acceder, pero si es de la 9 en Adelante si.

2)_ En el router de CBA para que al servidor 61 no le llegue ningún ping de cualquier red usamos el protocolo ICMP. Las páginas si van a poder verse. En el router de CBA hacemos:

Access-list 108 deny icmp any 192.168.10.61 0.0.0.0

Access-list 108 permit ip any any

```
ROUTER-CBA>ena
Password:
ROUTER-CBA#config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-CBA(config)#access-list 103 deny icmp any 192.168.10.61 0.0.0.0
ROUTER-CBA(config)#access-list 103 permit ip any any
ROUTER-CBA(config)#interface Ethernet
% Incomplete command.
ROUTER-CBA(config)#interface Ethernet 0/0/0
ROUTER-CBA(config-if)#ip access-group 103 out
ROUTER-CBA(config-if)#exit
ROUTER-CBA(config)#exit
ROUTER-CBA#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
ROUTER-CBA#
```

_ Hacemos ping desde cualquier PC de todas las redes al servidor 1 de Cordoba:

PC MZA 1

```
Physical  Config  Desktop  Programming  Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.61

Pinging 192.168.10.61 with 32 bytes of data:

Reply from 220.120.10.1: Destination host unreachable.
Reply from 220.120.10.1: Destination host unreachable.
Reply from 220.120.10.1: Destination host unreachable.
Reply from 220.120.10.1: Destination host unreachable.

Ping statistics for 192.168.10.61:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC VM 1

```
Physical  Config  Desktop  Programming  Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.61

Pinging 192.168.10.61 with 32 bytes of data:

Reply from 192.168.30.100: Destination host unreachable.
Reply from 192.168.30.100: Destination host unreachable.
Reply from 192.168.30.100: Destination host unreachable.
Reply from 192.168.30.100: Destination host unreachable.

Ping statistics for 192.168.10.61:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC JJY 1

```
Physical  Config  Desktop  Programming  Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.61

Pinging 192.168.10.61 with 32 bytes of data:

Reply from 120.120.10.1: Destination host unreachable.
Reply from 120.120.10.1: Destination host unreachable.
Reply from 120.120.10.1: Destination host unreachable.
Reply from 120.120.10.1: Destination host unreachable.

Ping statistics for 192.168.10.61:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Physical Config Services Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.10.61

Pinging 192.168.10.61 with 32 bytes of data:

Reply from 120.120.10.1: Destination host unreachable.
Reply from 120.120.10.1: Destination host unreachable.
Reply from 120.120.10.1: Destination host unreachable.
Reply from 120.120.10.1: Destination host unreachable.

Ping statistics for 192.168.10.61:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```