Práctica ACL

Alumnos: Malena Aguillón, Franco Balich, Barbara Covarrubias, Otto Gonzalez
Docente: Marcelo Semería
Fecha de Entrega: 11/11/2022

Elija la opción que mejor responda la pregunta. Puede no haber ninguna. **Explique** claramente el porque de su elección

1. ¿Cuál de los siguientes es un ejemplo de listas de acceso IP estándar?

a. access-list 125 permit host 10.10.10.10
b. access-list 5 deny 172.16.15.2 0.0.0.0
c. access-list 10 permit 172.16.15.2 255.255.0.0
d. access-list standard 10.10.10.10

La opción A es incorrecta debido a que las access-list pueden tener un numero identificador de 1 a 99, por lo que el 125 es imposible.
La opción B es incorrecta debido que se niega el acceso.
La opción C es incorrecta debido a que la máscara esta al revés.
La opción D también es incorrecta debido a que le falta la máscara y no tiene el número de access-list

2. Se le ha requerido crear una lista de acceso que evite el paso de los hosts que se encuentran en el rango de direcciones comprendido entre 192.168.160.0 y 192.168.191.0. ¿Cuál de las sentencias que se muestran a continuación deberá utilizar?

a. access-list 20 deny 192.168.160.0 255.255.224.0
b. access-list 20 deny 192.168.160.0 0.0.191.255
c. access-list 20 deny 192.168.160.0 0.0.31.255
d. access-list 20 deny 192.168.0.0 0.0.31.255

La opción A es incorrecta debido a que en la máscara esta al revés.
La opción B es incorrecta ya que la máscara no cumple los requisitos.
La opción C es correcta debido a que la máscara solo va a denegar los host con ips desde 192.168.160.0 31 direcciones en el tercer octeto y 255 en el último.
La opción D es incorrecta debido a que la ip esta mal declarada.

3. Usted ha creado una lista de acceso llamada "ventas". ¿Cuál de los siguientes comandos le permitirá aplicar esa lista para filtrar el tráfico entrante en la interfaz serial 0 de su router?

a. (config)#ip access-group 100 in
b. (config-if)#ip access-group 100 in
c. (config-if)#ip access-group ventas in
d. (config-if)#ventas ip access-list in

La opción B ya que es la única que llama a la lista de acceso "ventas" luego del comando ip access-group

4. ¿Cuál de los siguientes es un modo válido de referir solamente el nodo 172.16.15.95 en una lista de acceso IP extendida? (elija dos respuestas)

a. 172.16.15.95 0.0.0.255
b. 172.16.15.95 0.0.0.0
c. any 172.16.15.95
d. host 172.16.15.95
e. 0.0.0.0 172.16.15.95
f. 172.16.15.95
g. ip any 172.16.15.95

Las dos respuestas validas son la B debido a que la máscara indica que se va a controlar la dirección de la maquina inclusive y la D porque esta controla directamente el host con dicha ip

5. ¿Cuál de las siguientes sentencias de ACL permitirá solamente el tráfico http que ingresa a la red 196.15.7.0?

a. access-list 110 permit tcp any 196.15.7.0 0.0.0.255 eq www
b. access-list 15 deny tcp any 192.16.7.0 0.0.0.255 eq www
c. access-list 110 permit 196.15.7.0 0.0.0.255 eq www
d. access-list 110 permit ip any 192.168.7.0 0.0.0.255 eq www
e. access-list 110 permit www any 192.168.7.0 0.0.0.255

La respuesta correcta es la A, ya que es la única que permite el tráfico de cualquier origen a la red 196.15.7.0

6. ¿Qué comando de Cisco IOS le permite visualizar el contenido completo de todas las listas de acceso configuradas?

a. Router#show interfaces
b. Router>show ip interface
c. Router#show access-lists
d. Router>show all access-lists

El comando correcto es el A, debido a que solo así se pueden ver las interfaces de un router Cisco

7. Si usted debe denegar toda conexión telnet dirigida a la red 192.168.1.0. ¿Cuál de los siguientes comandos deberá utilizar?

a. access-list 120 deny tcp 192.168.1.0 255.255.255.0 any eq telnet
b. access-list 120 deny tcp 192.168.1.0 255.255.255.255 any eq telnet
c. access-list 120 deny tcp any 192.168.1.0 0.0.0.255 eq 23
d. access-list 120 deny 192.168.1.0 0.0.0.255 eq 23

La opción correcta es la C debido a que deniega el acceso de cualquier origen a la red indicada

8. Si usted debe denegar el acceso por ftp desde la red 200.42.15.0 a la red 200.199.11.0, y permitir todo lo demás, ¿Cuál de los siguientes conjuntos de comandos es el válido?

a. access-list 100 deny network 200.42.15.0 to network 200.199.11.0 eq ftp
access-list 100 permit ip any any
b. access-list 1 deny tcp 200.42.15.0 0.0.0.255 200.199.11.0 0.0.0.255 eq ftp
c. access-list 100 deny tcp 200.42.15.0 0.0.0.255 200.199.11.0 0.0.0.255 eq ftp
d. access-list 100 deny tcp 200.42.15.0 0.0.0.255 200.199.11.0 0.0.0.255 eq ftp
access-list 100 permit ip any 0.0.0.0 255.255.255.255

El conjunto de comandos valido es el D debido a que deniega el acceso de paquetes originados de la red 200.42.15.0 y luego indica que se permite todo lo demas.

9. Usted debe crear una lista de acceso estándar que deniegue solamente la subred en la que se encuentra el nodo 172.16.50.92/20. ¿Cuál de las siguientes sentencias deberá estar presente en su lista de acceso?

a. access-list 1 deny host 172.16.50.92
b. access-list 2 deny 172.16.50.80 0.0.0.15
c. access-list 3 deny 172.16.0.0 0.0.255.255
d. access-list 4 deny 172.16.16.0 0.0.31.255
e. access-list 5 deny 172.16.48.0 0.0.31.255
f. access-list 5 deny 172.16.48.0 0.0.15.255

La opción correcta es la A debido a que deniega el acceso directo al nodo/host 172.16.50.92

10. Dada la dirección IP 192.168.100.64 255.255.255.224, identifique la máscara de wildcard que va a machear los host 192.168.100.64 a 95.

a. 0.0.0.65
b. 0.0.0.31
c. 0.0.0.64
d. 0.0.0.255

La máscara de wildcard para los host 192.168.100.64 a 95 es la B debido a que la cantidad de host a que solo esa mascara permite los 31 host que hay en el rango determinado de ips

11. Dada la dirección IP 172.16.8.0 255.255.255.0, identifique la máscara wildcard que machea subredes 172.16.8.0 – 172.16.15.0 y todos los host de las subredes.

a. 0.0.7.0
b. 0.0.7.255
c. 0.0.255.255
d. 0.0.0.7

La opción correcta es la B debido a que solo esta permite en el segundo octeto 7 valores y los 255 posibles host de cada uno

12. Identifique la máscara de wildcard que va a denegar los host 8 a 15 asumiendo que la máscara de subred es de 24 bits.

a. access-list 1 deny 192.6.10.8 0.0.0.8
b. access-list 1 permit 192.6.10.8 0.0.0.7
c. access-list 1 deny 192.6.10.8 0.0.0.7
d. access-list 1 deny 192.6.10.8 0.0.0.255

La opción correcta es la C debido a que solo esa tiene una máscara que permite denegar el acceso a 7 host a partir de la ip del host 8

13. Dada la dirección IP 172.16.5.10 255.255.255.0, identifique la dirección IP y la máscara wildcard que machea el host dado.

a. 172.16.5.10 0.0.255.255
b. 172.16.5.10 0.0.0.0
c. 172.16.5.10 1.1.1.1
d. 172.16.5.10 255.255.255.255

La opción correcta es la B porque se está buscando un host concreto.
La A estamos considerando los primeros dos octetos
En cambio en la C la mascara esta en formato incorrecto

14. Dada la dirección IP 172.16.16.0 255.255.255.0, identifique la máscara wildcard que machea todos los hosts en la red dada.

a. 0.0.7.255
b. 0.0.0.255
c. 0.0.15.255
d. 0.0.0.254

La B es la correcta porque la mascara esta declarada.
La A y la C contienen host incorrectos
La D no contiene los host indicados.

15. Dada la dirección IP 201.100.165.32 255.255.255.224, identifique las direcciones y las máscaras wildcard que machean los hosts 32 a 40.

a. 201.100.165.32 0.0.0.255
b. 201.100.165.32 0.0.0.7
c. 201.100.165.32 0.0.0.7 & 201.100.165.40 0.0.0.0
d. 201.100.165.32 0.0.0.255 & 201.100.165.40 0.0.0.0

La A y la D indican mas host de los declarados
LA opción C porque nos esta indicadno el el rango.

16. Dada la dirección IP 10.0.0.0 255.0.0.0, identifique la máscara wildcard que machea todos los hosts de la red dada.

a. 0.255.255.255
b. 255.255.255.255
c. 0.0.0.0
d. 255.255.0.0

La correcta es la A porque permite todos los host.
La B permite todos los host basandose en cualquier red
La c y de son incorrectas las sintaxis.

17. Para especificar todos los hosts de la red clase B 172.16.0.0, ¿qué máscara de wildcard debería usar?.

a. 255.255.0.0
b. 255.255.255.255
c. 0.0.0.0
d. 0.0.255.255

La A es incorrecta porque refiere a la mascara de red
La B es incorrecta porque permite cualquier host
La C es incorrecta porque permite un solo host 172.16.0.0
La D es correcta permitiendo todos los host.

18. Usted quiere referenciar al host 172.16.50.1 en una lista de acceso IP, ¿qué máscara deberá usar para que la lista sea específica para ese host?.

a. 0.0.255.255
b. 0.0.0.0
c. 255.255.255.255
d. 255.255.0.0

La opción C es correcta proque permite el host indicado.
Las demas opciones permiten otros host, las mascaras no son correctas.

19. ¿Cuál es la máscara de wildcard que machea el rango 100.1.16.0 – 100.1.31.255 ?.

a. 0.0.255.255
b. 0.31.255.255
c. 0.0.31.255
d. 0.0.15.255
e. 0.0.7.255

La opción D es la correcta porque permite todos los host del rango 100.1.16.0 a 100.1.31.255
Por otro lado, las demas opciones son incorrectas ya que por ejemplo en el caso:
b-> la mascara no es de la clase especificada.
c-> Permite menos host del rango indicado
e-> supera el rango de host.

20. ¿Qué máscara de wildcard deberá utilizarse para machear el rango 157.89.64.0 a 157.89.127.255 ?.

a. 0.0.15.255
b. 0.0.63.255
c. 0.0.255.255
d. 0.0.31.255
e. 0.0.7.255

La opcion correcta es la C ya que permite todos los host dentro del rango estimado.

21. ¿Qué máscara de wildcard deberá utilizarse para machear el rango 157.89.64.0 a 157.89.95.255 ?.

a. 0.0.7.255
b. 0.0.15.255
c. 0.0.31.255
d. 0.0.63.255
e. 0.0.255.255

LA respuesta correcta es la C, ya que permite todos los host dentro del rango estipulado.
En cambio la b-> está involucrado dentro del rango 157.89.64.0 hasta 157.89.79.255
La opcion e-> permite todos los host
La opcion d se encuentra dentro del rango 157.89.64.0 hasta 157.89.127.255

22. La máscara de wildcard es una serie de 1's y 0's escrita en notación decimal, identifique la función de los 1 y 0.

a. 1 = porción de red, 0 = porción de host
b. 1 = revisa, 0 = no revisa
c. 1 = no revisa, 0 = revisa
d. Ninguno de los anteriores

La respuesta correcta es la C

23. ¿Cuál de las siguientes es la máscara de wildcard para una lista de acceso IP que incluya el rango de direcciones desde 172.30.16.0 hasta 172.30.31.255 ?.

a. 255.255.0.0
b. 255.255.192.0
c. 0.0.255.255
d. 0.0.15.255
e. 0.0.31.255

La mascara de subred sería 255.255.240.0 lo inverso sería 0.0.15.255

24. ¿Cuál o cuáles de las siguientes expresiones son válidas para referir sólo al host 172.16.30.55 en una lista de acceso?. (Seleccione todas las que aplican)

a. host 172.16.30.55
b. 172.16.30.55 0.0.0.0
c. 172.16.30.55 0.0.0.255
d. 0.0.0.0 172.16.30.55
e. 172.16.30.55 255.255.255.255

Se usa host seguido de la IP del dispositivo.

25. ¿Qué configuración de lista de acceso permite sólo el tráfico entrante de la red 172.17.0.0 a la int s0 ?.

a. access-list 10 permit 172.17.0.0 0.0.255.255 , int s0 , ip access-group 10 out
b. access-list 10 permit 172.17.0.0 0.0.255.255 , int s0 , ip access-list 10 in
c. access-group 10 permit 172.17.0.0 0.0.255.255 , int s0 , ip access-list 10 out
d. access-list 10 permit 172.17.0.0 0.0.255.255 , int s0 , ip access-group 10 in

La respuesta correcta es B.

26. ¿Cuál de las siguientes listas de acceso permitirá sólo tráfico FTP a la red 196.15.7.0 ?.

a. access-list 100 permit tcp any 196.15.7.0 0.0.0.255 eq ftp
b. access-list 10 deny tcp any 196.15.7.0 eq ftp
c. access-list 100 permit 196.15.7.0 0.0.0.255 eq ftp
d. access-list 10 permit tcp any 196.15.7.0 0.0.0.255

Especifica permitir tcp desde cualquier origen hacia destino red con puerto de ftp.

27. Identifique las 2 sentencias que describen correctamente dónde aplicar la lista de acceso.

a. Las listas de acceso extendidas deben aplicarse próximas al destino.
b. Las listas de acceso estándar deben aplicarse próximas al origen.
c. Las listas de acceso extendidas deben aplicarse próximas al origen.
d. Las listas de acceso estándar deben aplicarse próximas al destino.

La estandar debe localizarse mas cerca del destino posible, si se localiza en el origen, el permit o deny ocurirían basados solamente en la dirección de origen .

Las extendidas deben ser localizadas cerca del origen para prevenir que se envíe trafico no deseado a través de las multiples redes y ser denegado solamente cuando alcanza el origen.

28. Identifique la sentencia que permitirá acceso a SMTP sólo hacia el host 209.76.25.1 .

a. access-list 101 permit tcp any 209.76.25.1 eq smtp
b. access-list 101 permit ip 209.76.25.1 any eq 25
c. access-list 101 deny ip 209.76.25.1 any
d. access-list 101 deny ip any any
e. access-list 101 permit tcp any 209.76.25.1 eq smtp
f. access-list 101 permit tcp any host 209.76.25.1 eq smtp

La respuesta es F, el destino es 209.76.25.1 desde cualquier ip en puerto de smtp.

29 Cuantas listas de control de acceso pueden usarse como máximo en un router que tiene tres interfaces que soportan trafico bidireccional y corre los protocolos IP y Appletalk?

a. 8
b. 12
c. 16
d. No se pueden configurar ACLs

Se multiplican la cantidad de protocolos por 2 (in y out) y luego por la cantidad de interfaces.

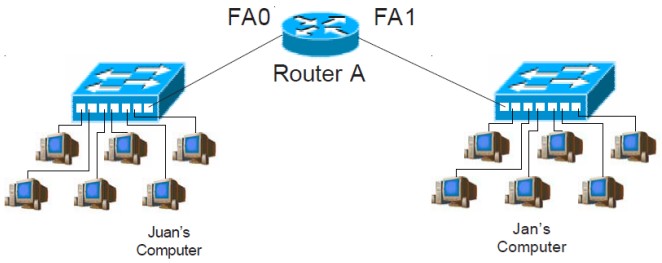
30 Una interface ha sido configurada con un ACL estándar definida con el comando access-list 10 permit 11.10.10.0 0.0.0.255 y ha sido aplicada en un router que tiene dos redes locales LAN, con los rangos 192.268.1.0/24 y 192.168.2.0/24, y una interface serial que le conecta con una WAN Frame Relay y tiene una ip 200.200.200.128/30. El comando usado para aplicar la ACL en el puerto Serial 0/0 es ip Access-group 10 in.
¿Cuáles de las siguientes aseveraciones son acertadas? (Seleccione 3).

a. Los paquetes de Telnet provenientes de la red 11.10.10.0/24 podrán pasar hacia las redes LAN conectadas al router.
b. Los paquetes HTTP provenientes de cualquier red del mundo pueden pasar hacia las dos redes LAN conectadas al router.
c. Todos los paquetes que vayan a las redes LAN del router y que respondan a una petición que se origina desde una de las dos redes LAN de router serán admitidos por el router.
d. Todos los paquetes son permitidos desde la WAN para todos los protocolos enrutables.
e. En caso de existir un servidor WEB en una de las redes LAN del router este será accesible para usuarios de la red 11.10.10.0/24

Respuestas A, D y E.

31. En la red dada se busca evitar que los paquetes de la PC de **Juan** lleguen a la PC de **Jan**.

¿ En qué interface del router colocaría la lista de acceso estándar ?.



Redondeé la correcta

FA0 / FA1

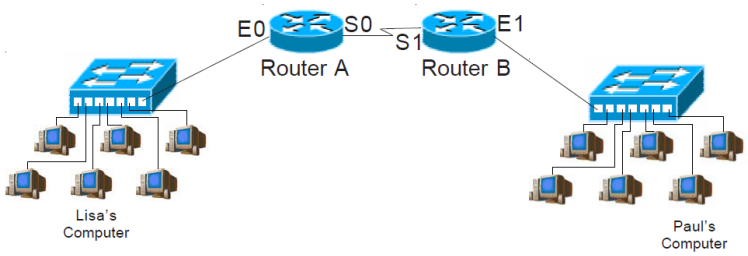
Explique porque.

FA1, ACL estandar mas cerca del destino indicando deny de los paquetes con destino IP de Jan y origen de Juan.

32. Para el mismo esquema del punto anterior y el mismo objetivo ¿Dónde ubicaría la lista de acceso si fuese extendida. Explique su respuesta.

FA0, ACL extendida mas cerca del origen para controlar los paquetes salientes de Juan y denegar los que tienen destino IP de Jan.

33. En la red dada. **Lisa** está acosando a **Paul**.



a. ¿Dónde ubicaría el ACL estándar que bloquee los paquetes?:

Ubicación ACL: Interface E1 Router B

b. ¿Dónde ubicaría el ACL que bloquee paquetes de Paul a Lisa?

Ubicación ACL: Interface E0 Router A

c. IDEM a con ACL extendida

Ubicación ACL: Interface E0 Router A

d. IDEM b con ACL extendida

Ubicacion ACL: Interface E1 Router B

34. Escriba una **Wildcard** tal que

a. Identifique exactamente la dirección IP:

192.168.95.70 con máscara de subred 255.255.255.0

192.168.95.70 0.0.0.0

b. IDEM a

210.150.10.0 con máscara de subred 255.255.255.0

210.150.10.0 0.0.0.0

c. Identifique el rango

192.10.10.16 con máscara de subred 255.255.255.224

Desde 192.10.10.16 hasta 192.10.10.47

d. IDEM c

171.50.75.128 con máscara de subred 255.255.255.192

Desde 171.50.75.128 hasta 171.50.75.191

e. IDEM c

172.18.0.0 con máscara de subred 255.255.224.0

Desde 172.18.0.0 hasta 172.18.31.255

f. IDEM c

135.35.230.32 con máscara de subred 255.255.255.248

Desde 135.35.230.32 hasta 135.35.230.39

35. Indique las fuentes (direcciones IP origen) permitidos para cada caso

a. access-list 10 permit 192.158.150.50 0.0.0.0

192.158.150.50

b. access-list 125 deny tcp 125.223.50.0 0.0.0.63 host 172.168.10.1 fragments

125.223.50.1 a 125.223.50.63

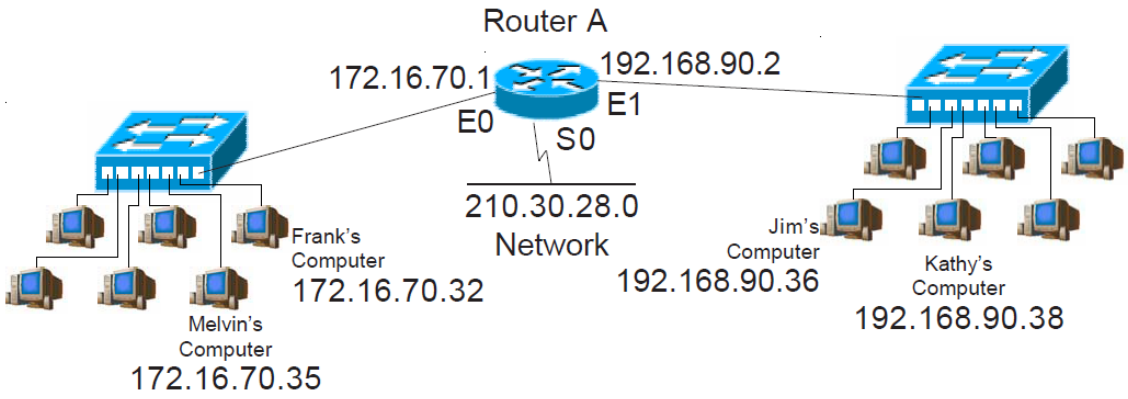
c. access-list 195 permit udp 172.30.12.0 0.0.0.127 172.50.10.0 0.0.0.255

172.30.12.1 a 172.30.12.127

d. Access-list 150 permit 192.168.15.0 0.0.0.63 192.168.30.10 0.0.0.0

192.168.15.1 a 192.168.15.63

36. Escriba las lista de acceso. *Se da un ejemplo de resolución*.



a. EJEMPLO: Escriba la lista de acceso estándar que impida a la computadora de Melvin enviar paquetes a la computadora de Kathy pero permita otro tráfico. Escriba en varios formatos

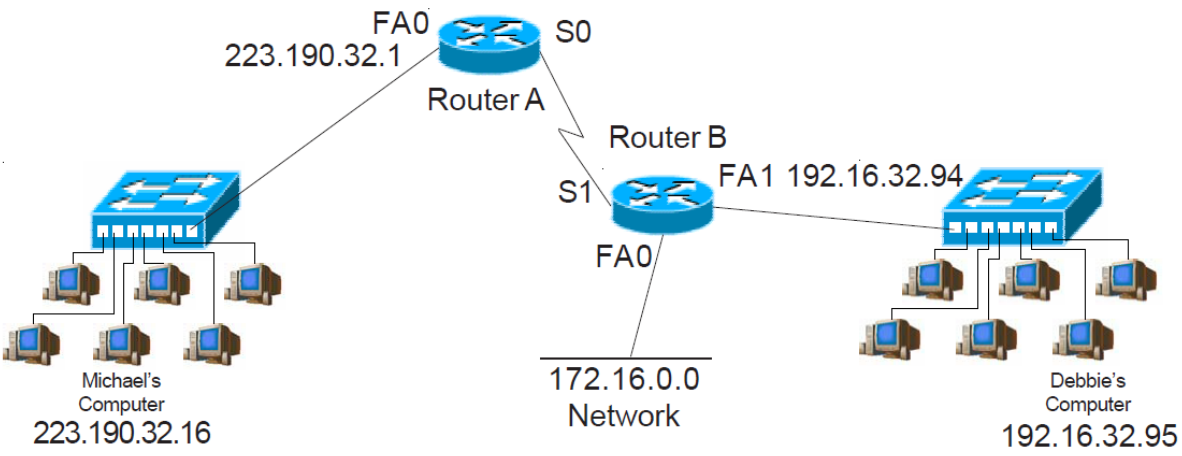
Solución

Ubicación: Interfaz E1 del router A

Lista de acceso:

```
Router# configure terminal (or config t)
Router(config)# access-list 10 deny 172.16.70.35
                              or
                access-list 10 deny 172.16.70.35 0.0.0.0
                              or
                access-list 10 deny host 172.16.70.35
Router(config)# access-list 10 permit 0.0.0.0 255.255.255.255
                              or
                access-list 10 permit any
Router(config)# interface e1
Router(config-if)# ip access-group 10 out
Router(config-if)# exit
Router(config)# exit
```

37. Escriba la lista de acceso.



Se busca evitar que la PC de Debbie reciba información de la PC de Michael, pero permita otro tráfico. Escriba opciones de formatos.

Ubicación:

Interface FA1 Router B

Route# configure terminal

Router (config)# :

access-list 10 deny 223.190.32.16

ó

access-list 10 deny 223.190.32.16 0.0.0.0

ó

access-list 10 deny host 223.190.32.16 0.0.0.0

Router (config)#

access-list 10 permit any

ó

access-list 10 permit 0.0.0.0

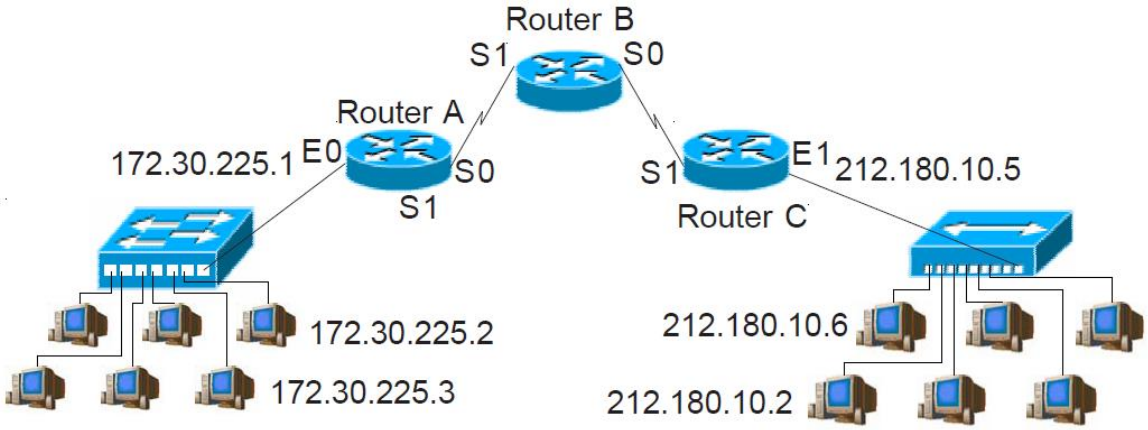
Router (config)# interface FA1

Router (config-if)# ip Access-group 10

Router (config-if)# exit

Router (config)# exit

38. Dada la red.



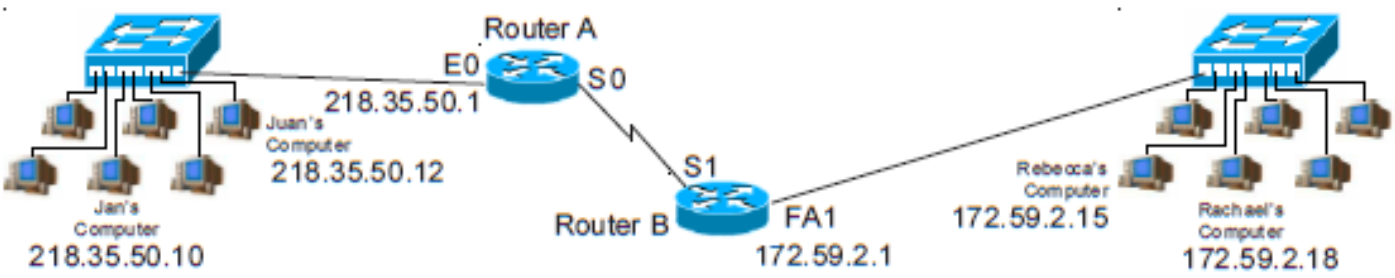
a. Escriba la lista de acceso estándar que impida que las direcciones 172.30.225.2 y 172.30.225.3envien información a la red 212.180.10.0, pero permita todos los demás tráfico. Escriba en más de un formato

Ubicación: Interface E1 Router C

access-list 1 deny host 172.30.255.2
access-list 1 deny host 172.30.255.3
access-list 1 permit any

b. Arme la red anterior usando el simulador packet tracer V6 y compruebe el funcionamiento de la lista de acceso anterior. Adjunte el archivo .pkt .

39. Dada la siguiente red.



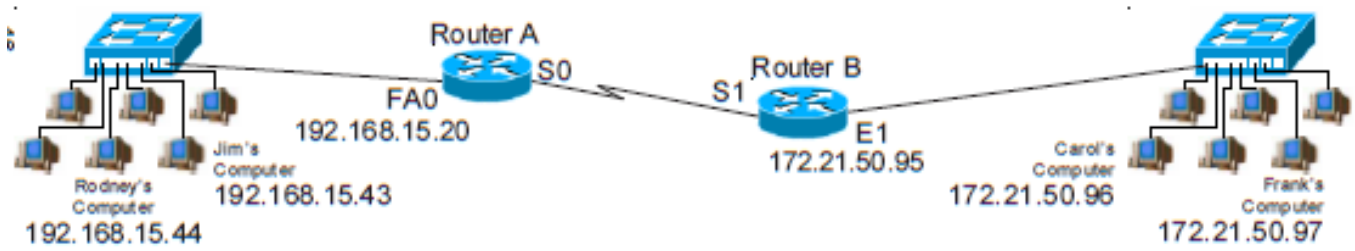
Escriba la lista de acceso extendida que permita que la computadora de Jan reciba paquetes desde la computadora de Rachael pero no de la de Rebeca. Impida todos los demás paquetes.

Escriba la lista de acceso y compruébela con el Packet Tracer V6

¬ Ubicación: Interface FA1 Router B

access-list 101 permit host 172.59.2.18 host 218.35.50.10
access-list 101 deny host 218.35.50.10 any

40. Dada la red



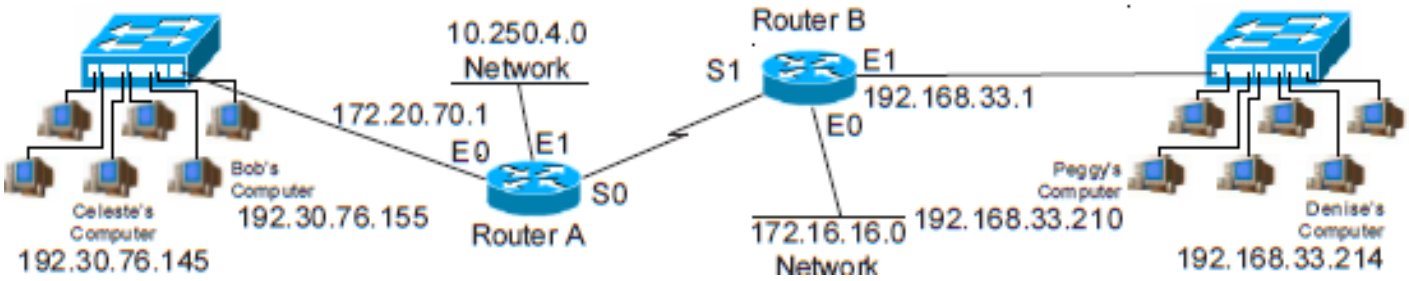
a. Escriba la lista de acceso extendida que impida que las primeras 15 direcciones usables d la red 192.168.15.0 alcancen la red 172.21.0.0. Permita todo otro tráfico.

b. Genere una maqueta con el Packet Tracer que permita comprobar el punto anbterior

Ubicación: Interface FA0 Router A

access-list 101 deny 192.168.15.0.0.0.0.15 172.21.0.0.0.0.255.255
access-list 101 permit any 172.21.0.0.0.0.255.255

41. Dada la red.



Escriba la lista de acceso extendida que permita a la computadora de Denise usar TFTP con la computadora de Bob. Impida todo el tráfico desde 192.168.33.0 a 192.30.76.0.

Compruebe con el simulador Packet Tracer.

Ubicación: Interface E1 Router B

access-list 101 permit host 192.30.76.155 host 192.168.33.214 eq tftp

access-list 101 deny 192.168.33.0 0.0.0.255 192.30.76.0 0.0.0.255

42. Dada las siguientes sentencias. Encuentra errores?

En caso afirmativo, indíquelo sobre la figura.

```
interface ethernet 1
 ip access-group 60 in
 ip access-group 161 in
access-list 60 deny host 1.3.5.7 0.0.0.0    -> no se puede usar: host y a su vez 0.0.0.0
access-list 60 deny 10.0.0.0 0.0.0.0 -> no es la forma que corresponde al host
access-list 60 deny 54.78.43.2 255.255.255.255 -> la mascara debe ser 0.0.0.0
access-list 60 deny ip host 101.2.5.7 eq telnet  -> no se puede negar el protocolo
access-list 161 permit ip 205.6.23.6 34.67.22.3
access-list 161 permit ipx a0b1c2 -1
access-list 161 deny telnet  -> falta información
access-list 161 permit ip host 225.0.0.5 any  -> no puede ser dirección de origen
access-list 161 deny ip any any
```