INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

Administración de servicios en red

Práctica 4:

ACL

Alumnos:

Meza Vargas Brandon David
Romero Angeles Abraham

Equipo:
ADR

Grupo:
4CM13

Profesor:

Gaspar Medina Fabian

INTRODUCCIÓN

¿Qué es una ACL?

Una ACL es una herramienta de seguridad que se utiliza para controlar el acceso a recursos de red. Se compone de una lista de reglas que especifican qué tráfico de red está permitido y qué tráfico está bloqueado. Las ACL se aplican en routers, switches y firewalls para controlar el tráfico que fluye a través de ellos. Cada regla de una ACL especifica una dirección IP de origen y destino, un protocolo de red y un puerto de origen y destino. También se pueden especificar otras opciones, como una máscara de subred y una acción de permitir o denegar.

Las ACL se pueden utilizar para una variedad de propósitos de seguridad, como restringir el acceso a recursos de red a usuarios específicos, bloquear tráfico malintencionado, limitar el ancho de banda disponible para ciertos tipos de tráfico o permitir el acceso a recursos de red solo en ciertos momentos del día.

Tipos de ACL:

Hay dos tipos principales de ACL: ACL estándar y ACL extendida. Estos tipos se diferencian en su alcance y en los criterios que se pueden utilizar para filtrar el tráfico.

ACL estándar:

Las ACL estándar se utilizan para controlar el acceso en función de la dirección IP de origen. Una ACL estándar permite o deniega el tráfico basándose únicamente en la dirección IP de origen. Pueden aplicarse a todas las direcciones IP o solo a un rango específico. Los números de las ACL estándar van del 1 al 99 o del 1300 al 1999.

ACL extendida:

Las ACL extendidas pueden controlar el acceso en función de una amplia gama de factores, como la dirección IP de origen y destino, el protocolo de red, el puerto y otros criterios. Las ACL extendidas pueden permitir o denegar el tráfico en función de un conjunto de criterios específicos que se definen en la regla. Los números de las ACL extendidas van del 100 al 199 o del 2000 al 2699.

Cómo funcionan las ACL:

Las ACL funcionan siguiendo una secuencia de comprobación de las reglas. Cuando se recibe un paquete, se compara con la primera regla de la ACL y se determina si el tráfico debe permitirse o denegarse en función de los criterios de esa regla. Si se permite el tráfico, se envía al siguiente nivel de la red. Si se deniega el tráfico, se descarta y no se procesa más.

El orden de las reglas de la ACL es importante. Si una regla permite el tráfico y otra regla en la lista lo deniega, se aplicará la acción de denegar. Por lo tanto, es importante planificar cuidadosamente la secuencia de las reglas para garantizar que se apliquen correctamente.

Aplicaciones de las ACL:

Las ACL se pueden utilizar para una variedad de propósitos de seguridad, como restringir el acceso a recursos de red a usuarios específicos, bloquear tráfico malintencionado, limitar el ancho de banda disponible para ciertos tipos de tráfico o permitir el acceso a recursos de red solo en ciertos momentos del día.

Consideraciones de implementación:

Es importante tener en cuenta que las ACL pueden ser complejas y pueden tener un impacto significativo en el rendimiento de la red. Por lo tanto, es esencial planificar cuidadosamente su implementación y monitorear su impacto en la red. También es importante mantener las ACL actualizadas y realizar pruebas regulares para garantizar que sigan siendo efectivas. Además, es recomendable aplicar las ACL en el perímetro de la red, en lugar de en cada dispositivo, para minimizar la complejidad y reducir el número de reglas necesarias.

Es importante asegurarse de que las ACL no bloqueen tráfico legítimo y que no permitan el acceso no autorizado a recursos de red. También es importante tener en cuenta que las ACL solo son una parte de una estrategia de seguridad más amplia y no deben ser consideradas como la única medida de seguridad.

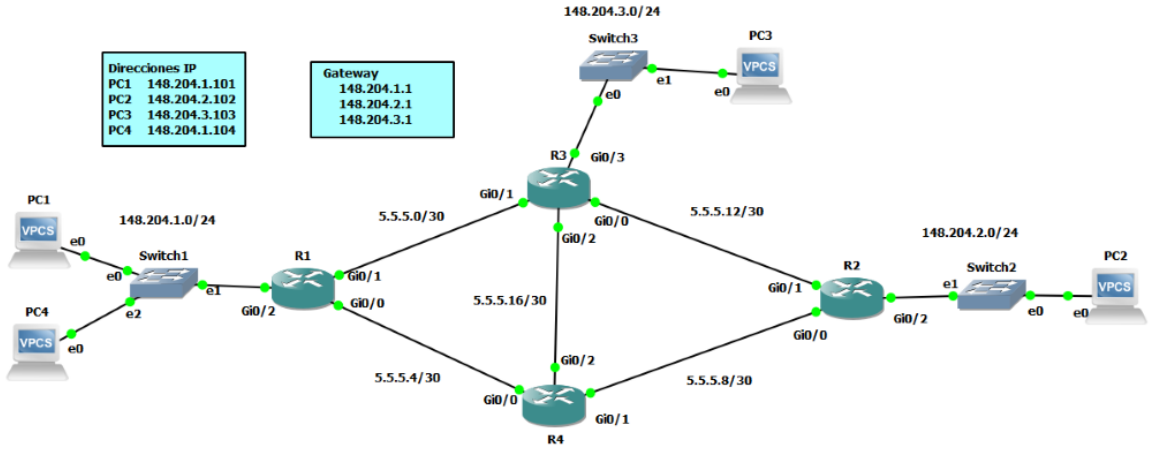
En resumen, las ACL son una herramienta de seguridad importante que se utiliza para controlar el acceso a recursos de red. Hay dos tipos principales de ACL: ACL estándar y ACL extendida. Las ACL se utilizan para una variedad de propósitos de seguridad y deben ser implementadas cuidadosamente para minimizar la complejidad y garantizar la efectividad. Además, es importante recordar que las ACL solo son una parte de una estrategia de seguridad más amplia y no deben ser consideradas como la única medida de seguridad.

Configuración de ACL

Valor de la actividad: 10 ptos

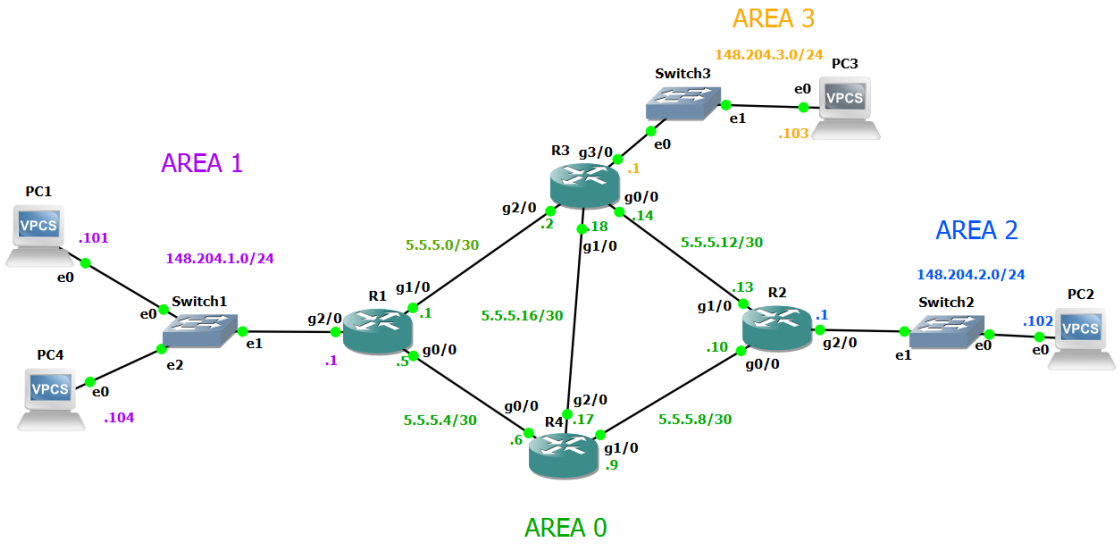
Fecha de entrega:

Realiza la siguiente topología en GNS3 y configura las interfaces y el enrutamiento.



En este ejemplo se usarán las direcciones IP 148.204.1.1, 148.204.2.1 y 148.204.3.1 como puertas de enlace en cada router. Y las direcciones IP 148.204.1.101, 148.204.1.102, 148.204.1.103 y 148.204.1.104 paras las PC1 a PC4, respectivamente.

A continuación, se presenta captura con la red armada y configurada, se utilizó ospf dividiendo en áreas la topología.



Una vez que tengas configuradas todas las interfaces y el enrutamiento, prueba haciendo *pings* desde y hacía todas las PC's.

A continuación, se presentan capturas con los pings a las computadoras.

Pings desde Router 1

```
R1#ping 148.204.1.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.1.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/15/20 ms
```

Ilustración 1. Ping a máquina 1

```
R1#ping 148.204.1.104

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.1.104, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/22/40 ms
```

Ilustración 2. Ping a máquina 4

```
R1#ping 148.204.2.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.2.102, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 76/338/1120 ms
```

Ilustración 3. Ping a máquina 2

```
R1#ping 148.204.3.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.3.103, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 44/308/1092 ms
```

Ilustración 4. Ping a máquina 3

Pings desde Router 2

```
R2#ping 148.204.1.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.1.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/80/92 ms
```

Ilustración 5. Ping a máquina 1

```
R2#ping 148.204.1.104

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.1.104, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 76/339/1096 ms
```

Ilustración 6. Ping a máquina 4

```
R2#ping 148.204.2.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.2.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/23/52 ms
```

Ilustración 7. Ping a máquina 2

```
R2#ping 148.204.3.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.3.103, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 44/306/1084 ms
```

Ilustración 8. Ping a máquina 3

Pings desde Router 3

```
R3#ping 148.204.1.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.1.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/41/48 ms
```

Ilustración 9. Ping a máquina 1

```
R3#ping 148.204.1.104

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.1.104, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/42/48 ms
```

Ilustración 10. Ping a máquina 4

```
R3#ping 148.204.2.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.2.102, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 44/303/1076 ms
```

Ilustración 11. Ping a máquina 2

```
R3#ping 148.204.3.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.3.103, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/21/52 ms
```

Ilustración 12. Ping a máquina 3

Pings desde Router 4

```
R4#ping 148.204.1.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.1.101, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 44/304/1068 ms
```

Ilustración 13. Ping a máquina 1

```
R4#ping 148.204.1.104

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.1.104, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 32/307/1104 ms
```

Ilustración 14. Ping a máquina 4

```
R4#ping 148.204.2.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.2.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/48/56 ms
```

Ilustración 15. Ping a máquina 2

```
R4#ping 148.204.3.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 148.204.3.103, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 44/307/1076 ms
```

Ilustración 16. Ping a máquina 3

1 – Bloquear el acceso desde PC1 hacía PC3

Crearemos una ACL en R3 que deniegue el paso de paquetes de PC1.

En el modo de configuración de R3 ingresa el siguiente comando:

R3(config)# **ip access-list standard 10**

Ingresarás al modo de configuración de la ACL estándar, ingresa los siguientes comandos:

R3(conf-std-nacl)# **deny host 148.204.1.101**

R3(conf-std-nacl)# **permit any**

R3(conf-std-nacl)# **exit**

A continuación, la captura de los comandos ingresados

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip access-list standard 10
R3(config-std-nacl)#deny host 148.204.1.101
R3(config-std-nacl)#permit any
R3(config-std-nacl)#exit
```

Ilustración 17. ACL para denegar paquetes de PC1

Ya tenemos la lista que bloquea el tráfico desde PC1, vamos a colocarla en una de las interfaces del router. La colocación queda a criterio del administrador de la red, pero se debe tener mucho cuidado de que no afecte el funcionamiento de la red.

Por ejemplo, vamos a colocarla en la interfaz que conecta con **R1**, en este caso es la GigabitEthernet 0/2. Nota también que se analizará el tráfico que **entra** a la interfaz. Ingresa los siguientes comandos en el modo de configuración de R3.

R3(config)# **interface GigabitEthernet 0/1**

R3(config-if)# **ip access-group 10 in**

```
R3(config)#interface g2/0
R3(config-if)#ip access-group 10 in
R3(config-if)#exit
R3(config)#exit
R3#wr
```

Ilustración 18. Colocando ACL en g2/0

Ahora manda pings de **PC1** a **PC3**. Si configuraste todo bien, deberás un mensaje similar a este:

icmp_seq=1 ttl=254 time=6.014 ms (ICMP type:3,
code:13, Communication administratively prohibited)

A continuación, se presenta captura del ping de PC1 a PC3, vemos que no se mandan paquetes gracias a la ACL configurada

```
PC1> ping 148.204.3.103
*5.5.5.2 icmp_seq=1 ttl=254 time=45.780 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
*5.5.5.2 icmp_seq=2 ttl=254 time=45.205 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
*5.5.5.2 icmp_seq=3 ttl=254 time=47.101 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
```

Intenta mandar pings desde **PC4** y **PC2** a **PC3** verás que llegarán sin problemas.

```
PC4> ping 148.204.3.103
84 bytes from 148.204.3.103 icmp_seq=1 ttl=62 time=60.003 ms
84 bytes from 148.204.3.103 icmp_seq=2 ttl=62 time=60.730 ms
84 bytes from 148.204.3.103 icmp_seq=3 ttl=62 time=64.017 ms
84 bytes from 148.204.3.103 icmp_seq=4 ttl=62 time=63.592 ms
84 bytes from 148.204.3.103 icmp_seq=5 ttl=62 time=61.718 ms
```

Ilustración 19. Ping de PC4 a PC3

```
PC2> ping 148.204.3.103
84 bytes from 148.204.3.103 icmp_seq=1 ttl=62 time=61.514 ms
84 bytes from 148.204.3.103 icmp_seq=2 ttl=62 time=61.374 ms
84 bytes from 148.204.3.103 icmp_seq=3 ttl=62 time=62.286 ms
84 bytes from 148.204.3.103 icmp_seq=4 ttl=62 time=63.904 ms
84 bytes from 148.204.3.103 icmp_seq=5 ttl=62 time=60.714 ms
```

Ilustración 20. Ping de PC2 a PC3

Curiosidades

Ahora, veremos algunas curiosidades sobre esta ACL.

Intenta enviar pings de **PC3** a **PC1**. Si obtienes un *timeout* es normal **¿por qué crees que esto ocurre?**

```
PC3> ping 148.204.1.101
148.204.1.101 icmp_seq=1 timeout
148.204.1.101 icmp_seq=2 timeout
148.204.1.101 icmp_seq=3 timeout
148.204.1.101 icmp_seq=4 timeout
148.204.1.101 icmp_seq=5 timeout
```

Ilustración 21. Ping de PC3 a PC1

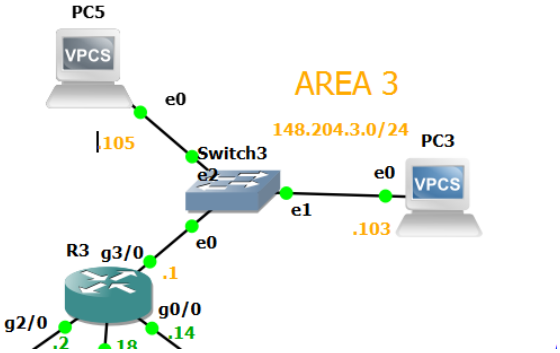
Solución: Recuerda que el ping envía una respuesta una vez que llegó a su destino, pero está respuesta se bloquea por la ACL.

Apaga **R4**. Espera unos segundos a que el protocolo de enrutamiento converja. Ahora Intenta enviar pings de **PC1** a **PC2**. **¿por qué no llegan los pings? ¿cómo lo solucionarías?**

```
PC1> ping 148.204.2.102
*5.5.5.2 icmp_seq=1 ttl=254 time=46.110 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
*5.5.5.2 icmp_seq=2 ttl=254 time=46.156 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
*5.5.5.2 icmp_seq=3 ttl=254 time=46.361 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
```

Solución: No llegan porque la ACL está bloqueando el tráfico en esa interfaz desde PC1 (no importa el destino). Una solución es poner la ACL en la interfaz que conecta al switch (GigabitEthernet 0/3), pero en este caso, deberás ponerla para tráfico saliente.

Agrega otra VPC (**PC5**) en el **Switch3** y asígnale una dirección IP en el mismo segmento de **PC3**. Intenta enviar pings de **PC1** a esa nueva **PC5**. **Los pings** no llegan **¿Por qué? ¿Cómo se solucionaría?**



```
PC1> ping 148.204.3.105
*5.5.5.2 icmp_seq=1 ttl=254 time=46.905 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
*5.5.5.2 icmp_seq=2 ttl=254 time=46.202 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
*5.5.5.2 icmp_seq=3 ttl=254 time=46.904 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
```

Ilustración 22. Ping de PC1 a PC5

Solución: Nuevamente, porque la ACL está bloqueando el tráfico desde PC1 hacía cualquier destino. Aquí puede haber muchas soluciones, una de ellas es utilizar ACL extendidas.

Para ver las soluciones, resalta los espacios en blanco.

2 – Bloquear el acceso desde todo el segmento de red de PC1 hacía PC3

Ahora bloquearemos el acceso de todo el segmento de red, en donde se encuentra **PC1**, a todo el segmento de red en donde está **PC3**.

Primero quitamos la lista de acceso anterior, usando el comando **no**.

R3(config)# **interface GigabitEthernet 0/2**

R3(config-if)# **no ip access-group 10 in**

Quitando la ACL creada anteriormente.

```
R3(config)#interface g2/0
R3(config-if)#no ip access-group 10 in
R3(config-if)#
R3(config-if)#exit
R3(config)#exit
R3#wr
```

Ahora creamos una nueva lista de acceso:

R3(config)# **ip access-list standard 20**

R3(conf-std-nacl)# **deny 148.204.1.0 0.0.0.255**

R3(conf-std-nacl)# **permit any**

R3(conf-std-nacl)# **exit**

```
R3(config)#ip access-list standard 20
R3(config-std-nacl)#deny 148.204.1.0 0.0.0.255
R3(config-std-nacl)#permit any
R3(config-std-nacl)#exit
R3(config)#exit
R3#wr
Building configuration...
```

Esta vez colocaremos la ACL en la interfaz que está conectada al **Switch3** (GigabitEthernet 0/3):

R3(config)# **interface GigabitEthernet 0/3**

R3(config-if)# **ip access-group 20 out**

```
R3(config)#interface g3/0
R3(config-if)#ip access-group 20 out
R3(config-if)#exit
R3(config)#exit
R3#wr
```

Verás que los pings desde **PC1** o **PC4** no llegarán (intenta cambiar las direcciones IP de ambas PC's por otras en el mismo segmento, obtendrás el mismo resultado).

```
PC1> ping 148.204.3.103
*5.5.5.2 icmp_seq=1 ttl=254 time=45.169 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
*5.5.5.2 icmp_seq=2 ttl=254 time=75.705 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
```

Ilustración 23. Ping desde PC1

```
PC4> ping 148.204.3.103
*5.5.5.2 icmp_seq=1 ttl=254 time=46.237 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
*5.5.5.2 icmp_seq=2 ttl=254 time=45.250 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
```

Ilustración 24. Ping desde PC4

Sin embargo, tampoco llegarán los pings que envíes hacía PC5, para solucionar esto usaremos una ACL extendida.

2 – Bloquear el acceso desde todo el segmento de red de PC1 hacía PC3 solamente

Primero quitamos la lista de acceso anterior, usando el comando **no**.

R3(config)# **interface GigabitEthernet 0/3**

R3(config-if)# **no ip access-group 20 out**

```
R3(config)#interface g3/0
R3(config-if)#no ip access-group 20 out
R3(config-if)#exit
R3(config)#exit
```

Ahora creamos una nueva lista de acceso extendida:

R3(config)# **ip access-list extended 110**

R3(conf-std-nacl)# **deny ip 148.204.1.0 0.0.0.255 host 148.204.3.103**

R3(conf-std-nacl)# **permit any any**

R3(conf-std-nacl)# **exit**

```
R3(config)#ip access-list extended 110
R3(config-ext-nacl)#deny ip 148.204.1.0 0.0.0.255 host 148.204.3.103
R3(config-ext-nacl)#permit any any
                           ^
% Invalid input detected at '^' marker.

R3(config-ext-nacl)#permit deny any
                           ^
% Invalid input detected at '^' marker.

R3(config-ext-nacl)#permit any
                           ^
% Invalid input detected at '^' marker.

R3(config-ext-nacl)#permit ip any any
R3(config-ext-nacl)#exit
R3(config)#exit
```

Ilustración 25. Creación ACL extendida

De nuevo la colocaremos en la interfaz que está conectada al **Switch3** (GigabitEthernet 0/3):

R3(config)# **interface GigabitEthernet 0/3**

R3(config-if)# **ip access-group 110 out**

```
R3(config)#interface g3/0
R3(config-if)#ip access-group 110 out
R3(config-if)#exit
R3(config)#exit
R3#wr
Building configuration...
```

Manda pings desde PC1 y PC4 hacía PC3, verás que estos no llegarán. Manda ahora desde PC1 y PC4 a PC5. Esta vez sí llegarán.

A continuación, vemos los pings a PC3

```
PC1> ping 148.204.3.103
*5.5.5.2 icmp_seq=1 ttl=254 time=46.281 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
*5.5.5.2 icmp_seq=2 ttl=254 time=45.986 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
```

Ilustración 26. Ping PC1 a PC3

```
PC4> ping 148.204.3.103
*5.5.5.2 icmp_seq=1 ttl=254 time=45.863 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
*5.5.5.2 icmp_seq=2 ttl=254 time=46.128 ms (ICMP type:3, code:13, Communicati
on administratively prohibited)
```

Ilustración 27. Ping de PC4 a PC3

A continuación, vemos los pings a PC5

```
PC1> ping 148.204.3.105
148.204.3.105 icmp_seq=1 timeout
84 bytes from 148.204.3.105 icmp_seq=2 ttl=62 time=61.601 ms
84 bytes from 148.204.3.105 icmp_seq=3 ttl=62 time=62.182 ms
84 bytes from 148.204.3.105 icmp_seq=4 ttl=62 time=62.290 ms
84 bytes from 148.204.3.105 icmp_seq=5 ttl=62 time=61.857 ms

PC1>
```

Ilustración 28. Ping de PC1 a PC5

```
PC4> ping 148.204.3.105
84 bytes from 148.204.3.105 icmp_seq=1 ttl=62 time=62.366 ms
84 bytes from 148.204.3.105 icmp_seq=2 ttl=62 time=62.090 ms
84 bytes from 148.204.3.105 icmp_seq=3 ttl=62 time=60.290 ms
84 bytes from 148.204.3.105 icmp_seq=4 ttl=62 time=62.399 ms
84 bytes from 148.204.3.105 icmp_seq=5 ttl=62 time=61.488 ms
```

Ilustración 29. Ping de PC4 a PC5

Ahora haremos una lista nombrada estándar que no permitirá el acceso de la subred 148.204.2.0 a la subred 148.204.3.0, permitiendo el acceso a las demás redes.

Primero probamos que se puede hacer ping entre la PC2 y la PC3.

```
PC2> ping 148.204.3.103
148.204.3.103 icmp_seq=1 timeout
84 bytes from 148.204.3.103 icmp_seq=2 ttl=62 time=62.695 ms
84 bytes from 148.204.3.103 icmp_seq=3 ttl=62 time=62.660 ms
84 bytes from 148.204.3.103 icmp_seq=4 ttl=62 time=62.217 ms
84 bytes from 148.204.3.103 icmp_seq=5 ttl=62 time=62.179 ms
```

Ilustración 30. Ping de PC2 a PC3

En la interfaz ethernet 3 del Router R2 ingresaremos el siguiente comando:

Router3(config)#ip access-list standard bloqsubred

Router3(config-std-nacl)#deny 148.204.2.0 0.0.0.255

Router3(config-std-nacl)#permit any

Router3(config-std-nacl)# interface GigabitEthernet3/0

Router3(config-if)#ip access-group bloqsubred out

```
R3(config)#ip access-list standard bloqsubred
R3(config-std-nacl)#deny 148.204.2.0 0.0.0.255
R3(config-std-nacl)#permit any
R3(config-std-nacl)#interface Giga
R3(config-std-nacl)#interface GigaE
R3(config-std-nacl)#interface Gigabit
R3(config-std-nacl)#interface GigabitEthernet3/0
R3(config-if)#ip access-group bloqsubred out
R3(config-if)#
R3#wr
*May  7 18:10:21.835: %SYS-5-CONFIG_I: Configured from console by console
R3#wr
Building configuration...
[OK]
R3#
```

Ilustración 31. Comandos para configurar la lista con nombre

Ahora si intentamos enviar un ping de PC2 a PC3 la ruta estará bloqueada

```
PC2> ping 148.204.3.103
148.204.3.103 icmp_seq=1 timeout
*5.5.5.14 icmp_seq=2 ttl=254 time=45.706 ms (ICMP type:3, code:13, Communication administr
atively prohibited)
148.204.3.103 icmp_seq=3 timeout
*5.5.5.14 icmp_seq=4 ttl=254 time=47.091 ms (ICMP type:3, code:13, Communication administr
atively prohibited)
148.204.3.103 icmp_seq=5 timeout

PC2> ping 148.204.3.103
*5.5.5.14 icmp_seq=1 ttl=254 time=45.093 ms (ICMP type:3, code:13, Communication administr
atively prohibited)
148.204.3.103 icmp_seq=2 timeout
*5.5.5.14 icmp_seq=3 ttl=254 time=45.425 ms (ICMP type:3, code:13, Communication administr
atively prohibited)
148.204.3.103 icmp_seq=4 timeout
*5.5.5.14 icmp_seq=5 ttl=254 time=43.926 ms (ICMP type:3, code:13, Communication administr
atively prohibited)

PC2>
```

Ilustración 32. Ping de PC2 a PC3

Conclusiones

Meza Vargas Brandon David

Esta practica fue muy interesante ya que pude aprender a hacer listas de acceso y listas de acceso nombradas, me pareció muy interesante que con una serie de comando nos muy complicados se pueda tener el control total del acceso o el bloqueo de pings de una red a otra o de un host a otro, pude ver la diferencia entre las listas de acceso normales y las nombradas, las nombradas me parecieron mas sencillas ya que además de tener un nombre identificador, solo se tienen que configurar en la salida de la red a la que queremos poner el bloqueo, en general una practica interesante y que me enseño las listas de acceso.

Romero Angeles Abraham

Esta practica fue un poco mas sencilla que las anteriores ya que ya se tenia practica con el enrutamiento OSPF y pudimos hacerlo de manera mas rápida, en cuanto a las listas de acceso me pareció muy interesante que exista una opción para bloquear los pings de un host en particular o incluso de una red completa, las pruebas detalladas que pide el reporte me ayudo a entender cómo se bloquea el acceso de la red a la salida del router que conecta esa red , aprendí mucho acerca de las listas de acceso y me sigo familiarizando cada vez mas con la herramienta de GNS3 y como trabajar en la consola de cada router.