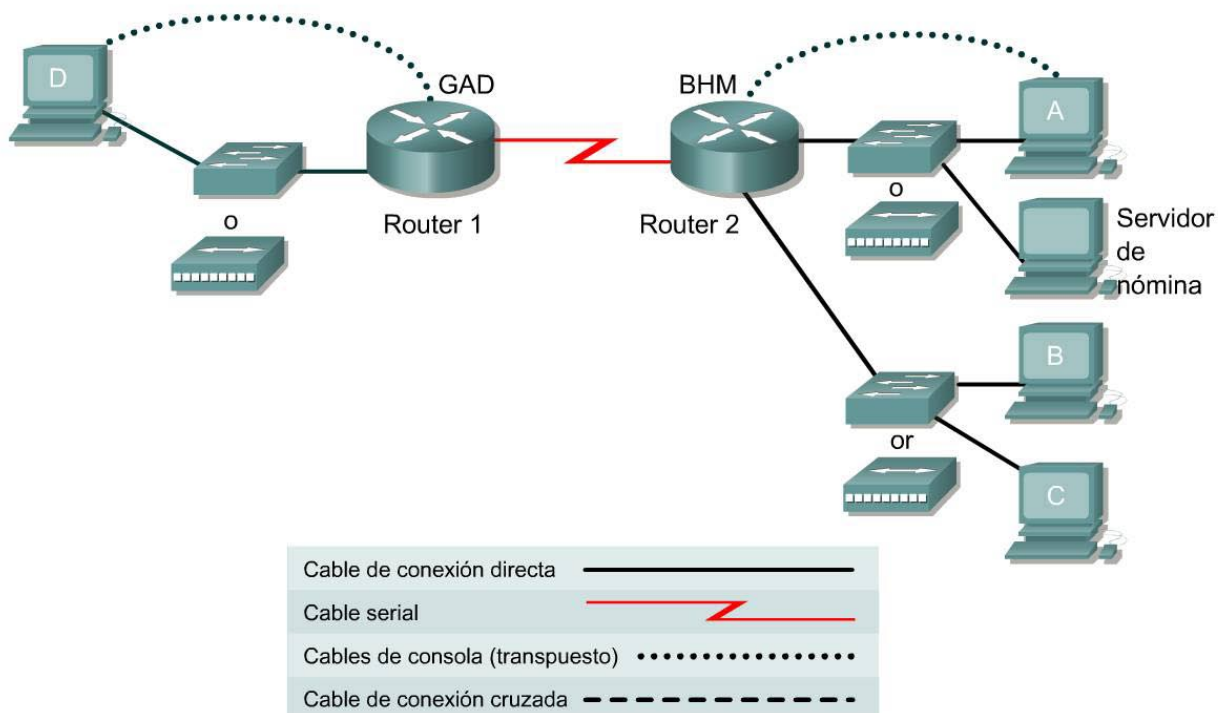


## Práctica de laboratorio 11.2.2b Listas de acceso extendidas sencillas



Designación del router	Nombre del router	Contraseña enable secret	Contraseña enable, VTY y consola	Protocolo de enrutamiento	Sentencias de red RIP
Router 1	GAD	class	cisco	RIP	172.16.0.0
Router 2	BHM	class	cisco	RIP	192.168.1.0 172.16.0.0

Designación del router	Dirección Fast Ethernet 0	Tipo de interfaz Serial 0	Dirección serial 0	Dirección Fast Ethernet 1	Entradas de tabla de host IP
Router 1	172.16.2.1/24	DTE	172.16.1.1/24		BHM
Router 2	192.168.1.18/28	DCE	172.16.1.2/24	192.168.1.33/28	GAD

Host	Dirección IP	Máscara de subred	Gateway
Servidor de nómina	192.168.1.18	255.255.255.240	192.168.1.17
A	192.168.1.19	255.255.255.240	192.168.1.17
B	192.168.1.34	255.255.255.240	192.168.1.33
C	192.168.1.35	255.255.255.240	192.168.1.33
D	172.16.2.2	255.255.255.0	172.16.2.1

## Objetivo

En esta práctica de laboratorio, se configuran listas de acceso extendidas para filtrar tráfico de red a red, de host a red y de red a host.

## Situación

Una empresa de marketing tiene dos instalaciones. La oficina principal es en Birmingham (BHM) y la sucursal es en Gadsden (GAD). El administrador de telecomunicaciones de ambas oficinas necesita planificar e implementar listas de control de acceso para mejorar la seguridad y el desempeño. En la oficina de BHM, hay dos grupos de usuarios de redes. Uno es el grupo Administrativo y el otro es el grupo de Producción, y cada grupo utiliza una red diferente. Las dos redes se interconectan con un router.

La oficina de GAD es una red stub y sólo tiene una LAN conectada a ella.

## Paso 1 Configuraciones básicas del router y el host

- a. Interconecte los routers y los hosts de acuerdo con el diagrama. Configure todos los aspectos básicos del router, como el nombre de host, contraseña enable, acceso de telnet, interfaces del router. Consulte el diagrama y las tablas que aparecen más arriba.

**Nota:** El router BHM requiere dos interfaces Ethernet.

- b. Las configuraciones de cada router deben realizarse de la siguiente manera:

```
BHM#show running-config
```

```
<Resultado omitido>
```

```
hostname BHM
!
enable secret class
!
interface FastEthernet0
 ip address 192.168.1.17 255.255.255.240
!
interface Serial0
 ip address 172.16.1.2 255.255.255.0
 clock rate 56000
!
interface FastEthernet 1
 ip address 192.168.1.33 255.255.255.240
!
router rip
 network 172.16.0.0
 network 192.168.1.0
!
line vty 0 4
 password cisco
 login
!
end
```

```
BHM#
```

```
GAD#show running-config
```

```
<Resultado omitido>
```

```
!
hostname GAD
!
enable password class
!
```

```

interface FastEthernet0
 ip address 172.16.2.1 255.255.255.0
!
interface Serial0
 ip address 172.16.1.1 255.255.255.0
!
router rip
 network 172.16.0.0
!
line vty 0 4
 password cisco
 login
!
no scheduler allocate
end

GAD#

```

- c. Configure los hosts con la información pertinente mediante la información definida anteriormente. Antes de aplicar cualquier tipo de lista de acceso, es importante verificar la conectividad entre sistemas.

Verifique la conectividad haciendo ping a todos los sistemas y routers desde cada sistema.

- d. Todos los hosts deben poder hacer ping los unos a los otros y a las interfaces del router. Si los pings a algunas interfaces no tienen éxito, es necesario encontrar y corregir el problema. Siempre se deben verificar las conexiones de la capa física, ya que con frecuencia son la fuente de los problemas de conectividad. A continuación, verifique las interfaces del router. Asegúrese de que no estén apagadas, configuradas de forma incorrecta, y de que RIP esté configurado correctamente. Finalmente, recuerde que junto con las direcciones IP válidas, los hosts también deben tener gateways por defecto especificados.
- e. Ahora que la infraestructura está armada, es el momento de implementar la seguridad de la red.

## Paso 2 Impedir que los usuarios de Producción accedan a la red GAD

- a. La política de la empresa especifica que sólo el grupo Administrativo debe poder acceder a la oficina de GAD. El acceso a la red por parte del grupo de Producción queda prohibido.
- b. Configure una lista de acceso extendida para permitir que el grupo Administrativo tenga acceso a la oficina de GAD. El grupo de producción no debe tener acceso a la oficina de GAD.
- c. Después de un análisis cuidadoso, se decide que la mejor opción será utilizar una lista de acceso extendida y aplicarla a la interfaz S0 de salida en el router BHM.

**Nota:** Recuerde que cuando se configura la lista de acceso, el router procesa cada sentencia de la lista en el orden en que se creó. No se puede reordenar una lista de acceso, ni saltar, editar o eliminar las sentencias de una lista de acceso numerada. Por este motivo, puede resultar conveniente crear la lista de acceso en un editor de texto como el Bloc de notas y luego pegar los comandos en el router, en lugar de escribirlos directamente en un router.

- d. Introduzca lo siguiente:

```

BHM#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
BHM(config)#access-list 100 deny ip 192.168.1.32 0.0.0.15 172.16.2.0
0.0.0.255

```

- e. Esta sentencia define una lista de acceso extendida denominada "100". Denegará el acceso ip por parte de cualquier usuario de la red 192.168.1.32 – 192.168.1.47 si intentan acceder a la red 172.16.2.0. Aunque se puede definir un acceso menos específico, esta lista de acceso podría

permitir a los usuarios de producción acceder a otros sitios (de estar disponibles) a través de la interfaz S0.

- f. Recuerde que existe un comando `deny all` implícito al final de cada lista de acceso. Debemos asegurarnos de que el grupo administrativo tenga permiso de acceder a la red de GAD. Aunque es posible imponer más restricciones, en este caso, simplemente dejaremos pasar cualquier otro tráfico. Introduzca la siguiente sentencia:

```
BHM(config)#access-list 100 permit ip any any
```

- g. Ahora es necesario aplicar la lista de acceso a una interface. Es posible aplicar la lista a cualquier tráfico entrante que vaya dirigido a la interfaz de red de producción Fa0/1. Sin embargo, si hubiera mucho tráfico entre la red administrativa y la de producción, el router tendría que verificar cada paquete. Existe la posibilidad de que esto implique una carga innecesaria a los recursos del router. Por lo tanto, la lista de acceso se aplica a cualquier tráfico de salida que pase por la interfaz S0 del router BHM.

Introduzca lo siguiente:

```
BHM(config)#interface s0
BHM(config-if)#ip access-group 100 out
```

- h. Verifique que la sintaxis de la lista de acceso sea correcta mediante el comando `show running-config`. A continuación se indican las sentencias válidas que deberían estar en la configuración.

```
interface Serial0
 ip access-group 100 out
```

<Resultado omitido>

```
access-list 100 deny ip 192.168.1.32 0.0.0.15 172.16.2.0 0.0.0.255
access-list 100 permit ip any any
```

- i. Otro comando valioso es el comando `show access-lists`. Un resultado de muestra se presenta a continuación:

```
BHM#show access-lists
Extended IP access list 100
    deny ip 192.168.1.32 0.0.0.15 172.16.2.0 0.0.0.255
    permit ip any any
```

- j. El comando `show access-lists` también muestra contadores, indicando cuántas veces se ha utilizado la lista. Aquí no se muestran los contadores dado que no se ha intentado la verificación aún.

**Nota:** Use el comando `clear access-list counters` para reiniciar los contadores de lista de acceso

- k. Ahora pruebe la lista de acceso verificando la conectividad a la red GAD por parte de los hosts administrativo y de producción.

¿Puede hacer ping el host de producción (B) al host de GAD (D)?

¿Puede hacer ping el host de producción (C) al host de GAD (D)?

¿Puede hacer ping el host administrativo (A) al host de GAD (D)?

¿Puede hacer ping el host de producción (B) al host de administración (A)?

¿Puede hacer ping el host de producción (B) a la interfaz serial del router de GAD?

- l. Los hosts de producción (B) y (C) deben poder hacer ping al host administrativo (A) y la interfaz serial del router de GAD. Sin embargo, no deben poder hacer ping al host de GAD (D). El router debe devolver un mensaje de respuesta al host que indique “Destination net unreachable” (Red destino inalcanzable).

Emita el comando `show access-lists`. ¿Cuántas coincidencias hay? \_\_\_\_\_

**Nota:** El comando `show access-lists` muestra la cantidad de coincidencias por línea. Por lo tanto, es posible que la cantidad de coincidencias de denegación parezca extraña, hasta darse cuenta de que los pings coinciden con la sentencia de denegar y la sentencia de permitir.

- m. Para ayudar a comprender de qué manera opera la lista de acceso, ejecute periódicamente el comando `show access-lists`.

### Paso 3 Permitir que un usuario de Producción acceda a la red GAD

- a. Se recibe una llamada de un usuario del grupo de producción (B). Esa persona es el responsable de intercambiar ciertos archivos entre la red de producción y la red de GAD. Es necesario modificar la lista de acceso extendida para permitirle que acceda a la red de GAD, denegando por otro lado el acceso de todos los demás de la red de producción.
- b. Configure una lista de acceso extendida para permitir el acceso de ese usuario a GAD.
- c. Desafortunadamente, no se puede reordenar una lista de acceso, ni saltar, editar o eliminar las sentencias de una lista de acceso numerada. Si se intenta eliminar una sola sentencia de una lista de acceso numerada, se eliminará la lista completa.
- d. Por lo tanto, es necesario eliminar la lista de acceso extendida inicial y crear una nueva. Para eliminar la lista de acceso 1010, introduzca lo siguiente:

```
BHM#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BHM(config)#no access-list 100
```

Verifique que se haya eliminado con el comando `show access-lists`.

- e. Ahora, cree una nueva lista de acceso extendida. Siempre se debe filtrar desde lo más específico hasta lo más general. Por lo tanto la primera línea de la lista de acceso debe permitir que el host de producción (B) acceda a la red de GAD. El resto de la lista de acceso debe ser igual a la que se introdujo anteriormente.
- f. Para filtrar el host de producción (B), la primera línea de la lista de acceso debe ser la siguiente:

```
BHM(config)#access-list 100 permit ip host 192.168.1.34 172.16.2.0
0.0.0.255
```

Por lo tanto, la lista de acceso permite que el host de producción (B) acceda a la red de GAD.

- g. Ahora deniegue acceso a los demás hosts de producción a la red de GAD y permita el acceso a cualquier otro. Consulte el paso anterior para saber las siguientes dos líneas de la configuración.

El comando **show access-list** muestra un resultado similar a lo siguiente:

```
BHM#show access-lists
Extended IP access list 100
    permit ip host 192.168.1.34 172.16.2.0 0.0.0.255
    deny ip 192.168.1.32 0.0.0.15 172.16.2.0 0.0.0.255
    permit ip any any
BHM#
```

- h. Ahora pruebe la lista de acceso verificando la conectividad a la red GAD por parte de los hosts administrativo y de producción.

¿Puede hacer ping el host de producción (B) al host de GAD (D)?

---

¿Puede hacer ping el host de producción (C) al host de GAD (D)?

---

El host de producción (B) ahora debe poder hacer ping al host de GAD (D). Sin embargo, todos los demás hosts de producción (C) no deben poder hacer ping al host de GAD (D). Nuevamente, el router debe devolver un mensaje de respuesta al host que indique “Destination net unreachable” (Red destino inalcanzable).

#### Paso 4 Permitir que los usuarios de GAD accedan al servidor de nómina de la Administración

- El grupo de administración tiene el servidor de nómina. Periódicamente, los usuarios de la oficina de GAD necesitan acceso FTP y HTTP al servidor de nómina para cargar y descargar informes de nómina.
- Configure una lista de acceso extendida para permitir que los usuarios de la oficina de GAD tengan acceso FTP, HTTP al servidor de nómina solamente. Se decide también permitir el acceso ICMP para que ellos hagan ping al servidor. Los usuarios de GAD no deben poder hacer ping a ningún otro host en la red de Administración.
- No conviene que haya tráfico innecesario entre los sitios, por lo tanto se decide configurar una lista de acceso extendida en el router de GAD.
- Tome en cuenta que de vez en cuando haría falta acceso EXEC privilegiado a GAD. Por este motivo, se ha configurado el acceso Telnet a GAD. De lo contrario, sería necesario viajar a la oficina de GAD para configurarlo.
- Haga Telnet al router de GAD desde el router de BHM y entre al modo enable. Haga diagnóstico de fallas según sea necesario.

**Nota:** Una trampa en la que se puede caer al configurar las listas de acceso en los routers remotos es “dejarse afuera” de forma inadvertida. Esto no es un problema grave cuando el router se encuentra en una ubicación física local. Sin embargo, podría ser un problema enorme si el router se encuentra físicamente ubicado en otro punto geográfico.

- Por este motivo, se recomienda enfáticamente que se emita el comando **reload in 30** en el router remoto. Esto recarga automáticamente el router remoto dentro de los 30 minutos después de emitir el comando. Así, si el administrador se queda bloqueado, con el tiempo se recargará la configuración anterior, permitiendo el acceso al router nuevamente. Use el comando **reload cancel** para desactivar la recarga pendiente.

- g. Configure una lista de acceso extendida para permitir el acceso FTP al servidor de nómina. La sentencia de la lista de acceso debe ser similar al siguiente:

```
GAD(config)#access-list 110 permit tcp any host 192.168.1.18 eq ftp
```

Esta línea permitirá que cualquier host de la red de GAD tenga acceso FTP al servidor de nómina, en la dirección 192.168.1.18.

¿Qué se podría haber definido en lugar de usar la palabra clave “any”?

---

¿Qué se podría haber definido en lugar de usar la palabra clave “host”?

---

¿Qué se podría haber definido en lugar de usar la palabra clave “ftp”?

---

- h. Ahora, configure la línea siguiente de la lista de acceso para permitir el acceso HTTP al servidor de nómina. La sentencia de la lista de acceso debe ser similar al siguiente:

```
GAD(config)#access-list 110 permit tcp any host 192.168.1.18 eq www
```

Esta línea permitirá que cualquier host de la red de GAD tenga acceso FTP al servidor de nómina, en la dirección 192.168.1.18.

¿Qué otra cosa se podría haber definido en lugar de usar la palabra clave “www”?

---

- i. Ahora, configure la línea siguiente de la lista de acceso para permitir el acceso HTTP al servidor de nómina. La sentencia de la lista de acceso debe ser similar al siguiente:

```
GAD(config)#access-list 110 permit icmp any host 192.168.1.18
```

Esta línea permitirá que cualquier host de la red de GAD haga ping al servidor de nómina, en la dirección 192.168.1.18.

- j. Por último, ningún usuario de GAD debe poder acceder a ningún otro host en la red de Administración. Aunque no es obligatorio, siempre es buena idea incluir una sentencia deny. La sentencia sirve como recordatorio y hace que sea más fácil comprender la lista de acceso. La sentencia de la lista de acceso debe ser similar al siguiente:

```
GAD(config)#access-list 110 deny ip any 192.168.1.16 0.0.0.15
```

- k. Ahora es necesario aplicar la lista de acceso a una interface. Para reducir el tráfico WAN no deseado, se decide aplicar la lista de acceso a cualquier tráfico de salida a través de la interfaz S0 del router de GAD.

Introduzca lo siguiente:

```
GAD(config)#interface s0  
GAD(config-if)#ip access-group 110 out
```

- I. Ahora pruebe la lista de acceso verificando la conectividad al servidor de nómina por parte del host de GAD (D).

¿Puede hacer ping el host de GAD (D) al servidor de nómina?

---

¿Puede hacer ping el host de GAD (D) al host (A)?

---

El host de GAD debe poder hacer ping al servidor de nómina solamente. El router debe devolver el mensaje "Destination net unreachable" (Red destino no alcanzable) al intentar hacer ping al host administrativo (D).

### Paso 5 Documente la ACL

- a. Como parte de toda la gestión de red, es necesario elaborar documentación. Agregue comentarios adicionales al archivo de texto creado para la configuración. Este archivo también debe contener resultados de los comandos **show access-lists** y **show ip interface**.
- b. El archivo debe guardarse junto con la demás documentación de red. La convención de nombres de archivos debe reflejar la función del archivo y la fecha de implementación.
- c. Con eso, se ha completado esta práctica de laboratorio de ACL extendida.
- d. Al terminar, borre la configuración inicial de los routers, quite y guarde los cables y el adaptador. Termine la sesión y apague el router.