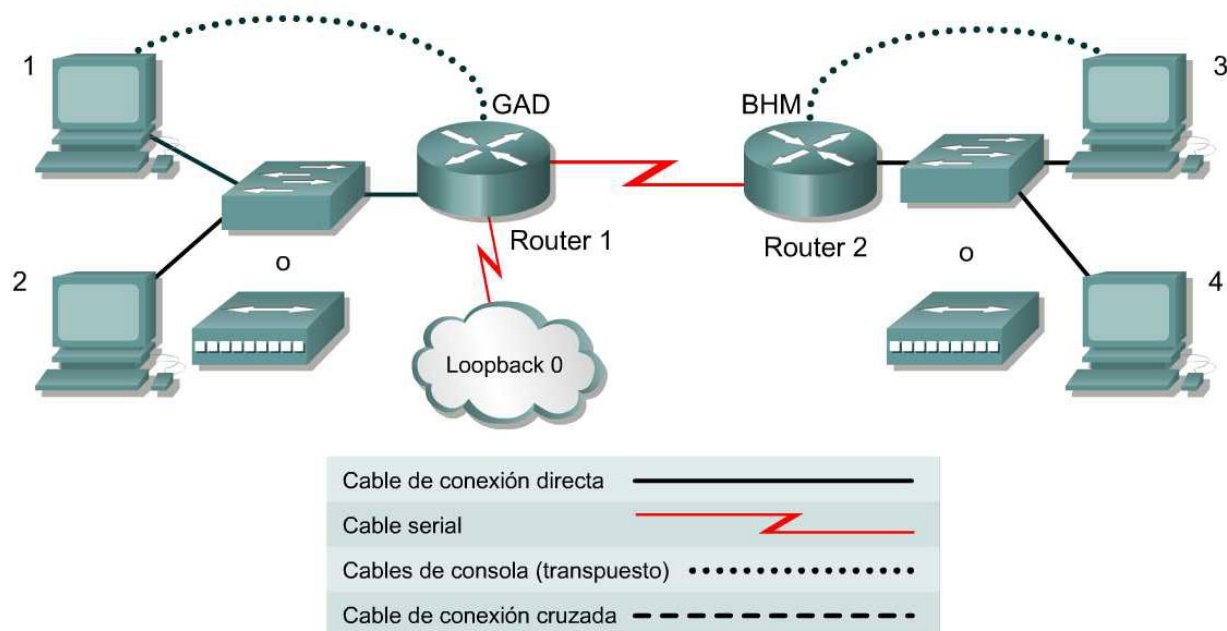


## Práctica de laboratorio 11.2.6 Restricción VTY



Nombre del router	Dirección FA0/0	Tipo de interface	Dirección S0/0	Dirección LO0	Enrutamiento	Contraseña enable	Contraseña VTY
GAD	192.168.1.1 /24	DCE	192.168.2.1 /24	172.16.1.1 /24	RIP	cisco	class
BHM	192.168.3.1 /24	DTE	192.168.2.2 /24	--	RIP	cisco	class

Host	Dirección IP	Máscara de subred	Gateway
1	192.168.1.2	255.255.255.0	192.168.1.1
2	192.168.1.3	255.255.255.0	192.168.1.1
3	192.168.3.2	255.255.255.0	192.168.3.1
4	192.168.3.3	255.255.255.0	192.168.3.1

### Objetivo

Usar los comandos access-class y line para controlar el acceso telnet al router.

### Situación

La sede de la empresa en Gadsden (GAD) ofrece servicios a las sucursales, como la oficina de Birmingham (BHM). Sólo los sistemas dentro de la red local deben poder hacer telnet al router. Para hacer esto se creará la lista de acceso estándar que permite que los usuarios de la red local hagan telnet al router local. La lista de acceso entonces se aplicará a las líneas de la Terminal Virtual (vty).

## Paso 1 Interconexión básica del router

- a. Interconecte los routers de acuerdo al diagrama.

## Paso 2 Configuración básica

- a. Es posible que el router tenga configuraciones de un uso anterior. Por este motivo, borre la configuración inicial y vuelva a cargar el router para eliminar cualquier configuración residual. Mediante la información que aparecía en las tablas, configure el router y las configuraciones del host y verifique la conectividad haciendo ping a todos los sistemas y routers de cada sistema.
- b. Entonces haga telnet desde los hosts al router local y al router remoto.

## Paso 3 Crear la lista de acceso que representa a la LAN Gadsden

- a. La red de área local de Gadsden tiene una dirección de red de 192.168.1.0 /24. Para crear la lista de acceso para permitir esto use los siguientes comandos:

```
GAD(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

## Paso 4 Aplicar la lista de acceso para permitir sólo la LAN Gadsden

- a. Ahora que se ha creado la lista para representar el tráfico, hace falta aplicarla a las líneas vty. Esto restringirá cualquier acceso de telnet al router. Si bien se pueden aplicar por separado a cada interfaz, es más fácil aplicar la lista a todas las líneas vty con una sola sentencia. Esto se hace entrando al modo de interfaz para todas las 5 líneas con el comando de configuración global `line vty 0 4`.

Para el router de Gadsden escriba:

```
GAD(config)#line vty 0 4
GAD(config-line)#access-class 1 in
GAD(config-line)#^Z
```

## Paso 5 Probar la restricción

- a. Pruebe la funcionalidad de la ACL estableciendo una conexión telnet desde el host y verifique que la lista de acceso trabaja correctamente.

```
[ ] verify that host 1 CAN telnet GAD
[ ] verify that host 2 CAN telnet GAD
[ ] verify that host 3 CANNOT telnet GAD
[ ] verify that host 4 CANNOT telnet GAD
```

## Paso 6 Crear las restricciones para el router Birmingham

- a. Repita el proceso anterior para restringir el acceso telnet a BHM. De esta manera, la restricción sólo debe permitir que los hosts de la LAN Birmingham hagan telnet a BHM
- b. Pruebe la funcionalidad de la ACL estableciendo una conexión telnet desde el host y verifique que la lista de acceso trabaja correctamente.

```
[ ] verify that host 1 CANNOT telnet BHM
[ ] verify that host 2 CANNOT telnet BHM
[ ] verify that host 3 CAN telnet BHM
[ ] verify that host 4 CAN telnet BHM
```

## Paso 7 Documente la ACL

- a. Como parte de toda la gestión de red, es necesario elaborar documentación. Capture una copia de la configuración y agregue comentarios adicionales para explicar el propósito del código ACL.
- 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. Al terminar, borre la configuración inicial de los routers, quite y guarde los cables y el adaptador. Termine la sesión y apague el router.