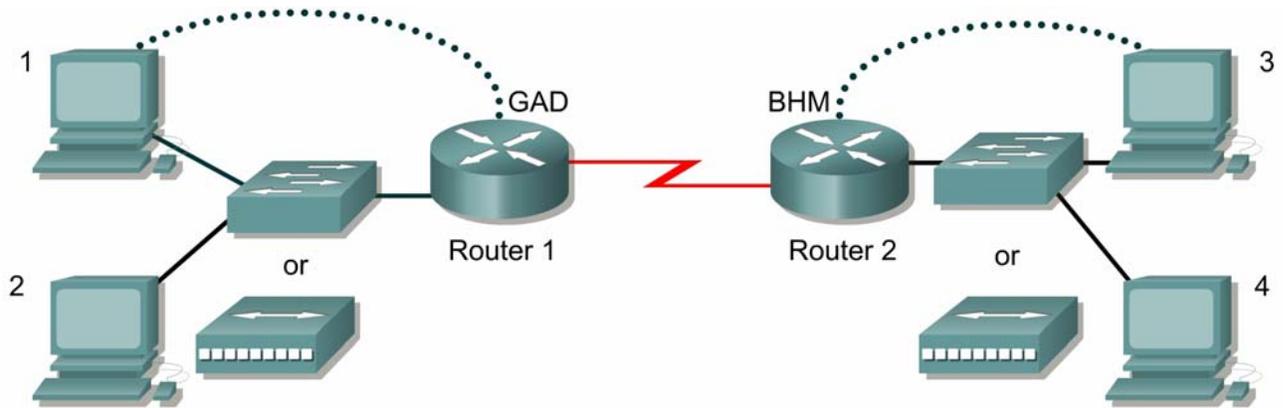


### Lab 11.2.6 VTY Restriction



Straight-through cable	—————
Serial cable	————— ⚡
Console (Rollover)	.....
Crossover cable	- - - - -

Router Name	FA0/0 Address	Interface Type S0/0	S0/0 Address	LO0 Address	Routing	Enable password	VTY password
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	IP Address	Subnet Mask	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

### Objective

Use the access-class and line commands to control Telnet access to the router.

### Scenario

The company home office in Gadsden (GAD) provides services to branch offices such as the Birmingham (BHM) office. Only systems within the local network should be able to Telnet to the router. To do this, a standard access-list will be created that will permit users on network the local

network to Telnet to local router. The access-list will then be applied to the Virtual Terminal (vty) lines.

### Step 1 Basic Router Interconnection

- a. Interconnect the routers as shown in the diagram.

### Step 2 Basic Configuration

- a. The router may contain configurations from a previous use. For this reason, erase the startup configuration and reload the router to remove any residual configurations. Using the information previously in the tables, setup the router and host configurations and verify reachability by pinging all systems and routers from each system.
- b. Telnet from the hosts to both the local router and the remote router.

### Step 3 Create the Access List that Represents the Gadsden LAN

- a. The Local Area Network in Gadsden has a network address of 192.168.1.0 /24. To create the access list to permit this use the following commands:

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

### Step 4 Apply the Access List to Permit Only the Gadsden LAN

- a. Now that the list is created to represent traffic, it needs to be applied to the vty lines. This will restrict any Telnet access to the router. While these could be applied separately to each interface, it is easier to apply the list to all vty lines in one statement. This is done by enter the interface mode for all 5 line with the global config command `line vty 0 4`.

For the Gadsden router type:

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

### Step 5 Test the Restriction

- a. Test the functionality of the ACL by trying to telnet to the host and verify that the access-list is working correctly.

```
[ ] 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
```

### Step 6 Create the Restrictions for Birmingham Router

- a. Repeat the above process to restrict the Telnet access to BHM. Thus restriction should allow only hosts in the Birmingham LAN to Telnet to BHM.
- b. Test the functionality of the ACL by trying to telnet to the host and verify that it is to be permitted or denied as appropriate.

```
[ ] 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
```

## Step 7 Document the ACL

- a. As a part of all network management, documentation needs to be created. Capture a copy of the configuration and add additional comments to explain the purpose to ACL code.
- b. The file should be saved with other network documentation. The file naming convention should reflect the function of the file and the date of implementation.
- c. Once finished, erase the start-up configuration on routers, remove and store the cables and adapter. Also logoff and turn the router off.