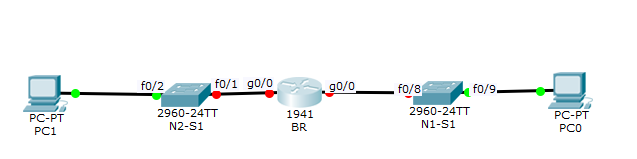
Topology:

**Requirements**

1. **Configure PCs host IP settings**
2. **Configure the basic router**
3. Prevent the router from attempting to translate incorrectly entered commands
4. Configure host names as shown in the topology.
5. Configure interface IP addresses .
6. set ***ciscoprv*** *as* the privilege password and ***ciscocon*** as the console passwords .
7. Vty lines accept Telnet connection only. Set ***ciscovty*** as the password for these lines.
8. Test vty connection using a telnet command and make any required setting to complete this connection.
9. **Configure the switches:**
   1. **The initial settings:**

* Configure host names as shown in the topology.
* Banner that includes the word warning
* Console port login and password ***cPass***
* Encrypted enable password of ***pPass***
* Encrypt plain text passwords
* Management interface addressing
  1. **Configure SSH to secure remote access with the following settings:**
* RSA key-pair parameters to support SSH version 2
* *Set SSH version 2*
* VTY lines only accept SSH connections and use local login for authentication
* Test this secure connection and make any required setting to complete this connection.

**Note : To configure the above topology , use valid IPs of the private address ranges.**