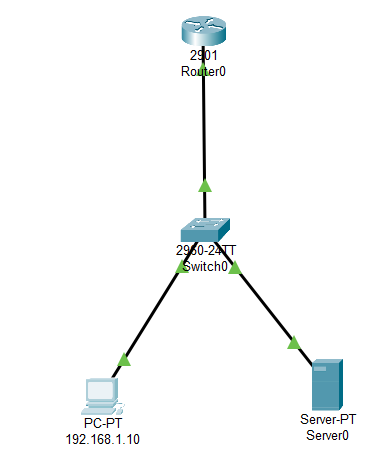
**11. Implement ACLs to restrict traffic based on source and destination ports. Test rules by simulating legitimate and unauthorized traffic.**

* Created a network with a router, switch, a PC and a server.
* Connected PC and server to the switch and the switch to the router.
* Assigned IP addresses to PC, server and configure the router interface.
* Created an extended ACL to allow HTTP (port 80) from PC1 to Server.
* Blocked Telnet (port 23) from PC1 to server.
* Allowed all other traffic.
* Applied the ACL to the router’s interface in the inbound direction.
* Tested HTTP access from PC1 to server using a web browser (worked).
* Tested Telnet access from PC1 to server using the command prompt (failed).

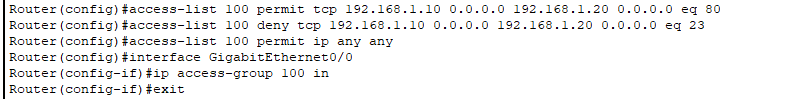
**Setting Up:**

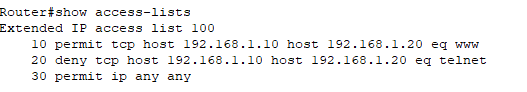
****

**Configuring the Access-Lists:**

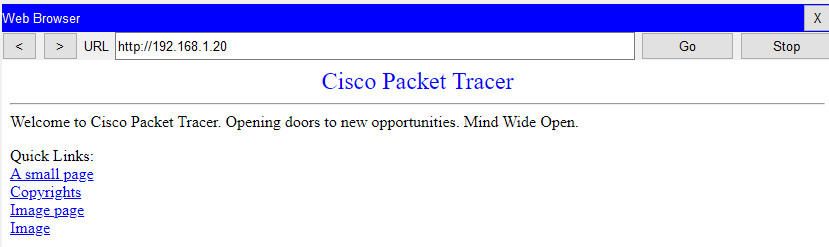
**Allow – Port 80 (HTTP)**

**Deny – Port 23 (TELNET)**

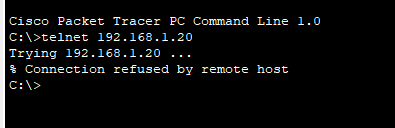
****

****

**Trying HTTP:**

****

**Trying to access TELNET:**

****