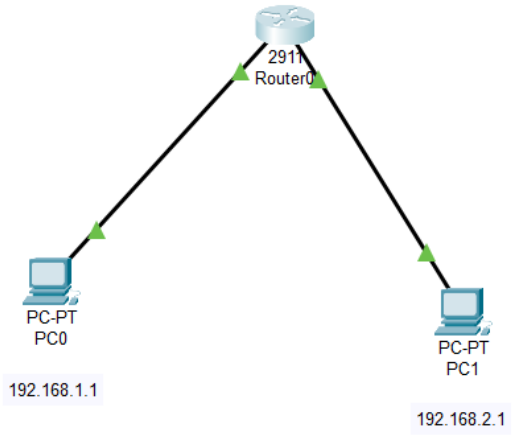
Q11. Implement ACLs to restrict traffic based on source and destination ports. Test rules by simulating legitimate and unauthorized traffic.



Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Translating "enbable"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit ip host 192.168.1.100 any
Router(config)#access-list 100 deny ip host 192.168.2.100 any
Router(config)#access-list 100 permit ip any any
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Router#
Router#enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/1ip access-group 100 in^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
ip access-group 100 in
          ^
% Invalid input detected at '^' marker.

Router#enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
```

Test ACL Rules:

In the above setup pc0 -> pc1 ping is success.

Pc1 -> pc0 ping is blocked