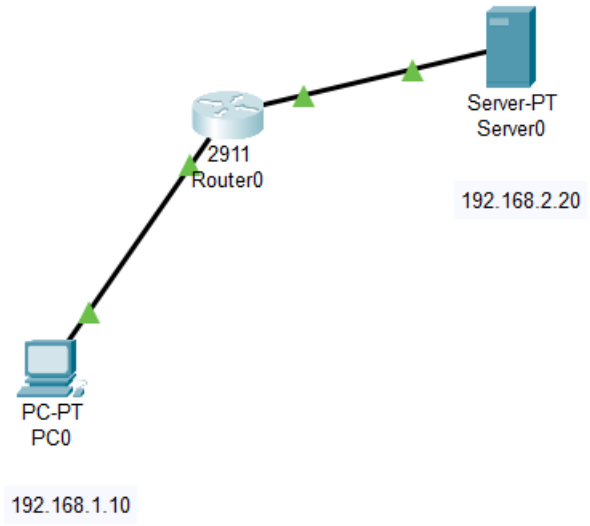
Q13. Create an extended ACL to block specific applications, such as HTTP or FTP traffic. Test the ACL rules by attempting to access blocked services.



Router Configuration

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.1.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.1.254 255.255.255.0
% 192.168.1.0 overlaps with GigabitEthernet0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#p route 192.168.2.0 255.255.255.0 192.168.2.1
% Ambiguous command: "p route 192.168.2.0 255.255.255.0 192.168.2.1"
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write memory
```

Extended ACL to Block HTTP and FTP

Applied the ACL to the Router

ip access-group 101 in (on the inbound interface)

ip access-group 100 out (on the outbound interface)

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 deny tcp any host 192.168.2.20 eq 80
Router(config)#access-list 101 deny tcp any host 192.168.2.20 eq 21
Router(config)#access-list 101 permit ip any any
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Router#
```

Ping from pc to Server is success but telnet 192.168.2.20 80 Fand tp 192.168.2.20 are blockd in ACL

HTTPS and FTP procol are enabled in Server's Service tab manually but the connection is blocked using ACL

```
C:\>ping 192.168.2.20

Pinging 192.168.2.20 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.20: bytes=32 time<1ms TTL=127
Reply from 192.168.2.20: bytes=32 time<1ms TTL=127
Reply from 192.168.2.20: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25%
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```