Extended ACL block :

To create that, I developed a network in Packet tracer which has two PCs (PC0 and PC1).

- a Cisco router (e.g., 2911 series).
- a switch (e.g., 2950 series).
- a server (Server0) to simulate HTTP and FTP services.

The Devices are configured to connect

PC0: 192.168.1.2/24, Gateway: 192.168.1.1

PC1: 192.168.1.3/24, Gateway: 192.168.1.1

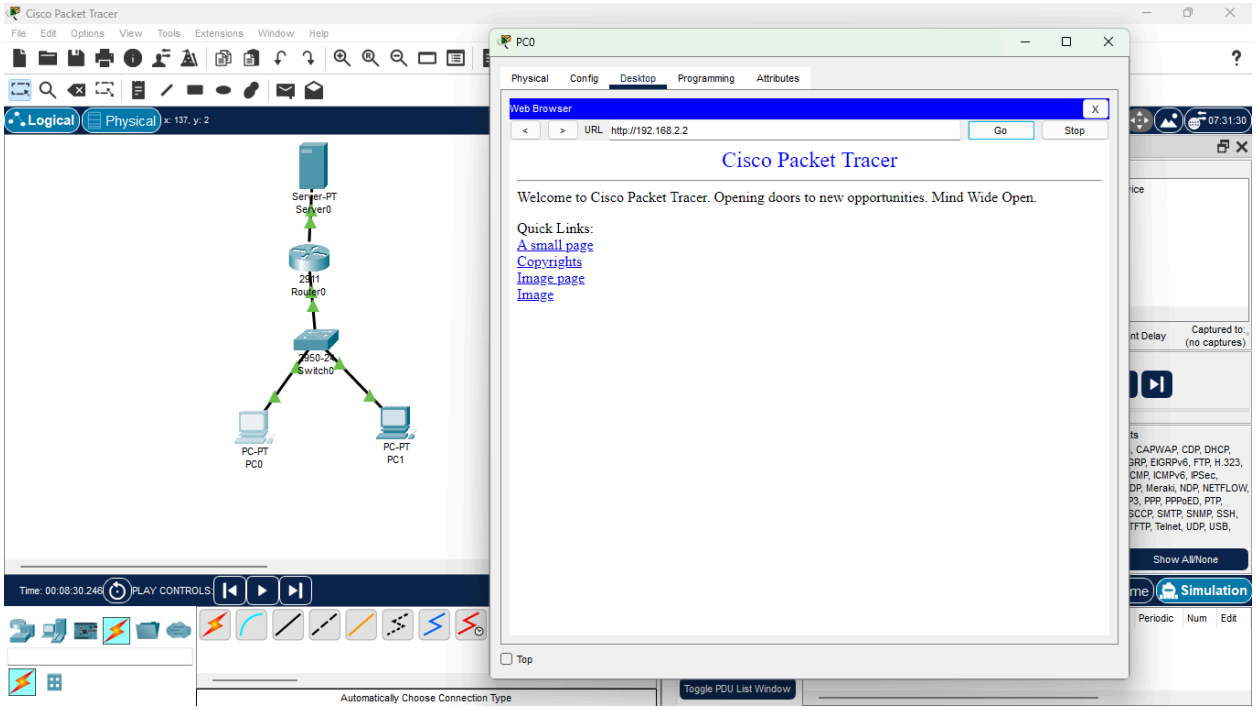
Server0: 192.168.2.2/24, Gateway: 192.168.2.1

Router:

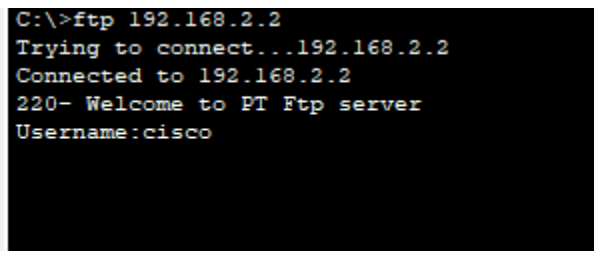
FastEthernet0/0: 192.168.1.1/24 (LAN for PCs)

FastEthernet0/1: 192.168.2.1/24 (LAN for Server)

By Turning on HTTP and FTP service in the server ,



Through Browser we can view this page and telnet can be connected



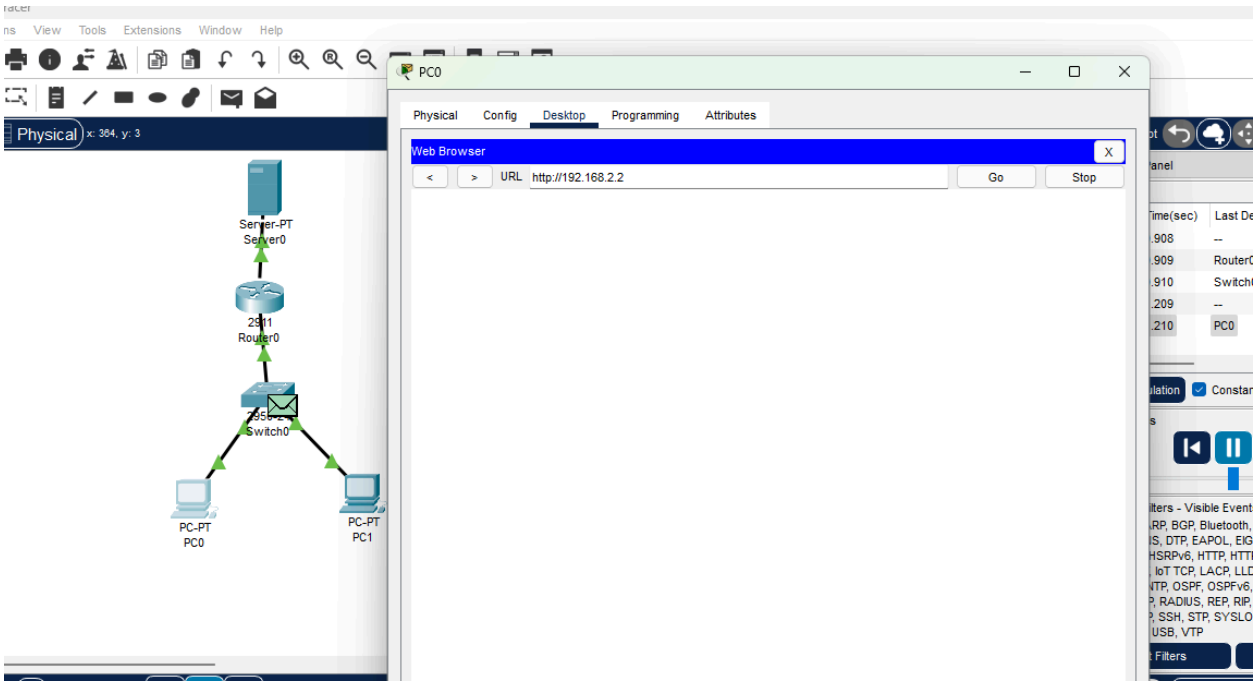
Here,Extended ACLs are numbered 100–199 and allow you to specify source/destination IPs and specific protocols/ports. We'll block HTTP (port 80) and FTP (ports 20 and 21) traffic from the 192.168.1.0/24 network (PCs) to the server.

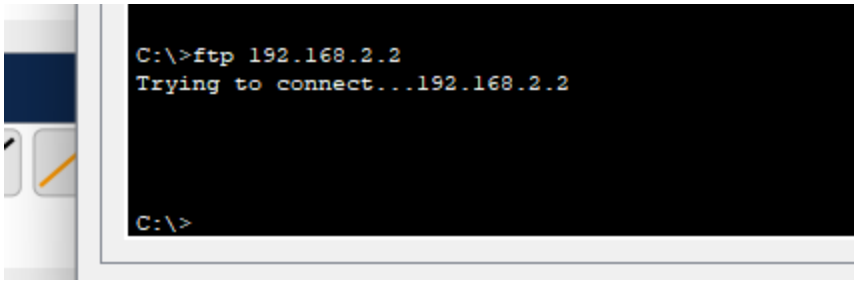
CLI passed :

access-list 100 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 80
access-list 100 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 21
access-list 100 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 20
access-list 100 permit ip any any

Since we want to block traffic heading toward the server, apply the ACL on the router's FastEthernet0/1 interface
ip access-group 100 out
Command is passed

Then , we can block HTTP and FTP services but the connectivity of receiving ICMP packets are still visible






```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=9ms TTL=127
Reply from 192.168.2.2: bytes=32 time=6ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 3, Received = 2, Lost = 1 (34% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 9ms, Average = 7ms

Control-C
^C
C:\>
```