# Access Control Lists (ACL)

- **Access Control Lists (ACLs)**: ACLs are sets of rules used across various devices in the OSI model, including routers, firewalls, and switches, to control network traffic. An ACL can operate as a blacklist, which allows all traffic except those specified on the list, or as a whitelist, which denies all traffic except those explicitly allowed.

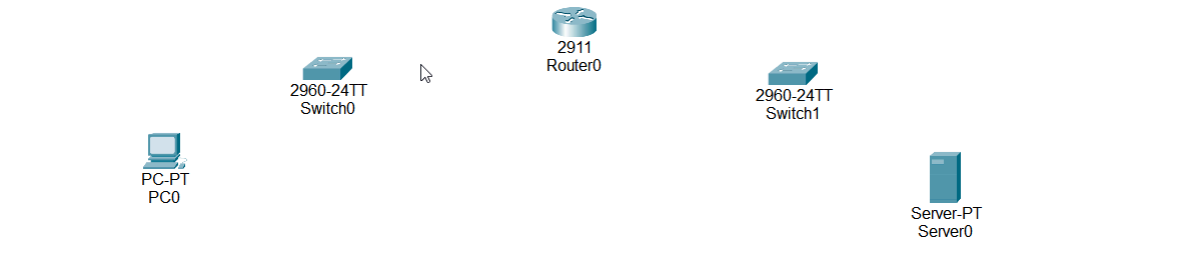
- **Functionality and Configuration of ACLs**: When a packet is received, it is compared against each ACL rule from top to bottom until a match is found. For example, a packet using UDP port 53 from IP 192.168.1.5 to IP 10.0.5.0 would be checked against ACL entries to determine if it matches criteria such as protocol type, source IP, and destination port. If a match is found, subsequent rules are ignored, demonstrating the sequential nature of ACL processing.

## Equipment and Setup

- Cisco Packet Tracer
- A router, two switches, one PC, and one server

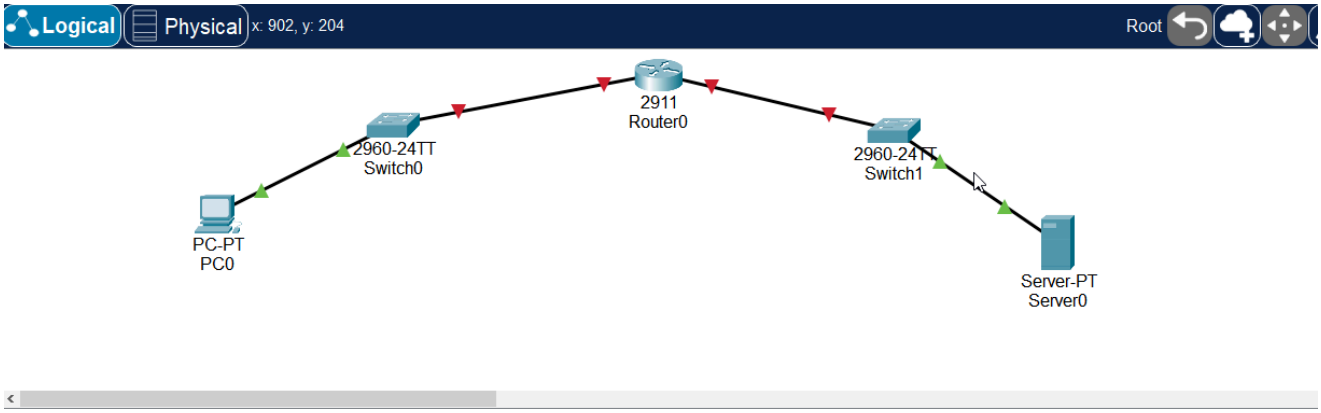
## Step 1: Set Up the Network

1. Place Devices:
    - Add a single router, two switches, a PC, and a server to the workspace.




2. Make Connections:

- Connect the PC to one switch and the server to the other. Connect both switches to different interfaces on the router (e.g., PC to switch to G0/0 on the router, server to switch to G0/1 on the router).




## Step 2: Configure IP Addresses

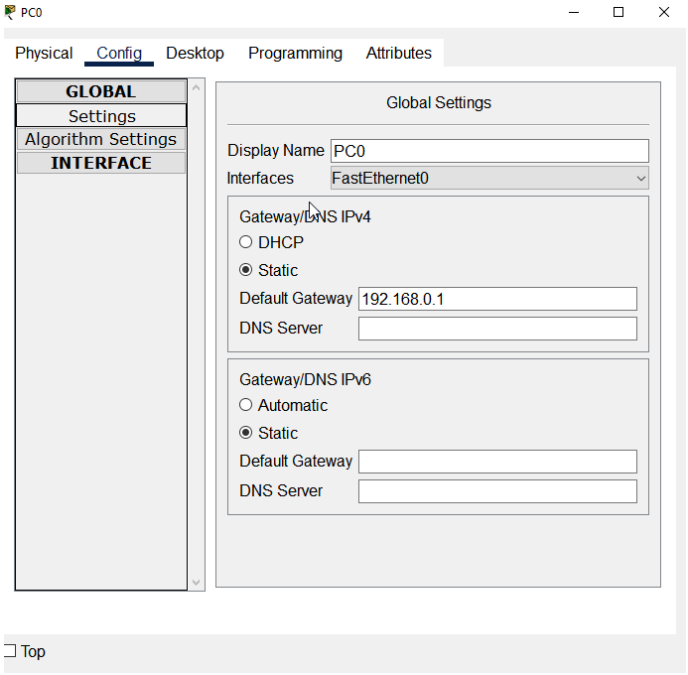
1. Router Configuration:
   - Access the router's CLI and configure IP addresses for each interface

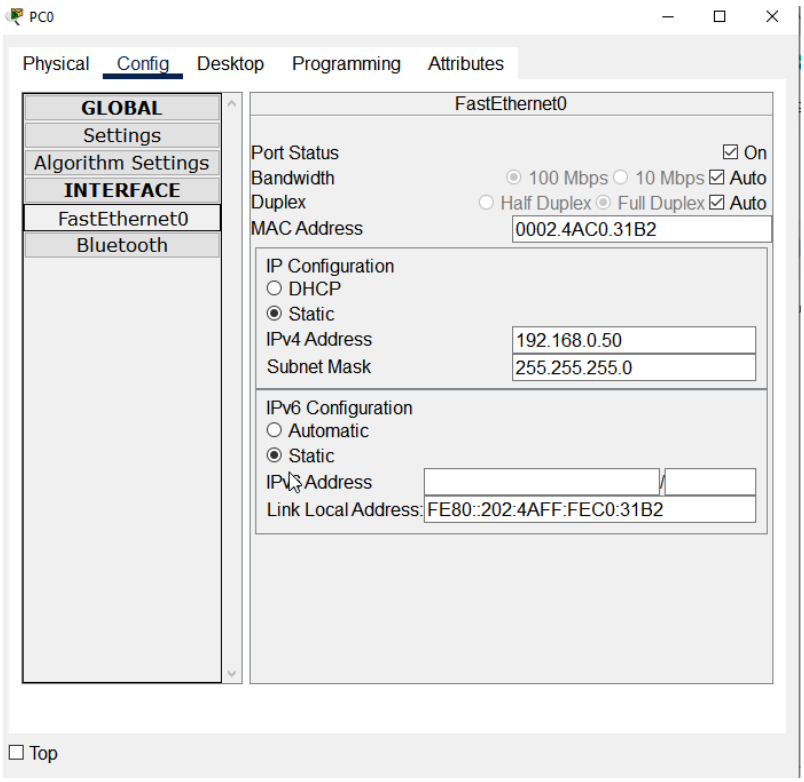
interface G0/0
ip address 192.168.0.1 255.255.255.0
no shutdown
exit
interface G0/1
ip address 172.16.0.1 255.255.255.0
no shutdown
exit
exit

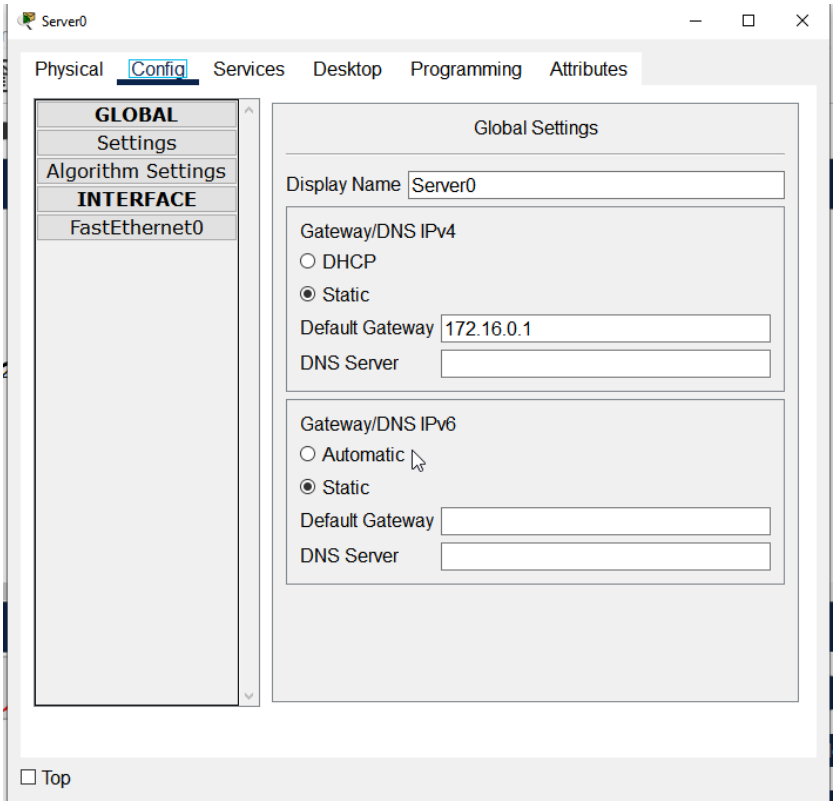
```
Router(config)#interface G0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

Router(config-if)#exit
```

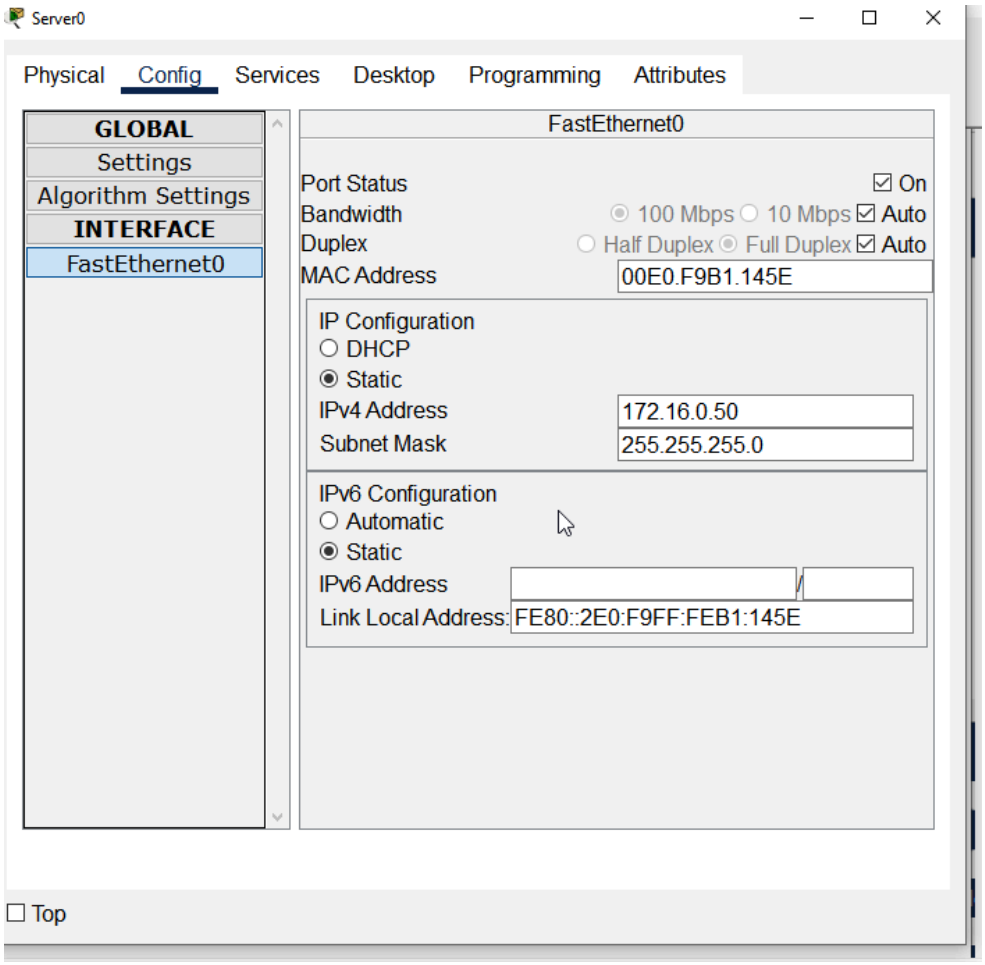
```
Router(config)#interface G0/1
Router(config-if)#ip address 172.16.0.1 255.255.255.0
Router(config-if)#no shutdown

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

Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

1. PC and Server Configuration:
    - Set the PC IP to 192.168.0.50 (with gateway 192.168.0.1).
    - Set the server IP to 172.16.0.50 (with gateway 172.16.0.1).



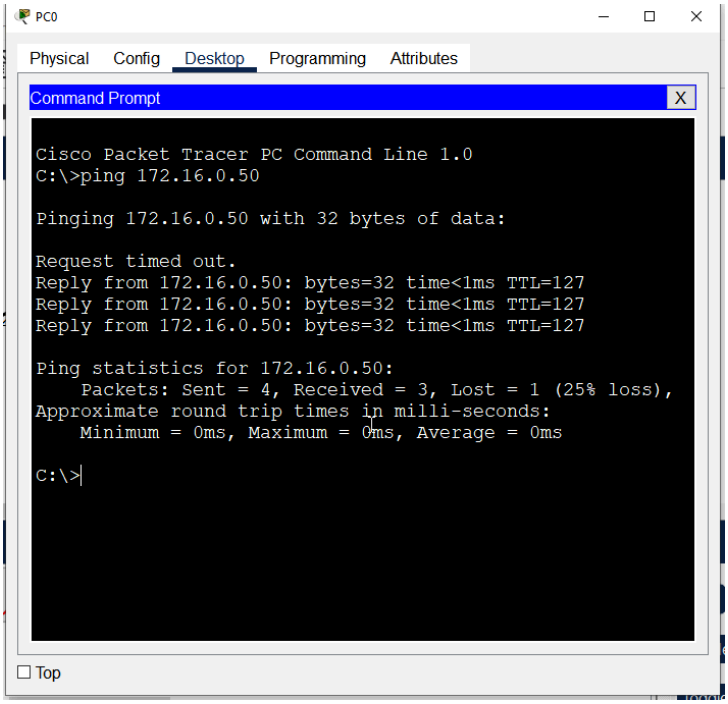

PC0
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0002.4AC0.31B2
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.50
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::202:4AFF:FEC0:31B2
Top

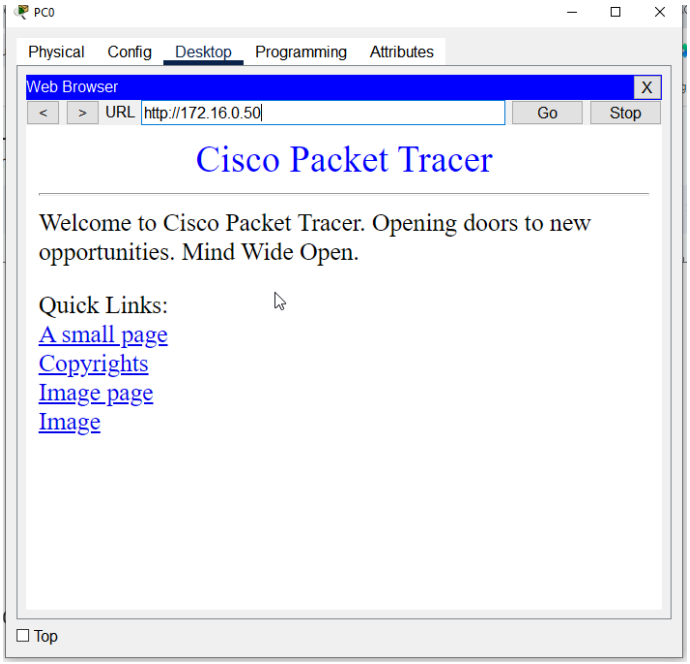

Server0
Physical
Config
Services
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Global Settings
Display Name
Server0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
172.16.0.1
DNS Server
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top




## Step 3: Verify Connectivity

1. Test Ping and Web Access:
    - From the PC, ensure that you can ping the server and access a simple web page hosted on it to confirm both ICMP and HTTP traffic are flowing without ACL intervention.



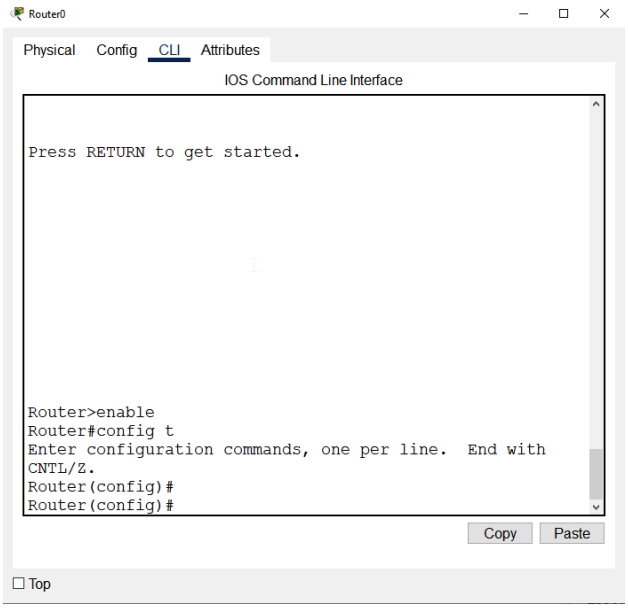




## Step 4: Configure the ACL

1. Create and Apply the ACL:

- Access the router's CLI and enter configuration mode

configure terminal




*Define an ACL that blocks HTTP traffic and apply it to the outgoing interface:*

access-list 100 deny tcp any any eq 80

access-list 100 permit icmp any any

exit

interface G0/0

ip access-group 100 out

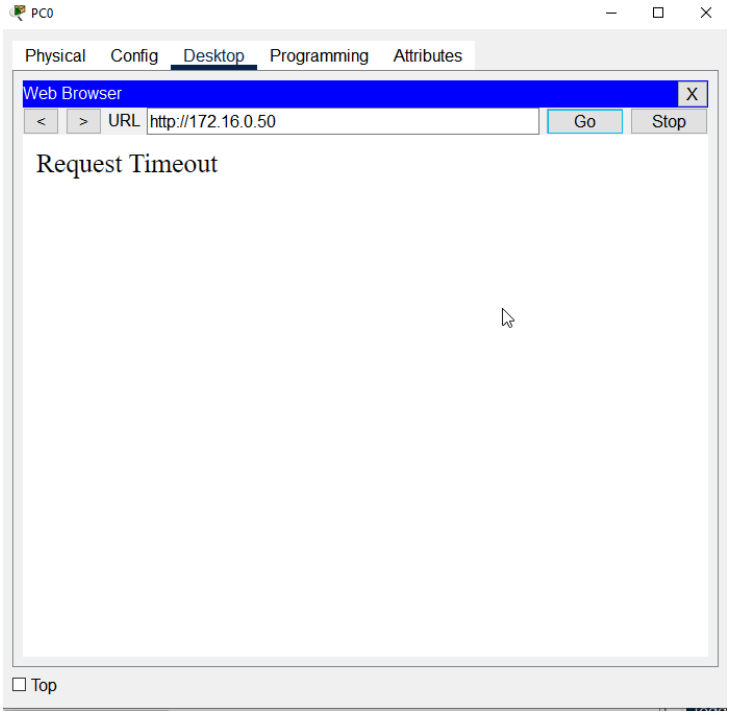
exit

```
Router(config)#access-list 100 deny tcp any any eq 80
Router(config)#access-list 100 permit icmp any any
Router(config)#interface G0/0
Router(config-if)#ip access-group 100 out
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

*This setup denies all TCP traffic on port 80 (HTTP) and permits all ICMP traffic across all networks, while applying the ACL to outgoing traffic on interface G0/0.*

## Step 5: Test the ACL

1. Verify HTTP Blocking and ICMP Allowance:
    - Attempt to access the web page from the PC again; the access should now be blocked.




    - Ping the server from the PC; the ICMP traffic should still succeed, indicating that the ACL is correctly distinguishing between the traffic types.

```
Pinging 172.16.0.50 with 32 bytes of data:

Reply from 172.16.0.50: bytes=32 time<1ms TTL=127
Reply from 172.16.0.50: bytes=32 time<1ms TTL=127
Reply from 172.16.0.50: bytes=32 time<1ms TTL=127
Reply from 172.16.0.50: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

# Conclusion

This guide demonstrates configuring and applying an ACL on a router in Cisco Packet Tracer, specifically to control and restrict types of traffic based on protocol and port number, illustrating essential skills in network security management.