

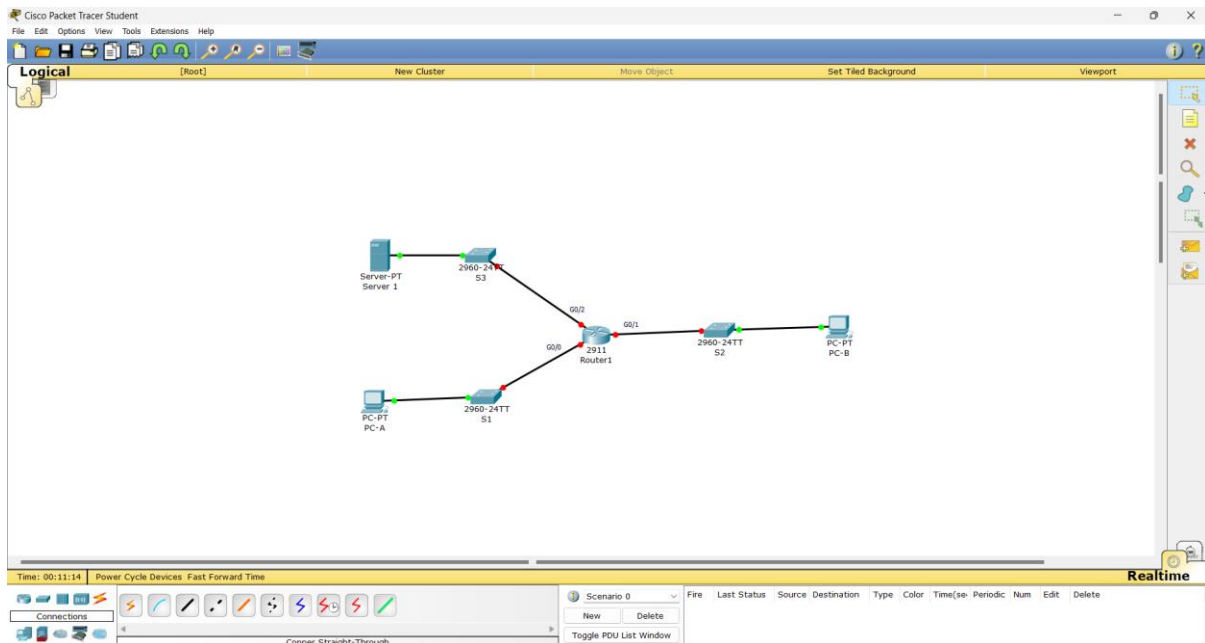
Date: 24/01/2024

Security in Computing

Practical 3A:

Aim: Configure Extended ACLs.

Topology:



➤ Assign IP Addresses:

PC-A

Physical Config Desktop Custom Interface

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IP Address 172.22.34.66

Subnet Mask 255.255.255.224

Default Gateway 172.22.34.65

DNS Server

PC-B

Physical Config Desktop Custom Interface

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IP Address 172.22.34.98

Subnet Mask 255.255.255.240

Default Gateway 172.22.34.97

DNS Server

Server 1

Physical Config Services Desktop Custom Interface

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IP Address: 172.22.34.62

Subnet Mask: 255.255.255.192

Default Gateway: 172.22.34.1

DNS Server:

Router1

Physical Config CLI

GigabitEthernet0/0

Port Status ☒

Bandwidth: ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps

Duplex: ☐ Half Duplex ☒ Full Duplex

MAC Address: 00E0.8F9D.EC01

IP Configuration

IP Address: 172.22.34.65

Subnet Mask: 255.255.255.224

Tx Ring Limit: 10

Router1

Physical Config CLI

GigabitEthernet0/1

Port Status ☒

Bandwidth: ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps

Duplex: ☐ Half Duplex ☒ Full Duplex

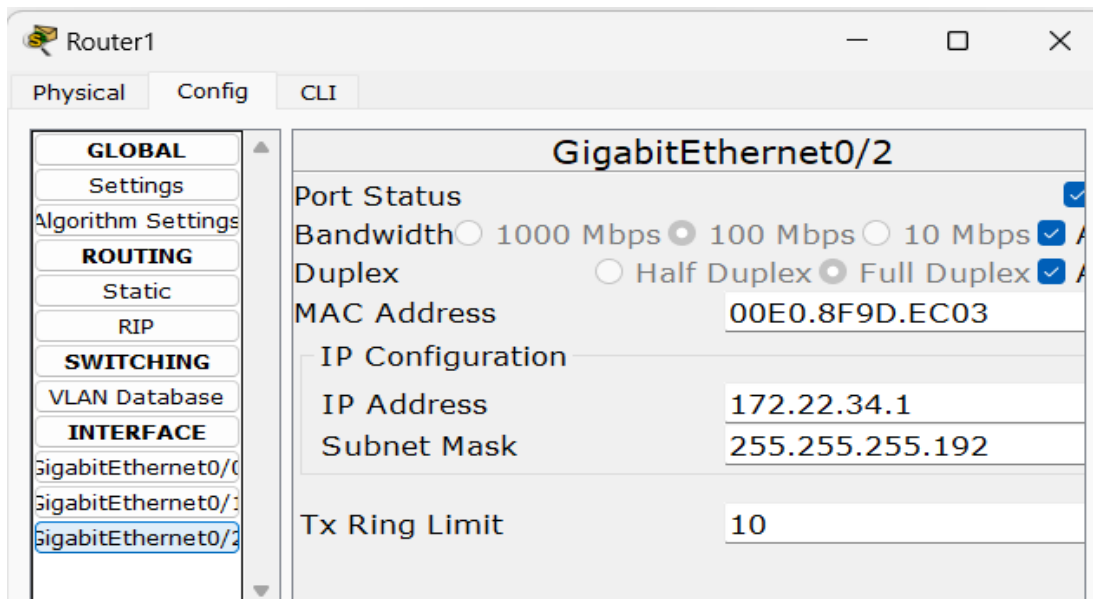
MAC Address: 00E0.8F9D.EC02

IP Configuration

IP Address: 172.22.34.97

Subnet Mask: 255.255.255.240

Tx Ring Limit: 10



Router1

Physical Config CLI

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/2

GigabitEthernet0/2

Port Status ☒

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒

Duplex ☐ Half Duplex ☒ Full Duplex ☒

MAC Address 00E0.8F9D.EC03

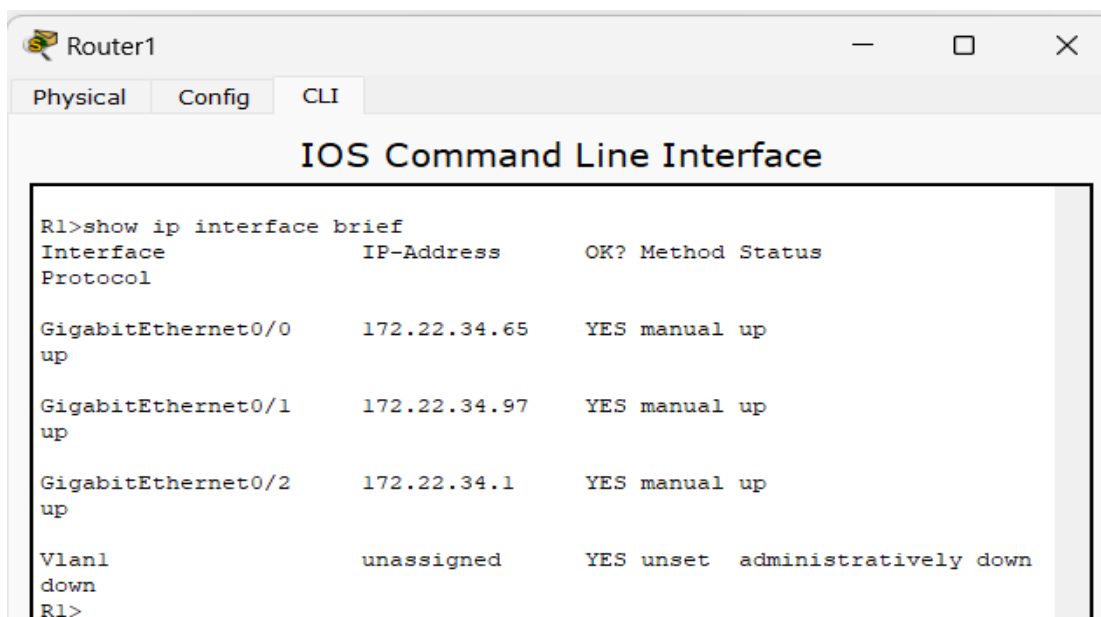
IP Configuration

IP Address 172.22.34.1

Subnet Mask 255.255.255.192

Tx Ring Limit 10

➤ Displaying IP Address Details of R1



Router1

Physical Config CLI

IOS Command Line Interface

```
R1>show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol

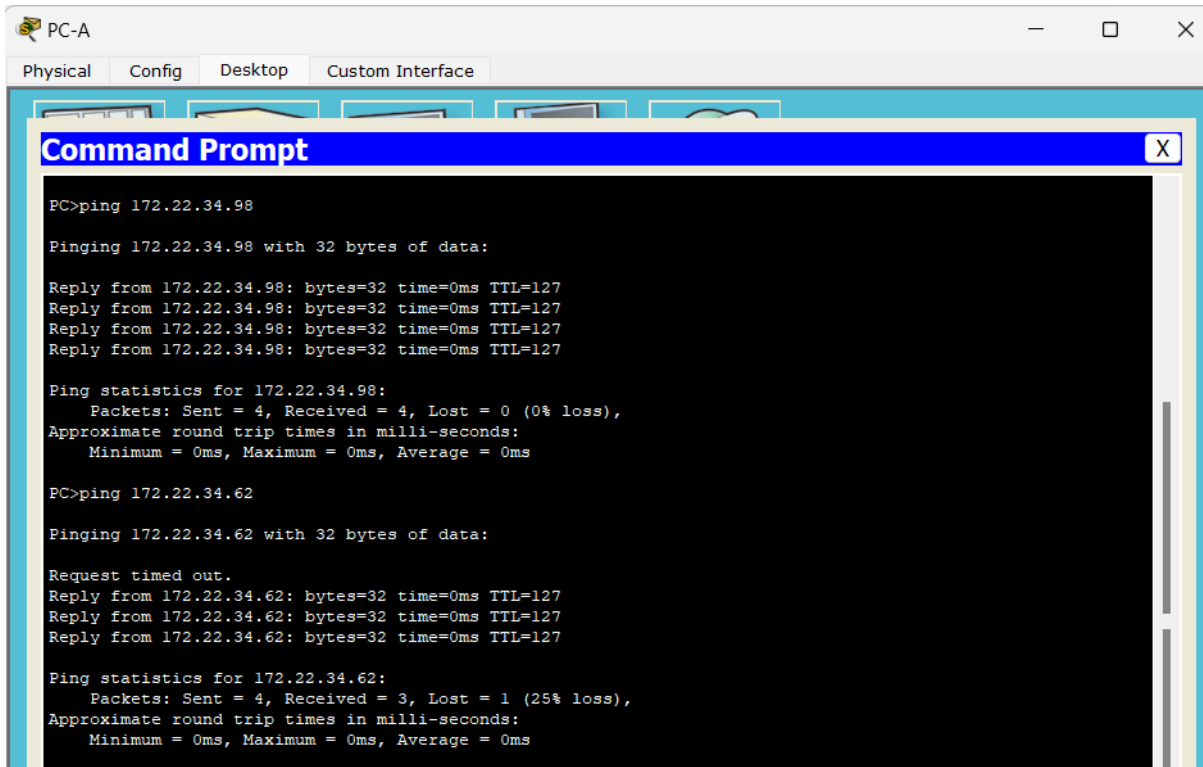
GigabitEthernet0/0  172.22.34.65    YES manual up
up

GigabitEthernet0/1  172.22.34.97    YES manual up
up

GigabitEthernet0/2  172.22.34.1     YES manual up
up

Vlan1              unassigned      YES unset  administratively down
down
R1>
```

➤ Performing Ping from PC-A to Server and PC-B



The screenshot shows the Command Prompt window of PC-A. The window has tabs for Physical, Config, Desktop, and Custom Interface. The Command Prompt displays the following output:

```
PC>ping 172.22.34.98

Pinging 172.22.34.98 with 32 bytes of data:

Reply from 172.22.34.98: bytes=32 time=0ms TTL=127
Reply from 172.22.34.98: bytes=32 time=0ms TTL=127
Reply from 172.22.34.98: bytes=32 time=0ms TTL=127
Reply from 172.22.34.98: bytes=32 time=0ms TTL=127

Ping statistics for 172.22.34.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

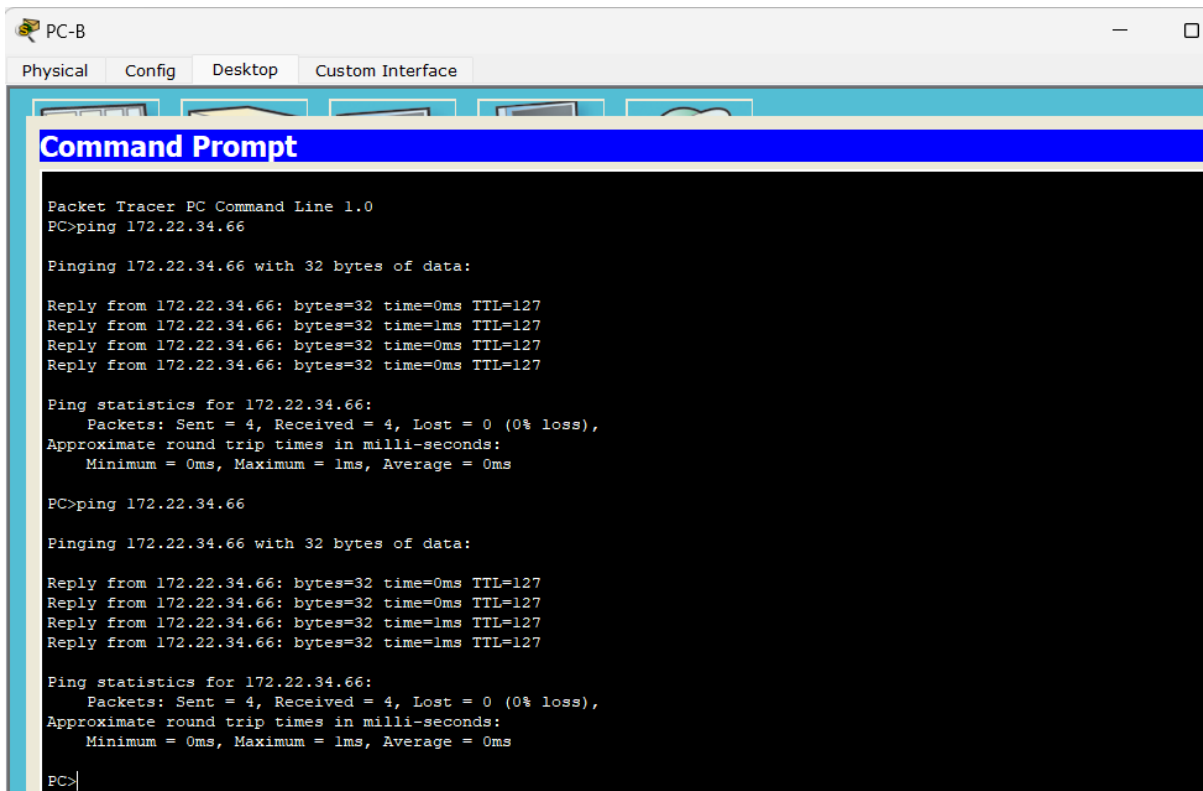
PC>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Request timed out.
Reply from 172.22.34.62: bytes=32 time=0ms TTL=127
Reply from 172.22.34.62: bytes=32 time=0ms TTL=127
Reply from 172.22.34.62: bytes=32 time=0ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

➤ Performing Ping from PC-B to Server and PC-A



The screenshot shows the Command Prompt window of PC-B. The window has tabs for Physical, Config, Desktop, and Custom Interface. The Command Prompt displays the following output:

```
Packet Tracer PC Command Line 1.0
PC>ping 172.22.34.66

Pinging 172.22.34.66 with 32 bytes of data:

Reply from 172.22.34.66: bytes=32 time=0ms TTL=127
Reply from 172.22.34.66: bytes=32 time=1ms TTL=127
Reply from 172.22.34.66: bytes=32 time=0ms TTL=127
Reply from 172.22.34.66: bytes=32 time=0ms TTL=127

Ping statistics for 172.22.34.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 172.22.34.66

Pinging 172.22.34.66 with 32 bytes of data:

Reply from 172.22.34.66: bytes=32 time=0ms TTL=127
Reply from 172.22.34.66: bytes=32 time=0ms TTL=127
Reply from 172.22.34.66: bytes=32 time=1ms TTL=127
Reply from 172.22.34.66: bytes=32 time=1ms TTL=127

Ping statistics for 172.22.34.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

- Configure, Apply and Verify an Extended Numbered ACL
(PC-A needs only FTP access and should be able to ping the server, but not PC-B)

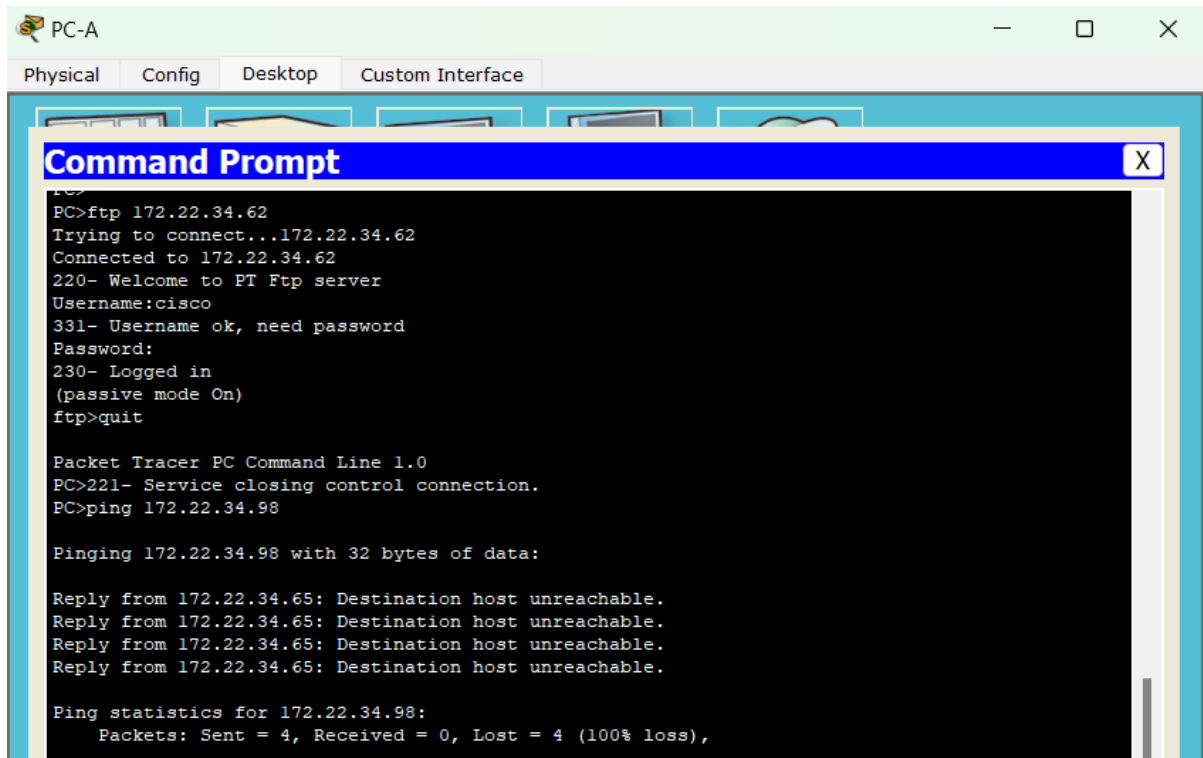
```

Router1
Physical Config CLI
IOS Command Line Interface

R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access- ?
<1-99>      IP standard access list
<100-199>   IP extended access list
R1(config)#access- 100 ?
deny        Specify packets to reject
permit      Specify packets to forward
remark      Access list entry comment
R1(config)#access- 100 permit ?
ahp          Authentication Header Protocol
eigrp        Cisco's EIGRP routing protocol
esp          Encapsulation Security Payload
gre          Cisco's GRE tunneling
icmp         Internet Control Message Protocol
ip           Any Internet Protocol
ospf         OSPF routing protocol
tcp          Transmission Control Protocol
udp          User Datagram Protocol
R1(config)#access- 100 permit tcp ?
% Unrecognized command
R1(config)#access- 100 permit tcp ?
A.B.C.D      Source address
any          Any source host
host         A single source host
R1(config)#access- 100 permit tcp 172.22.34.64 ?
A.B.C.D      Source wildcard bits
R1(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 ?
A.B.C.D      Destination address
any          Any destination host
eq           Match only packets on a given port number
gt           Match only packets with a greater port number
host         A single destination host
lt           Match only packets with a lower port number
neq          Match only packets not on a given port number
range        Match only packets in the range of port numbers
R1(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host ?
A.B.C.D      Destination address
range        Match only packets in the range of port numbers
R1(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host ?
A.B.C.D      Destination address
R1(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?
dscp         Match packets with given dscp value
eq           Match only packets on a given port number
established   established
gt           Match only packets with a greater port number
lt           Match only packets with a lower port number
neq          Match only packets not on a given port number
precedence   Match packets with given precedence value
range        Match only packets in the range of port numbers
<cr>
R1(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?
<0-65535>    Port number
ftp          File Transfer Protocol (21)
pop3         Post Office Protocol v3 (110)
smtp         Simple Mail Transport Protocol (25)
telnet       Telnet (23)
www          World Wide Web (HTTP, 80)
R1(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
R1(config)#access- 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit

```

- Performing Ping from PC-A to Server and PC-B to check the working of ACL



The screenshot shows a Packet Tracer PC window for PC-A. The 'Config' tab is selected. A Command Prompt window is open, displaying the following text:

```

PC>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

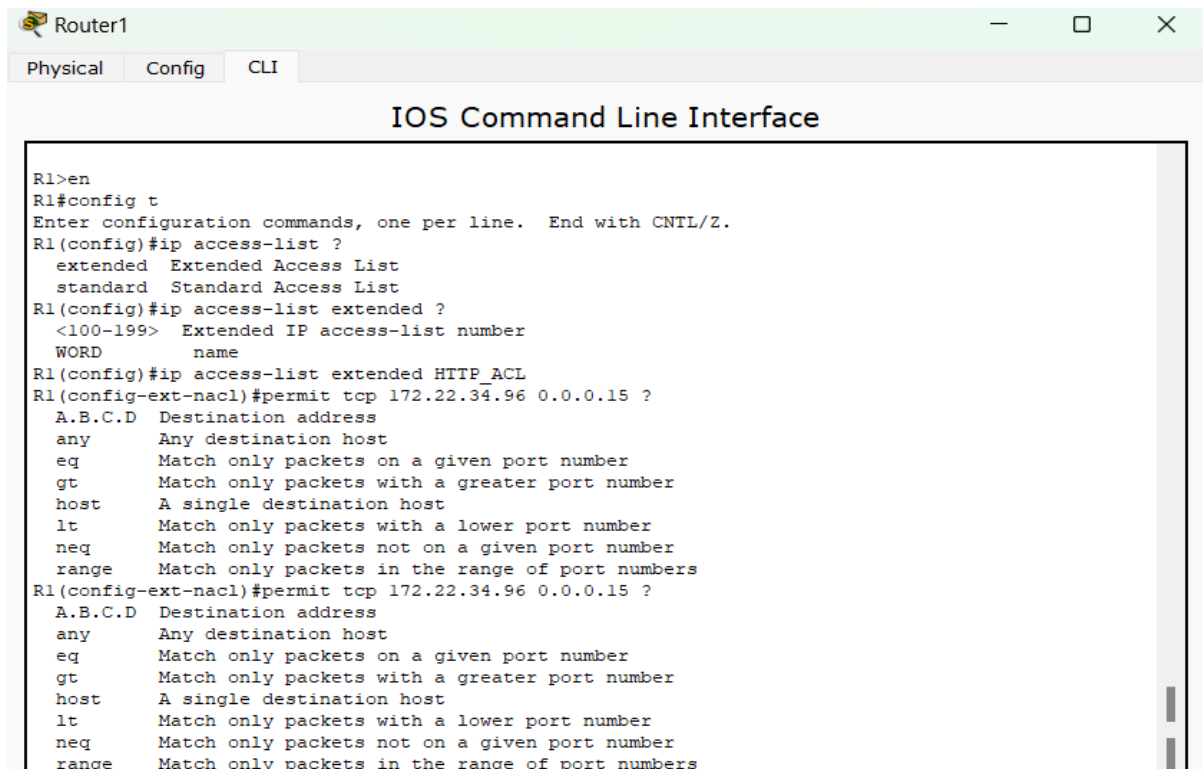
Packet Tracer PC Command Line 1.0
PC>221- Service closing control connection.
PC>ping 172.22.34.98

Pinging 172.22.34.98 with 32 bytes of data:

Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.

Ping statistics for 172.22.34.98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  
```

- Configure, Apply and Verify an Extended Named ACL
(PC-B needs only web access and should be able to ping the server, but not PC-A)



The screenshot shows a Packet Tracer Router window for Router1. The 'CLI' tab is selected. The 'IOS Command Line Interface' window displays the following configuration commands:

```

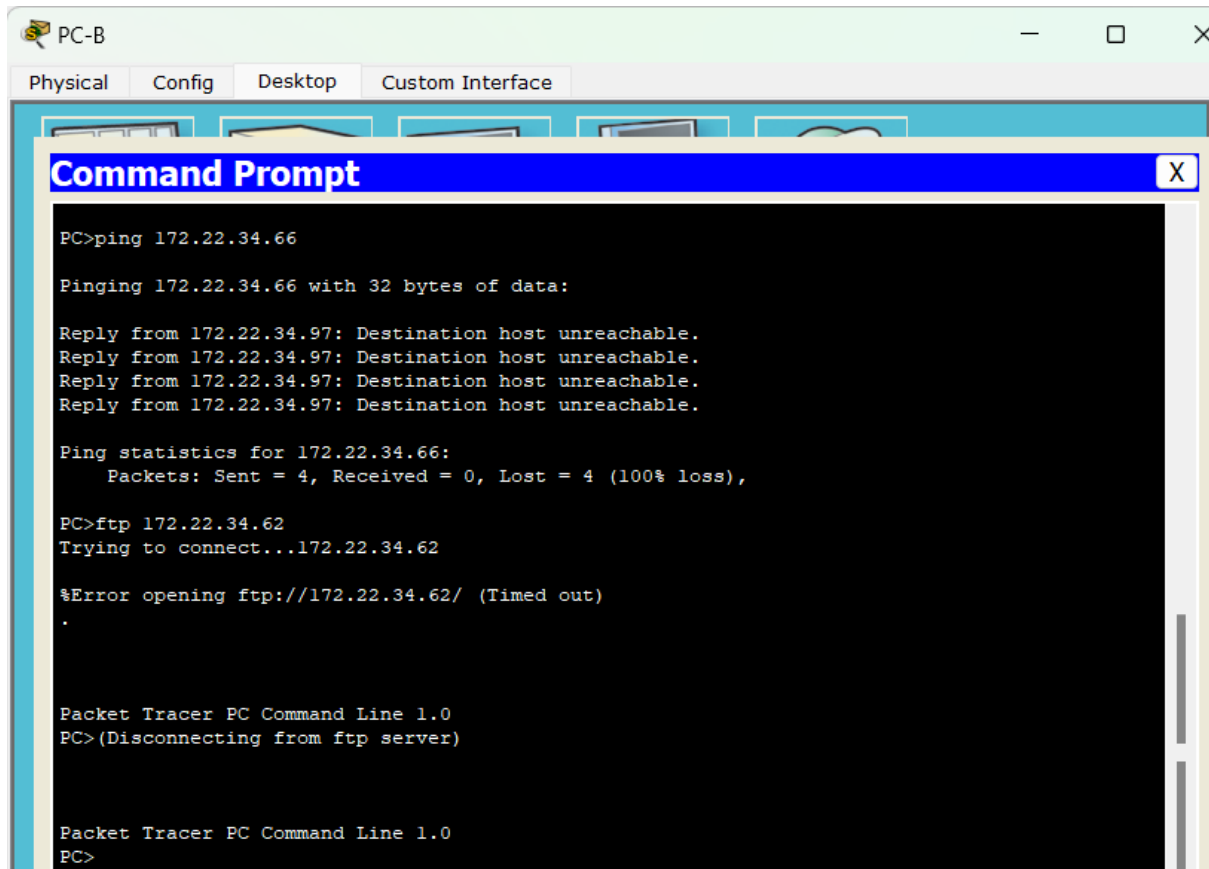
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list ?
    extended Extended Access List
    standard Standard Access List
R1(config)#ip access-list extended ?
    <100-199> Extended IP access-list number
    WORD name
R1(config)#ip access-list extended HTTP_ACL
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 ?
    A.B.C.D Destination address
    any Any destination host
    eq Match only packets on a given port number
    gt Match only packets with a greater port number
    host A single destination host
    lt Match only packets with a lower port number
    neq Match only packets not on a given port number
    range Match only packets in the range of port numbers
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 ?
    A.B.C.D Destination address
    any Any destination host
    eq Match only packets on a given port number
    gt Match only packets with a greater port number
    host A single destination host
    lt Match only packets with a lower port number
    neq Match only packets not on a given port number
    range Match only packets in the range of port numbers
  
```

```

    neq      Match only packets not on a given port number
    range    Match only packets in the range of port numbers
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host ?
A.B.C.D Destination address
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 ?
eq          Match only packets on a given port number
established established
gt          Match only packets with a greater port number
lt          Match only packets with a lower port number
neq         Match only packets not on a given port number
range       Match only packets in the range of port numbers
<cr>
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq /?
% Unrecognized command
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq ?
<0-65535> Port number
domain      Domain Name Service (DNS, 53)
ftp         File Transfer Protocol (21)
pop3        Post Office Protocol v3 (110)
smtp        Simple Mail Transport Protocol (25)
telnet      Telnet (23)
www         World Wide Web (HTTP, 80)
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
R1(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
R1(config-ext-nacl)#interface GigabitEthernet0/1
R1(config-if)#ip access-group HTTP_ACL in
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit

```

- Performing Ping from PC-B to Server and PC-A to check the working of ACL



➤ Checking http connection from PC-B

