

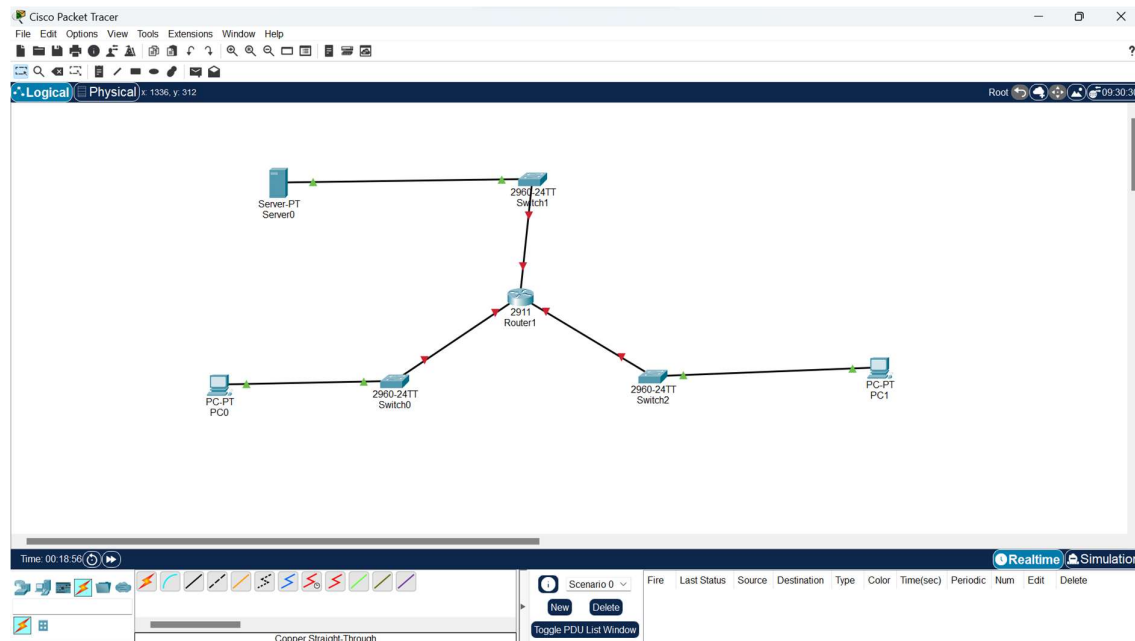
Date: 05/02/2024

Security in Computing

Practical 3A:

Aim: Configure Extended ACLs.

Topology:



➤ Assign IP Addresses:

The screenshot shows the configuration window for PC1, specifically the FastEthernet0 interface. The configuration is as follows:

FastEthernet0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	000A.F326.2A8B
IP Configuration	
<input type="radio"/> DHCP <input checked="" type="radio"/> Static	
IPv4 Address	172.22.34.66
Subnet Mask	255.255.255.224
IPv6 Configuration	
<input checked="" type="radio"/> Automatic <input type="radio"/> Static	
IPv6 Address	/
Link Local Address	FE80::20A:F3FF:FE26:2A8B

PC2

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 00D0.BC6A.3CE9

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 172.22.34.98

Subnet Mask 255.255.255.240

IPv6 Configuration

☒ Automatic

☐ Static

IPv6 Address /

Link Local Address: FE80::2D0:BCFF:FE6A:3CE9

Server

Physical **Config** Services Desktop Programming Attributes

GLOBAL

- Settings
- Algorithm Settings
- INTERFACE**
- FastEthernet0

FastEthernet0

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 00D0.FFA6.99B8

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 172.22.34.62

Subnet Mask 255.255.255.192

IPv6 Configuration

☒ Automatic

☐ Static

IPv6 Address /

Link Local Address: FE80::2D0:FFFF:FEA6:99B8

R1

Physical **Config** CLI Attributes

GLOBAL

- Settings
- Algorithm Settings
- ROUTING**
- Static
- RIP
- SWITCHING**
- VLAN Database
- INTERFACE**
- GigabitEthernet0/0
- GigabitEthernet0/1
- GigabitEthernet0/2

GigabitEthernet0/0

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 00E0.B07A.8301

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 172.22.34.65

Subnet Mask 255.255.255.224

Tx Ring Limit 10

R1

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/2

GigabitEthernet0/1

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 00E0.B07A.8302

IP Configuration

IPv4 Address 172.22.34.97

Subnet Mask 255.255.255.240

Tx Ring Limit 10

R1

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/2

GigabitEthernet0/2

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 00E0.B07A.8303

IP Configuration

IPv4 Address 172.22.34.1

Subnet Mask 255.255.255.192

Tx Ring Limit 10

➤ Displaying IP Address Details of R1

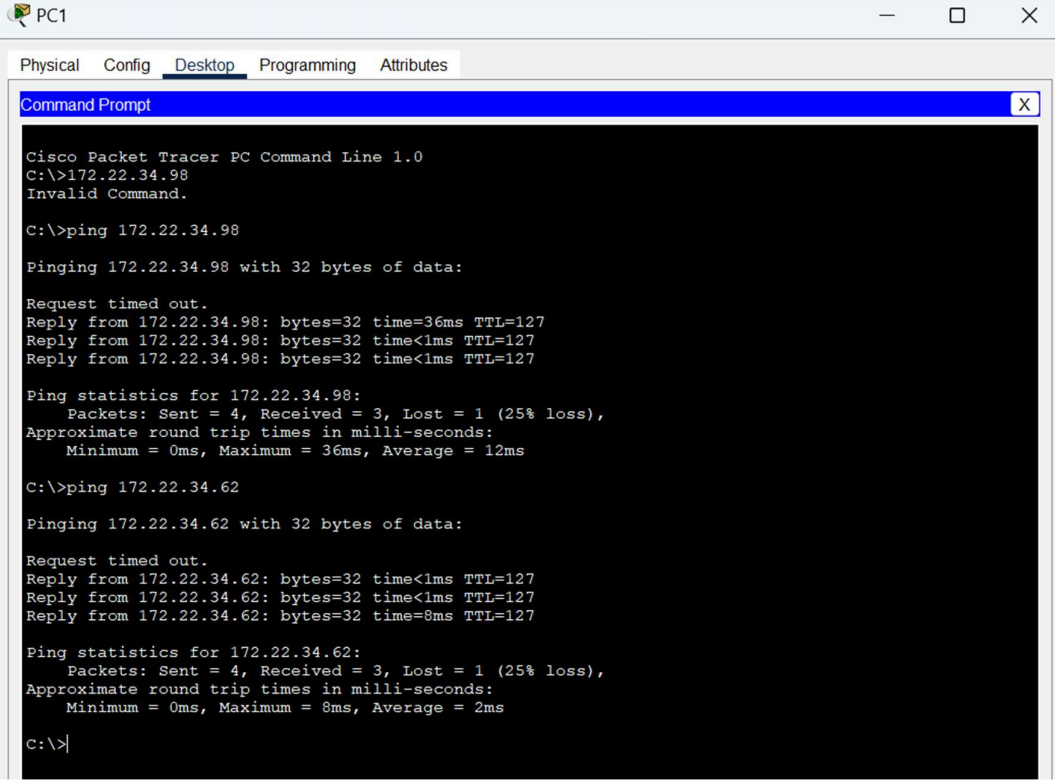
R1

Physical Config **CLI** Attributes

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 a Cisco Packet Tracer PC window for PC1. The 'Desktop' tab is active, displaying a Command Prompt window. The prompt shows the user entering 'ping 172.22.34.98' and 'ping 172.22.34.62'. The output for the first ping shows a 25% loss (3 out of 4 packets received) with an average round trip time of 12ms. The output for the second ping also shows a 25% loss (3 out of 4 packets received) with an average round trip time of 2ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>172.22.34.98
Invalid Command.

C:\>ping 172.22.34.98

Pinging 172.22.34.98 with 32 bytes of data:

Request timed out.
Reply from 172.22.34.98: bytes=32 time=36ms TTL=127
Reply from 172.22.34.98: bytes=32 time<1ms TTL=127
Reply from 172.22.34.98: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 36ms, Average = 12ms

C:\>ping 172.22.34.62

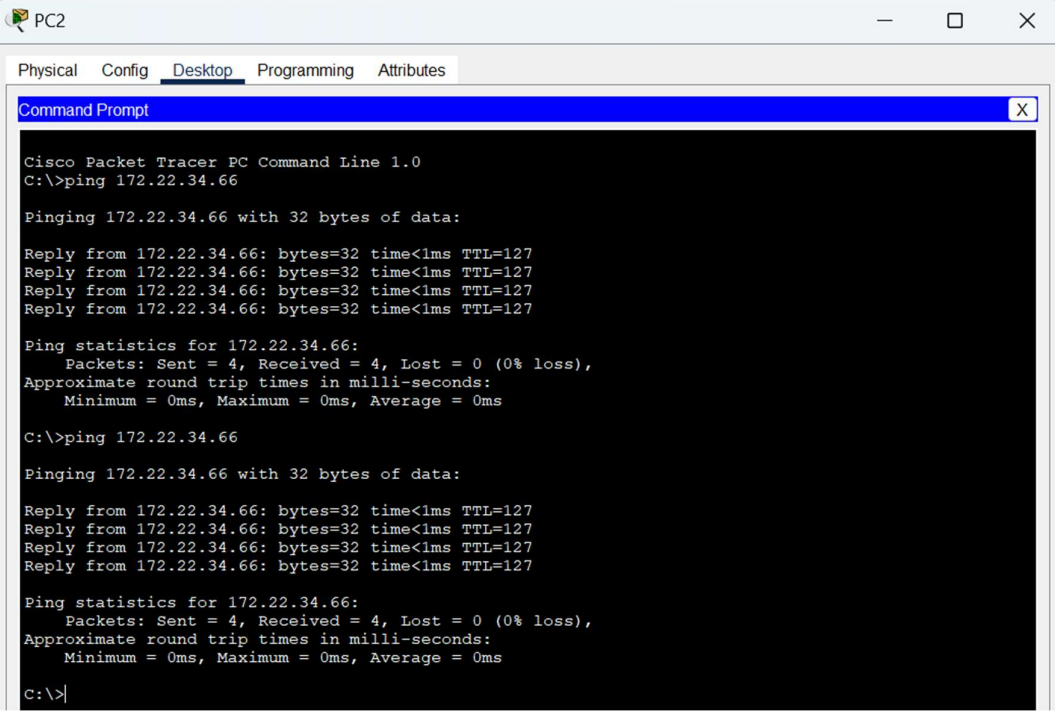
Pinging 172.22.34.62 with 32 bytes of data:

Request timed out.
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time=8ms 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 = 8ms, Average = 2ms

C:\>
```

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



The screenshot shows a Cisco Packet Tracer PC window for PC2. The 'Desktop' tab is active, displaying a Command Prompt window. The prompt shows the user entering 'ping 172.22.34.66' twice. Both times, the output shows 100% success (4 out of 4 packets received) with an average round trip time of 0ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.66

Pinging 172.22.34.66 with 32 bytes of data:

Reply from 172.22.34.66: bytes=32 time<1ms 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
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 = 0ms, Average = 0ms

C:\>ping 172.22.34.66

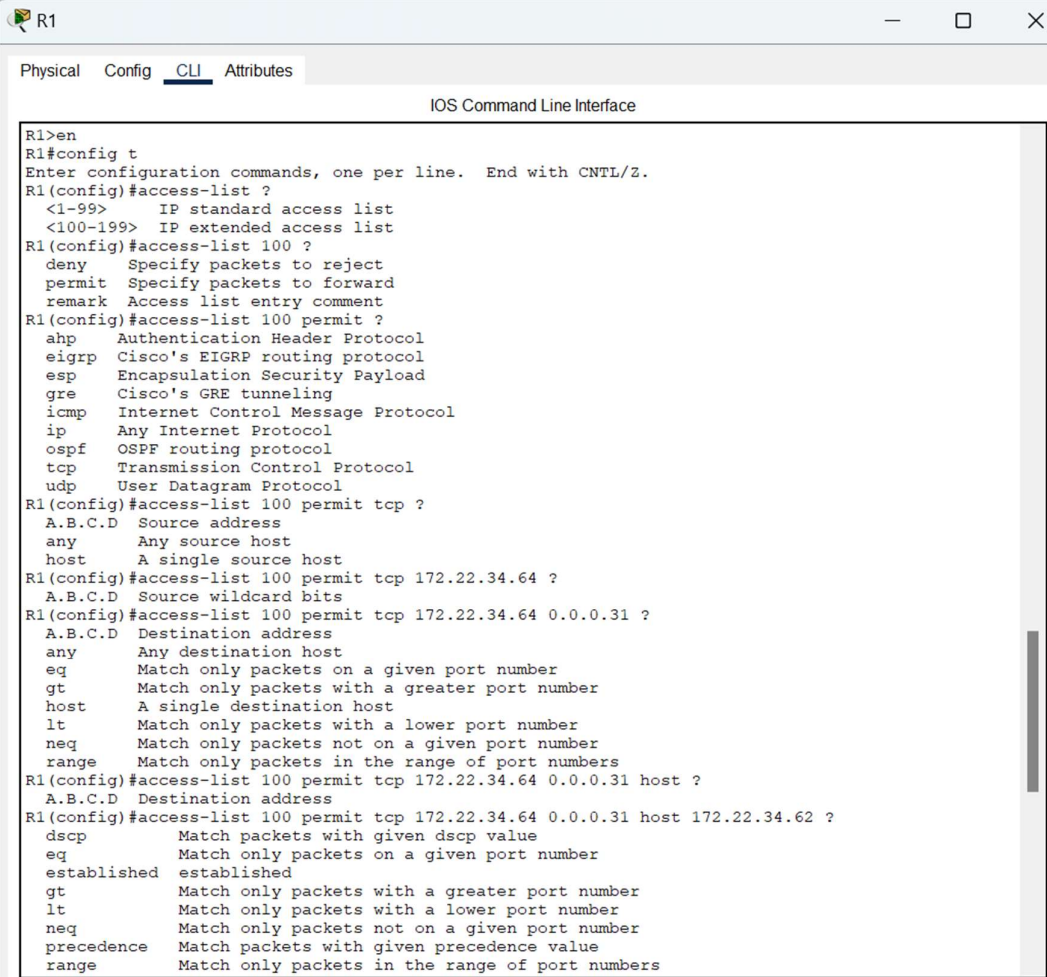
Pinging 172.22.34.66 with 32 bytes of data:

Reply from 172.22.34.66: bytes=32 time<1ms 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
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 = 0ms, Average = 0ms

C:\>
```

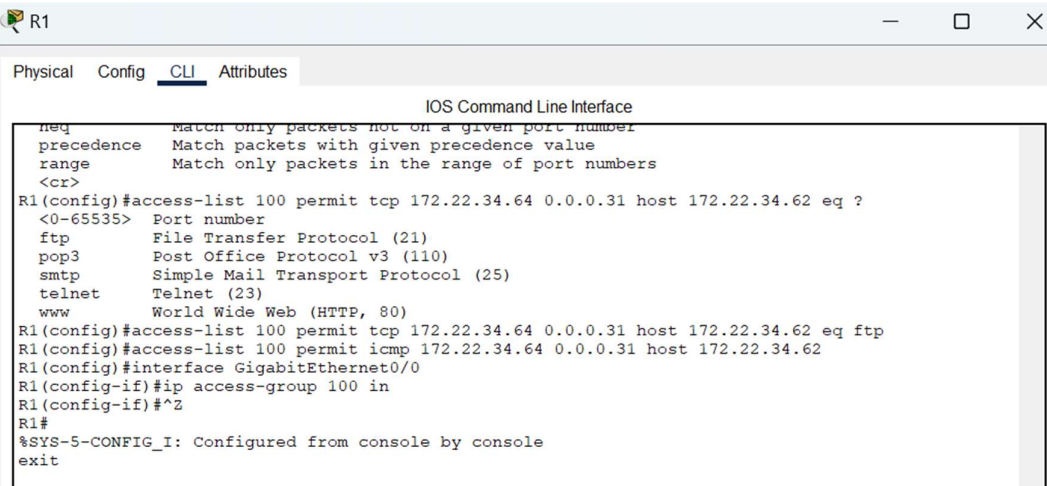
- Configure, Apply and Verify an Extended Numbered ACL
(PC-A needs only FTP access and should be able to ping the server, but not PC-B)



```

R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list ?
  <1-99>      IP standard access list
  <100-199>   IP extended access list
R1(config)#access-list 100 ?
  deny       Specify packets to reject
  permit     Specify packets to forward
  remark     Access list entry comment
R1(config)#access-list 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-list 100 permit tcp ?
  A.B.C.D    Source address
  any        Any source host
  host       A single source host
R1(config)#access-list 100 permit tcp 172.22.34.64 ?
  A.B.C.D    Source wildcard bits
R1(config)#access-list 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-list 100 permit tcp 172.22.34.64 0.0.0.31 host ?
  A.B.C.D    Destination address
R1(config)#access-list 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

```

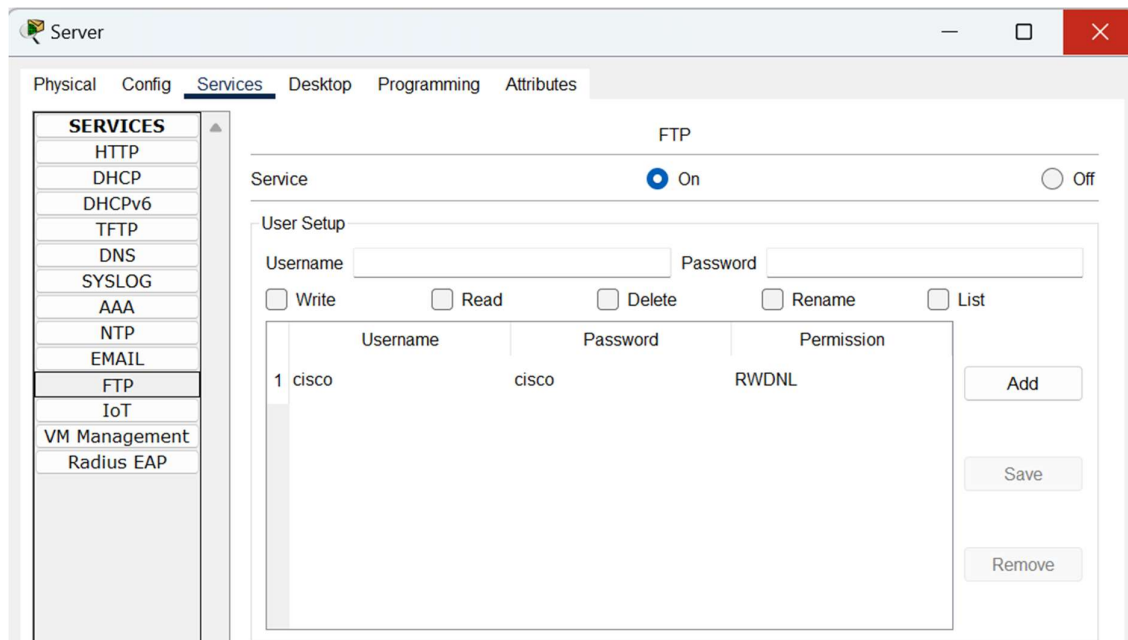


```

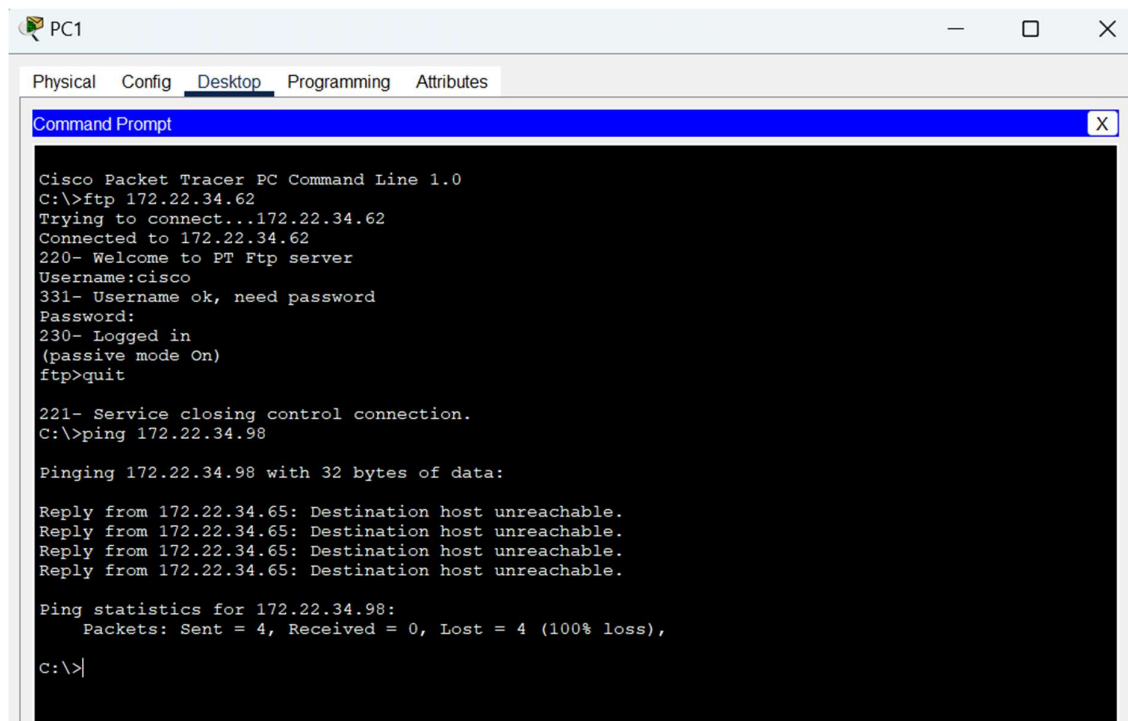
  neq        Match only packets not on a given port number
  precedence Match packets with given precedence value
  range      Match only packets in the range of port numbers
<cr>
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?
<0-65535>   Port number
  ftp        File 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-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
R1(config)#access-list 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
exit

```

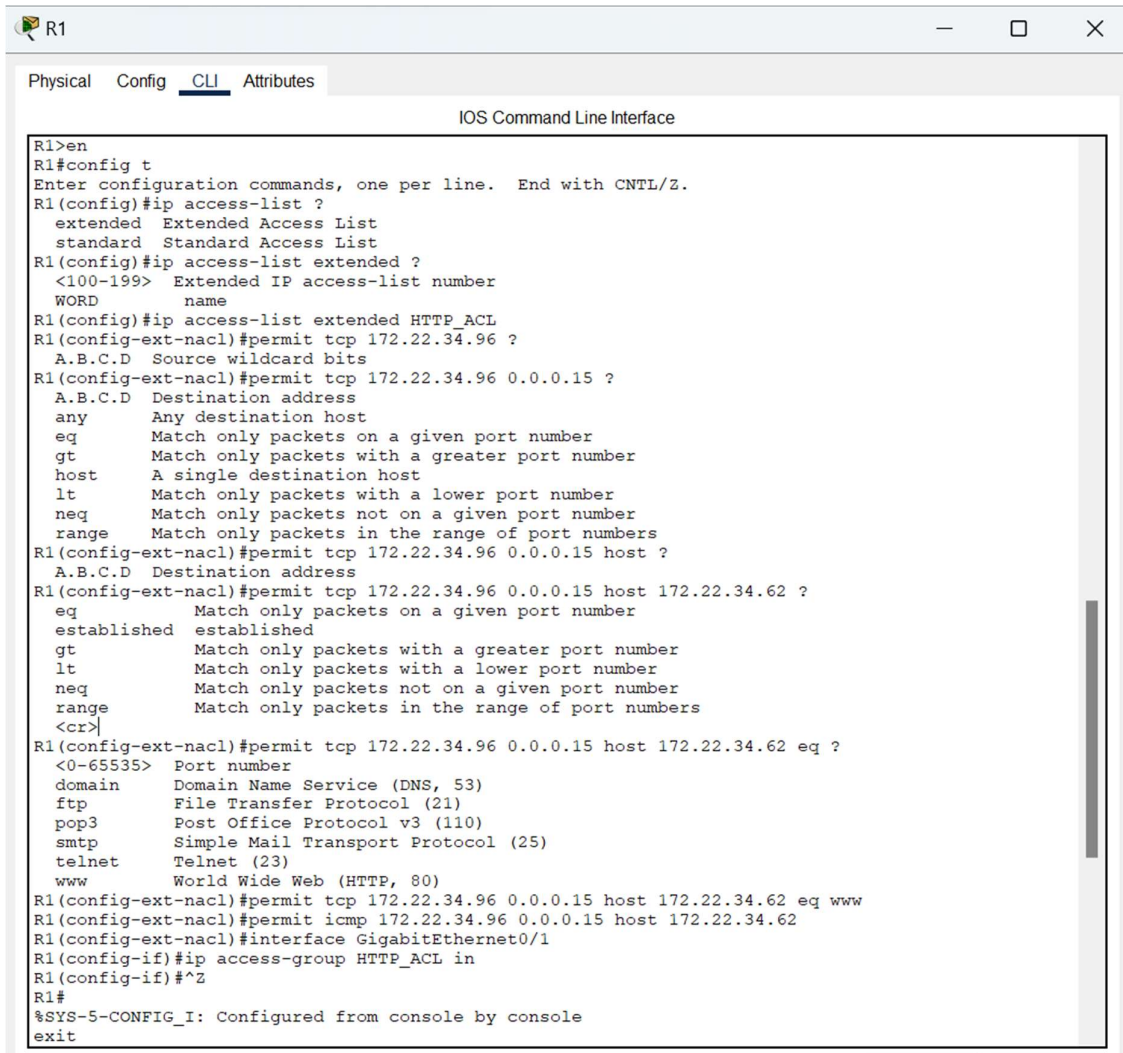
➤ Checking username and password from server



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



- 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)

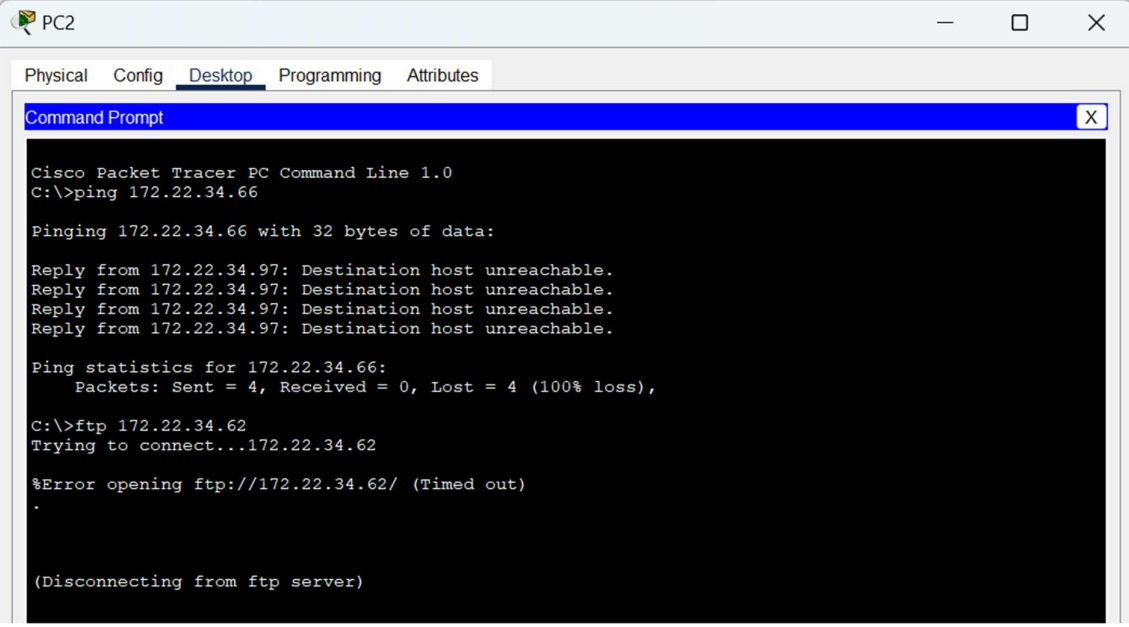


```

R1
Physical Config CLI Attributes
IOS Command Line Interface

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 ?
    A.B.C.D Source wildcard bits
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 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 ?
    <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
exit
  
```

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



The screenshot shows a window titled 'PC2' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.66

Pinging 172.22.34.66 with 32 bytes of data:

Reply from 172.22.34.97: Destination host unreachable.
Reply from 172.22.34.97: Destination host unreachable.
Reply from 172.22.34.97: Destination host unreachable.
Reply from 172.22.34.97: Destination host unreachable.

Ping statistics for 172.22.34.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62

%Error opening ftp://172.22.34.62/ (Timed out)
.

(Disconnecting from ftp server)
```

- Checking http connection from PC-B

