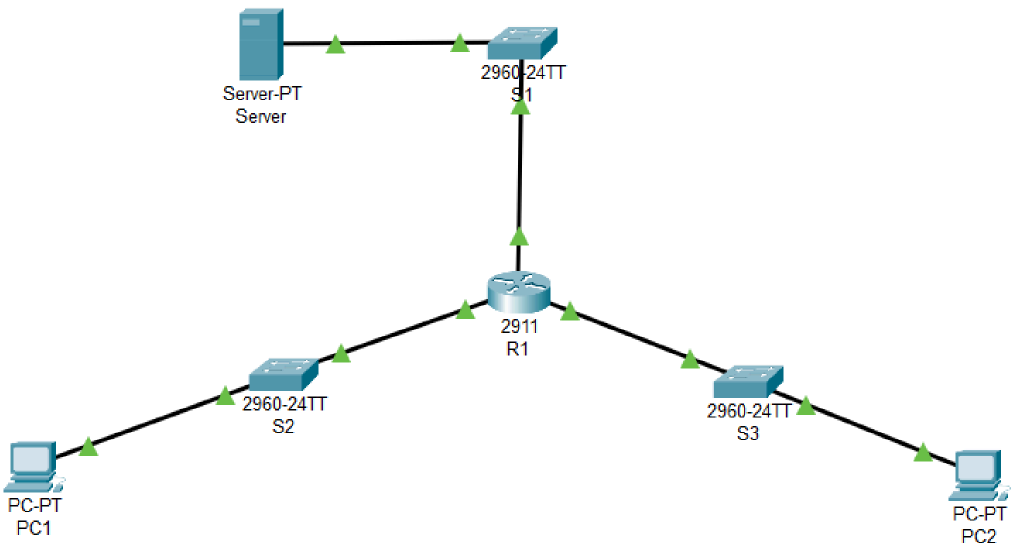
Security in Computing
Practical - 3A

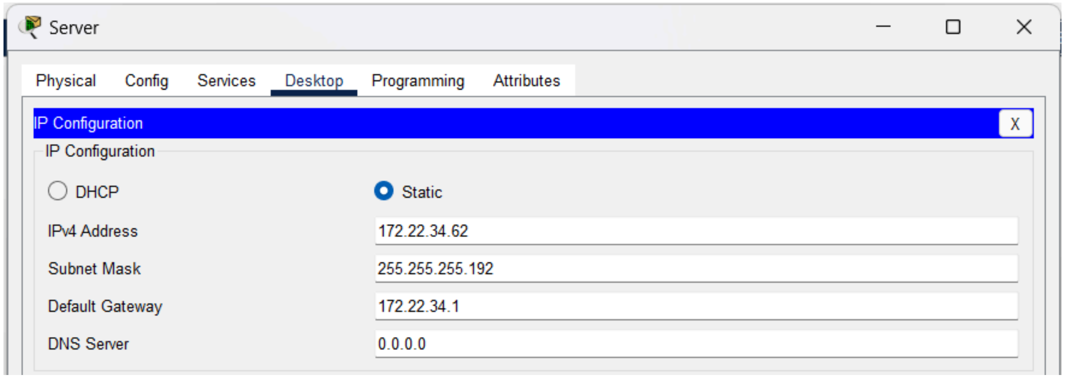
➢Aim: Configure IP ACLs to Mitigate Attacks

a. Verify connectivity among devices before firewall configuration.
b. Use ACLs to ensure remote access to routers is only available on from management station PC-C

Topology Diagram:



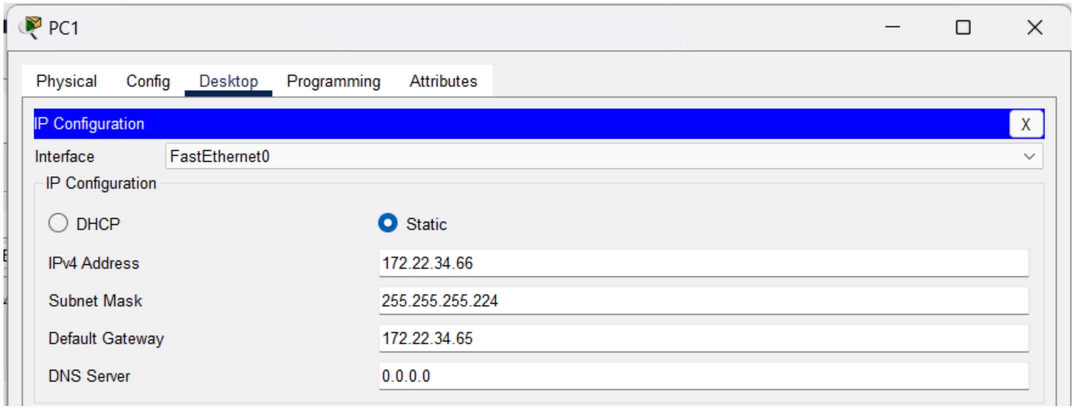
Assign IP Addresses:



IP Configuration

○ DHCP ● Static

IPv4 Address	172.22.34.62
Subnet Mask	255.255.255.192
Default Gateway	172.22.34.1
DNS Server	0.0.0.0



IP Configuration

Interface: FastEthernet0

IP Configuration

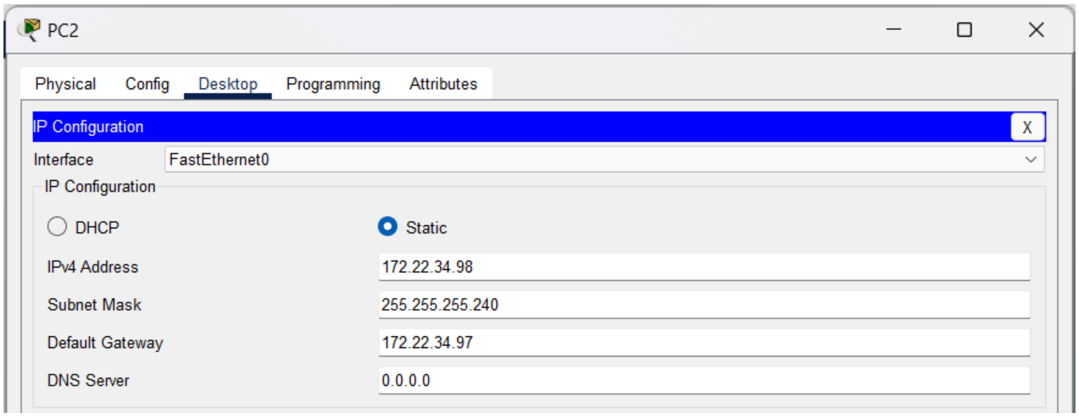
○ DHCP ● Static

IPv4 Address: 172.22.34.66

Subnet Mask: 255.255.255.224

Default Gateway: 172.22.34.65

DNS Server: 0.0.0.0



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 172.22.34.98

Subnet Mask: 255.255.255.240

Default Gateway: 172.22.34.97

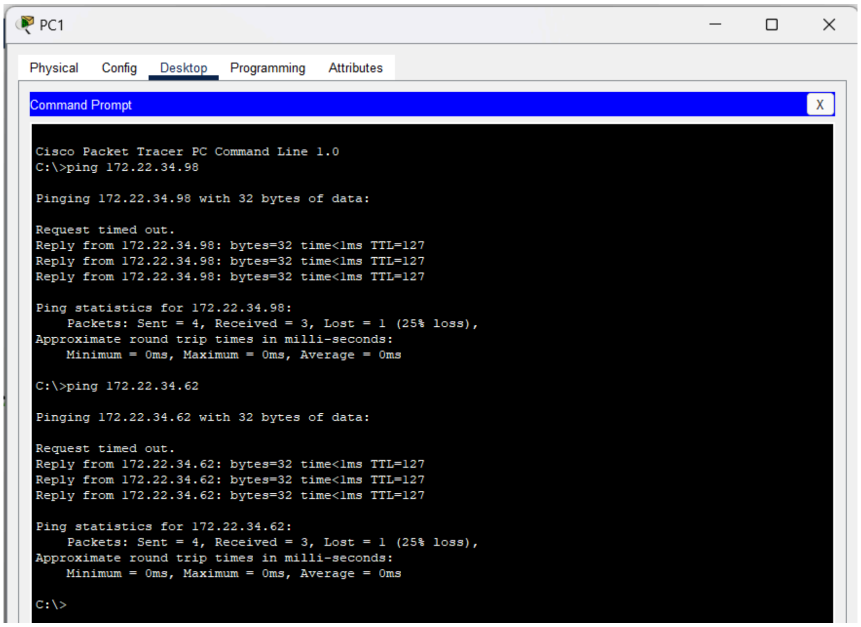
DNS Server: 0.0.0.0

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R1
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip address 172.22.34.65 255.255.255.224
R1(config-if)#no shut

R1(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

R1(config-if)#interface GigabitEthernet0/1
R1(config-if)#ip address 172.22.34.97 255.255.255.240
R1(config-if)#no shut

R1(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

R1(config-if)#interface GigabitEthernet0/2
R1(config-if)#ip address 172.22.34.1 255.255.255.192
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

Displaying IP Addresses Details of R1:

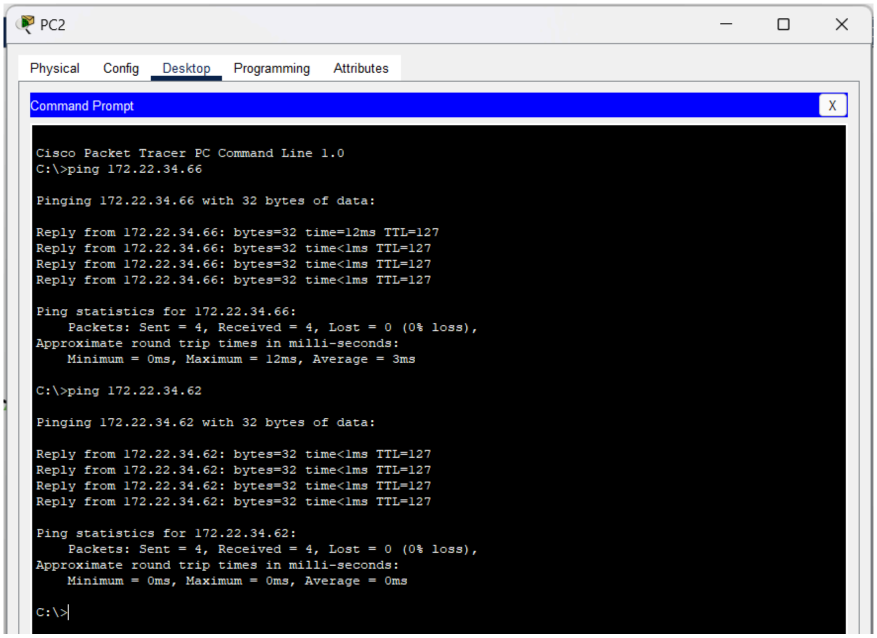
```
R1>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     172.22.34.65    YES manual up                    up
GigabitEthernet0/1     172.22.34.97    YES manual up                    up
GigabitEthernet0/2     172.22.34.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Performing Ping from PC1 to Server and PC2:



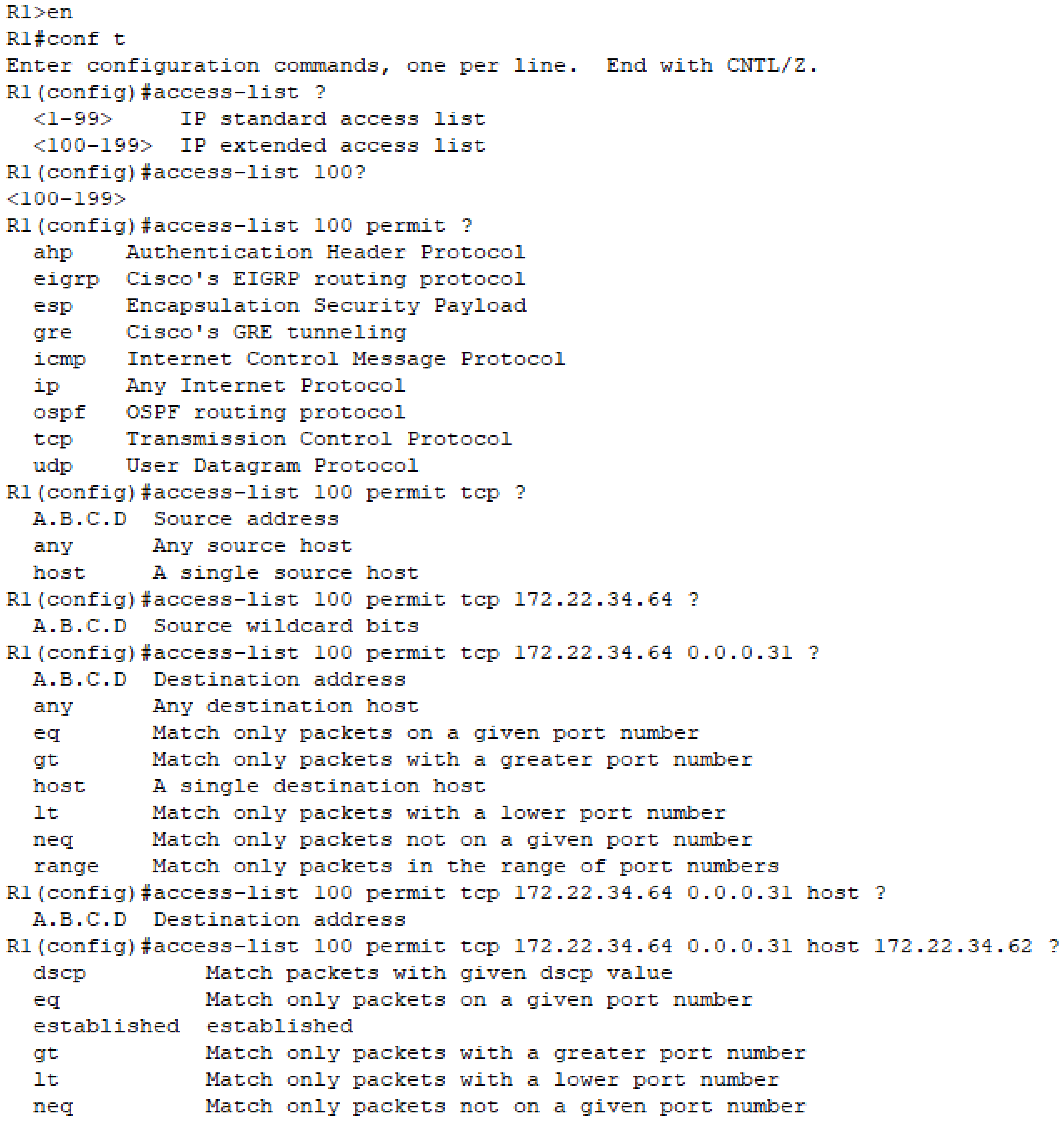
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.98

Pinging 172.22.34.98 with 32 bytes of data:

Request timed out.
Reply from 172.22.34.98: bytes=32 time<1ms 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 = 0ms, Average = 0ms

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<1ms 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

C:\>
```

Performing Ping from PC2 to Server and PC1:



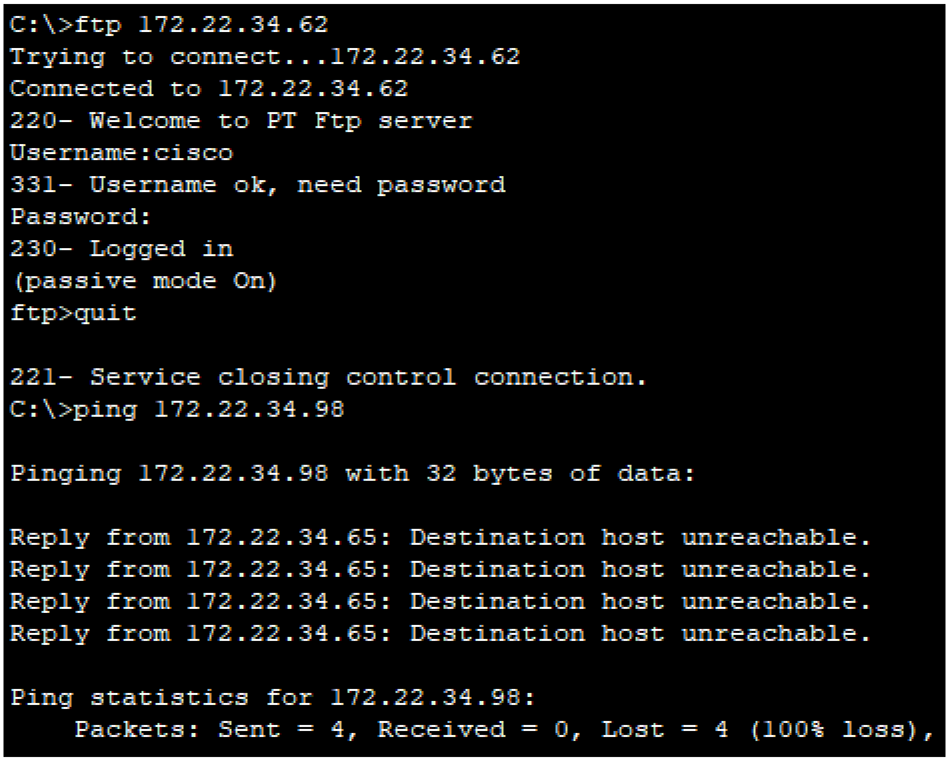
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.66

Pinging 172.22.34.66 with 32 bytes of data:

Reply from 172.22.34.66: bytes=32 time=12ms 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 = 12ms, Average = 3ms

C:\>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

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<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    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
(PC1 needs only FTP access and should be able to ping the server, but not PC2):



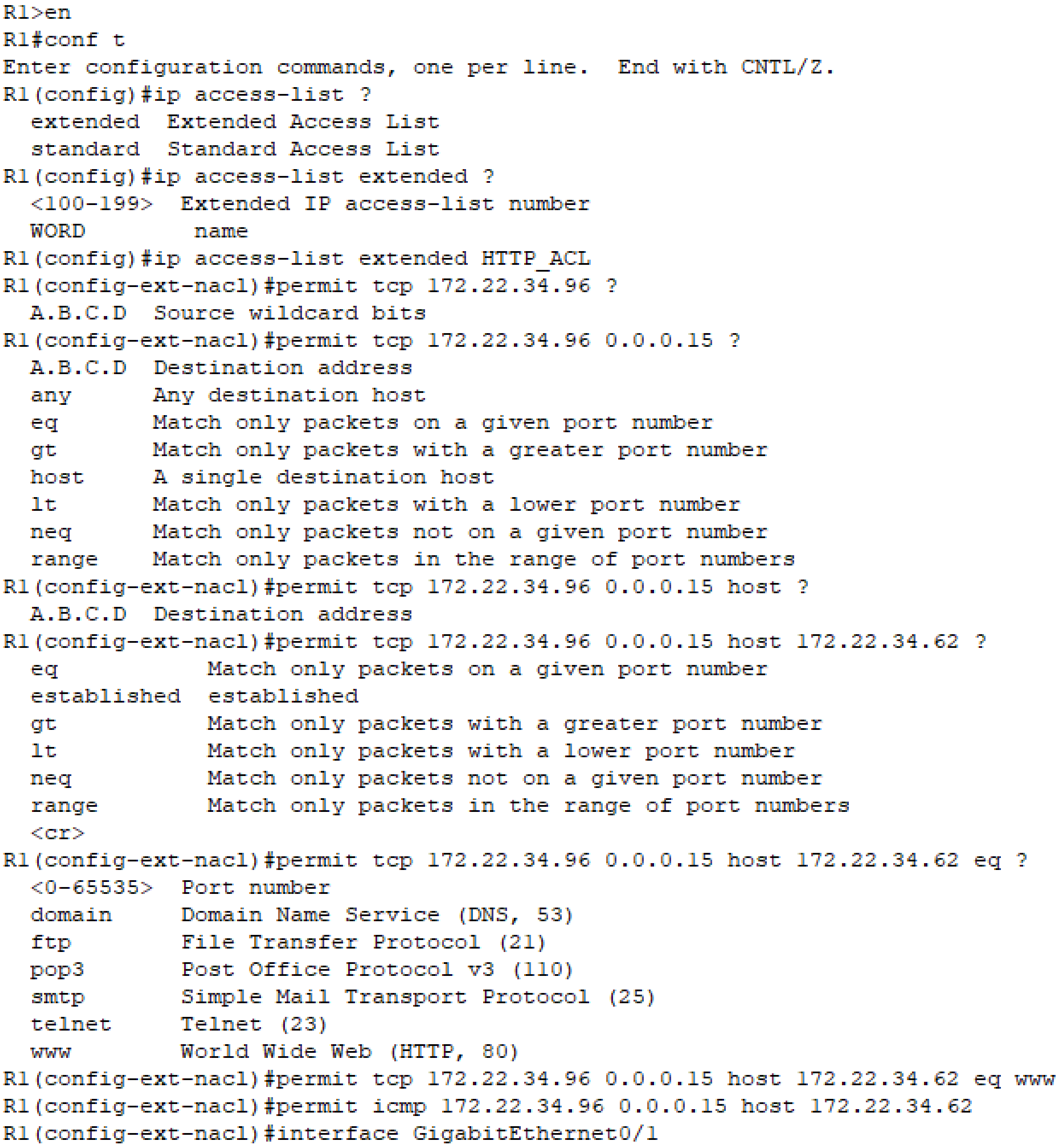
```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
R1(config)#access-list 100?
<100-199>
R1(config)#access-list 100 permit ?
  ahp    Authentication Header Protocol
  eigrp  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
  <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

R1#exit
```

Performing Ping from PC1 to Server and PC2 to check the working of ACL:

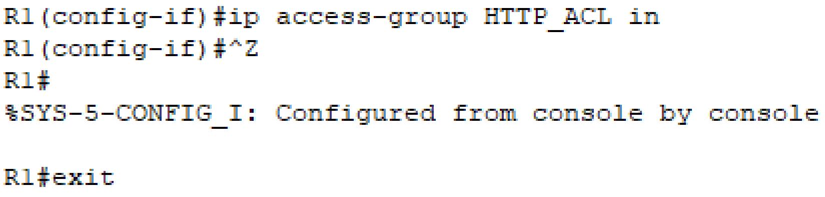


```
C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>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
(PC2 needs only web access and should be able to ping the server, but not PC1):

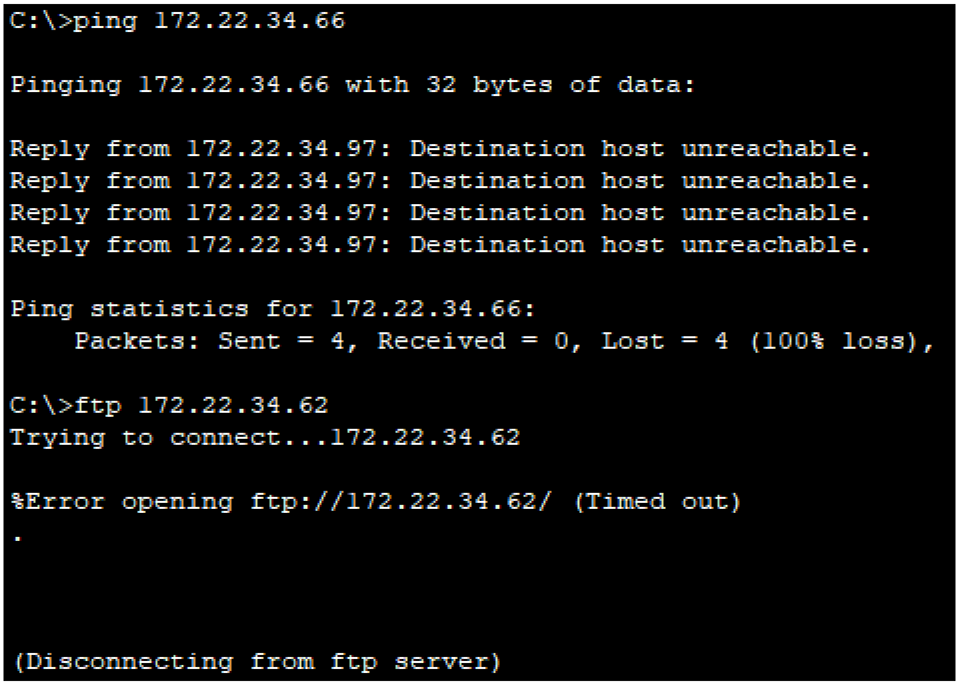


```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list ?
  extended  Extended Access List
  standard  Standard Access List
R1(config)#ip access-list extended ?
  <100-199>  Extended IP access-list number
  WORD        name
R1(config)#ip access-list 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
```

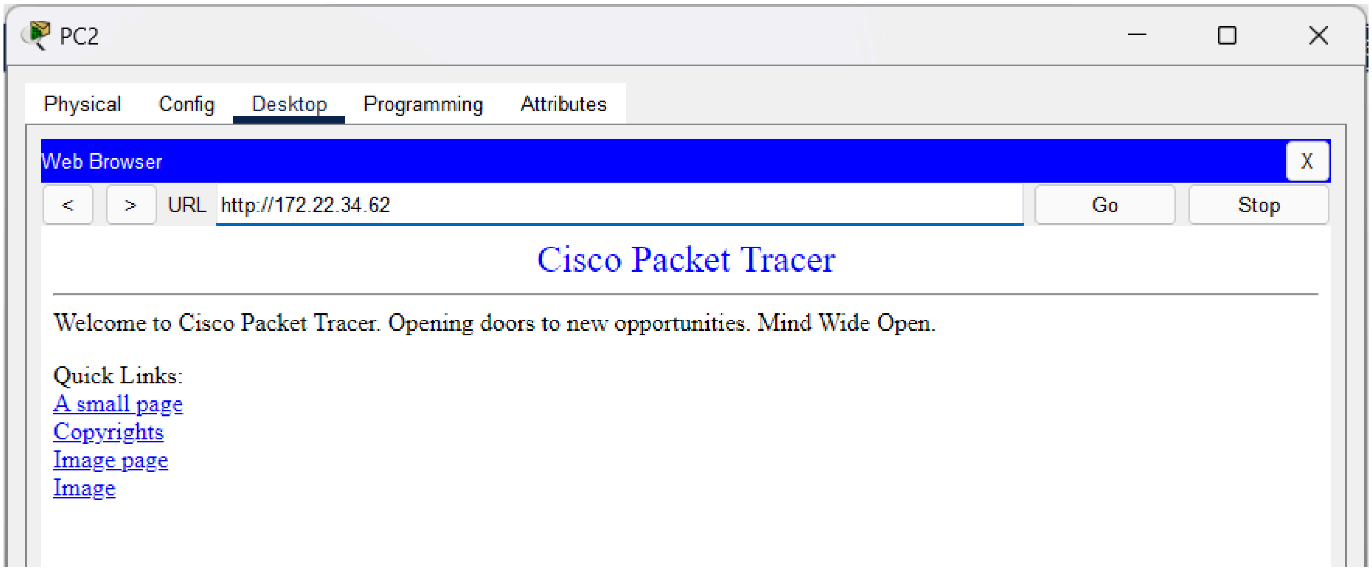


```
R1(config-if)#ip access-group HTTP_ACL in
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

Performing Ping from PC2 to Server and PC1 to check the working of ACL:



```
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)
```



URL http://172.22.34.62

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image