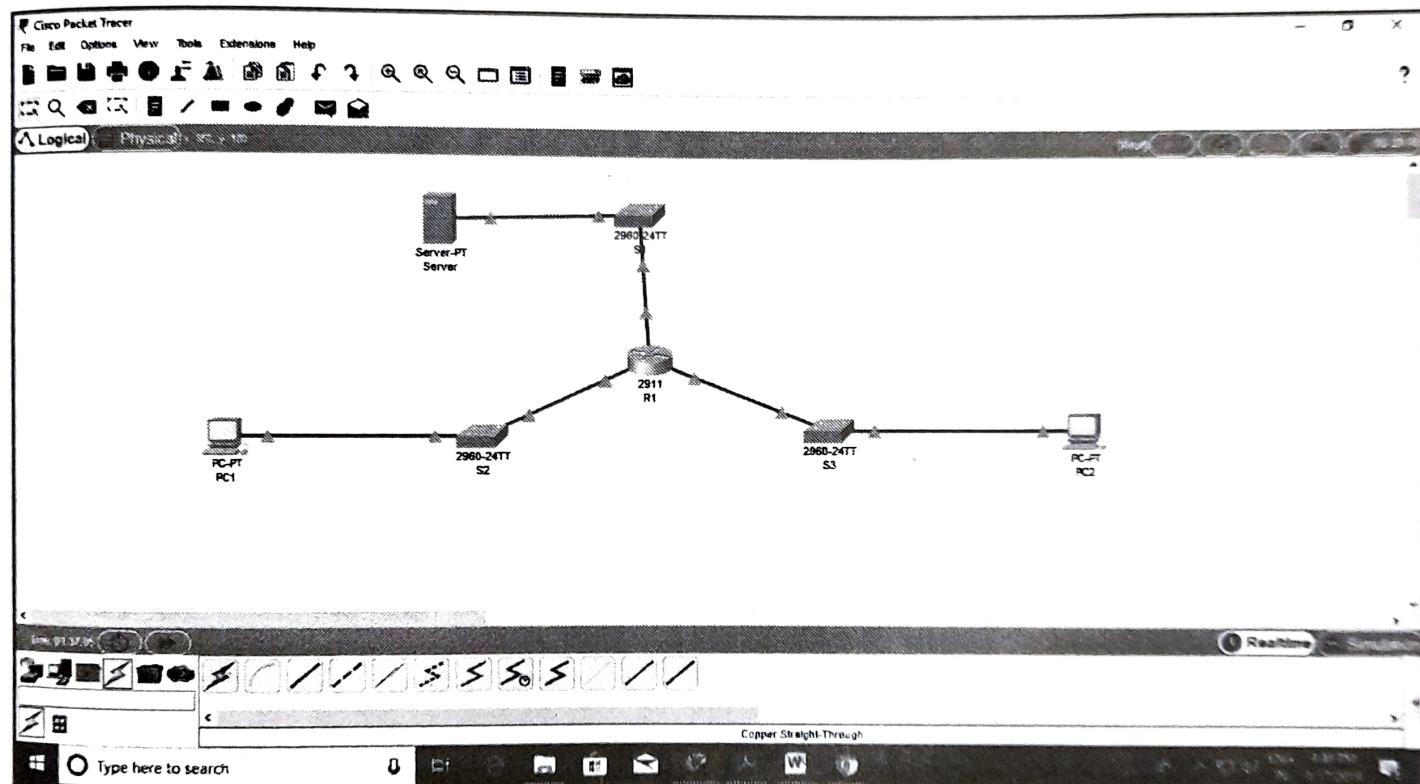


## Practical 3(A)

### ► Aim : Configuring Extended ACLs

#### Topology Diagram





## Assign IP Addresses

The image displays three separate windows, each representing a different device's configuration interface:

- Server**: Shows static IP configuration. IP Address: 172.22.34.62, Subnet Mask: 255.255.255.192, Default Gateway: 172.22.34.1, DNS Server: 0.0.0.0.
- PC1**: Shows static IP configuration. IP Address: 172.22.34.66, Subnet Mask: 255.255.255.224, Default Gateway: 172.22.34.65, DNS Server: 0.0.0.0.
- PC2**: Shows static IP configuration. IP Address: 172.22.34.96, Subnet Mask: 255.255.255.240, Default Gateway: 172.22.34.97, DNS Server: 0.0.0.0.

```
Router>en
Router#conf t
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)#interface GigabitEthernet0/1
R1(config-if)#ip address 172.22.34.97 255.255.255.240
R1(config-if)#no shut
R1(config)#interface GigabitEthernet0/2
R1(config-if)#ip address 172.22.34.1 255.255.255.192
R1(config-if)#no shut
R1(config-if)#^Z
R1#exit
```

## Displaying IP Address 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

## Performing Ping from PC1 to Server and PC2

The screenshot shows a Windows Command Prompt window titled "PC1". The window has tabs at the top: Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is selected. The command prompt window contains the following text:

```
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=12ms 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 = 12ms, Average = 4ms

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=3ms TTL=127
Reply from 172.22.34.62: bytes=32 time=12ms 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 = 12ms, Average = 5ms
```

At the bottom left of the window, there is a small checkbox labeled "Top".



## ☛ Performing Ping from PC2 to Server and PC1

PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
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 = 1ms, 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

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
```

## ☛ 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
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

anyAny 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

anyAny 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

establishedestablished

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#exit

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

The screenshot shows a Windows Command Prompt window titled "PC1". The window has tabs at the top: Physical, Config, Device, Programming, and Attributes. The "Device" tab is selected. The command prompt window contains the following text:

```
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
(pассив 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.

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
R1(config)#ip access-list ?
      extendedExtended Access List
      standardStandard 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
anyAny 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
establishedestablished
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
domainDomain Name Service (DNS, 53)
ftp File Transfer Protocol (21)
pop3 Post Office Protocol v3 (110)
smtp Simple Mail Transport Protocol (25)
telnetTelnet (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)#interface GigabitEthernet0/1
R1(config-if)#ip access-group HTTP_ACL in
R1(config-if)# ^ Z
R1#exit
```



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

The screenshot shows a Windows Command Prompt window titled "PC2". The window has tabs at the top: Physical, Config, **Desktop**, Programming, and Attributes. The desktop tab is selected. The command prompt window contains the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.66
Pinging 172.22.34.66 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

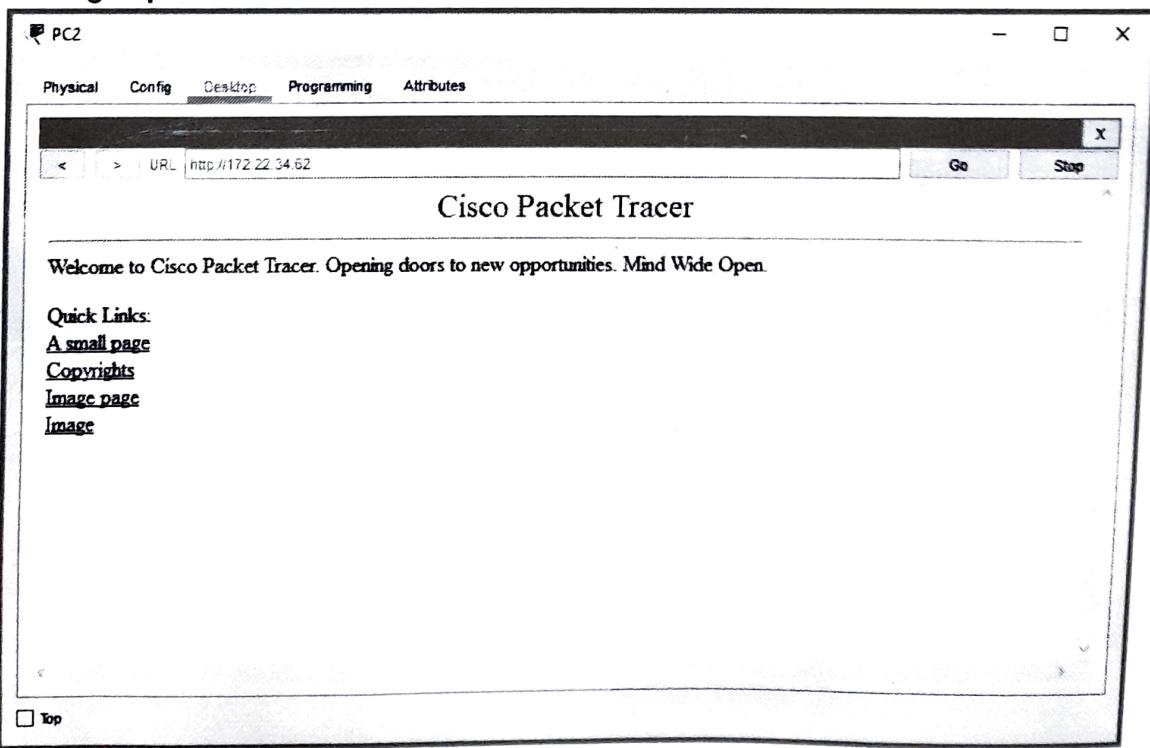
Ping statistics for 172.22.34.66:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
**error opening ftp://172.22.34.62/ (Timed 'out')

(Disconnecting from ftp server)


```

At the bottom left of the command prompt window, there is a checkbox labeled "Top".

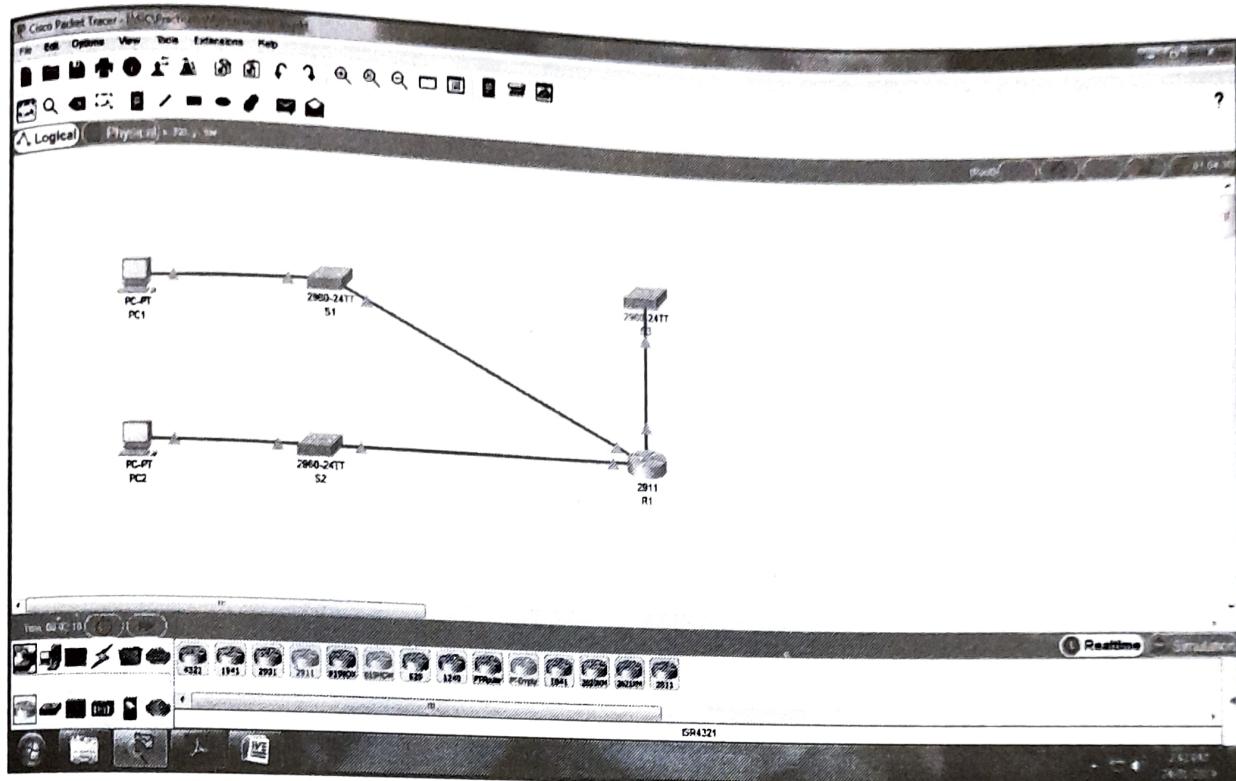
### ☛ Checking http connection from PC2



### Practical 3(B)

Aim : Configure, Apply and Verify an Extended Numbered ACL

#### Topology Diagram



#### Assign IP Addresses

PC1

Physical	Config	Desktop	Programming	Attributes
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static			
IP Address				10.101.117.51
Subnet Mask				255.255.255.248
Default Gateway				10.101.117.49
DNS Server				0.0.0.0

PC2

Physical	Config	Desktop	Programming	Attributes
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static			
IP Address				10.101.117.35
Subnet Mask				255.255.255.240
Default Gateway				10.101.117.33
DNS Server				0.0.0.0



```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip address 10.101.117.49 255.255.255.248
R1(config-if)#no shut
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip address 10.101.117.33 255.255.255.240
R1(config-if)#no shut
R1(config)#interface GigabitEthernet0/2
R1(config-if)#ip address 10.101.117.1 255.255.255.224
R1(config-if)#no shut
R1(config-if)# ^ Z
R1#exit
```

```
Switch>en
Switch#conf t
Switch(config)#host S1
S1(config)#interface vlan 1
S1(config-if)#ip address 10.101.117.50 255.255.255.248
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip default-gateway 10.101.117.49
S1(config)# ^ Z
S1#exit
```

```
Switch>en
Switch#conf t
Switch(config)#host S2
S2(config)#interface vlan 1
S2(config-if)#ip address 10.101.117.34 255.255.255.240
S2(config-if)#no shut
S2(config-if)#exit
S2(config)#ip default-gateway 10.101.117.33
S2(config)# ^ Z
```

```

S2#exit
Switch>en
Switch#conf t
Switch(config)#host S3
S3(config)#interface vlan 1
S3(config-if)#ip address 10.101.117.2 255.255.255.224
S3(config-if)#no shut
S3(config-if)#exit
S3(config)#ip default-gateway 10.101.117.1
S3(config)#^Z
S3#exit

```

## Displaying IP Address Details

```

R1>show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 10.101.117.49 YES manual up up
GigabitEthernet0/1 10.101.117.33 YES manual up up
GigabitEthernet0/2 10.101.117.1 YES manual up up

```

```

S1>show ip interface brief
Interface IP-Address OK? Method Status Protocol
Vlan1 10.101.117.50 YES manual up up

```

```

S2>show ip interface brief
Interface IP-Address OK? Method Status Protocol
Vlan1 10.101.117.34 YES manual up up

```

```

S3>show ip interface brief
Interface IP-Address OK? Method Status Protocol
Vlan1 10.101.117.2 YES manual up up

```



### ☛ Configuring Telnet on S3

```
S3>en
S3#conf t
S3(config)#username admin password teacher
S3(config)#line vty 0 4
S3(config-line)#login local
S3(config-line)#^Z
S3#exit
```

### ☛ Configure, Apply and Verify an Extended Numbered ACL

**(Devices on LAN 10.101.117.32 are allowed to remotely access devices in LAN 10.101.117.0 using the TELNET protocol. Besides ICMP, all traffic from other networks is denied.)**

```
R1>en
R1#conf t
R1(config)#access-list ?
  <1-99> IP standard access list
  <100-199> IP extended access list
R1(config)#access-list 199 ?
  deny Specify packets to reject
  permit Specify packets to forward
  remark Access list entry comment
R1(config)#access-list 199 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 199 permit tcp ?
  A.B.C.D Source address
  anyAny source host
  host A single source host
  R3(config)#access-list 199 permit tcp 10.101.117.32 ?
  A.B.C.D Source wildcard bits
```



R1(config)#access-list 199 permit tcp 10.101.117.32 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)#access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 ?

A.B.C.D Destination wildcard bits

R1(config)#access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 ?

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 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 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 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq telnet

R1(config)#access-list 199 ?

deny Specify packets to reject

permit Specify packets to forward

remark Access list entry comment

R1(config)#access-list 199 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 199 permit icmp ?

A.B.C.D Source address

anyAny source host

host A single source host

R1(config)#access-list 199 permit icmp any ?

A.B.C.D Destination address

anyAny destination host

host A single destination host

R1(config)#access-list 199 permit icmp any any

R1(config)#interface GigabitEthernet0/2

R1(config-if)#ip access-group 199 out

R1(config-if)# ^ Z

R1#exit

## ☛ Verify the extended ACL implementation

The screenshot shows a Windows Command Prompt window titled "PC2". The window has tabs at the top: Physical, Config, Desktop, Programming, and Attributes. The "Command Prompt" tab is active. The window displays the following output:

```
C:\>ping 10.101.117.61
Pinging 10.101.117.61 with 32 bytes of data:
Request timed out.
Reply from 10.101.117.61: bytes=32 time=15ms TTL=127
Reply from 10.101.117.61: bytes=32 time=13ms TTL=127
Reply from 10.101.117.61: bytes=32 time=9ms TTL=127

Ping statistics for 10.101.117.61:
    Packets: Sent = 3, Received = 3, Lost = 1 (33% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 11ms, Average = 10ms

C:\>telnet 10.101.117.2
Trying 10.101.117.2 . . . Open
[Connection to 10.101.117.2 closed by foreign host]
C:\>telnet 10.101.117.2
Trying 10.101.117.2 . . . Open

User Access Verification

Username: admin
Password: S3|
```

At the bottom left of the window, there is a "Top" button.

PC1



Physical Config Desktop Programming Attributes

Command Prompt



Packet Tracer PC Command Line 1.0

C:\&gt;ping 10.101.117.35

Pinging 10.101.117.35 with 32 bytes of data:

Reply from 10.101.117.35: bytes=32 time&lt;1ms TTL=127

Reply from 10.101.117.35: bytes=32 time=11ms TTL=127

Reply from 10.101.117.35: bytes=32 time=12ms TTL=127

Reply from 10.101.117.35: bytes=32 time&lt;1ms TTL=127

Ping statistics for 10.101.117.35:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 12ms, Average = 5ms

C:\&gt;telnet 10.101.117.2

Trying 10.101.117.2 ...

Connection timed out, remote host not responding

C:\&gt;