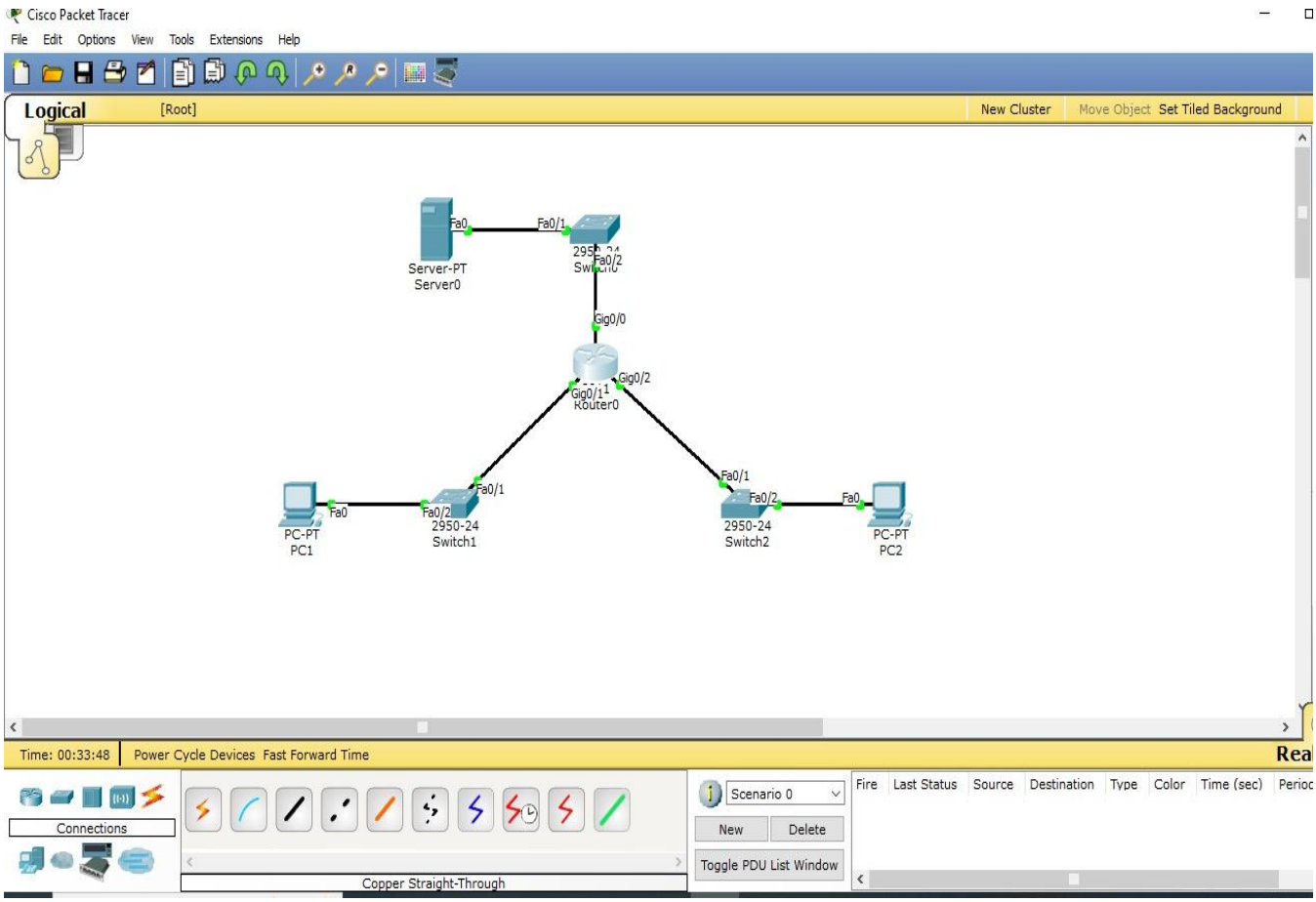
T.Y.B.Sc.IT
IT21036 **Security In Computing**

Date : 24/01/2024
Practical No : 3A

- **Aim : Configuring Extended ACLs**

➢ **Topology Diagram**

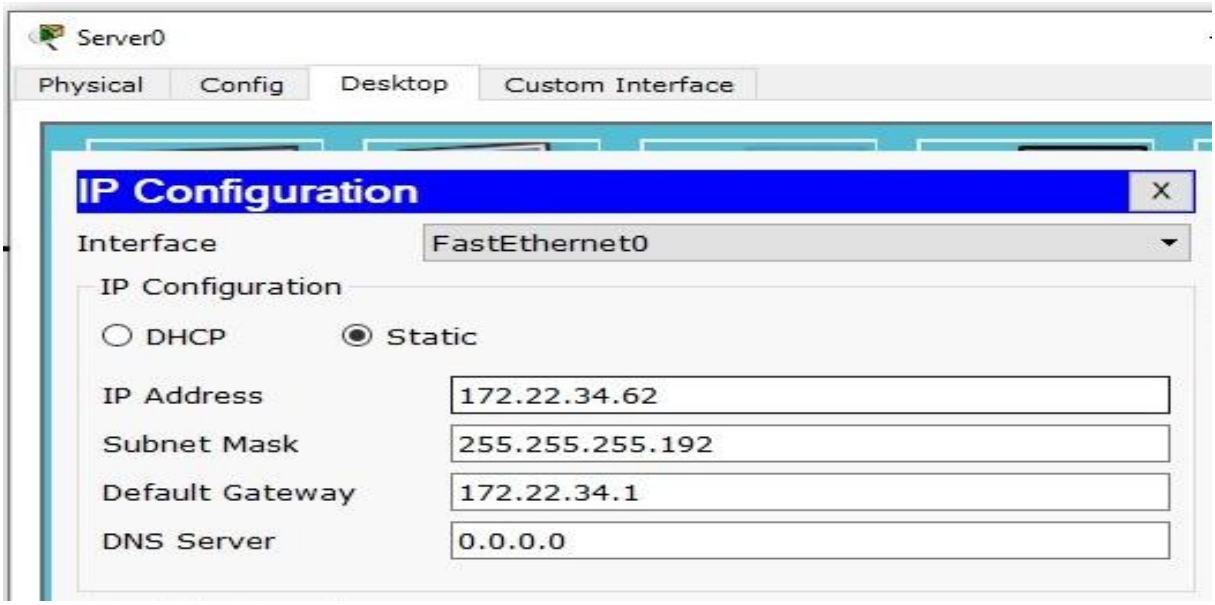


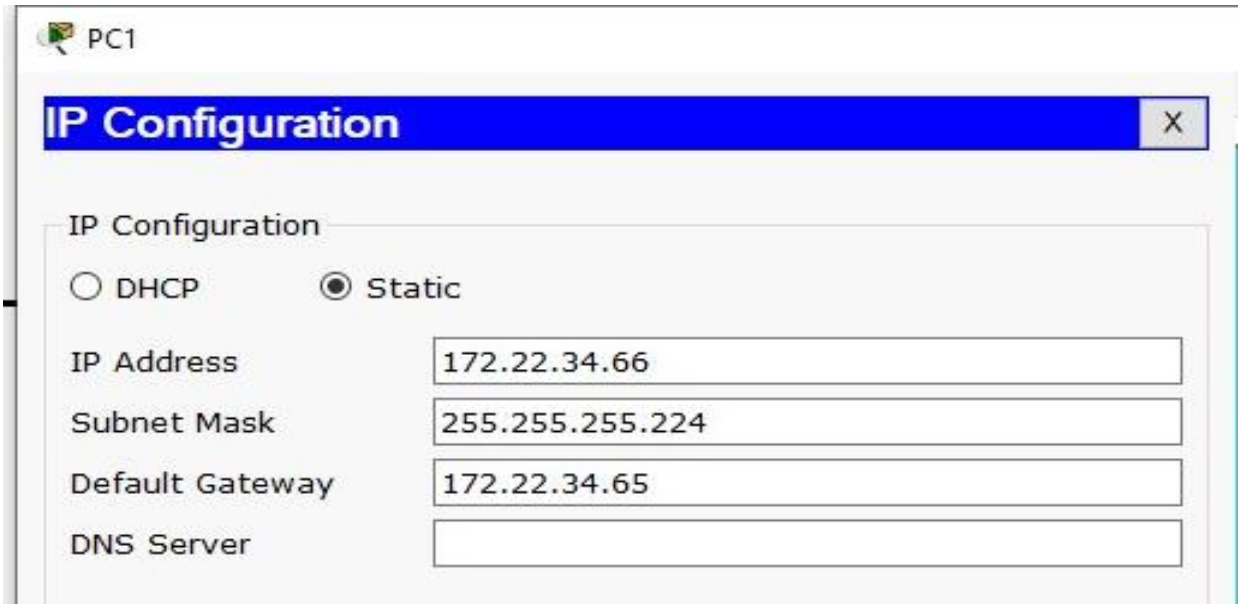
T.Y.B.Sc.IT
IT21036

Security In Computing

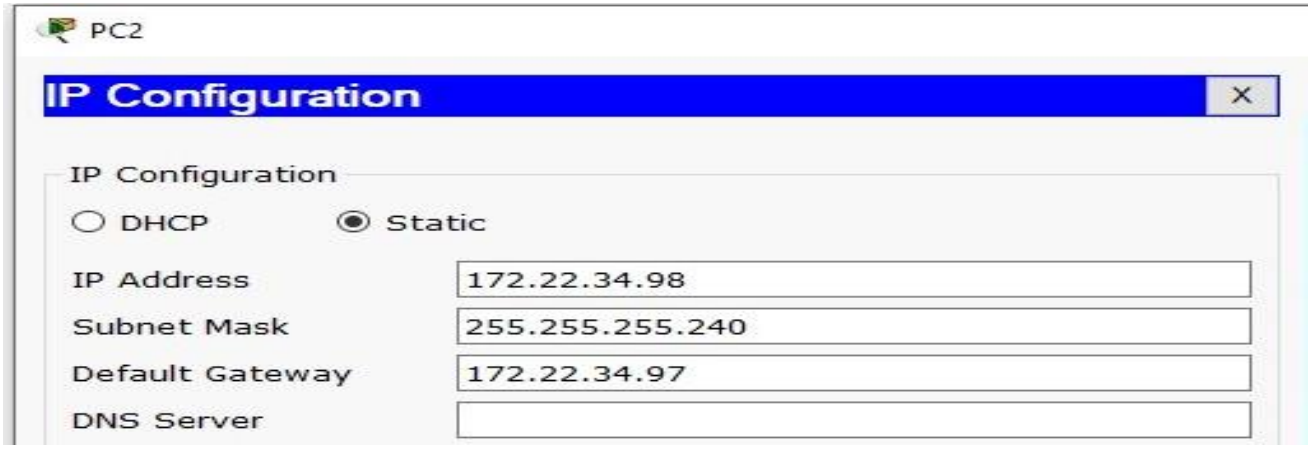
Date : 24/01/2024
Practical No : 3A

- **Assign IP Addresses**

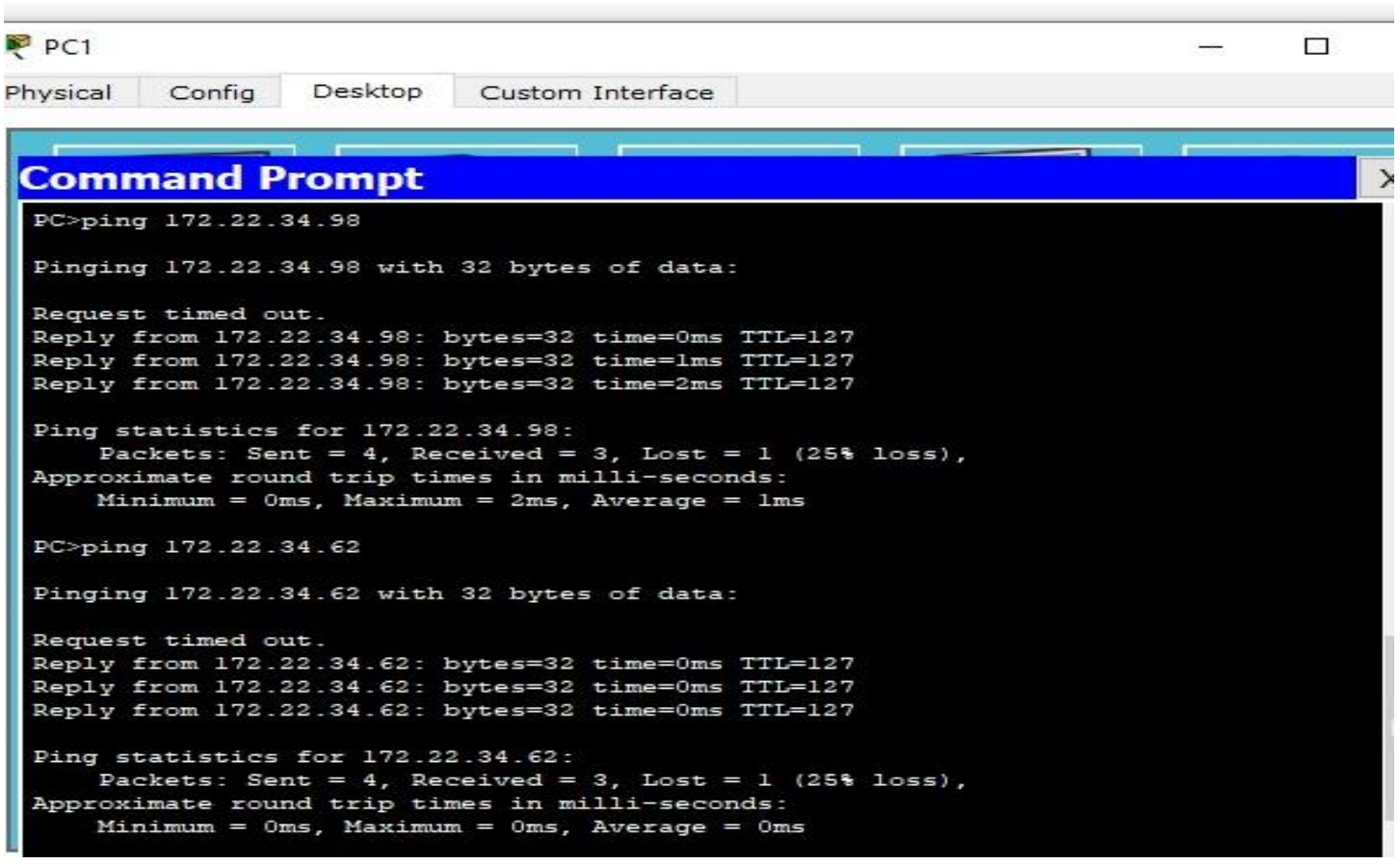




Date : 24/01/2024
Practical No : 3A



- **Performing Ping from PC1 to Server and PC2**

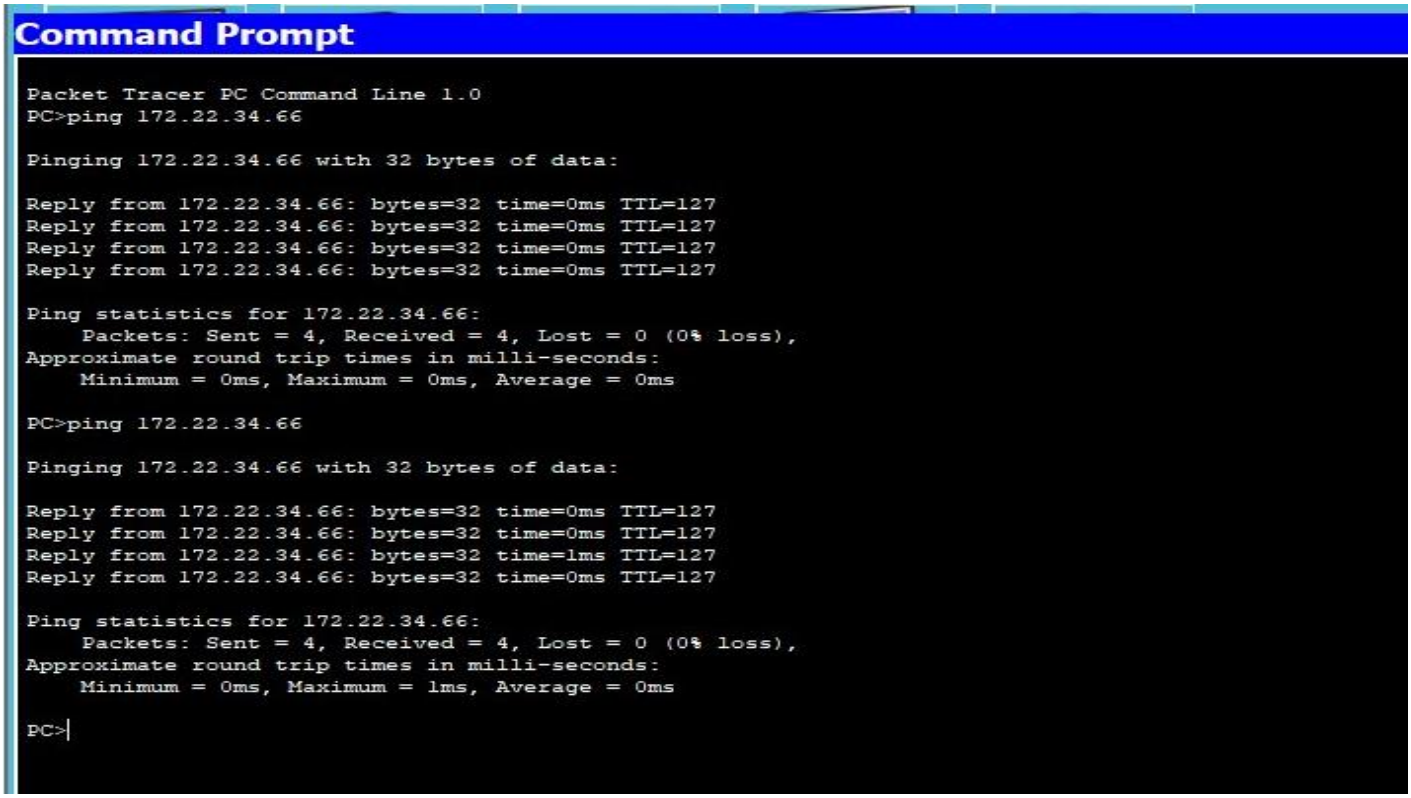


T.Y.B.Sc.IT
IT21036

Security In Computing

Date : 24/01/2024
Practical No : 3A

- **Performing Ping from PC2 to Server and PC1**



T.Y.B.Sc.IT
IT21036 **Security In Computing**

Date : 24/01/2024
Practical No : 3A

- **Configure, Apply and Verify an Extended Numbered ACL**

  (PC1 needs only FTP access and should be able to ping the server, but not PC2)

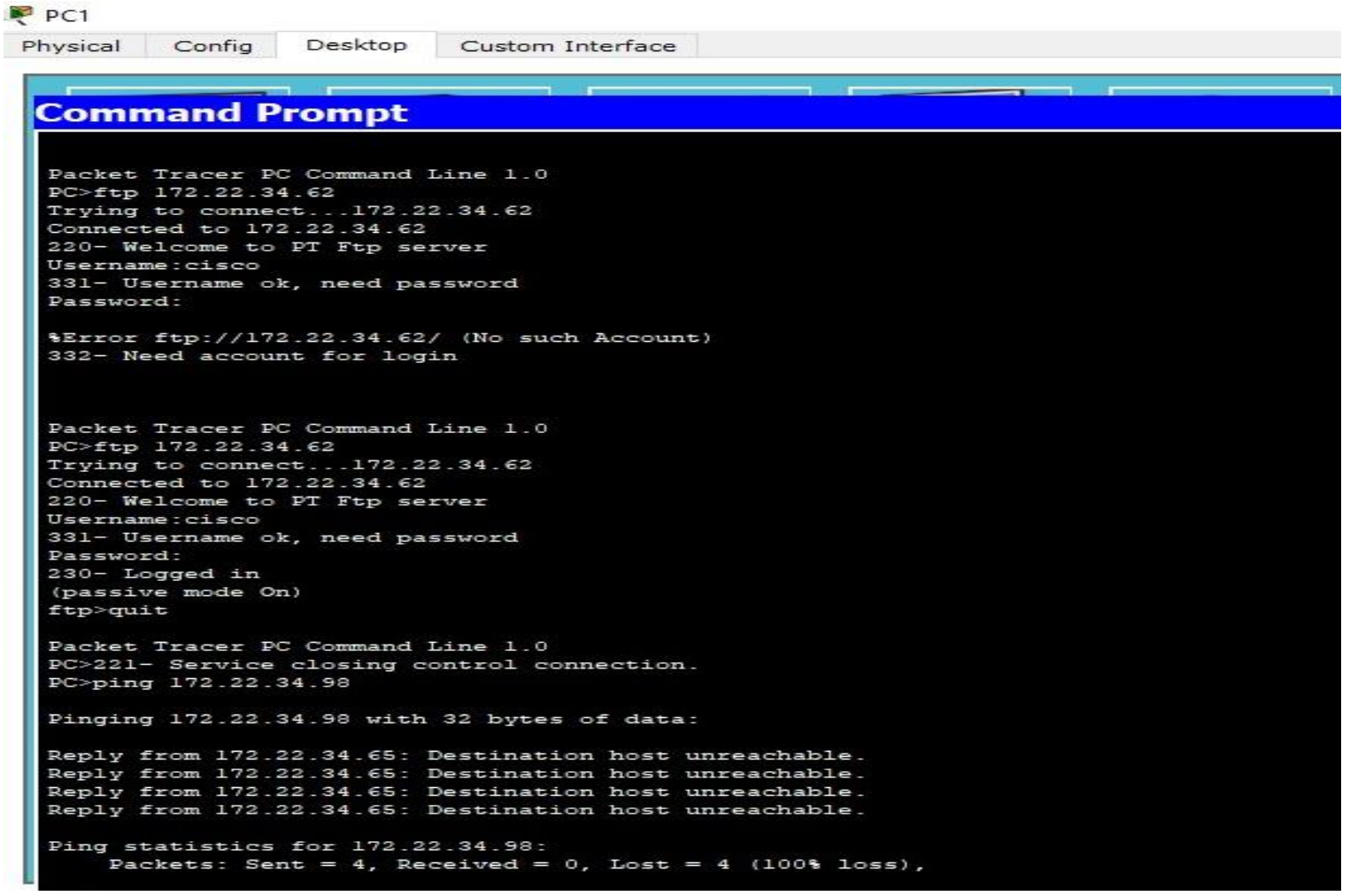
```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list ?
  extended  Extended Access List
  standard  Standard Access List
Router(config)#ip access-list extended ?
  <100-199>  Extended IP access-list number
  WORD        name
Router(config)#ip access-list extended HTTP-ACL
Router(config-ext-nacl)#permit tcp 172.22.34.96 ?
  A.B.C.D  Source wildcard bits
Router(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
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host ?
  A.B.C.D  Destination address
Router(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>
Router(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)
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq ww
w
```

T.Y.B.Sc.IT
IT21036 **Security In Computing**

Date : 24/01/2024
Practical No : 3A

```
Router(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
Router(config-ext-nacl)#interface GigabitEthernet0/1
Router(config-if)#ip access-group HTTP_ACL in
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

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



T.Y.B.Sc.IT
IT21036

Security In Computing

Date : 24/01/2024
Practical No : 3A

- **Configure, Apply and Verify an Extended Numbered ACL**

  (PC2 needs only web access and should be able to ping the server, but not PC1)

Date : 24/01/2024
Practical No : 3A

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list ?
  extended  Extended Access List
  standard  Standard Access List
Router(config)#ip access-list extended ?
  <100-199>  Extended IP access-list number
  WORD        name
Router(config)#ip access-list extended HTTP-ACL
Router(config-ext-nacl)#permit tcp 172.22.34.96 ?
  A.B.C.D  Source wildcard bits
Router(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
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host ?
  A.B.C.D  Destination address
Router(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>
Router(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)
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq ww
w
```

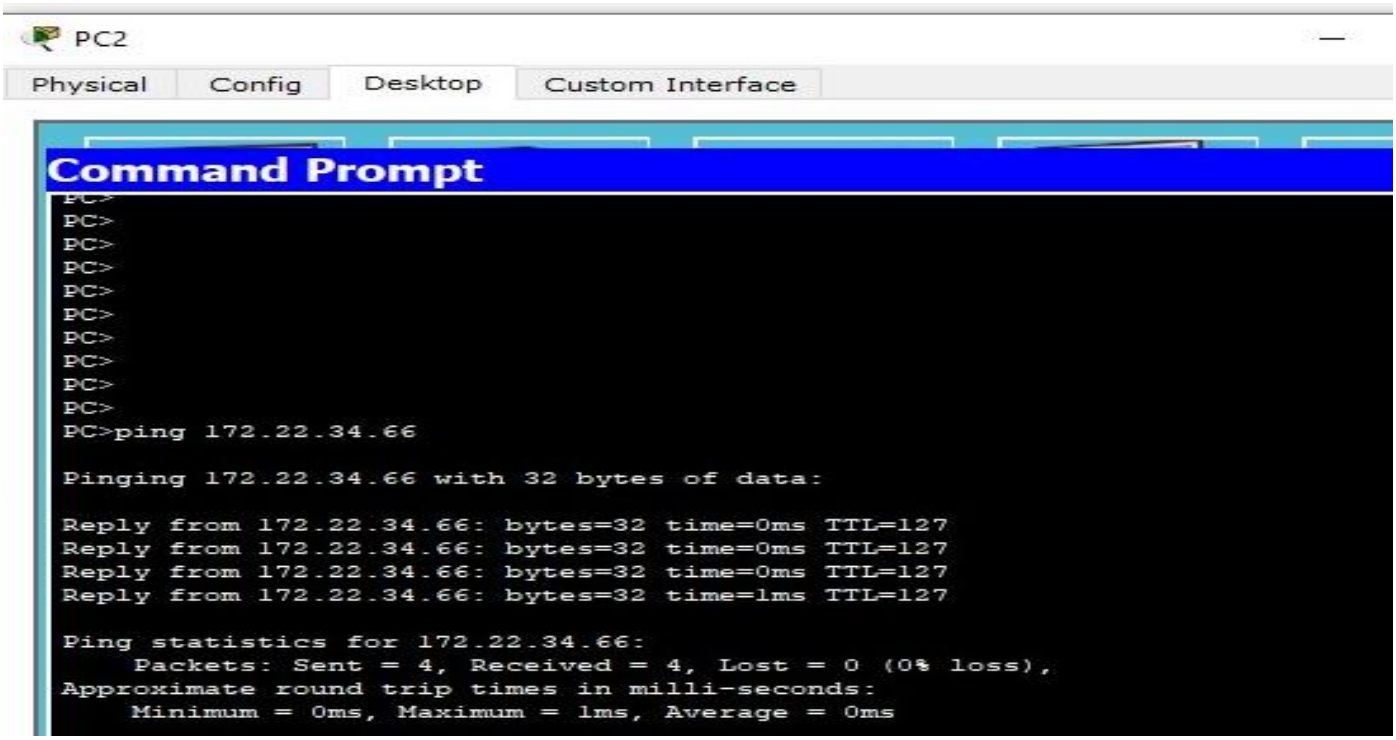
```
Router(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
Router(config-ext-nacl)#interface GigabitEthernet0/1
Router(config-if)#ip access-group HTTP_ACL in
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

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

T.Y.B.Sc.IT
IT21036 **Security In Computing**

Date : 24/01/2024
Practical No : 3A

- **Checking http connection from PC2**

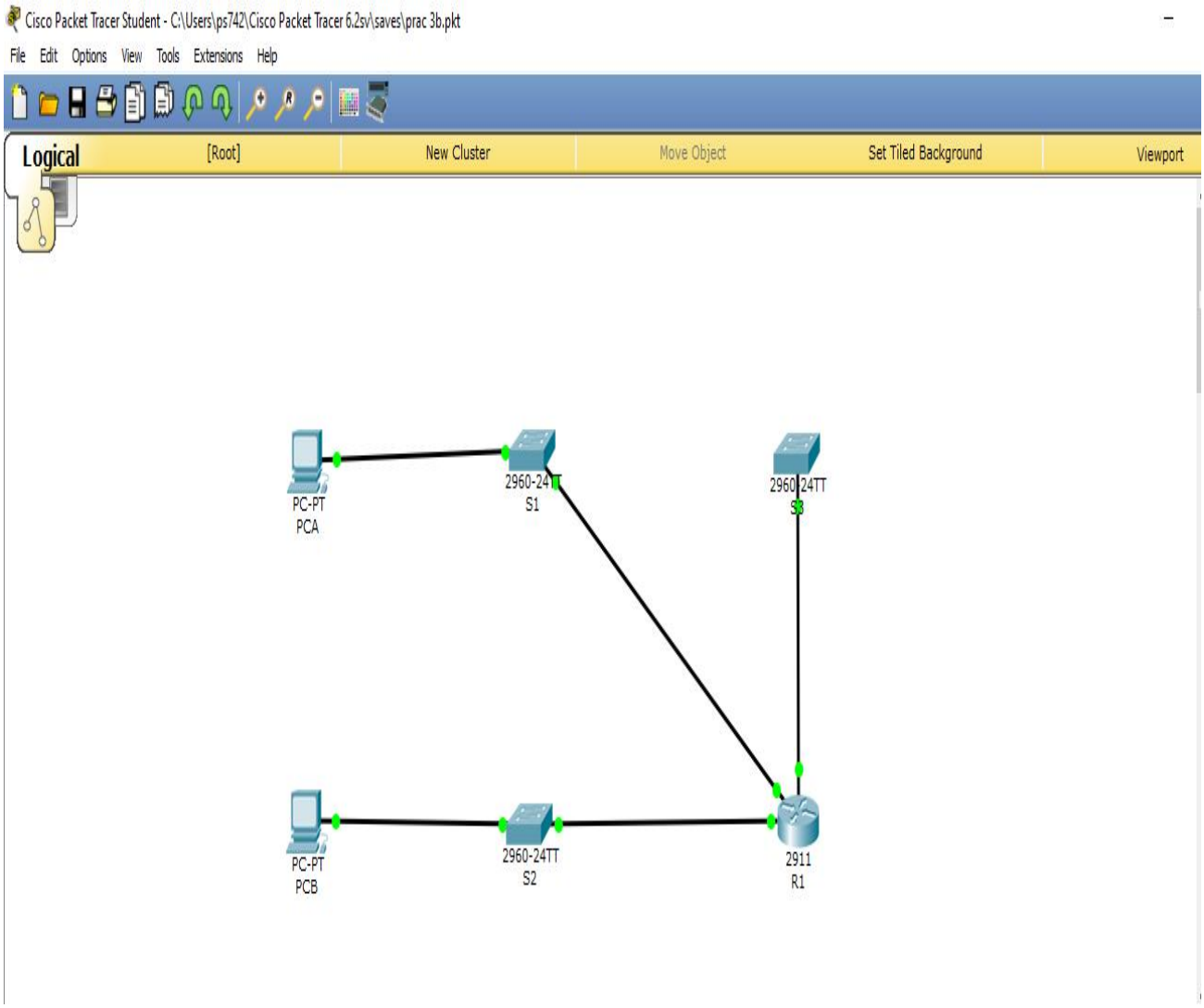


T.Y.B.Sc.IT
IT21036 **Security In Computing**

Date : 24/01/2024
Practical No : 3B

- **Aim :- Configure, Apply and Verify an Extended Numbered ACL**

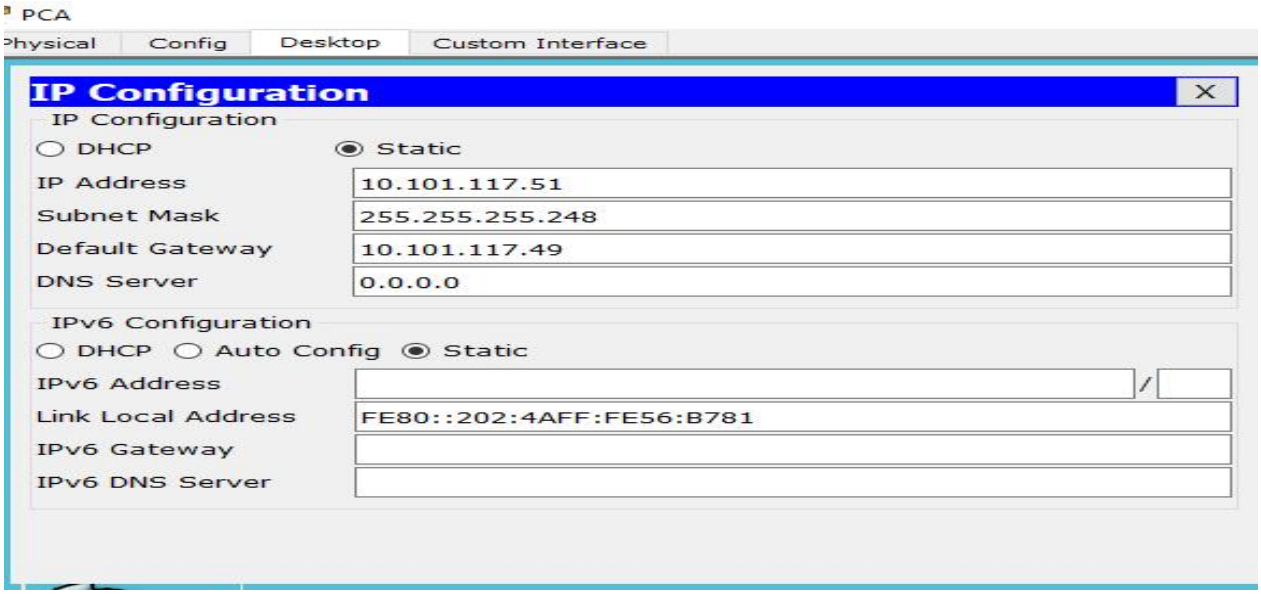
➢ **Topology Diagram**

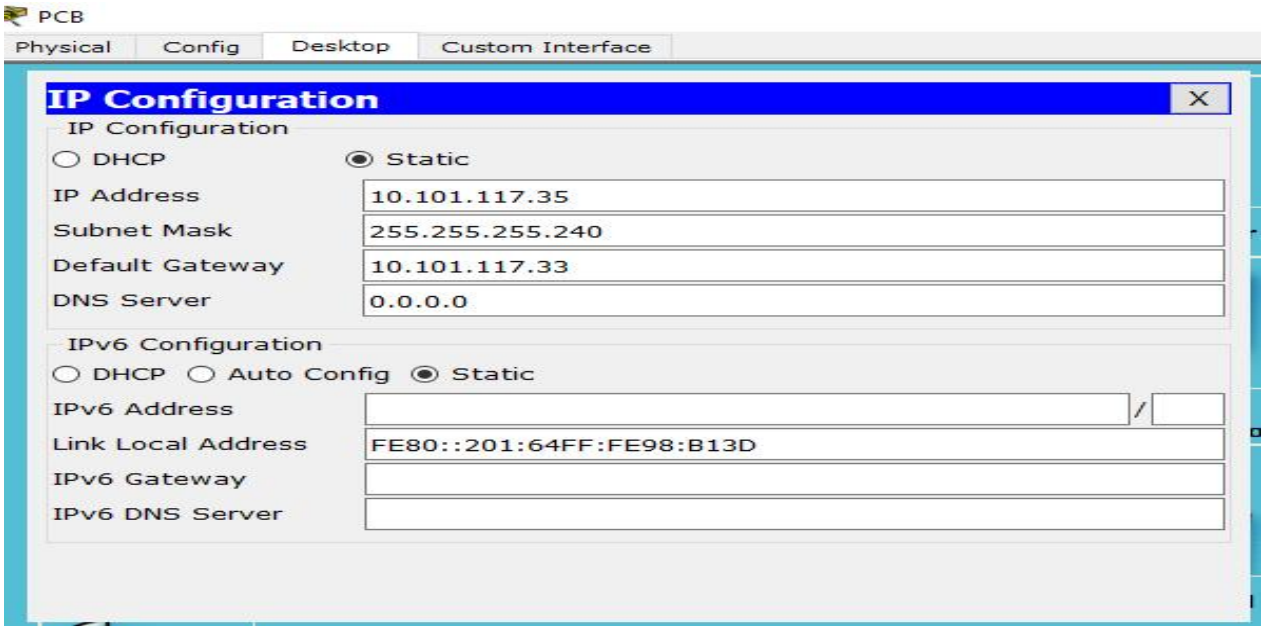


T.Y.B.Sc.IT
IT21036 **Security In Computing**

Date : 24/01/2024
Practical No : 3B

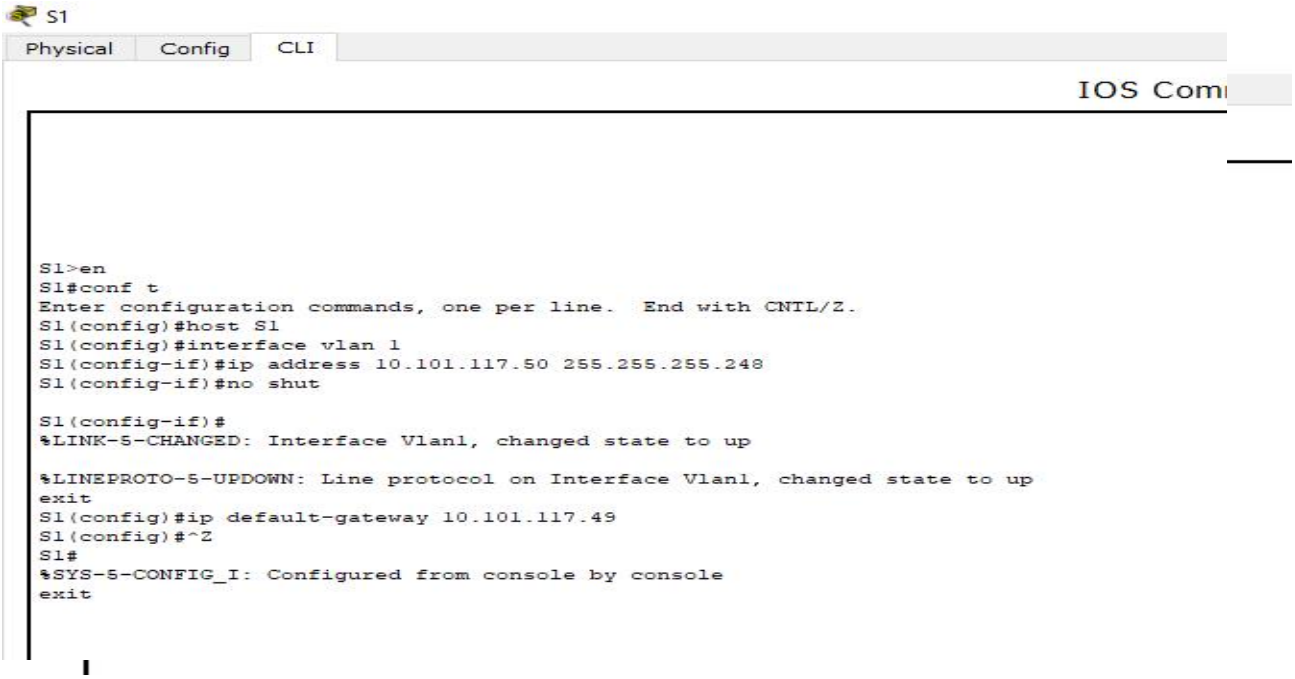
- **Assign IP Addresses**





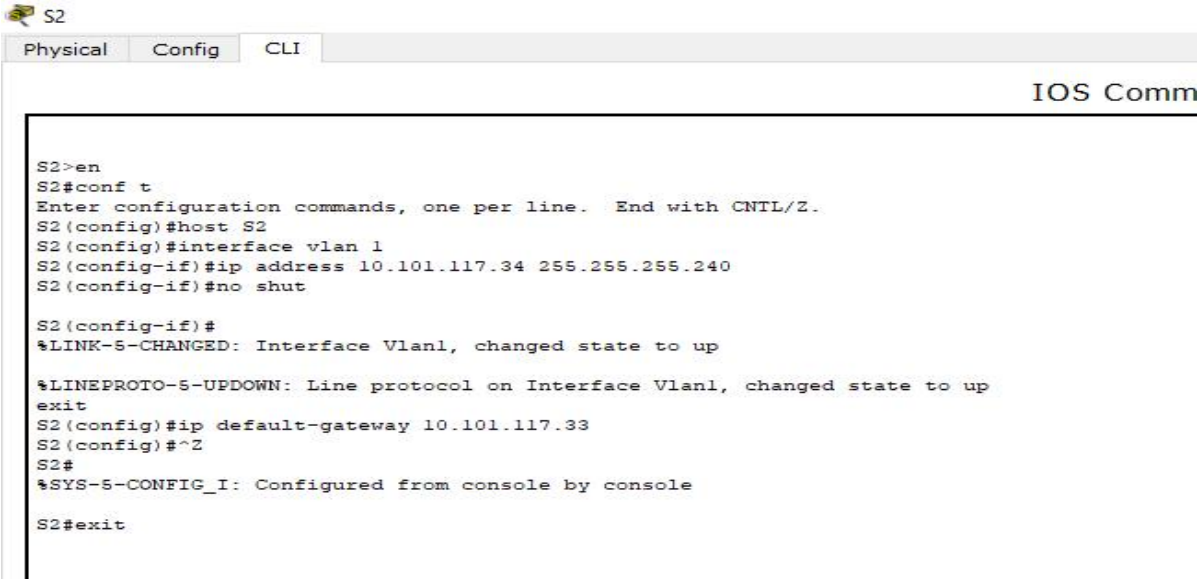
T.Y.B.Sc.IT
IT21036 **Security In Computing**

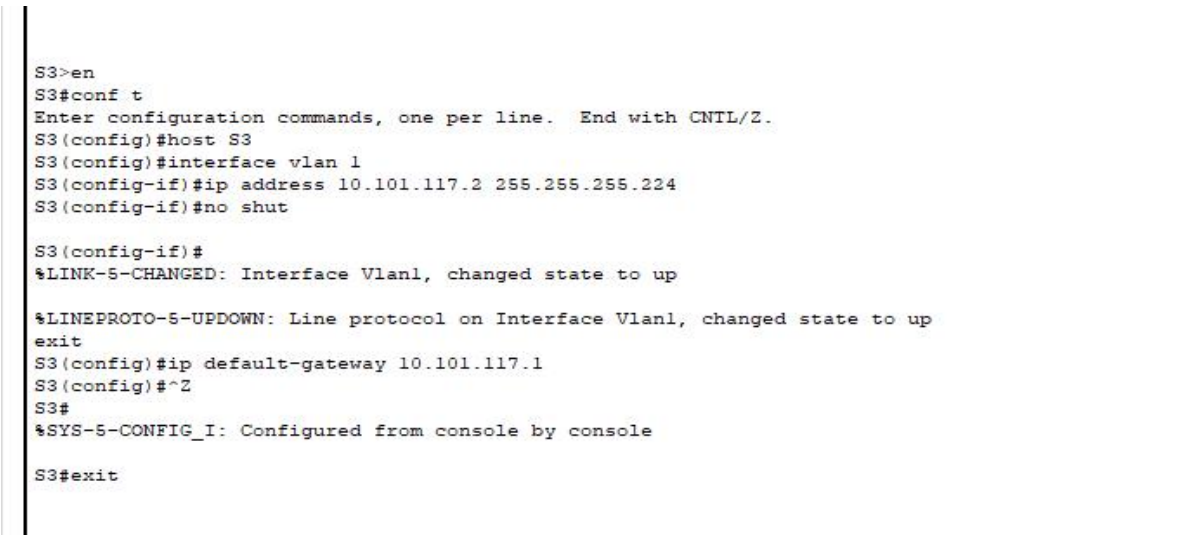
Date : 24/01/2024
Practical No : 3B



T.Y.B.Sc.IT
IT21036 **Security In Computing**

Date : 24/01/2024
Practical No : 3B





T.Y.B.Sc.IT
IT21036 **Security In Computing**

Date : 24/01/2024
Practical No : 3B

- **Displaying IP Addresses 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
```

- **Configuring Telnet on S3**

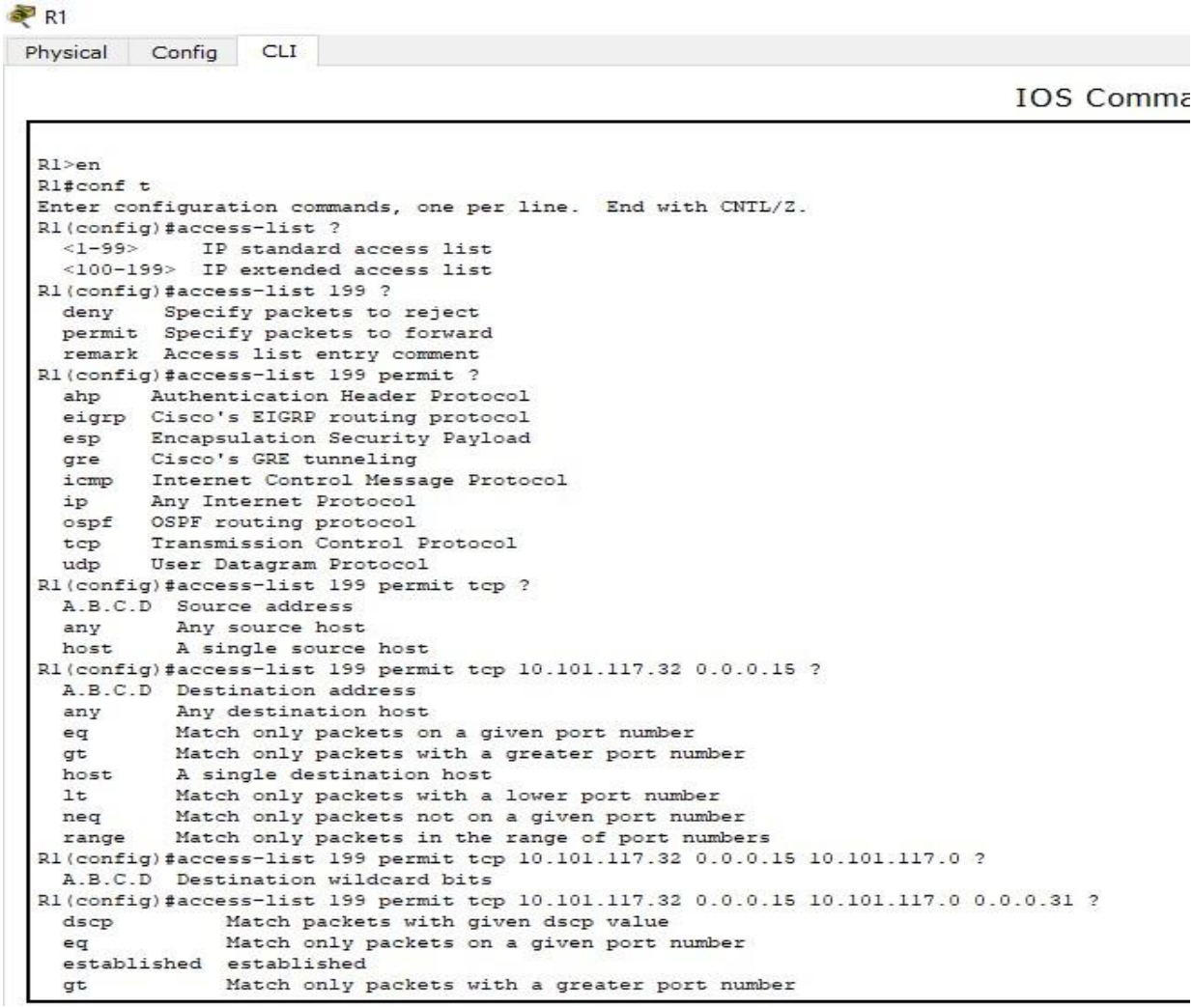
```
S3>en
S3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#username admin password teacher
S3(config)#line vty 0 4
S3(config-line)#login local
S3(config-line)#^Z
S3#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

T.Y.B.Sc.IT
IT21036 **Security In Computing**

Date : 24/01/2024
Practical No : 3B

◆ 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.)



T.Y.B.Sc.IT
IT21036 **Security In Computing**

Date : 24/01/2024
Practical No : 3B

R1

Physical Config CLI

IOS Command

```
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
  any      Any source host
  host     A single source host
R1(config)#access-list 199 permit icmp any ?
  A.B.C.D  Destination address
  any      Any 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#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

- **Verify the extended ACL implementation**

PC-B

```
PC>ping 10.101.117.51

Pinging 10.101.117.51 with 32 bytes of data:

Reply from 10.101.117.51: bytes=32 time=0ms TTL=127
Reply from 10.101.117.51: bytes=32 time=0ms TTL=127
Reply from 10.101.117.51: bytes=32 time=20ms TTL=127
Reply from 10.101.117.51: bytes=32 time=0ms TTL=127

Ping statistics for 10.101.117.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 20ms, Average = 5ms

PC>telnet 10.101.117.2
Trying 10.101.117.2 ...Open


User Access Verification

Username: admin
Password:
S3>
```

T.Y.B.Sc.IT
IT21036 **Security In Computing**

Date : 24/01/2024
Practical No : 3B

PC-A