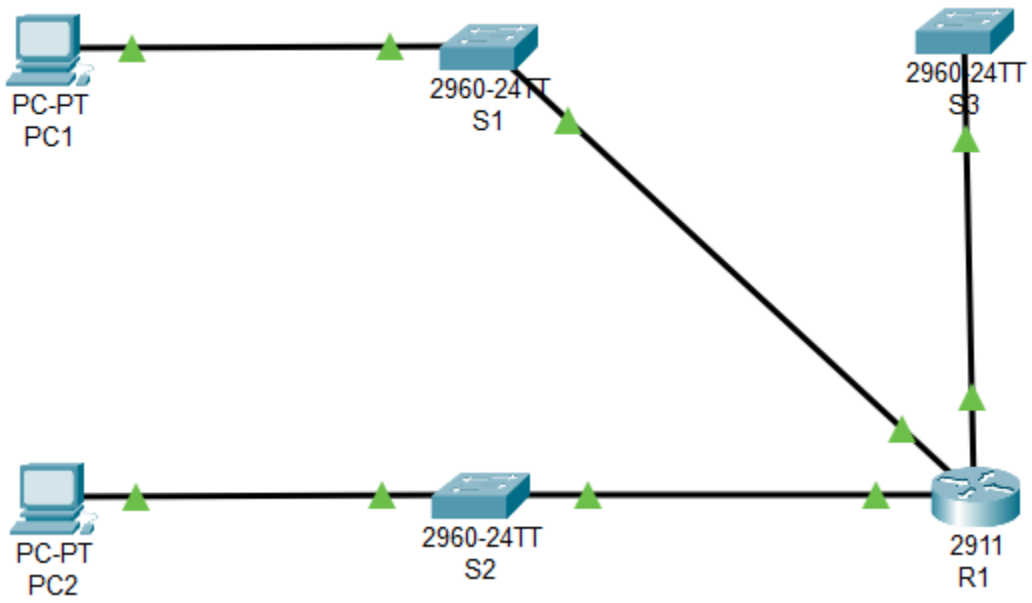
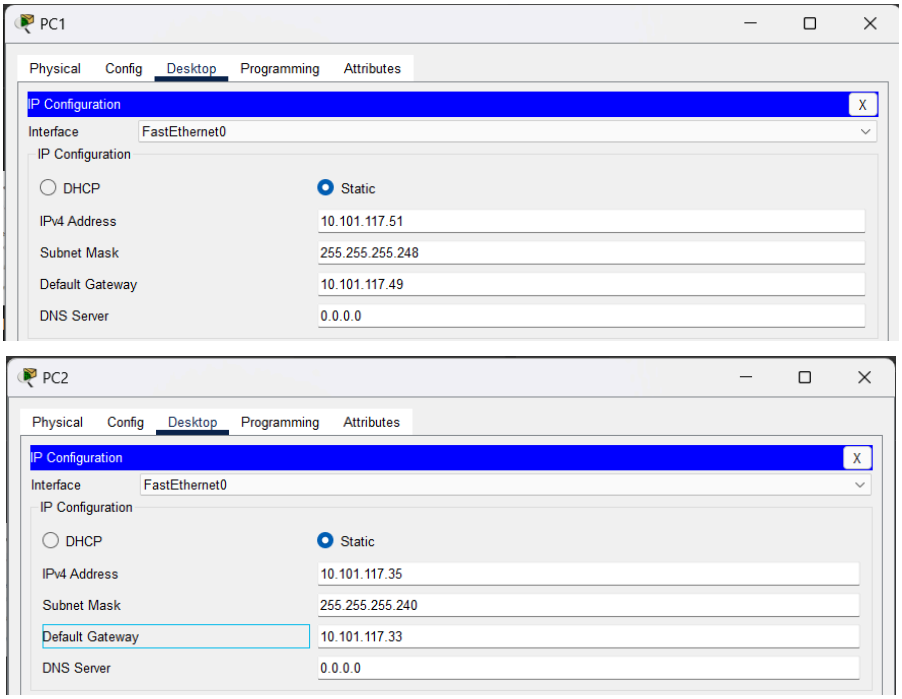
Security in Computing
Practical - 3B

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

Topology Diagram:



Assign IP Addresses:



```
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 10.101.117.49 255.255.255.248
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 10.101.117.33 255.255.255.240
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 10.101.117.1 255.255.255.224
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
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#exit
S1(config)#ip default-gateway 10.101.117.49
S1(config)#^Z
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#exit
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if)#exit
S2(config)#ip default-gateway 10.101.117.33
S2(config)#^Z
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#exit
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S3(config-if)#exit
S3(config)#ip default-gateway 10.101.117.1
S3(config)#^Z
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#exit
```

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
Vlan1                  unassigned      YES unset  administratively down down
```

```
S1>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  10.101.117.50   YES manual up                    up
```

```
S2>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  10.101.117.34   YES manual up                    up
```

```
S3>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  10.101.117.2    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

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
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 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
  any      Any source host
  host     A single source host
R1(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
  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 GigabitInterface0/2
                           ^
% Invalid input detected at '^' marker.

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

R1#exit
```

Verify the Extended ACL implementation: