

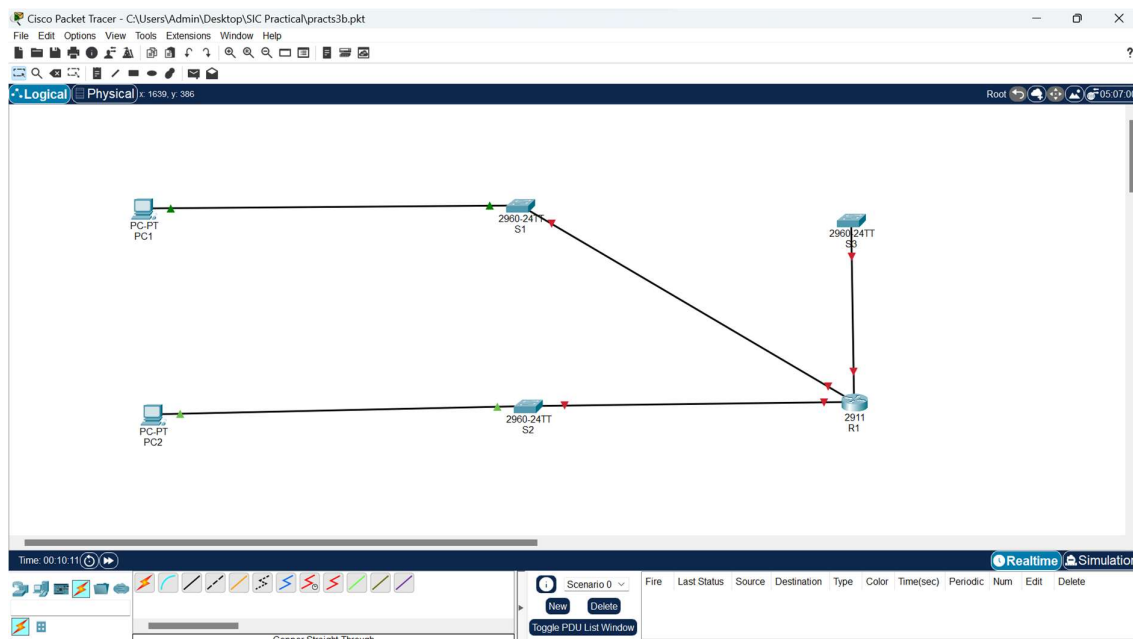
Date: 05/02/2024

Security in Computing

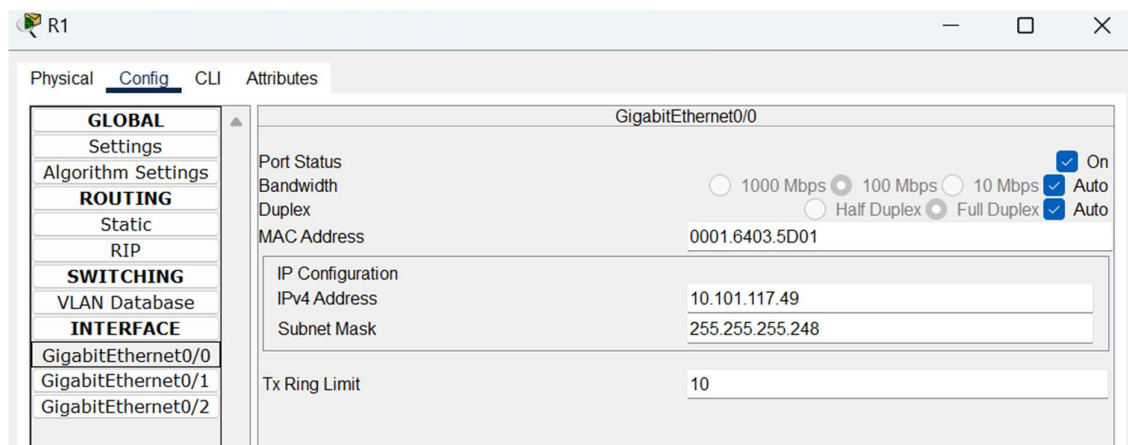
Practical 3B:

Aim: Configure, Apply and Verify an Extended Numbered ACL

➤ Topology Diagram:



➤ Assign IP Addresses



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 ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ On

Bandwidth ☐ Half Duplex ☒ Full Duplex ☒ Auto

Duplex

MAC Address 0001.6403.5D02

IP Configuration

IPv4 Address 10.101.117.33

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 ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ On

Bandwidth ☐ Half Duplex ☒ Full Duplex ☒ Auto

Duplex

MAC Address 0001.6403.5D03

IP Configuration

IPv4 Address 10.101.117.1

Subnet Mask 255.255.255.224

Tx Ring Limit 10

S1

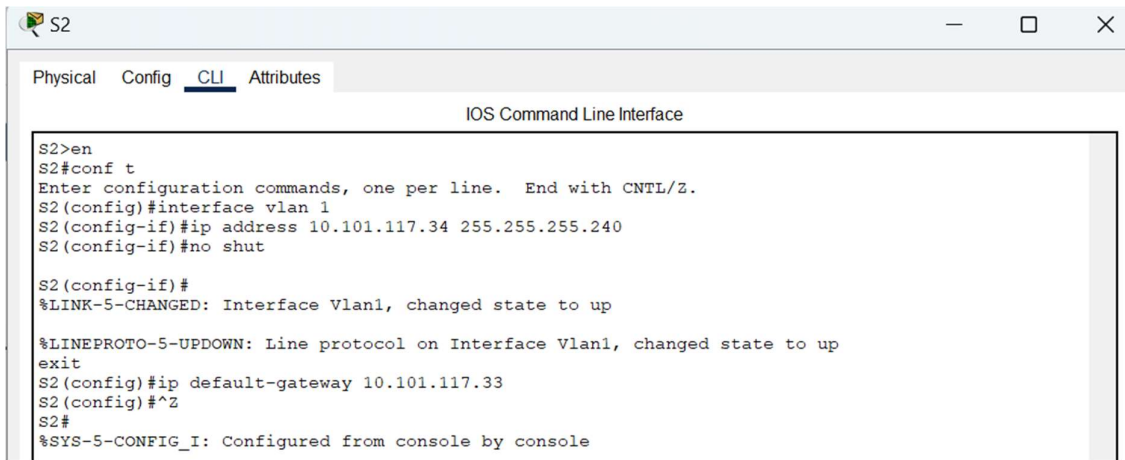
Physical Config CLI Attributes

IOS Command Line Interface

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



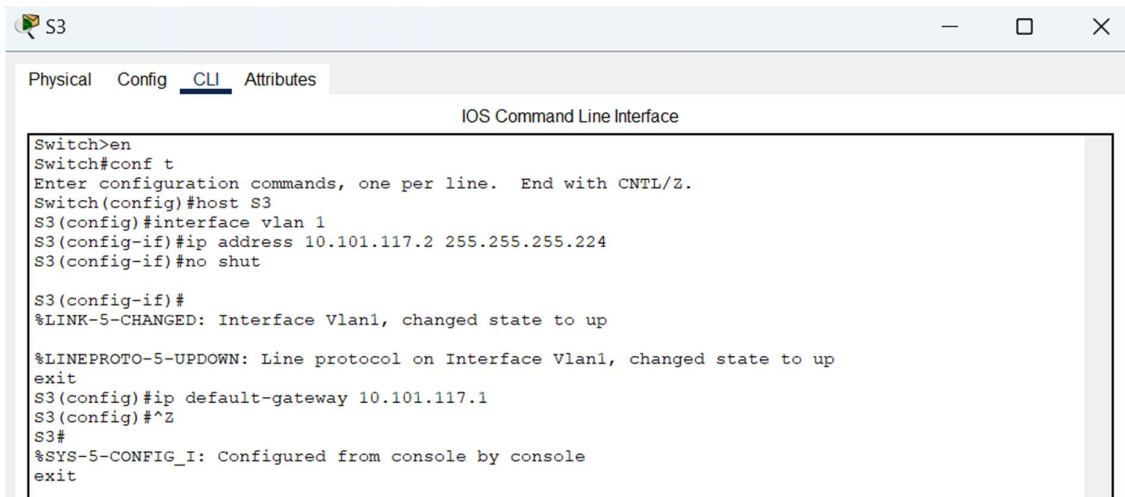
S2

Physical Config CLI Attributes

IOS Command Line Interface

```
S2>en
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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
exit
S2(config)#ip default-gateway 10.101.117.33
S2(config)#^Z
S2#
%SYS-5-CONFIG_I: Configured from console by console
```



S3

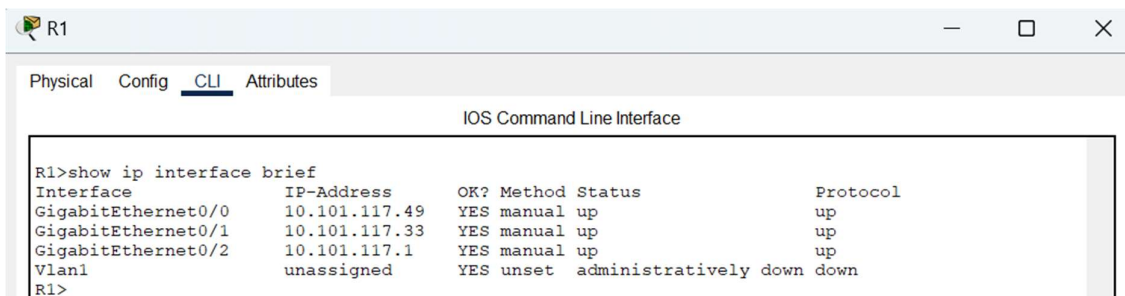
Physical Config CLI Attributes

IOS Command Line Interface

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

➤ Displaying IP Address Details



R1

Physical Config CLI Attributes

IOS Command Line Interface

```
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

```
R1>
```

S1

Physical Config CLI Attributes

IOS Command Line Interface

```
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

S1>

S2

Physical Config CLI Attributes

IOS Command Line Interface

```
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

S2>

```

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
S3>

```

➤ 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

```

➤ 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

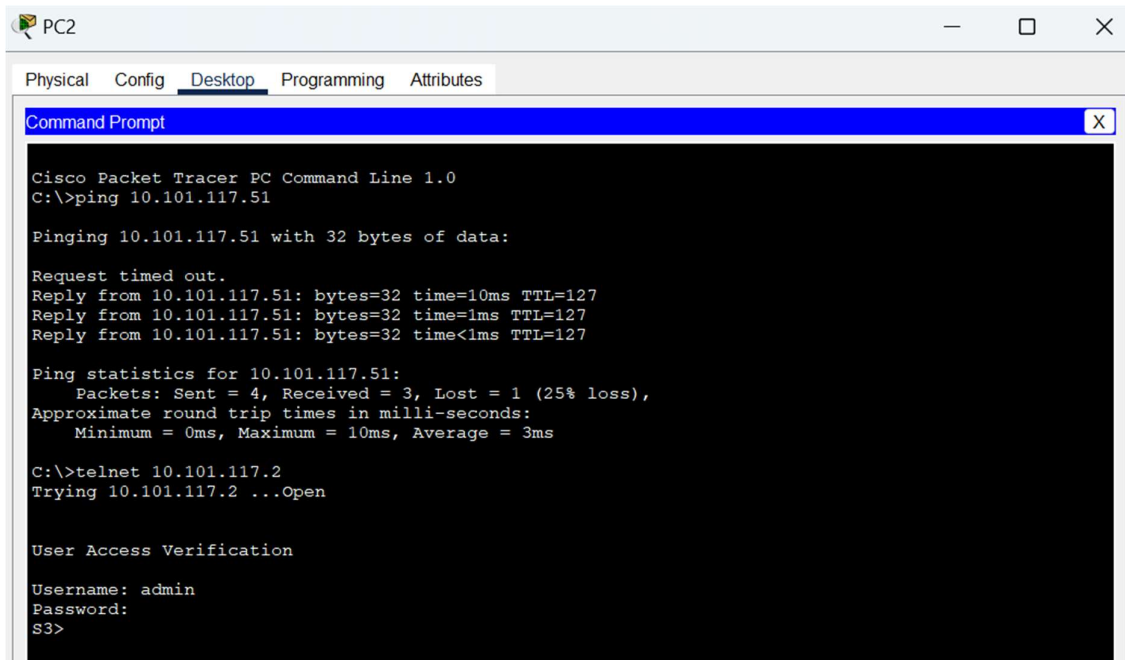
```

```

R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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



The screenshot shows the PC2 window in Cisco Packet Tracer. The 'Desktop' tab is selected, and a 'Command Prompt' window is open. The command prompt displays the output of a ping command to 10.101.117.51 and a telnet command to 10.101.117.2. The ping command shows a 25% loss of packets. The telnet command shows a successful connection to the user 'admin'.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.101.117.51

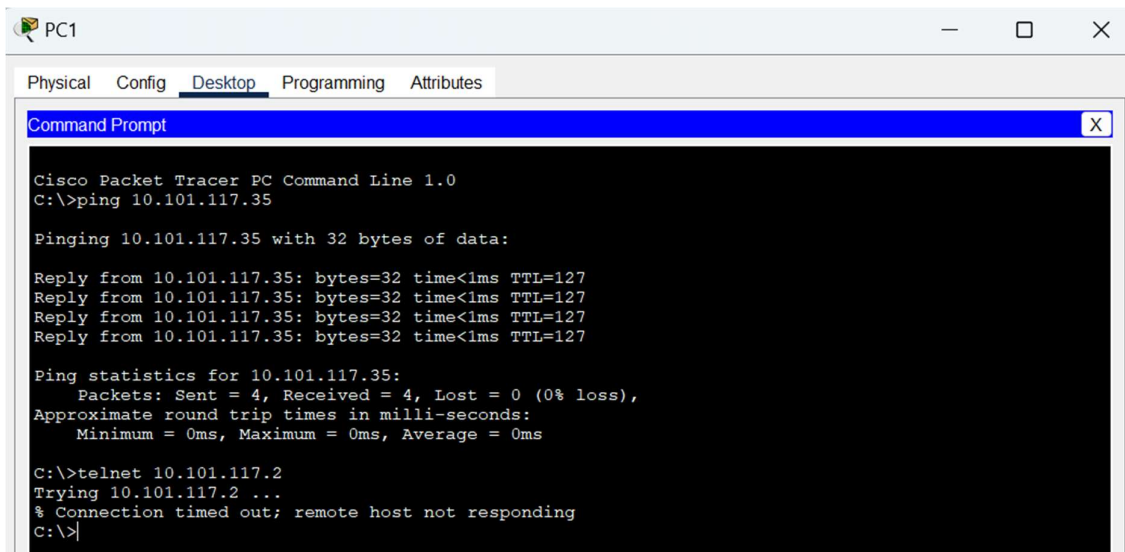
Pinging 10.101.117.51 with 32 bytes of data:

Request timed out.
Reply from 10.101.117.51: bytes=32 time=10ms TTL=127
Reply from 10.101.117.51: bytes=32 time=1ms TTL=127
Reply from 10.101.117.51: bytes=32 time<1ms TTL=127

Ping statistics for 10.101.117.51:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>telnet 10.101.117.2
Trying 10.101.117.2 ...Open

User Access Verification
Username: admin
Password:
S3>
```



The screenshot shows the PC1 window in Cisco Packet Tracer. The 'Desktop' tab is selected, and a 'Command Prompt' window is open. The command prompt displays the output of a ping command to 10.101.117.35 and a telnet command to 10.101.117.2. The ping command shows 0% loss of packets. The telnet command shows a connection timed out.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.101.117.35

Pinging 10.101.117.35 with 32 bytes of data:

Reply from 10.101.117.35: bytes=32 time<1ms TTL=127
Reply from 10.101.117.35: bytes=32 time<1ms TTL=127
Reply from 10.101.117.35: bytes=32 time<1ms TTL=127
Reply from 10.101.117.35: bytes=32 time<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 = 0ms, Average = 0ms

C:\>telnet 10.101.117.2
Trying 10.101.117.2 ...
% Connection timed out; remote host not responding
C:\>
```