

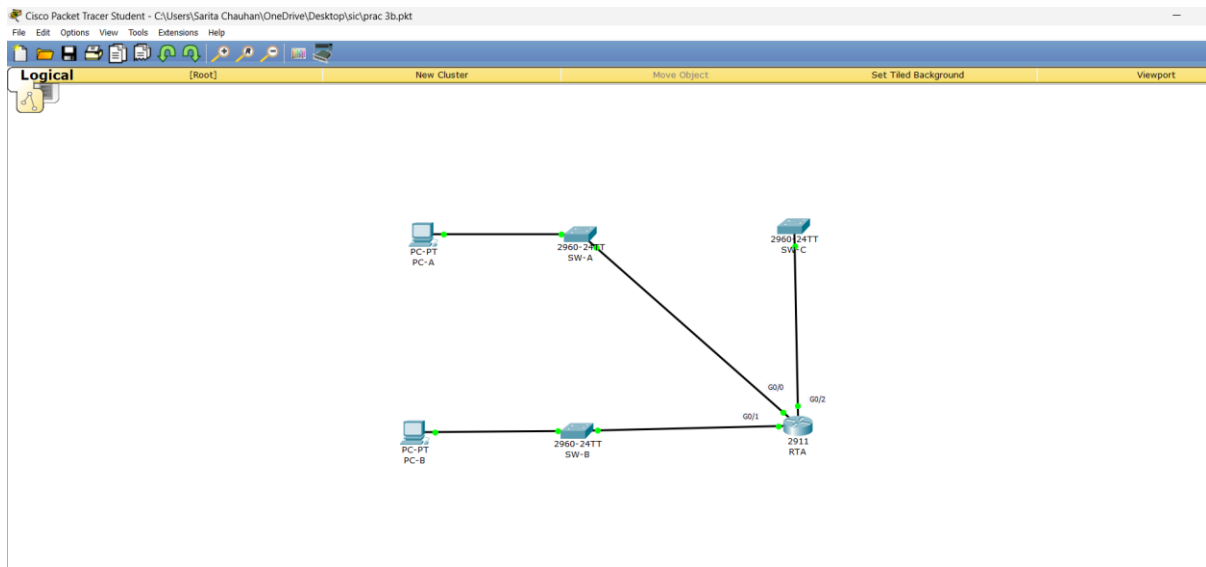
Date: 24/01/2024

Security in Computing

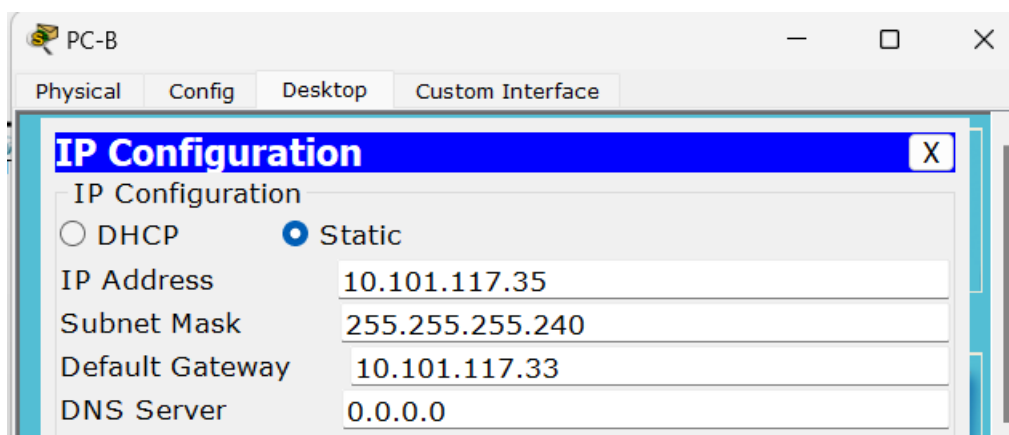
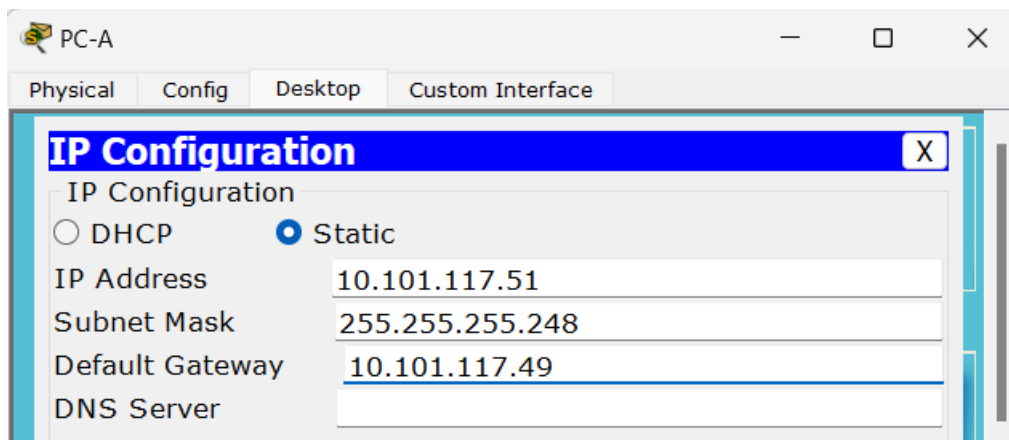
Practical 3B:

Aim: Configure, Apply and Verify an Extended Numbered ACL

➤ **Topology Diagram:**



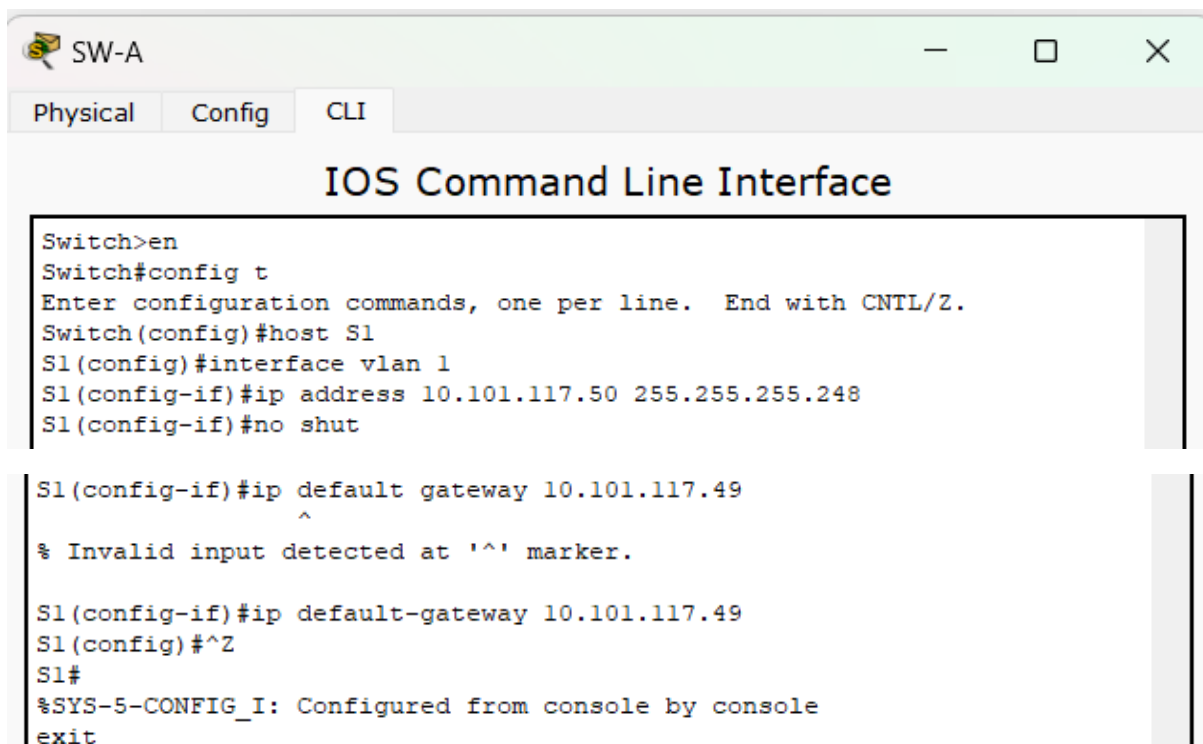
➤ **Assign IP Addresses**





The image shows a network simulator window titled 'RTA' with tabs for 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal shows a sequence of commands to configure a router named R1. It enters configuration mode, sets three interfaces (GigabitEthernet0/0, 0/1, and 0/2) with IP addresses 10.101.117.49, 10.101.117.33, and 10.101.117.1 respectively, all with a 255.255.255.248 subnet mask. It then exits configuration mode and saves the configuration.

```
RTA>en
RTA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RTA(config)#interface GigabitEthernet0/0
RTA(config-if)#ip address 10.101.117.49 255.255.255.248
RTA(config-if)#no shut
RTA(config-if)#interface GigabitEthernet0/1
RTA(config-if)#ip address 10.101.117.33 255.255.255.240
RTA(config-if)#no shut
RTA(config-if)#interface GigabitEthernet0/2
RTA(config-if)#ip address 10.101.117.1 255.255.255.224
RTA(config-if)#no shut
RTA(config-if)#^Z
RTA#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

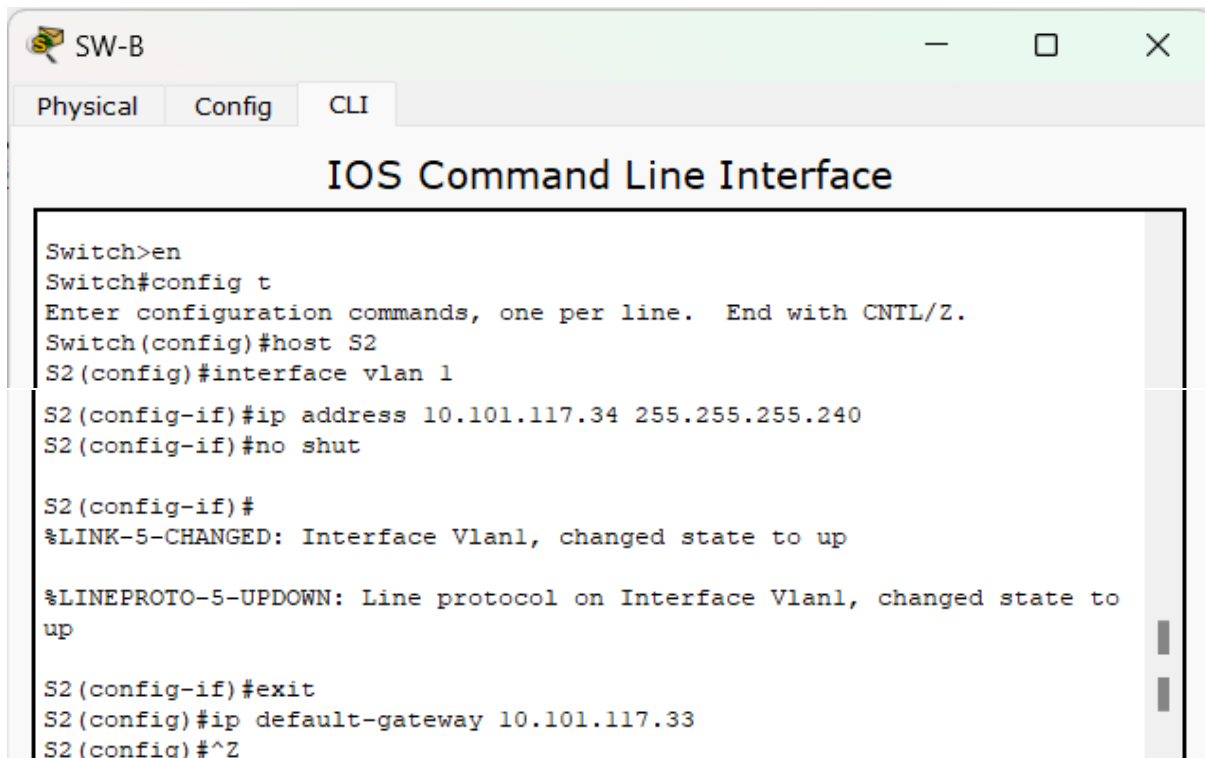


The image shows a network simulator window titled 'SW-A' with tabs for 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal shows a sequence of commands to configure a switch named S1. It enters configuration mode, sets the host name to S1, and configures interface vlan 1 with IP address 10.101.117.50 and a 255.255.255.248 subnet mask. It then attempts to set a default gateway to 10.101.117.49 but receives an error for an invalid input marker. It corrects the command to 'default-gateway' and then exits configuration mode and saves the configuration.

```
Switch>en
Switch#config 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)#ip default gateway 10.101.117.49
      ^
% Invalid input detected at '^' marker.

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



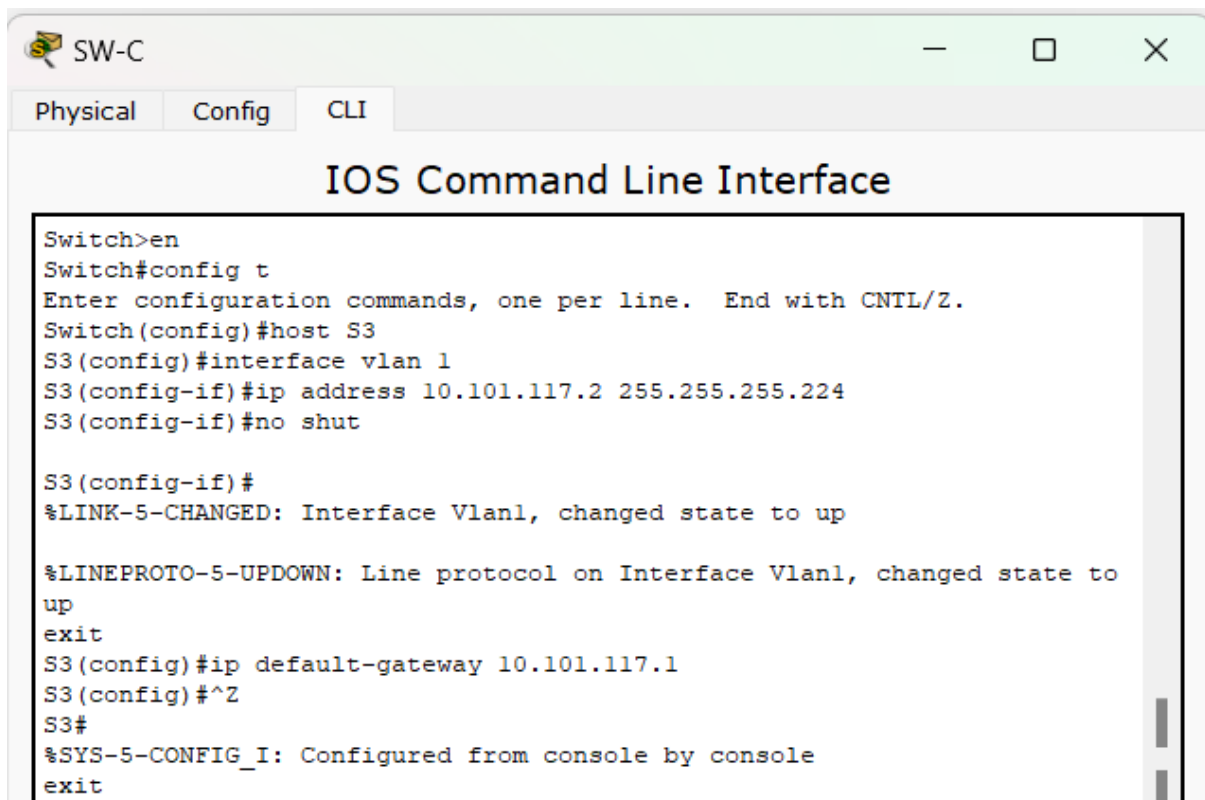
The screenshot shows a window titled 'SW-B' with tabs for 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal text shows the configuration of interface Vlan1 on switch S2, including IP address assignment and enabling the interface.

```
Switch>en
Switch#config 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
```



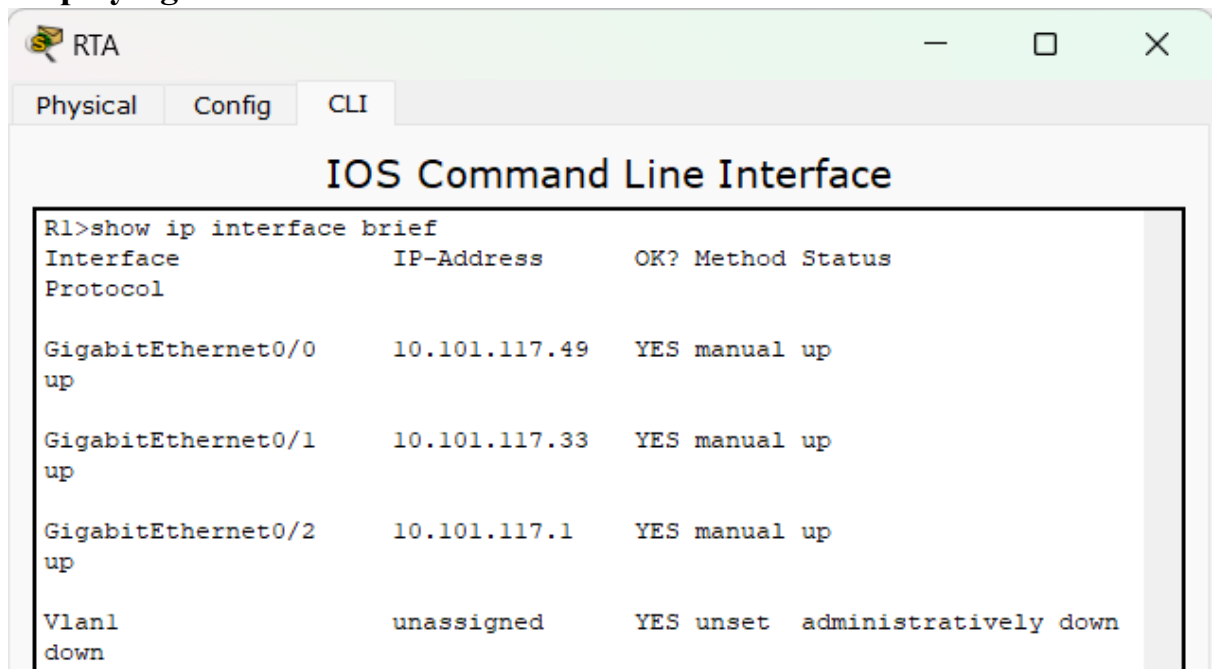
The screenshot shows a window titled 'SW-C' with tabs for 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal text shows the configuration of interface Vlan1 on switch S3, including IP address assignment and enabling the interface.

```
Switch>en
Switch#config 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**



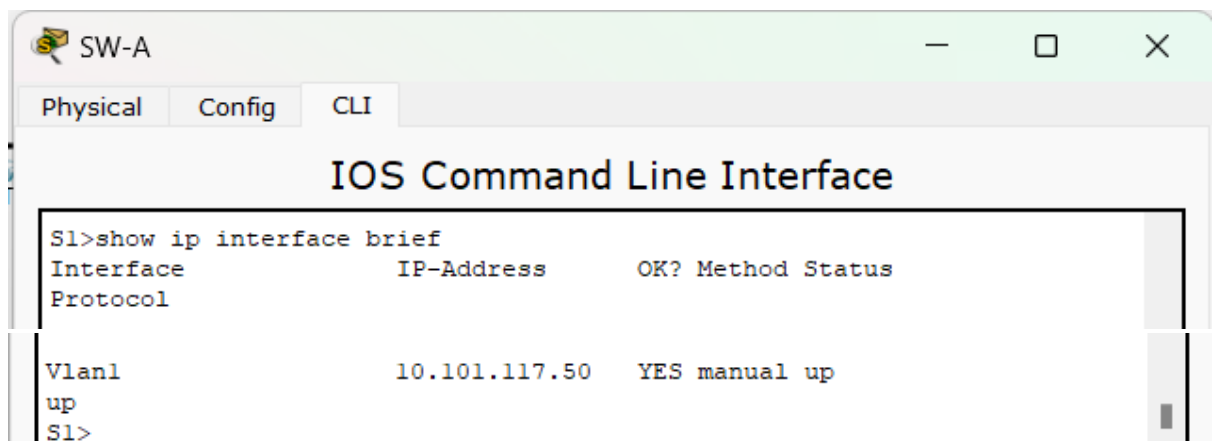
RTA

Physical Config CLI

IOS Command Line Interface

```
RT>show ip interface brief
```

Interface	IP-Address	OK?	Method	Status
GigabitEthernet0/0	10.101.117.49	YES	manual	up
GigabitEthernet0/1	10.101.117.33	YES	manual	up
GigabitEthernet0/2	10.101.117.1	YES	manual	up
Vlan1	unassigned	YES	unset	administratively down



SW-A

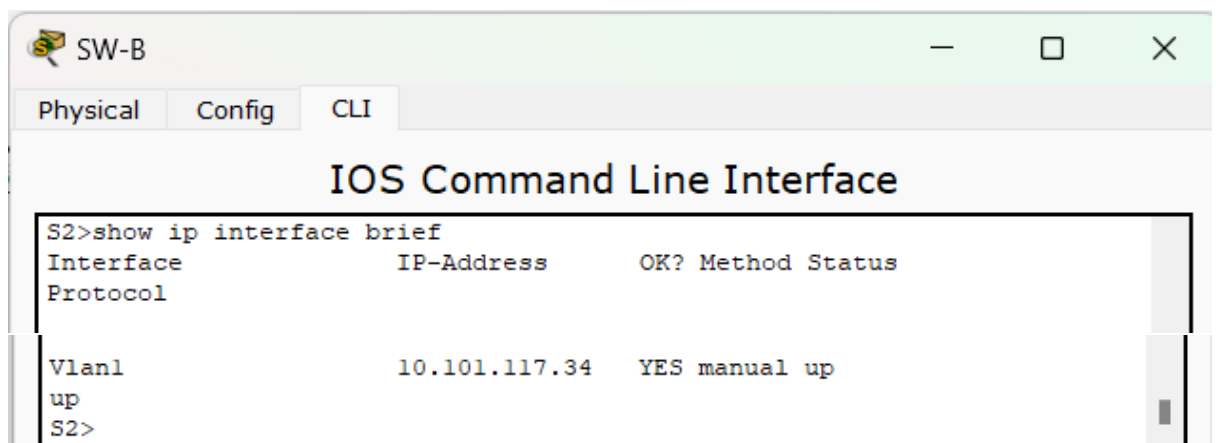
Physical Config CLI

IOS Command Line Interface

```
S1>show ip interface brief
```

Interface	IP-Address	OK?	Method	Status
Vlan1	10.101.117.50	YES	manual	up

S1>



SW-B

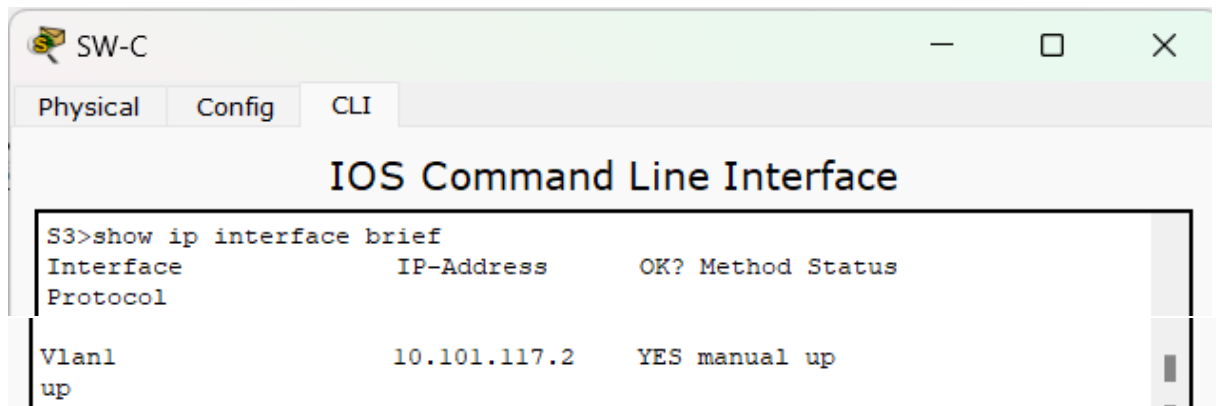
Physical Config CLI

IOS Command Line Interface

```
S2>show ip interface brief
```

Interface	IP-Address	OK?	Method	Status
Vlan1	10.101.117.34	YES	manual	up

S2>



SW-C

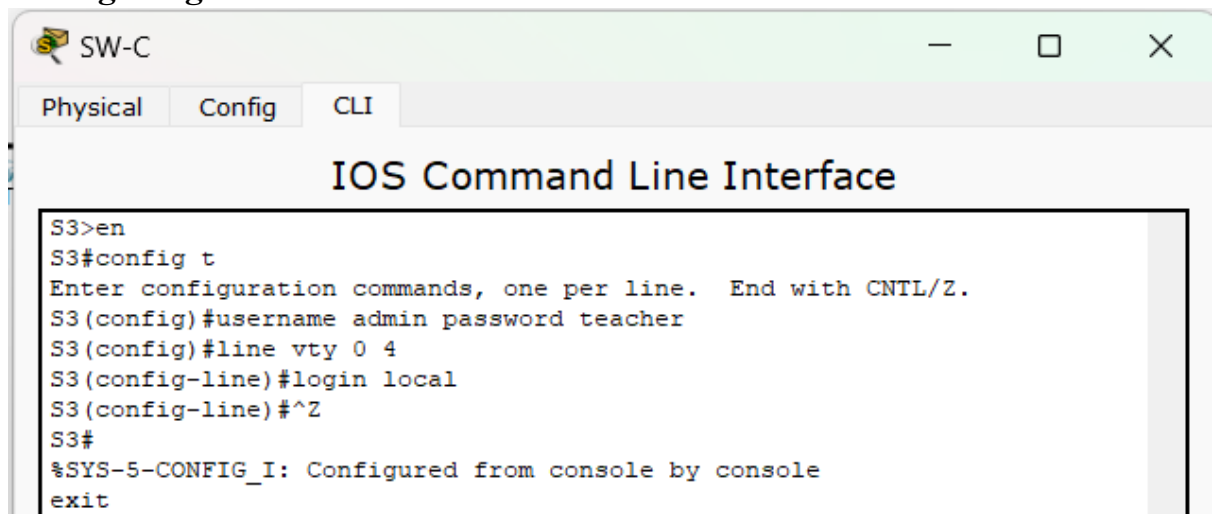
Physical Config CLI

IOS Command Line Interface

```
S3>show ip interface brief
```

Interface	IP-Address	OK?	Method	Status
Vlan1	10.101.117.2	YES	manual	up

➤ **Configuring Telnet on S3**



SW-C

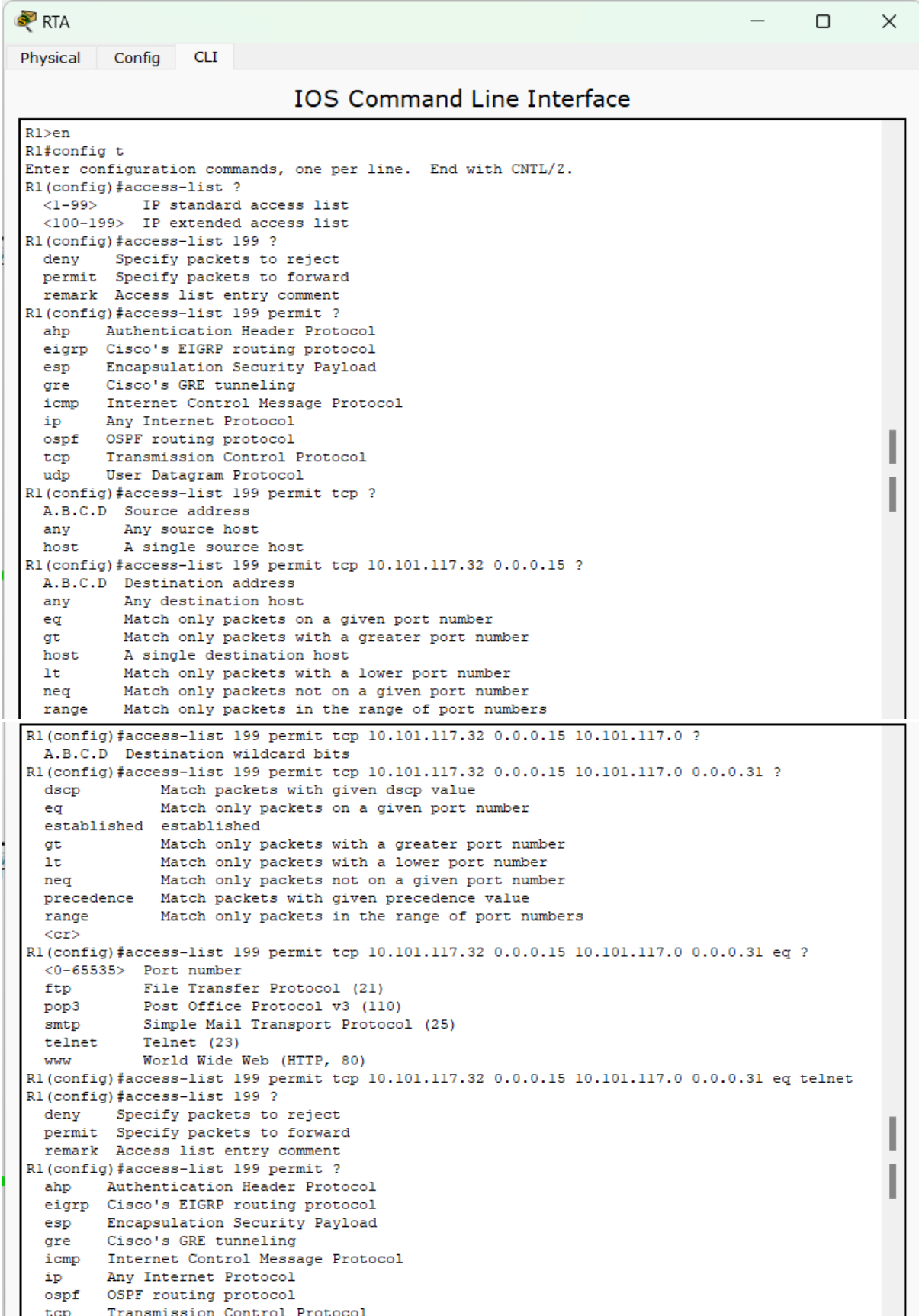
Physical Config CLI

IOS Command Line Interface

```
S3>en
S3#config 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.)



The screenshot shows a terminal window titled "RTA" with tabs for "Physical", "Config", and "CLI". The main title is "IOS Command Line Interface". The terminal output shows the following commands and prompts:

```

R1>en
R1#config 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 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

```

```
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

R1#exit
```

➤ Verify the extended ACL implementation

