**Aim:- Configuring Extended ACLs - Scenario 1.**

**Part 1: Configure, Apply and Verify an Extended Numbered ACL**

**Step 1: Configure an ACL to permit FTP and ICMP.**

1. From global configuration mode on R1, enter the following command to determine the first valid number for an extended access list.

R1(config)# access-list ?

<1-99> IP standard access list

<100-199> IP extended access list

b. Add 100 to the command, followed by a question mark.

R1(config)# access-list 100 ?

deny Specify packets to reject

permit Specify packets to forward

remark Access list entry comment

c. To permit FTP traffic, enter permit, followed by a question mark.

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

d. This ACL permits FTP and ICMP. ICMP is listed above, but FTP is not, because FTP uses TCP. Therefore,enter tcp to further refine the ACL help.

R1(config)# access-list 100 permit tcp ?

A.B.C.D Source address any

Any source host host A

single source host

e. Notice that we could filter just for PC1 by using the host keyword or we could allow any host. In this case, any device is allowed that has an address belonging to the 172.22.34.64/27 network. Enter the network address, followed by a question mark.

R1(config)# access-list 100 permit tcp 172.22.34.64 ?

A.B.C.D Source wildcard bits

f. Calculate the wildcard mask determining the binary opposite of a subnet mask.

11111111.11111111.11111111.11100000 = 255.255.255.224

00000000.00000000.00000000.00011111 = 0.0.0.31

g. Enter the wildcard mask, followed by a question mark.

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?

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

h. Configure the destination address. In this scenario, we are filtering traffic for a single destination, which is the server. Enter the host keyword followed by the server’s IP 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 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>

i. Notice that one of the options is <cr> (carriage return). In other words, you can press Enter and the statement would permit all TCP traffic. However, we are only permitting FTP traffic; therefore, enter the eq keyword, followed by a question mark to display the available options. Then, enter ftp and press Enter.

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

j. Create a second access list statement to permit ICMP (ping, etc.) traffic from PC1 to Server. Note that the access list number remains the same and no particular type of ICMP traffic needs to be specified.

R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

k. All other traffic is denied, by default.

**Step 2: Apply the ACL on the correct interface to filter traffic.**

From R1’s perspective, the traffic that ACL 100 applies to is inbound from the network connected to Gigabit Ethernet 0/0 interface. Enter interface configuration mode and apply the ACL.

R1(config)# interface gigabitEthernet 0/0

R1(config-if)# ip access-group 100 in

**Step 3 :Verify the ACL implementation.**

a. Ping from PC1 to Server. If the pings are unsuccessful, verify the IP addresses before continuing.

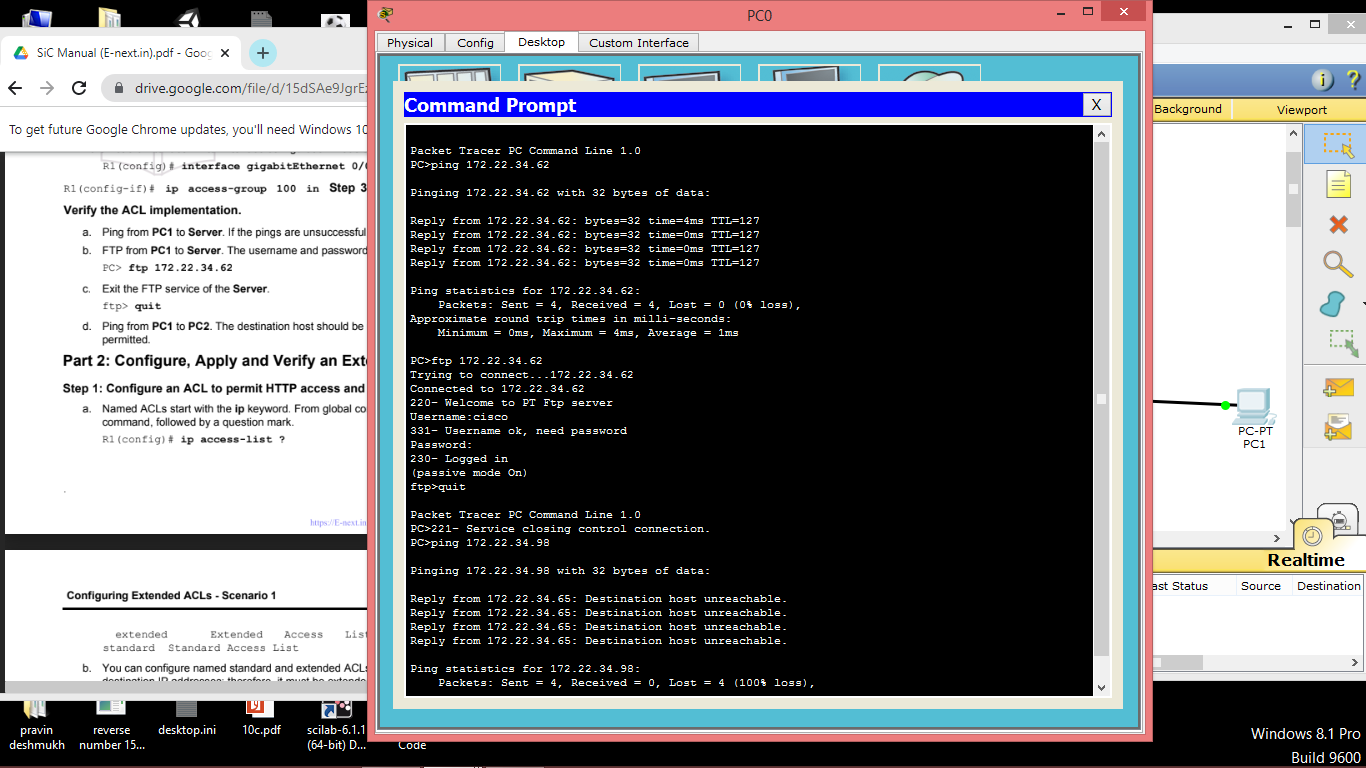
b. FTP from PC1 to Server. The username and password are both cisco.

PC> ftp 172.22.34.62

c. Exit the FTP service of the Server.

ftp> quit

d. Ping from PC1 to PC2. The destination host should be unreachable, because the traffic was not explicitly permitted.



**Part 2: Configure, Apply and Verify an Extended Named ACL**

**Step 1: Configure an ACL to permit HTTP access and ICMP.**

a. Named ACLs start with the ip keyword. From global configuration mode of R1, enter the following command, followed by a question mark.

R1(config)# ip access-list ?

extended Extended Access List

standard Standard Access List

b. You can configure named standard and extended ACLs. This access list filters both source and destination IP addresses; therefore, it must be extended. Enter HTTP\_ONLY as the name. (For Packet Tracer scoring, the name is case-sensitive.)

R1(config)# ip access-list extended HTTP\_ONLY

c. The prompt changes. You are now in extended named ACL configuration mode. All devices on the PC2 LAN need TCP access. Enter the network address, followed by a question mark.

R1(config-ext-nacl)# permit tcp 172.22.34.96 ?

A.B.C.D Source wildcard bits

d. An alternative way to calculate a wildcard is to subtract the subnet mask from 255.255.255.255.

255.255.255.255

- 255.255.255.240

= 0. 0. 0. 15

R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 ?

e. Finish the statement by specifying the server address as you did in Part 1 and filtering www traffic.

R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www

f. Create a second access list statement to permit ICMP (ping, etc.) traffic from PC2 to Server. Note: The prompt remains the same and a specific type of ICMP traffic does not need to be specified.

R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62

g. All other traffic is denied, by default. Exit out of extended named ACL configuration mode.

**Step 2: Apply the ACL on the correct interface to filter traffic.**

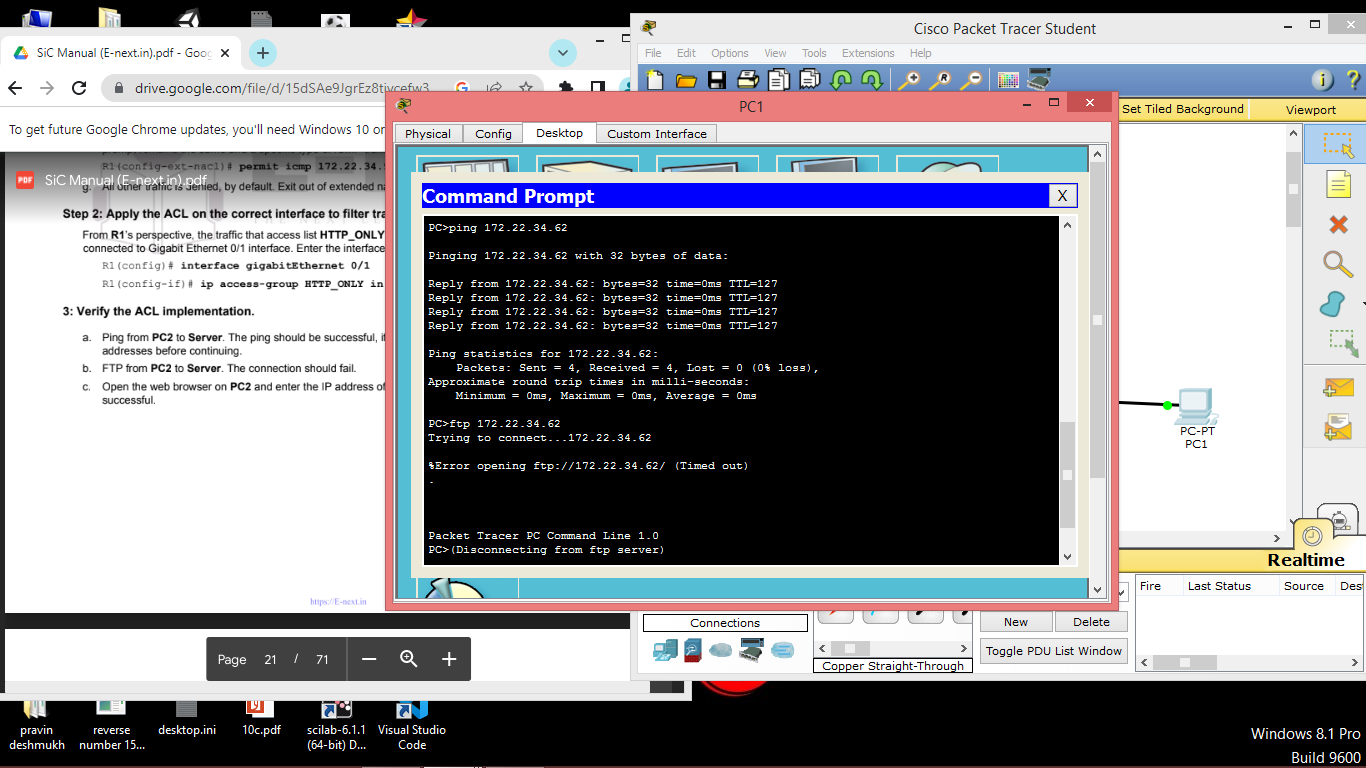
From R1’s perspective, the traffic that access list HTTP\_ONLY applies to is inbound from the network connected to Gigabit Ethernet 0/1 interface. Enter the interface configuration mode and apply the ACL.

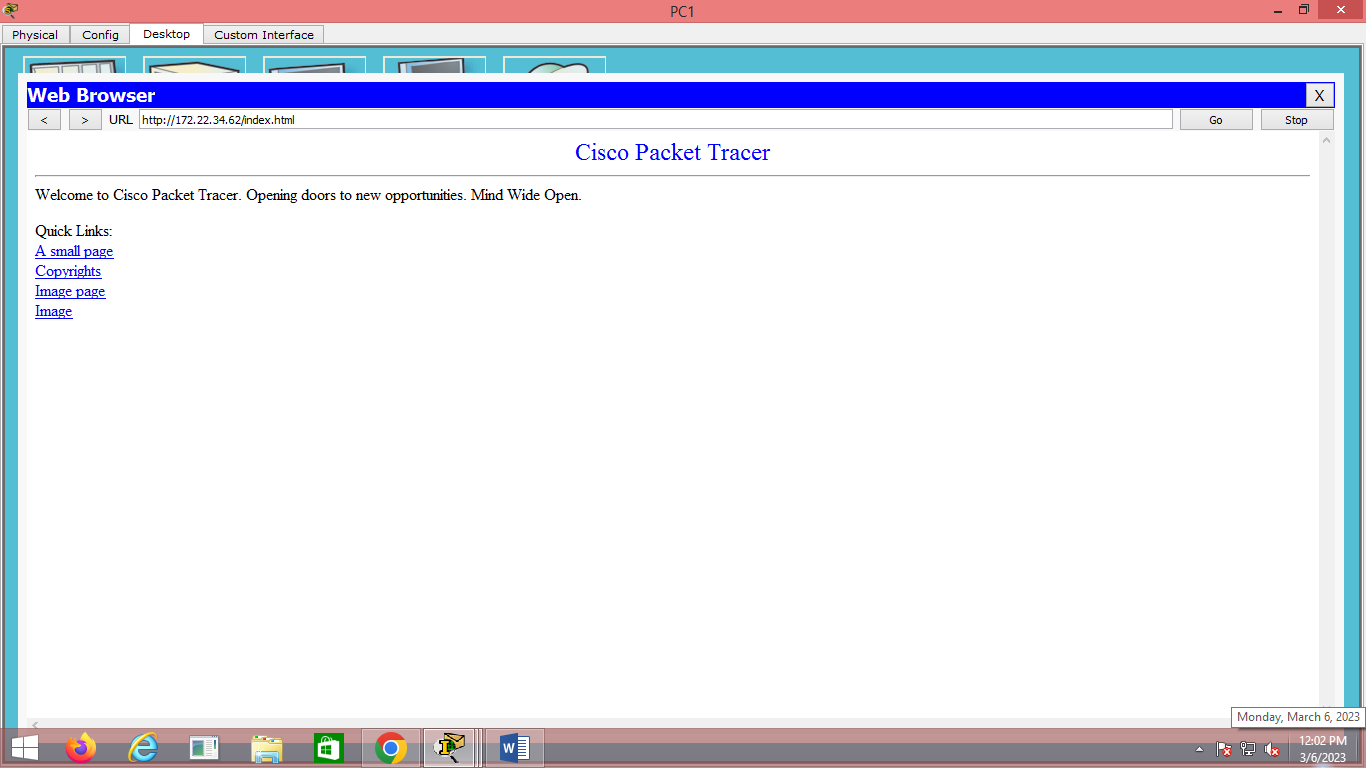
R1(config)# interface gigabitEthernet 0/1

R1(config-if)# ip access-group HTTP\_ONLY in

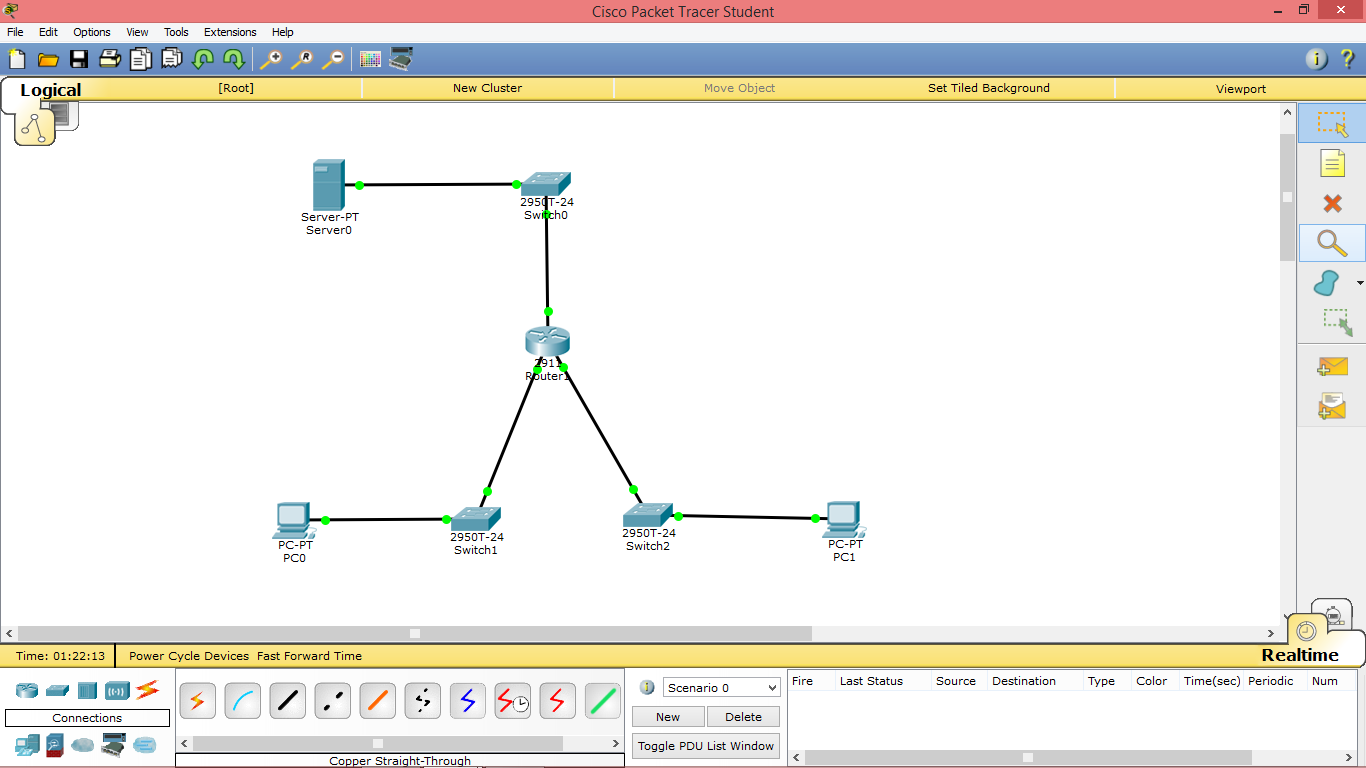
**Step** **3: Verify the ACL implementation.**

1. Ping from PC2 to Server. The ping should be successful, if the ping is unsuccessful, verify the IP addresses before continuing.
2. FTP from PC2 to Server. The connection should fail.
3. the web browser on PC2 and enter the IP address of Server as the URL. The connection should be successful.





**Output :-**

****

**Aim: Configuring Extended ACLs - Scenario 2**

**Part 1: Configure, Apply and Verify an Extended Numbered ACL.**

1. Step 1: Set the SWA, SWB and SWC ip Address and default gateway.

SWA(config)#**int vlan 1**

SWA(config-if)#**ip address 10.101.117.50 255.255.255.248**

SWA(config-if)#**no shutdown**

SWA(config-if)#**ip default-gateway 10.101.117.49**

SWB(config)#**int vlan 1**

SWB(config-if)#**ip address 10.101.117.34 255.255.255.240**

SWB(config-if)#**no shutdown**

SWB(config-if)#**ip default-gateway 10.101.117.33**

SWA(config)#**int vlan 1**

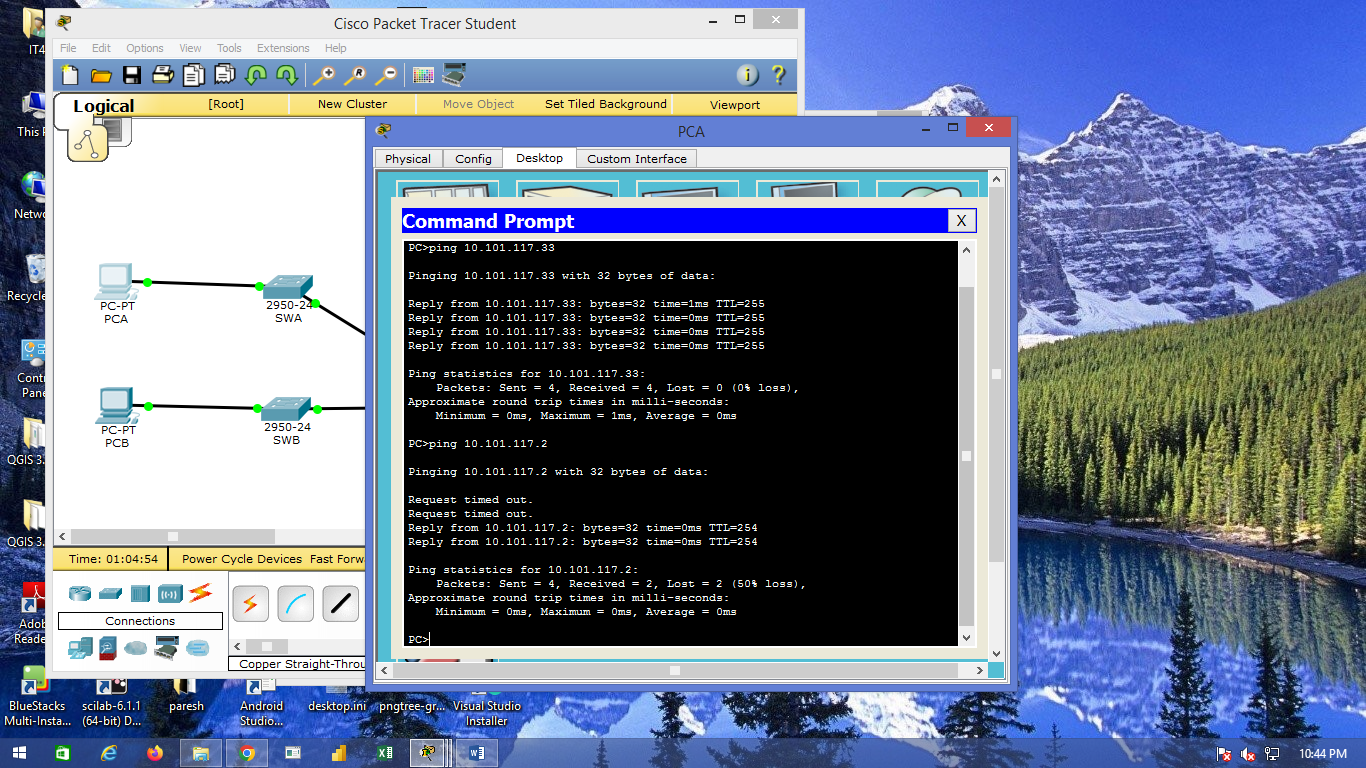
SWA(config-if)#**ip address 10.101.117.2 255.255.255.224**

SWA(config-if)#**no shutdown**

SWA(config-if)#**ip default-gateway 10.101.117.1**

1. **Test Connectivity.**

* Ping PC-A To PC-B
* ping PC-A to SWB



1. Generate rsa key for security.(similarly for SWA,SWB and SWC).

SWA(config)#**enable secret enpa55**

SWA(config)#**line console 0**

SWA(config-line)#**password conpa55**

SWA(config-line)#**login**

SWA(config-line)#**en**

SWA(config)#**ip domain-name ccnasecurity.com**

SWA(config)#**username admin secret adminpa55**

SWA(config)#**line vty 04**

SWA(config)#**login local**

SWA(config)#**crypto key generate rsa**

1. A) From the appropriate configuration mode on RTA, use the last valid extended access list number to configure the ACL. Use the following steps to construct the first ACL statement: 1) The last extended list number is 199.

**access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq 22**

B) ICMP is allowed, and a second ACL statement is needed. Use the same ace

ss list number to permit all ICMP traffic, regardless of the source or destination address. What is the second ACL statement? (Hint: Use the any keywords)

**access-list 199 permit icmp any any**

C) All other IP traffic is denied, by default.

1. Step 2: Apply the extended ACL.

The general rule is to place extended ACLs close to the source. However, because access list 199 affects traffic originating from both networks 10.101.117.48/29 and 10.101.117.32/28, the best placement for this ACL might be on interface Gigabit Ethernet 0/2 in the outbound direction. What is the command to apply ACL 199 to the Gigabit Ethernet 0/2 interface?

**ip access-group 199 out**

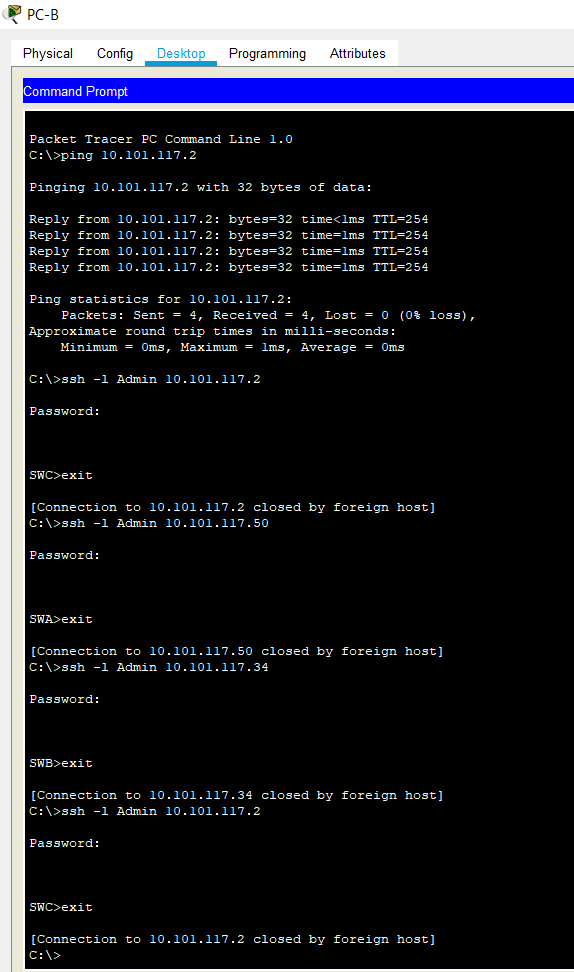
**6) Step 3: Verify the extended ACL implementation.**

a) Ping from PCB to all of the other IP addresses in the network. If the pings are unsuccessful, verify the IP addresses before continuing.

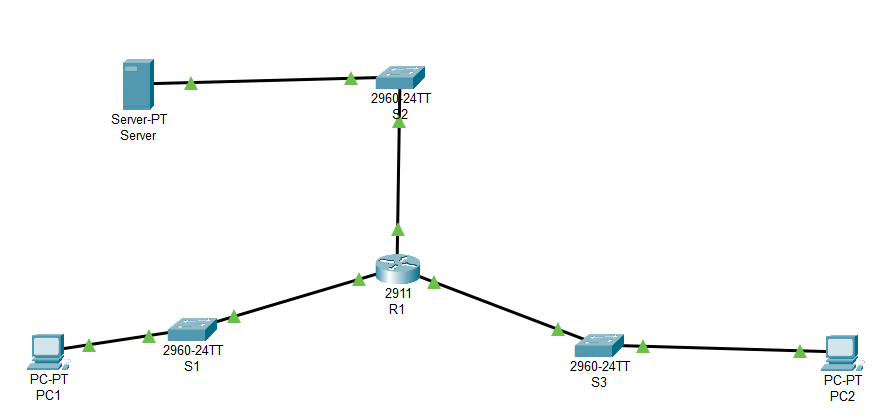
1. SSH from PCB to SWC. The username is Admin, and the password is Adminpa55. PC> ssh -l Admin 10.101.117.2
2. Exit the SSH session to SWC.
3. Ping from PCA to all of the other IP addresses in the network. If the pings are unsuccessful, verify the IP addresses before continuing.
4. SSH from PCA to SWC. The access list causes the router to reject the connection.

Packet Tracer - Configuring Extended ACLs - Scenario 2

1. SSH from PCA to SWB. The access list is placed on G0/2 and does not affect this connection. The username is Admin, and the password is Adminpa55.
2. After logging into SWB, do not log out. SSH to SWC in privileged EXEC mode. SWB# ssh -l Admin 10.101.117.2



**Output:**

****