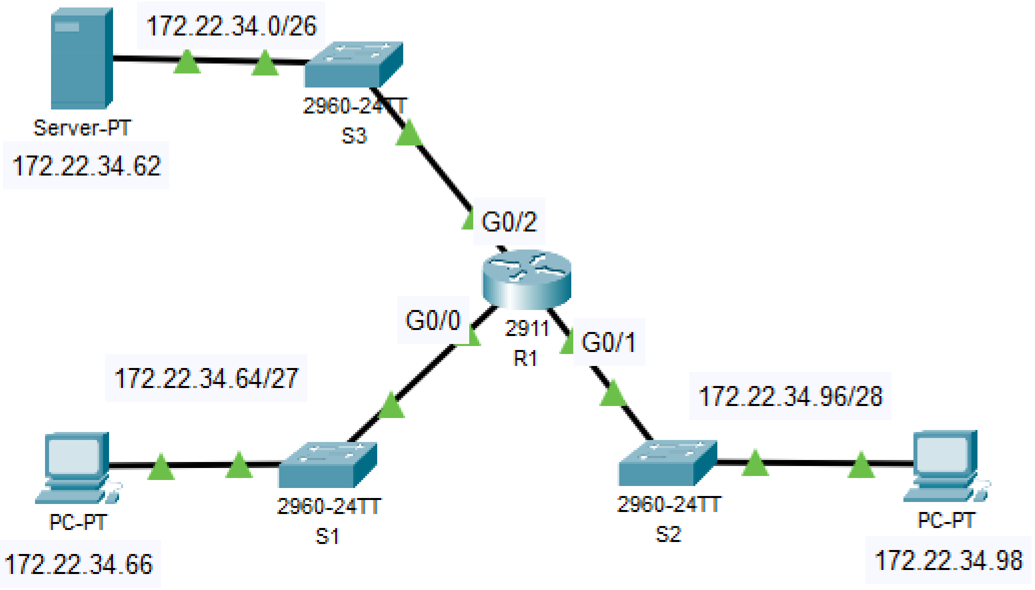
Packet Tracer - Configure Extended ACLs - Scenario 1

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	
	G0/2	172.22.34.1	255.255.255.192	
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Objectives

Part 1: Build the Network and Configure Basic Device Settings and IP addressing

Part 2: Configure, Apply and Verify an Extended Numbered ACL

Part 3: Configure, Apply and Verify an Extended Named ACL

Background / Scenario

Two employees need access to services provided by the server. **PC1** only needs FTP access while **PC2** only needs web access. Both computers need to be able to ping the server, but not each other.

Instructions

Part 1: Build the Network and Configure Basic Device Settings and IP addressing

Step 1: Cable the network as shown in the topology.

Step 2: Configure basic settings for each device.

Step 3: Configure IP addressing for each device.

Part 2: Configure, Apply and Verify an Extended Numbered ACL

Step 1: Configure an ACL to permit FTP and ICMP from PC1 LAN (172.22.34.64/27).

a. From global configuration mode on **R1**, find the first valid number for an extended access list.

b. Create an access list statement to permit FTP.

c. Create a second access list statement to permit ICMP.

d. Execute the **show access-list** command and verify that the access list contains the correct statements. Notice that the statement **deny any any** does not appear at the end of the access list. The default execution of an access list is that if a packet does not match a statement in the access list, it is not permitted through the interface.

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

Appropriate ACL placement depends on the relationship of the traffic with respect to **RT1**. In general, extended access lists should be placed on the interface closest to the source of the traffic.

On which interface should the numbered ACL be applied, and in which direction?

a. Enter the configuration commands to apply the ACL to the interface.

Note: On an actual operational network, it is not a good practice to apply an untested access list to an active interface.

Step 3: Verify the ACL implementation.

Use the **show access-lists** command to verify the ACL configuration. Use the **show run** or **show ip interface <xyz>** command to verify that the ACL is applied correctly to the interface.

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.

```
ftp> quit
```

d. Ping from PC1 to PC2. The destination host should be unreachable, because the ACL did not explicitly permit the traffic.

Part 3: Configure, Apply and Verify an Extended Named ACL

Step 1: Configure an ACL to permit HTTP access and ICMP from PC2 LAN (172.22.34.96/28).

a. From global configuration mode on R1, issue the ip command. Remember that Named ACLs must start with the ip keyword.

b. Enter **HTTP_ONLY** as the name for the ACL.

c. Create the first access list statement. All devices on the **PC2** LAN need web access to the **Server**.

d. Create a second access list statement to permit ICMP traffic from **PC2** to **Server**.

e. All other traffic is denied, by default. Exit extended named ACL configuration mode.

f. Execute the **show access-list** command and verify that access list **HTTP_ONLY** contains the correct statements.

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

Appropriate ACL placement depends on the relationship of the traffic with respect to **RT1**. In general, extended access lists should be placed on the interface closest to the source of the traffic.

On which interface should the named ACL be applied, and in which direction?

a. Enter the configuration commands to apply the ACL to the interface.

Note: On an actual operational network, it is not a good practice to apply an untested access list to an active interface.

Step 3: Verify the ACL implementation.

a. Ping from **PC2** to **Server**. If the ping is unsuccessful, verify the IP addresses before continuing.

b. From **PC2** open a web browser and enter the IP address of the Server. The web page of the Server should be displayed.

c. FTP from **PC2** to **Server**. The connection should fail. If not, troubleshoot the access list statements and the access-group configurations on the interfaces.