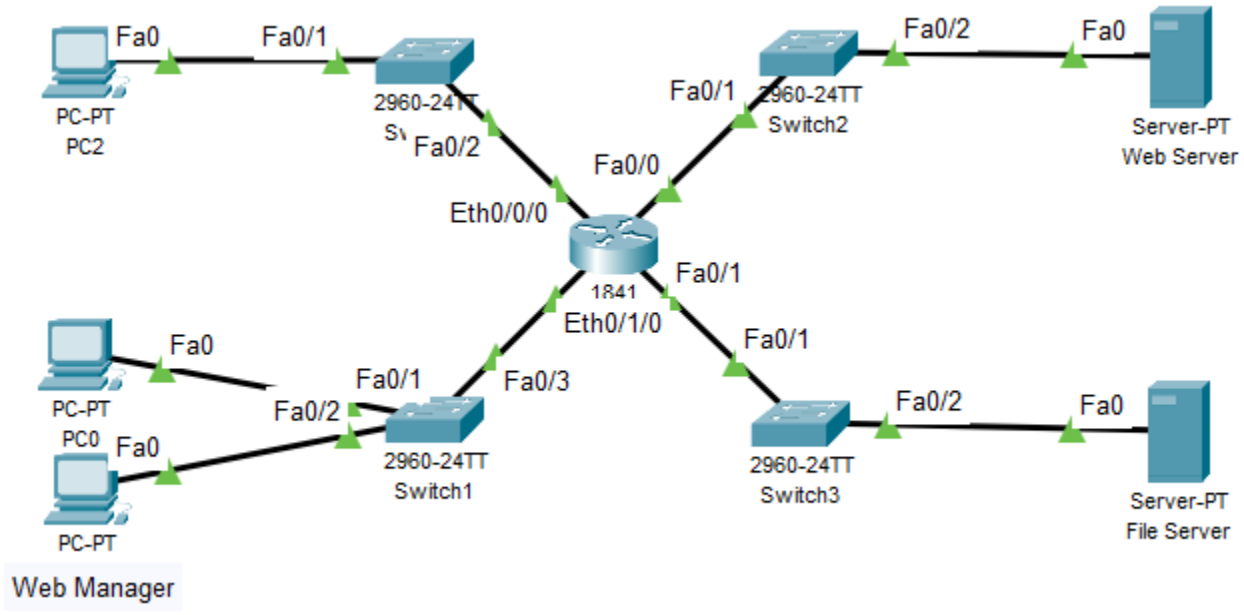
Packet Tracer - Configure Named Standard IPv4 ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Eth0/0/0	192.168.10.1	255.255.255.0	N/A
	Eth0/1/0	192.168.20.1	255.255.255.0	
	Fa0/0	192.168.100.1	255.255.255.0	
	Fa0/1	192.168.200.1	255.255.255.0	
File Server	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web Server	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
Web Manager	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Objectives

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

Part 2: Configure and Apply a Named Standard ACL

Part 3: Verify the ACL Implementation

Background / Scenario

The senior network administrator has asked you to create a standard named ACL to prevent access to a file server. The file server contains the data base for the web applications. Only the Web Manager workstation PC1 and the Web Server need to access the File Server. All other traffic to the File Server should be denied.

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 and Apply a Named Standard ACL

Step 1: Verify connectivity before the ACL is configured and applied.

All three workstations should be able to ping both the **Web Server** and **File Server**.

Step 2: Configure a named standard ACL.

a. Configure a named ACL on **R1** to satisfy the initial security requisite.

b. Use the **show access-lists** command to verify the contents of the access list before applying it to an interface. Make sure you have not mistyped any IP addresses and that the statements are in the correct order.

Step 3: Apply the named ACL.

Appropriate ACL placement depends on the relationship of the traffic with respect to **RT1**.

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.

b. Save the configuration.

Part 3: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the interface.

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.

Step 2: Verify that the ACL is working properly.

All three workstations should be able to ping the **Web Server**, but only **PC1** and the **Web Server** should be able to ping the **File Server**. Repeat the **show access-lists** command to see the number of packets that matched each statement.