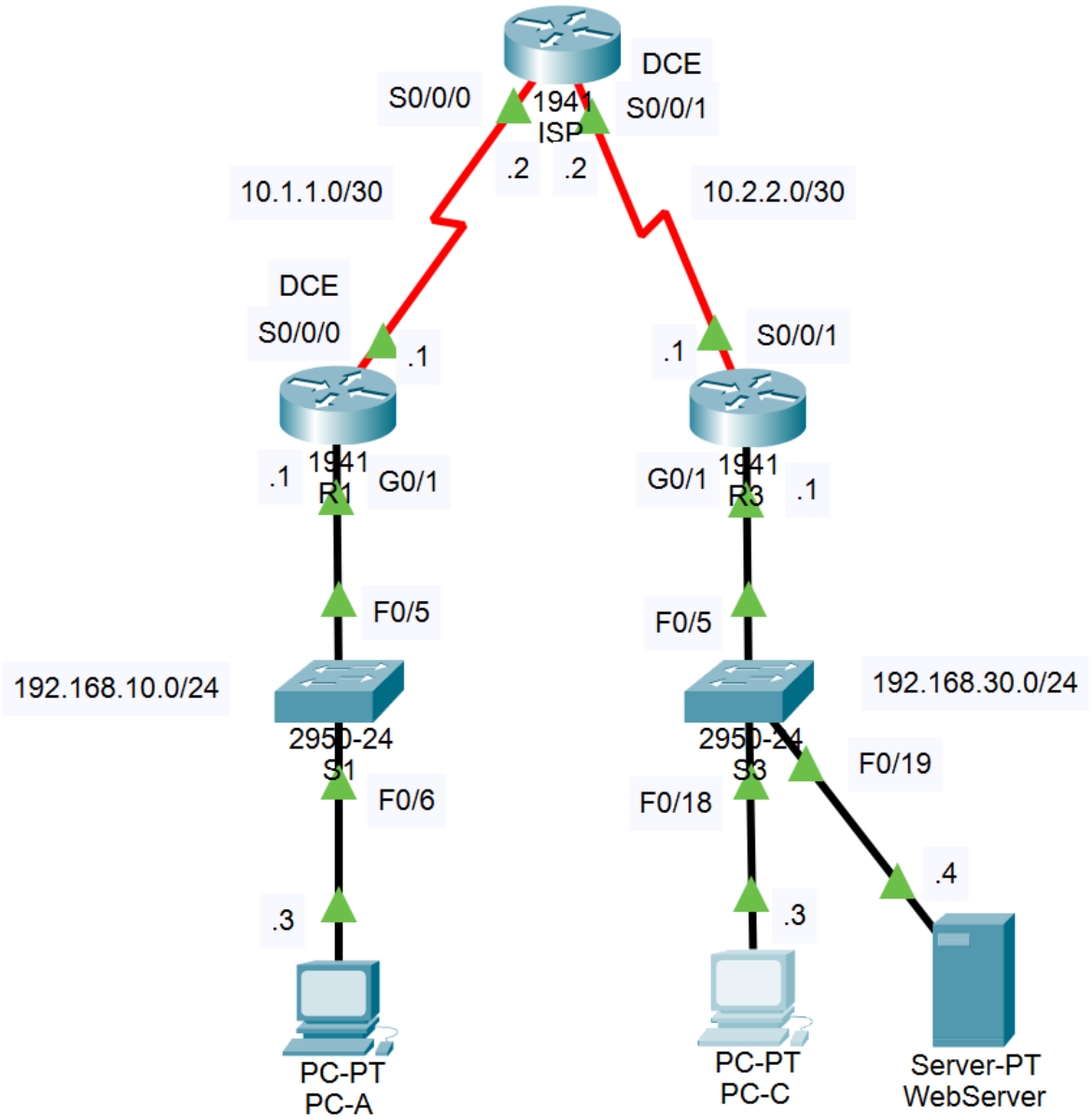
Lab 4: Configuring and Verifying Extended ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.30.4	255.255.255.0	192.168.30.1

Objectives

- Configure OSPF routing.
- Configure, apply, and verify a numbered and a named extended ACL.
- Modify and verify extended ACLs.

Background / Scenario

Extended access control lists (ACLs) are extremely flexible. They offer a much greater degree of control than “standard” ACLs regarding the filtered traffic types.

In this lab, you will set up filtering rules for two offices represented by R1 and R3. Management has established access policies between the LANs at R1 and R3, which you must implement. The ISP router has no ACLs configured. You are not allowed administrative access to the ISP router; you can only control and manage your equipment.

Use Packet Tracer for this lab.

Required Resources

In Packet Tracer, use 1941 routers and 2650-24 switches. As you did in previous labs, you must install a wide-area interface module (HWIC-2T) in the routers. Also, be careful to connect the DCE end of the wide-area links to the appropriate router, as shown in the diagram above.

Part 1: Set Up the Topology and Initialize Devices

In Part 1, set up the network topology shown above, apply the basic settings to each router, and configure all network interfaces. Do not forget to configure the network interfaces on the PCs and the web server. Also, be sure to create and configure the three loopback interfaces (one on each router). You do not need to apply any configuration to the switches for this lab.

Verify that the HTTP server is running on the web server machine. Click on the “Services” tab in the GUI configuration dialog and then click on the HTTP tab on the left side of the window. The service should be “on” by default. If not, select the appropriate radio button to turn it on.

Verify connectivity between adjacent devices, but note that there will be no connectivity to devices that are more than one hop away since routing is not configured.

Verify that PC-C can access the web server by viewing the URL http://192.168.30.4/ in PC-C’s web browser. Note that this should work even without routing configured since PC-C and the web server are on the same link.

Part 2: Configure Services

In Part 2, configure some additional services on your devices. These services will be used to test ACL settings later.

Step 1: Configure remote SSH access to R1.

a. Using the Basic Settings document, configure SSH access to R1 using the commands shown under “SSH Access.”

Step 2: Configure remote SSH access to R3.

Follow the same steps as for R1 to enable SSH access to R3.

Step 3: Configure OSPF routing on R1, ISP, and R3.

a. Assign 1 as the OSPF process ID and advertise all networks on R1, ISP, and R3. The OSPF configuration for R1 is included for reference. Use a router ID of 3.3.3.3 for R3 and 100.0.0.0 for the ISP router. Be careful with the network addresses and wildcard masks. *Note: In real life, the ISP would not be in the same area as your organization’s routers!*

```
R1(config)# router ospf 1
R1(config)# router-id 1.1.1.1
R1(config-router)# network 192.168.10.0 0.0.0.255 area 0
R1(config-router)# network 192.168.20.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

b. After configuring OSPF on R1, ISP, and R3, verify that all routers have complete routing tables listing all networks. Troubleshoot if this is not the case.

Step 4: Verify connectivity between devices.

Note: Verifying connectivity before you configure and apply ACLs is very important. Ensure that your network is functioning properly before you filter out traffic. Otherwise, you won’t be able to distinguish between a lack of connectivity because of your ACL filtering rules and a lack of connectivity because of some problem with the configuration.

a. From PC-A, ping PC-C.

b. From PC-A, ping all the loopback interfaces throughout the system.

c. From PC-C, ping all the loopback interfaces throughout the system.

d. From PC-A, SSH to R3, and verify that you can log in successfully. Use the command **ssh -l admin <ip-address>** on the PC’s console. Use the **exit** command to end the SSH session.

e. From PC-C, SSH to R1, and verify that you can log in successfully.

f. From PC-A, verify that you can access the web server and view web pages.

Part 3: Configure and Verify Extended Numbered and Named ACLs

Extended ACLs can filter traffic in many different ways. Extended ACLs can filter on source IP addresses, source ports, destination IP addresses, destination ports, and various protocols and services.

The organizational security policy is as follows.

1. Allow web traffic originating from the 192.168.10.0/24 network to go to any network.
2. Allow an SSH connection to the R3 serial interface from PC-A.
3. Allow users on 192.168.10.0/24 network access to 192.168.20.0/24 network.
4. Allow web traffic originating from the 192.168.30.0/24 network to access R1 via the web interface and the 209.165.200.224/27 network on ISP. The 192.168.30.0/24 network should NOT be allowed to access any other network via the web.

In looking at the security policies listed above, you will need at least two ACLs to fulfill the security policies. A best practice is to place extended ACLs as close to the source as possible. We will follow this practice for these policies.

Step 1: Configure a numbered extended ACL on R1 for security policy numbers 1 and 2.

You will use a numbered extended ACL on R1. What are the ranges for extended ACLs?

a. Configure the ACL on R1. Use 100 for the ACL number.

```
R1(config)# access-list 100 remark Allow Web & SSH Access
R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22
R1(config)# access-list 100 permit tcp any any eq 80
```

What does the 80 signify in the command output listed above?

b. Apply ACL 100 to the S0/0/0 interface.

```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 100 out
```

c. Verify ACL 100.

1) Open a web browser on PC-A and access http://209.165.200.225 (the ISP router). It should be successful; troubleshoot if not.

2) Establish an SSH connection from PC-A to R3 using 10.2.2.1 for the IP address. Log in as **admin**. It should be successful; troubleshoot if not.

3) From the privileged EXEC mode prompt on R1, issue the **show access-lists** command.

4) From the PC-A command prompt, issue a ping to 10.2.2.1. Explain your results.

Step 2: Configure a named extended ACL on R3 for security policy number 3.

a. Configure the policy on R3. Name the ACL WEB-POLICY.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq 80
```

b. To which interface on R3 and in which direction should the WEB-POLICY ACL be applied? Show the commands you used.

c. Verify the ACL WEB-POLICY.

1) Open a web browser on PC-C and access http://209.165.200.225 (the ISP router). It should be successful; troubleshoot if not.

2) Open a web session from PC-C to http://10.1.1.1 (R1). It should be successful; troubleshoot if not.
3) Open a web session from PC-C to http://209.165.201.1 (ISP router). It should fail; troubleshoot if not.
4) From a PC-C command prompt, ping PC-A. What was your result and why?

_____

Part 4: Modify and Verify Extended ACLs

Because of the ACLs applied on R1 and R3, no pings or any other kind of traffic is allowed between the LAN networks on R1 and R3. Management has decided that all traffic between the 192.168.10.0/24 and 192.168.30.0/24 networks should be allowed. You must modify both ACLs on R1 and R3.

Step 1: Modify ACL 100 on R1.

a. From R1 privileged EXEC mode, issue the **show access-lists** command.

How many lines are there in this access list?

b. Enter global configuration mode and modify the ACL on R1.

```
R1(config)# ip access-list extended 100
R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
R1(config-ext-nacl)# end
```

c. Issue the **show access-lists** command again.

Where did the new line that you just added appear in ACL 100?

_____

Step 2: Modify ACL WEB-POLICY on R3.

a. From R3 privileged EXEC mode, issue the **show access-lists** command.

How many lines are there in this access list?

b. Enter global configuration mode and modify the ACL on R3.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
R3(config-ext-nacl)# end
```

c. Issue the **show access-lists** command again to verify that the new line was added at the end of the ACL.

Step 3: Verify modified ACLs.

a. From PC-A, ping the IP address of PC-C. Were the pings successful?

b. From PC-C, ping the IP address of PC-A. Were the pings successful?

Why did the ACLs work immediately for the pings after you changed them?

Reflection

1. Why is careful planning and testing of ACLs required?
2. Which type of ACL is better: standard or extended?
3. Why are OSPF hello packets and routing updates not blocked by the implicit **deny any** access control entry (ACE) or ACL statement of the ACLs applied to R1 and R3?