Packet Tracer - Explore a Simple Network

Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0/0	209.165.200.225	255.255.255.248	N/A
	G0/0/1	10.1.1.2	255.255.255.252	
R3	G0/0/0	10.2.2.2	255.255.255.252	N/A
	G0/0/1	172.16.3.1	255.255.255.0	
FIREWALL	VLAN1	192.168.1.1	255.255.255.0	N/A
	VLAN2	209.165.200.226	255.255.255.248	
	VLAN3	192.168.2.1	255.255.255.0	
DEVASC Server	NIC	IN: 192.168.2.3	255.255.255.0	192.168.1.1
	VLAN1	OUT: 209.165.200.227	255.255.255.248	209.165.200.225
Example Server	NIC	64.100.0.10	255.255.255.0	64.100.0.1
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-B	NIC	172.16.3.2	255.255.255.0	172.16.3.1

Note: You will add PC-A and PC-B to the topology in Step 1.

Objectives

Part 1: Add PCs to the Topology

Part 2: Test Connectivity Across the Network

Part 3: Create a Web Page and View it

Part 4: Examine the FIREWALL Access Lists

Background / Scenario

Packet Tracer is a great tool for building and testing networks and network equipment. As a developer, it is important that you are familiar with network devices and how they communicate with each other. The simple network in this Packet Tracer activity is pre-configured to give you an opportunity to explore the devices.

Note: In this activity, the two web servers are referred to as **DEVASC Server** and **Example Server**. In the topology, they are named with their URL: **www.devasc-netacad.pka** and **www.example.com**.

Instructions

Part 1: Add PCs to the Topology

In this Part, you will add PCs to the topology and configure them with IPv4 addressing.

Step 1: Place the PCs and connect them to the network.

Note: Device names are case-sensitive. If you use a different case or different name, your score will be impacted.

a. Drag a PC to the work area and place it near S2.

b. Rename the PC as **PC-A**.

c. Drag a PC to the work area and place it near S3.

d. Rename the PC as **PC-B**.

e. Connect a **Copper Straight-Through** cable from the **FastEthernet0** port a PC-A to any available FastEthernet port on S2.

f. Connect a **Copper Straight-Through** cable from the **FastEthernet0** port a PC-B to any available FastEthernet port on S3.

Step 2: Configure the IPv4 addressing for the PCs.

a. Click **PC-A**.

b. Click **Desktop**.

c. Click **IP Configuration**.

d. Assign the following IPv4 addressing information:

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

e. Repeat this for PC-B, but use the following IPv4f addressing information:

IPv4 Address: 172.16.3.2

Subnet Mask: 255.255.255.0

Default Gateway: 172.16.3.1

f. In the Instructions window for this activity, your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed. The rest of this activity is not scored.

Part 2: Test Connectivity Across the Network

a. Click **PC-B**.

b. Click **Command Prompt**.

c. Attempt to ping R3. Type **ping 172.16.3.1** (your default gateway).

You may have to issue the command a couple of times, but you should start receiving replies from the router.

d. Ping the **Example Server** at the 64.100.0.10 address.

You may have issues initially as the network converges. Repeat the ping if necessary. Now you know you have connectivity through the internet.

e. Ping the **DEVASC Server** at the 209.165.200.227 address.

You may have issues initially as the network converges. Repeat the ping if necessary. Now you know that you have end-to-end connectivity across the network topology.

Part 3: Create a Web Page and View it

In this Part, you will create a simple web page on the DEVASC server and then verify that PC-B can access the web page.

Step 1: Create a web page.

a. Click the **Server-PT www.devasc-netacad.pka** server.

b. Click **Services**.

c. Under **Services**, you default to the first service, which is HTTP. Click **New File**.

d. Name the file **index.html**.

e. Packet Tracer understands basic Hypertext Markup Language (HTML). Place the following html code in the box below the file name. If you know HTML, feel free to customize the code.

```
<html>
<center><font size='+2' color='blue'>DevNet Associate</font></center>
<hr>Welcome to the NetAcad DEVASC course!
```

f. Click **Save**. Click **Yes** to the warning.

Step 2: View the web page.

a. Click **PC-B**.

b. Click **Desktop**. If necessary, close the **Command Prompt** window.

c. Click **Web Browser**.

d. Place the following address in the URL box: **http://209.165.200.227**.

Your web page should display. If not, check your configurations, and try again.

Part 4: Modify the FIREWALL Access List

In this Part, you will examine the access list of the FIREWALL device, edit the access list, and test that the FIREWALL now denies ping access.

Step 1: Examine the access list on the FIREWALL device.

a. Click **FIREWALL**

b. Click **CLI**.

c. Press **Enter** a couple of times to get a prompt.

d. Type **en** and press **Enter**.

e. There is no password. Press **Enter** again.

f. Type **show run** and press **Enter**.

g. Press the **space bar** to scroll through the running configuration.

h. Notice the following access-list:

```
access-list OUTSIDE-DMZ extended permit icmp any host 192.168.2.3
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.2.3 eq www
```

Host 192.168.2.3 is the internal IPv4 address of the DEVASC server in the DMZ.

- The first **access-list** statement allows any device to access to the server using Internet Control Message Protocol (ICMP), which is the protocol used by the **ping** command.

- The second **access-list** statement allows any device to access the server using Hypertext Transfer Protocol (HTTP), which is the protocol used by web browsers.

i. If necessary, press the **space bar** until you are at the command prompt.

```
FIREWALL#
```

Step 2: Modify and test the effectiveness of the access list.

Typically, you do not want the outside world to be able to ping your internal servers. Therefore, you should remove the **access-list** statement that explicitly allows ping access.

a. Enter global configuration mode with the **configure terminal** command.

```
FIREWALL# configure terminal
```

b. Remove the **access-list** statement that permits ping with the following command and press **Enter**.

Note: The command is on one line although it may word wrap in the terminal

```
FIREWALL(config)# no access-list OUTSIDE-DMZ extended permit icmp any host
192.168.2.3
```

c. From the **Command Prompt** on **PC-B**, ping the **DEVASC Server** outside IPv4 address. The ping should now fail.

d. From the **Web Browser** on **PC-B**, access the **DEVASC Server** web page at **http://209.165.200.227**. You should still see the web page as you did not remove this **access-list** statement that allows HTTP access.