Packet Tracer - Explore Network Protocols (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Answers: 5.5.7 Packet Tracer - Explore Network Protocols

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	DHCP Assigned	255.255.255.0	192.168.1.1
PC-B	NIC	172.16.3.2	255.255.255.0	172.16.3.1

Objectives

Part 1: Configure DNS

Part 2: Configure DHCP

Part 3: Configure NTP

Part 4: Use SSH to Configure a Switch

Part 5: Use SNMP

Part 6: Configure HTTPS

Part 7: Configure EMAIL

Part 8: Configure FTP

Background / Scenario

Many services run on networks behind the scene to make things happen reliably and efficiently. As a developer, you should understand what services are available and how they can help you. You should also understand the basics of how the most useful and popular services are configured. In Packet Tracer, these services are simulated and the configuration is simple and straightforward. However, Packet Tracer does a very good job at simulating the actual traffic. As you work through this lab and send traffic, we encourage you to switch to Simulation mode to explore the contents of the various types of packets that the network is generating.

Note: Packet Tracer does not grade everything you do in this activity. However, you should be able to verify your configurations by following the steps. At the end of the activity, your completion percentage should be 100%.

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: Configure DNS

All of the hosts on a network are assigned an IP address. The IP address can be an IPv4 address, and IPv6 address, or both. This includes all of the hosts on the internet too. But you do not use their IP address to communicate with them. You use common names such as cisco.com. Domain Name System (DNS) is the service that automatically translates the common, easy to remember names into IP addresses so that communication can take place between devices. In this Packet Tracer activity, the devices are using IPv4 addresses.

Step 1: Configure a local DNS server.

a. Click the **Corporate** server.

b. Click **Services**.

c. Click **DNS**.

d. Click the **On** radio button to turn on DNS Service.

   Now that DNS has been enabled, you will need to provide the information for all of the hosts on the network(s) to which you would like to translate their name to an IPv4 address.

e. In the **Name** box, type **www.example.com**.

f. The IPv4 address of the server is 64.100.0.10. In the **Address** box, type the IPv4 address.

g. Click **Add**.

   You will now see an entry that shows the hostname and IPv4 address of the **Example Server**. This is where DNS will look for the hostname and return the IPv4 address of that host to any device that requests it.

Step 2: Configure and test the use of a local DNS server.

a. Click **PC-A**.

b. Click **Config**.

c. In the **DNS Server** box, type the IPv4 address of the **Corporate** DNS server: 192.168.1.3.

   Now when PC-A uses common hostnames, it will send out a DNS request for the IPv4 address of the host with that name.

d. Click **Desktop > Command Prompt**.

e. Ping **www.example.com**. The ping may not work the first time, or even the second, as the network converges. But by your third attempt, it should succeed. Notice that the very first line of the output shows that PC-A is using the right IPv4 address for the **Example Server**.

```
Packet Tracer PC Command Line 1.0
C:\> ping www.example.com
```

```
Pinging 64.100.0.10 with 32 bytes of data:

Request timed out.
<output omitted>

C:\> ping www.example.com

Pinging 64.100.0.10 with 32 bytes of data:

Reply from 64.100.0.10: bytes=32 time=3ms TTL=125
<output omitted>

C:\>
```

Note: There is a known issue with Packet Tracer's implementation of the FIREWALL. You will not be able to access the web servers from PC-A. However, PC-A will be able to send and receive email through the **Example Server** later in the activity.

Step 3: Configure and test the use of a remote DNS server.

PC-B does not have a local DNS server. Therefore, it will use the **Example Server** as its DNS server.

a. Click **PC-B**.

b. Click **Config**.

c. In the **DNS Server** box, type the IPv4 address of the **Corporate** DNS server: 64.100.0.10.

d. Click **Desktop > Command Prompt**.

e. Ping **www.example.com**. The ping may take a few seconds, but it should be successful.

f. Ping **www.devasc-netacad.pka**. The ping may not work the first time, or even the second, as the network converges. But by your third attempt, it should succeed.

g. Close the **Command Prompt** window and click **Web Browser**.

h. Enter **www.example.com** in the URL field and click **Go**. You should now see the Example.com web page displayed in the Web Browser.

i. Enter **www.devasc-netacad.pka** in the URL field and click **Go**. You should now see the DEVASC server web page displayed in the Web Browser.

Part 2: Configure DHCP

Manual configuration of IPv4 addresses is fine for very small networks, but on larger networks it is necessary to automatically provide IPv4 addressing to devices when they connect to the network. Dynamic Host Configuration Protocol (DHCP) provides this service. It is also convenient when devices are moved because if they move to a different subnet, they will get a new address and be able to communicate with other hosts.

Another great feature abut DHCP is that it automatically sets not only the IPv4 address for a host, but also the subnet, default gateway, and DNS server address. This makes it very easy for multiple pieces of information to be configured on hosts automatically.

Step 1: Configure DHCP on the Corporate server.

Note: Your **Completion** percentage will not increase until you click **Save** at the end of this step.

a. Click the **Corporate** server, then **Services**, if necessary.

b. Click **DHCP**.

c. Click the **On** radio button to turn on the DHCP Service.

You will now define a pool of IPv4 addresses that you wish to assign to hosts. You will use IPv4 addresses in the 192.168.1.0 subnet. You cannot use the address of 192.168.1.1 because it is already in use by the **FIREWALL** interface. You also cannot use the Corporate server address of 192.168.1.3. In addition, it is a good practice to leave some addresses free for statically assigning to servers or other devices where you want their address to remain the same.

d. The **Pool Name** is currently **serverPool**. Do not change it.

e. For **Default Gateway**, enter the IPv4 address of the INSIDE interface of the **FIREWALL**: 192.168.1.1.

This will provide each DHCP host a route to other networks.

f. For **DNS Server**, enter the IPv4 address of the **Corporate** server: 192.168.1.3.

This will provide each DHCP host an address to use to send DNS messages.

g. For **Start IP Address**, use 192.168.1.10.

This provides for a few statically-assigned devices on the network in the future.

h. For **Subnet Mask**, use 255.255.255.0.

i. For Maximum number of users, enter 245, the remaining amount after setting 10 aside.

j. Click **Save** to overwrite the default **serverPool** name.

Step 2: Test the DHCP configuration.

a. Click **PC-A**.

b. Close the **Command Prompt**, if it is still open.

c. Click **IP Configuration**.

d. Click **DCHP**.

This may take a little time, but you should be supplied with an IPv4 address from the router outside of the first 10 addresses. You should also see the subnet mask, default gateway, and DNS server all supplied for you automatically.

Part 3: Configure NTP

The clock on a router or a switch is important for managing, securing, and troubleshooting networks. Even on small networks, it is important to synchronize the time across all devices. Trying to do this manually is almost impossible especially for large networks. Network Time Protocol (NTP) can be used to synchronize the time on each device by receiving it from an NTP server, ensuring that the times are all the same.

Step 1: Turn the NTP service on.

a. Click the **Corporate** server.

b. Click **Services**.

c. Click **NTP**.

d. Click the **On** radio button next to **Service**.

Step 2: Investigate NTP on S2.

S2 has already been configured to use the Corporate server as its NTP server.

a. Click **S2**.

b. Click **CLI**.

c. Press **Enter** to get a command prompt. The enter privileged EXEC mode with the **enable** command. Use **cisco** as the password.

```
S2> enable
Password: <cisco>
S2#
```

d. Display the current time and date using the **show clock detail** command. Notice that the time is set by hardware and is not accurate.

```
S2# show clock detail
*0:3:44.318 UTC Mon Mar 1 1993
Time source is hardware calendar
S2#
```

e. You can manually configure the time with the **clock** command. However, a better practice is to use an NTP server. Enter global configuration mode with the **configure terminal** command.

```
S2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#
```

f. Configure S2 to use the Corporate server as its NTP server. Exit global configuration mode and verify S2 is now using NTP. Your time and date should now be accurate.

```
S2(config)# ntp server 192.168.1.3
S2(config)# exit
S2# show clock detail
14:1:26.216 UTC Thu May 21 2020
Time source is NTP
S2#
```

Note: It may take some time before the source is updated to NTP. You can click **Fast Forward Time** (the double arrow button) to speed up the simulation.

Part 4: Use SSH to Securely Access a Switch

Secure Shell (SSH) is a protocol that is used to encrypt communication between a client and a host. SSH is the preferable connection type because it is secure in comparison to Telnet. SSH has already been configured on S2.

a. Click PC-A. Close **IP Configuration**, if necessary.

b. Click **Desktop > Command Prompt**.

c. Attempt to establish an insecure Telnet session to S2.

```
C:\> telnet 192.168.1.4
Trying 192.168.1.4 ...Open

[Connection to 192.168.1.4 closed by foreign host]
```

d. S2 denies your request because it is configured for SSH access only. Enter the command **ssh** and press **Enter** to see how to use the command. Note that the option is a lowercase **L**, not a number **1**.

```
C:\> ssh
Packet Tracer PC SSH

Usage: SSH -l username target.
```

```
C:\>
```

e. Attempt to establish an SSH connection to S2. The password is **cisco.**

```
C:\> ssh -l administrator 192.168.1.4

Password:


S2>
```

You can now securely configure S2.

f. You are now accessing the command line for S2 over a secure connection. Enter global configuration mode with the **enable** command to verify you can configure the switch remotely. Use **cisco** as the password. Then enter **exit** to terminate the SSH session.

```
S2> enable
Password:
S2# exit

[Connection to 192.168.1.4 closed by foreign host]
C:\>
```

Part 5: Investigate SNMP MIB Object IDs

Simple Network Management Protocol (SNMP) can be used to get and set variables related to the status and configuration of network hosts like routers and switches, as well as network client computers. The SNMP manager can poll SNMP agents for data, or data can be automatically sent to the SNMP manager by configuring traps on the SNMP agents. In this part, you will retrieve the Management Information Base (MIB) Object ID codes to learn the details of the messages using the MIB browser.

Cisco devices use community strings to authenticate access to the Management Information Base (MIB). This is where all of the information about the device is stored. A community string is simply a plaintext password. Community strings can be either read-only (ro) or read-write (rw). These community strings have been created for you on R3 so that you can investigate the MIB.

Note: Although SNMP can be programmatically accessed to managed the network, more sophisticated tools are now available, as you will see in the rest of this course. However, SNMP has a large install base in networks today and will continue to be a valuable management tool for the foreseeable future.

Follow these steps to investigate the simulation of SNMP in Packet Tracer.

a. Click **PC-B**. Close **Web Browser**, if necessary.

b. Click **MIB Browser**.

c. Enter the address of **R3** in the **Address** field: 172.16.3.1.

d. Click **Advanced**.

e. Enter **read** in the field for **Read Community**.

f. Enter **write** in the field for **Write Community**.

g. Change the **SNMP Version** to **v3**.

h. Click **OK**.

i. Click the arrow next to **MIB Tree** to expand the tree.

j. Click the arrow next to **router_std MIBs**.

k. Continue expanding the tree until you reach **.mgmt**.

l. Expand **.mgmt**.

m. Continue expanding the tree until you reach **.system**.

n. Expand **.system**. You may need to make the window wider at the point. You can also grab the middle bar between the **MIB Tree** on the left and the **Result Table** on the right.

o. Click **.sysName**.

p. Click the **GO** button.

You will now see the Value of the object is **R3**. You can look at other objects in the MIB such as the interfaces on the router.

q. Expand the tree **.interfaces > .ifTable > .ifEntry > .ifOperStatus** and click **GO**.

You will see that two of three interfaces are up. You can now easily query anything about the router.

Part 6: Configure HTTPS

When you connect to a server using HTTP, you connect and assume that it is the correct server. The data transferred between you and the server is sent in plaintext, so if anyone captured that data, they could read it and manipulate it. Normally, this isn't a problem if you are simply browsing the internet. But if you are creating an account, accessing an account, or providing any personal information, it can be captured and used by someone else. Secure HTTP (HTTPS) adds a layer of security by encrypting the connection between you and the server. A site must posses a security certificate from a trusted source, to verify that the site is legitimate. Your browser checks that the certificate is valid and from a trusted source before connecting you to the site.

Step 1: Open your web page from a PC.

a. Click **PC-B**.

b. Click **Desktop**.

c. Click **Web Browser**.

d. Enter **www.devasc-netacad.pka** in the **URL** box and click **Go**. You verified access earlier. However, after you click **Go**, notice the protocol is HTTP (http://).

Step 2: Examine the FIREWALL.

a. Click **FIREWALL**.

b. Click **CLI**.

c. Press **Enter**.

d. Enter **enable** and press **Enter**.

There is no password, so press **Enter**.

e. Enter **show run** and press **Enter**.

f. Use the space bar to scroll through the firewall configuration.

Notice the following two configurations in the OUTSIDE-DMZ access-list:

```
<output omitted>
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
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.2.3 eq 443
<output omitted>
```

The line with **www** allows port 80, which is unsecured HTTP traffic. The line with port **443** allows port 443, which is secured HTTP (HTTPS) traffic.

g. Remove the **access-list** statement that allows unsecured HTTP traffic on port 80. Enter the **no** version of the access-list statement as shown below. The command will wrap to the next line, but do not press **Enter** until you have completed the full command.

```
FIREWALL# configure terminal
FIREWALL(config)# no access-list OUTSIDE-DMZ extended permit tcp any host
192.168.2.3 eq www
FIREWALL(config)#
```

Step 3: Configure HTTPS.

a. Click the **DEVASC Server**.

b. Click **Services > HTTP**. Notice that HTTP is set to **On**, but HTTPS is **Off**.

c. Turn HTTP off and turn HTTPS on. Even though the FIREWALL will no longer allow HTTP access, it is best practice to also configure the server to only allow HTTPS.

d. Click the radio button for HTTPS to turn it **On**.

Step 4: Verify HTTPS configuration.

a. Click **PC-B**.

b. Close the **MIB Browser**, if necessary. Click the **Web Browser** to reopen it.

c. Verify **PC-B** can no longer access **www.devasc-netacad.pka** using HTTP. After a few seconds, you should get a **Request Timeout** message. Click **Fast Forward Time** to speed this up.

d. Change **http** to **https** and click **Go**. You should now see the web page.

https://www.devasc-netacad.pka

Part 7: Configure EMAIL

Email clients use Simple Mail Transfer Protocol (SMTP), port 25, to send email to a server. SMTP is also used to send email between servers. Email client uses Post Office Protocol 3 (POP3), port 110, to retrieve mail from the server.

Step 1: Configure the EMAIL server.

a. Click the **Example Server**.

b. Click **Services**.

c. Click **EMAIL**.

d. Turn on both **SMTP** and **POP3** services.

e. Enter **www.example.com** in the **Domain Name** box.

f. Click **Set**.

Step 2: Create users.

a. In the **User** box, type **Student1**.

b. Enter **class** for the password.

c. Click the **plus (+)** box to add the user.

d. Repeat this step to add a user called **Student2** with the same password.

Step 3: Configure the clients.

a. Click **PC-A**.

b. Click **Desktop**.

c. Click **Email**.

d. Enter the following information:

Your Name: **Student1**

Email Address: **Student1@www.example.com**

Incoming Mail Server: **64.100.0.10**

Outgoing Mail Server: **64.100.0.10**

User Name: **Student1**

Password: **class**

e. Click **Save**.

f. Repeat this configuration on **PC-B** replacing **Student1** with **Student2**.

Step 4: Send and receive Email

a. On **PC-B**, open **Email** if it is not open.

b. Click **Compose**.

c. Fill in the following information:

To: Student1@www.example.com

Subject: Email

In the message box, type a message to Student1 such as "How are you?"

d. Click **Send**.

e. On **PC-A**, open **Email** if it is not open.

f. Click **Receive**. This may take a little time and a few tries to complete.

g. Double-click the message when it arrives to read it.

h. Click **Reply**.

i. Enter a response to the email and click **Send**.

j. Click **Send**.

k. Return to **PC**-B, click **Receive** to read the reply.

Part 8: Configure FTP

File Transfer Protocol (FTP) is a commonly used application to transfer files between clients and servers on the network. The server is configured to run the service where clients connect, login, and transfer files. FTP uses port 21 as the server command port to create the connection. FTP then uses port 20 for data transfer.

Step 1: Configure the server.

a. Click the **Corporate** server.

b. Click **Services**.

c. Click **FTP**.

d. Click the **On** radio button to turn on the FTP service.

e. In the **Username** box, type **Student**.

f. In the **Password** box, type **class**.

g. Check all of the boxes below these fields to set the user permission to allow write, read, delete, rename, and list.

h. Click **Add.**

Note: At this point, 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 graded.

Step 2: Use the FTP service.

a. Click **PC-A**.

b. Click **Desktop**.

c. Click **Command Prompt.**

d. Enter **dir** to see the files on the PC.

```
C:\> dir
Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

2/6/2106 23:28 PM 26 sampleFile.txt
26 bytes 1 File(s)
C:\>
```

e. FTP to the Corporate server IPv4 address.

```
C:\> ftp 192.168.1.3
Trying to connect...192.168.1.3
Connected to 192.168.1.3
220- Welcome to PT Ftp server
Username:
```

f. Enter the username and password you configured previously to gain access.

g. Enter**?** and press **Enter** to see the commands available in the ftp client.

```
ftp> ?
         ?
         cd
         delete
         dir
         get
         help
         passive
         put
         pwd
         quit
         rename
ftp>
```

h. Enter **dir** to see the files available on the server.

```
ftp> dir

Listing /ftp directory from 192.168.1.3:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
<output omitted>
```

i. Enter **put sampleFile.txt** to send the file to the server.

```
ftp> put sampleFile.txt

Writing file sampleFile.txt to 192.168.1.3:
File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0.08 secs (325 bytes/sec)
ftp>
```

j. Use the **dir** command again to list the contents of the FTP server again to see the file.

k. Enter **get asa842-k8.bin** to retrieve the file from the server. This can take 30 seconds or more to complete as the file is big. **Fast Forward Time** does not help.

```
ftp> get asa842-k8.bin

Reading file asa842-k8.bin from 192.168.1.3:
File transfer in progress...

[Transfer complete - 5571584 bytes]

5571584 bytes copied in 46.893 secs (42706 bytes/sec)
ftp>
```

l. Enter **delete sampleFile.txt** to remove the file from the server.

```
ftp> delete sampleFile.txt

Deleting file sampleFile.txt from 192.168.1.3: ftp>
[Deleted file sampleFile.txt successfully ]
ftp>
```

m. Enter **quit** to exit the FTP client.

n. Display the contents of the directory on the PC again to see the image file from the FTP server.

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.