Packet Tracer Network Simulation

2020

Extracted from cisco public documents

Contents

Lesson 1 Getting Started

Introduction

Packet Tracer (PT) is a network simulation package. It represents a learning environment for use in the exploration of the design and analysis of computer networks. It is based around a simple but effective model of networking devices and associated protocols. (It is not a replacement for the hands-on experience which can only come from the investigation of real systems obtained in the labs.)

In this sequence of activities, we concentrate on the processes required when developing models of networks. The student should note that the package is much more than a simple model network development tool; the simulation aspects of the package are explored in a different series of activities.

Objectives

Part 1: Introducing the workspace

Part 2: Creating a simple network

Part 3: Configuring the network

Part 1 Introducing the workspace

In this activity we get the Packet Tracer (PT) program up and running. Then we place a model PC into the workspace and look at some of the options available with it.

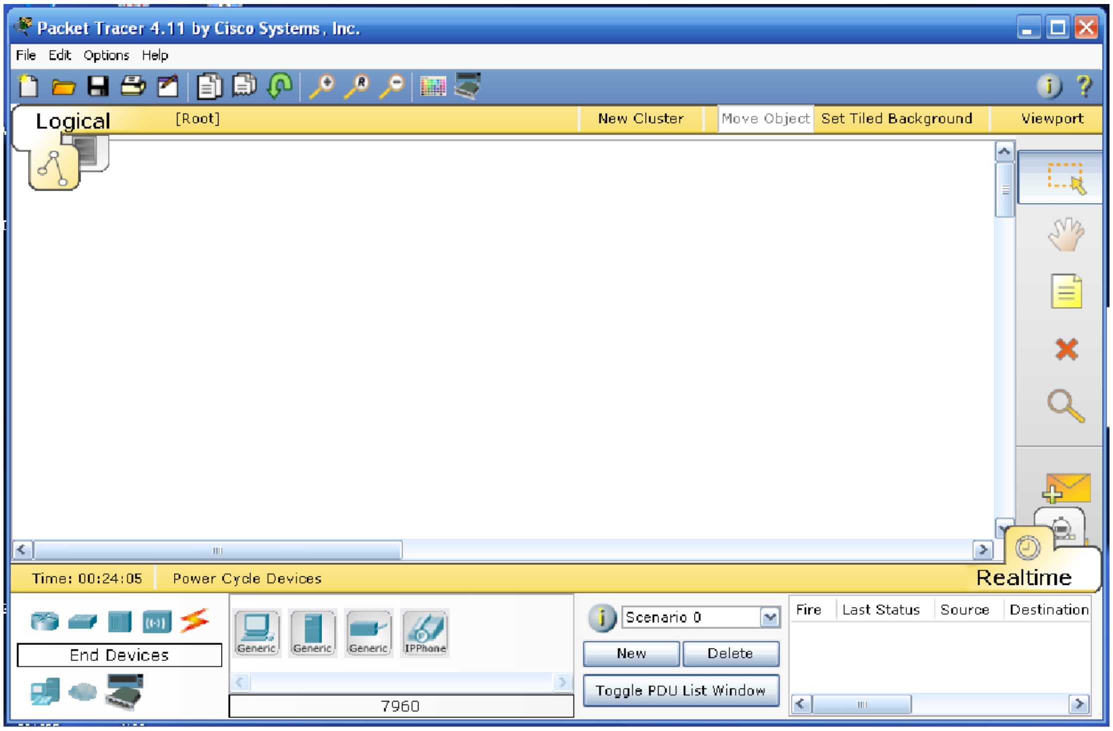
Step 1: Starting PT

If the following PT icon

Packet Tracer version 6.0.1.0011

is showing on the desktop then double-click on it. Alternatively, look for the package under ‘start/all programs’. If this does not work try appsanywhere.

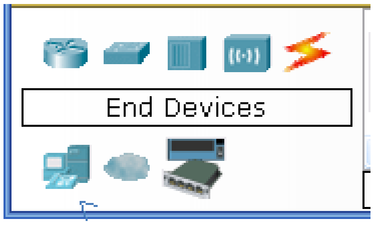
After you have the program running, the first screen – shown in diagram 1- will be displayed. Check that the Realtime tab towards the bottom right of the window (see diagram 1) is on top of the Simulation tab – if the simulation tab is showing then click the tab behind to bring the Realtime tab to the fore.



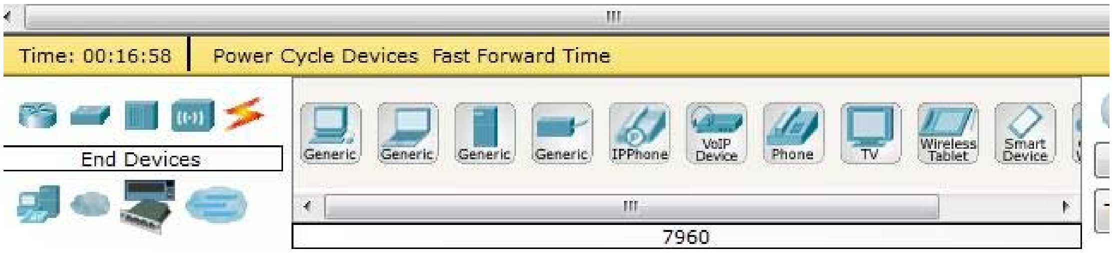
For the first few activities we will be concentrating on the icons found towards the bottom left of this opening screen.

Step 2: Load a virtual computer into the workspace

Look at the bottom left hand side of the PT window; there is a group of icons presented there, as shown in the next diagram.



The icons in the group indicate the range of devices that can be represented in a PT simulation. The icon at the bottom left of this group represent potential end devices for the network (PCs, Printers, Phones and Servers). Click on this icon and note that the box adjacent to it takes the following form.



The displayed icons represent (from left to right) a computer, a laptop, a server, a printer, a phone… Scroll along this bottom part of the screen to see the other end devices.

To introduce a computer into the simulation click on the Generic icon and then click on the work area. A picture of the computer icon should appear in the main screen, with the symbols

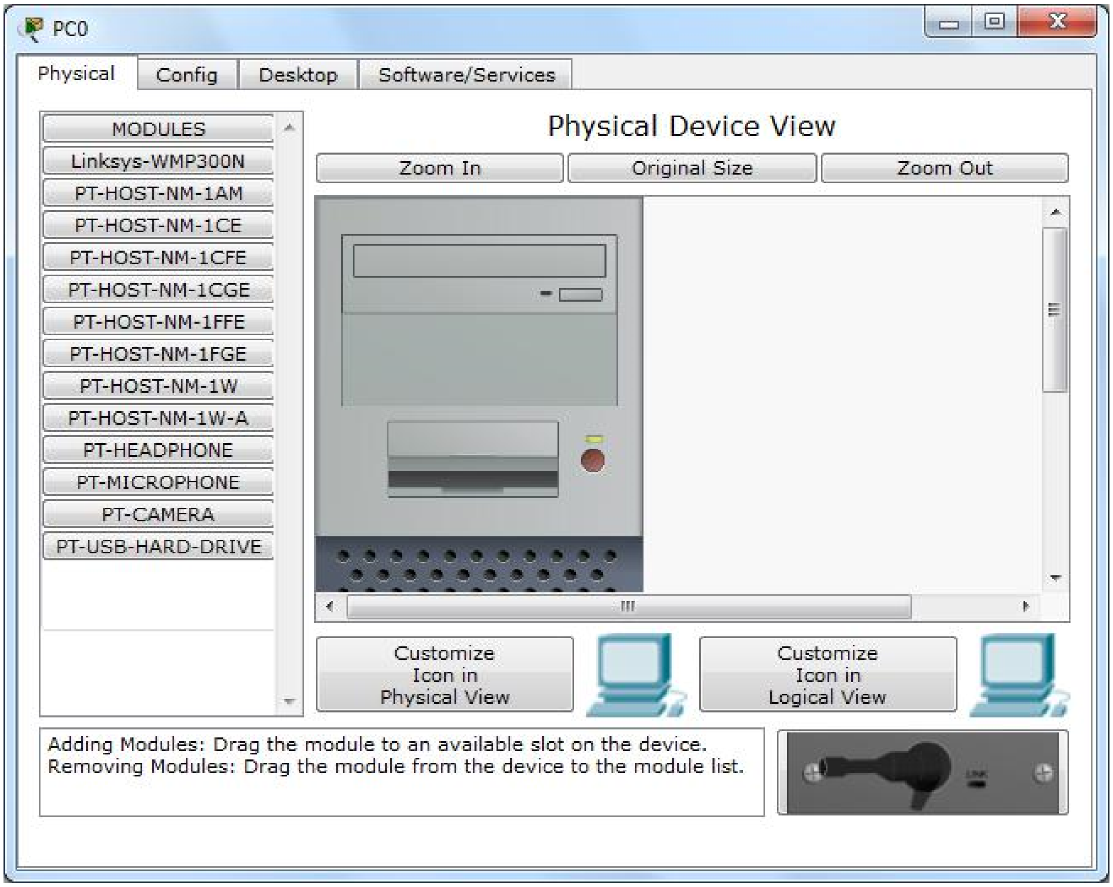
PC-PT
PC0

appearing beneath it.

The top PC indicates personal computer; the adjacent PT refers to Packet Tracer. The symbols on the second row are the name assigned to this PC (i.e. PC0) − this name can be changed to suit the user (see later).

Step 3: Investigating the PC

The personal computer in the window is more than a simple graphic: it models the behaviour of a PC well enough to demonstrate behaviour relevant to network modelling. To see this, click on the PC. You should see the following (don't worry if you haven't got this – it will be a minor error: check that you have created a PC and not some other PT object)



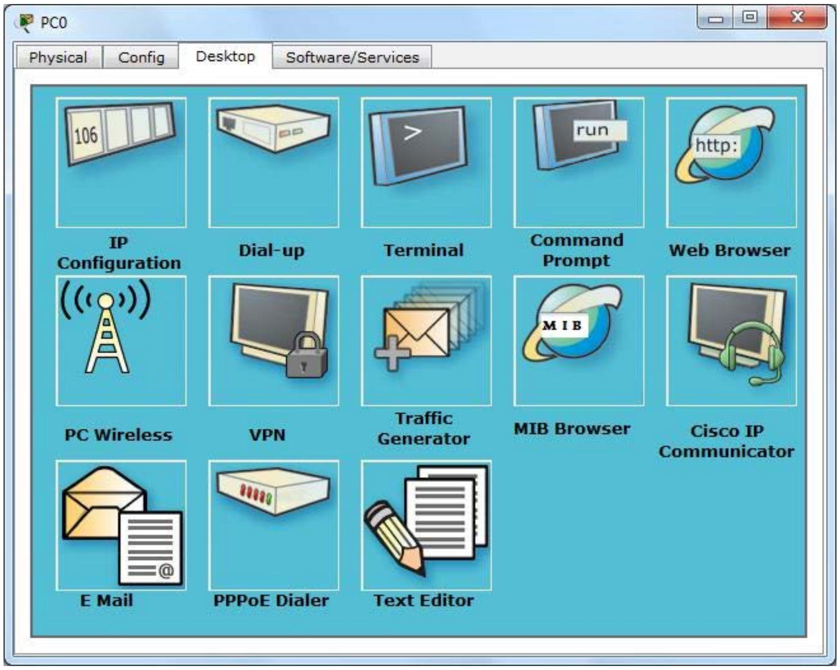
Adding Modules: Drag the module to an available slot on the device.
Removing Modules: Drag the module from the device to the module list.

Note the current name of the PC is displayed at top left (in our case the default, PC0, as supplied by the program). Below this name are four tabs:

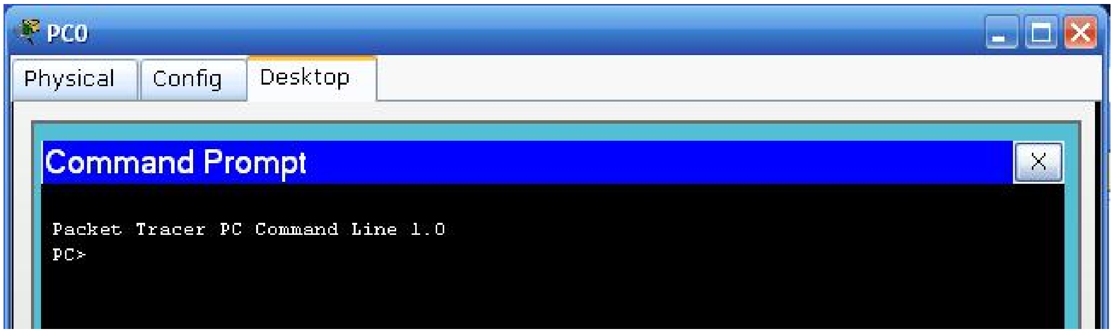
The currently selected tab is the Physical one, as can be seen from its different background. Observe the button halfway down and to the right of the PC image, with the green indicator light above it. This is an On/Off switch for the device – the default is for the device to be on. Click the switch and you will observe that the machine becomes switched off. Make sure that the device is switched on before proceeding.

Click on the Config and Desktop tabs and have a look at what is displayed.

Select the Desktop tab. You should have a screen like the following.



The desktop offers some of the tools you might expect from a personal computer. The following gives a partial screen shot of the command prompt.



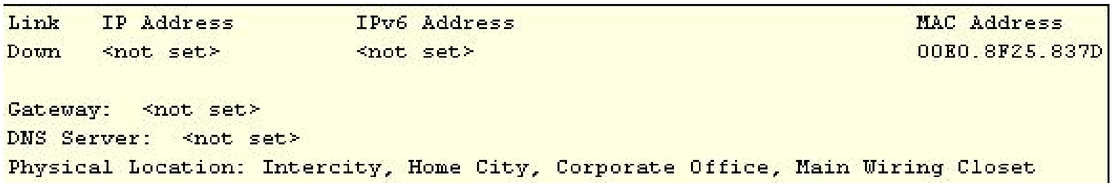
```
Packet Tracer PC Command Line 1.0
PC>
```

Try typing ipconfig at the prompt. You will see that the computer is not currently configured with an IP address. The PT simulation of a computer is limited to functions that are useful when modelling a network. Try the arp –a command (this will be empty since we are not connected to a network yet.).

Close the command prompt using the ☒ in the top right of the Command Prompt box – this will take you back to the PCs desktop. (Note if you type the cross at the very top right of the widget, i.e. ☒, then the model computer interface will close – don't worry, you can open it again by double clicking on the icon.).

Step 4 : Revisiting the PC

Close the interface to the PC (you should return to the opening screen with the placed PC on it). Let the cursor rest on the PC icon and you will get an information box displayed like the following.



```
Link   IP Address          IPv6 Address                                  MAC Address
Down   <not set>           <not set>                                     00E0.8F25.837D

Gateway:  <not set>
DNS Server:  <not set>
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

The information in the box is limited – we have not set an IP address, gateway and DNS server yet.

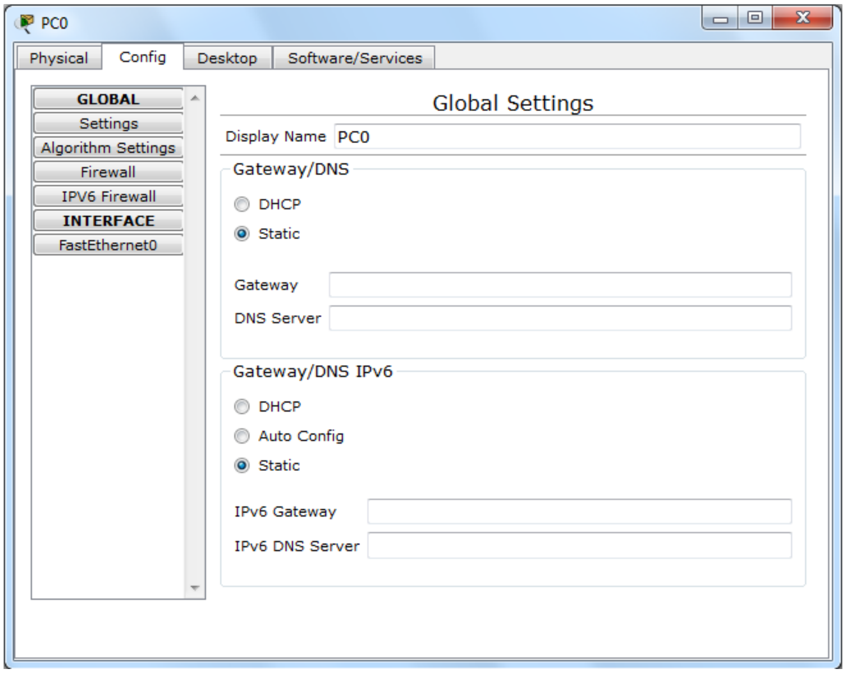
Though the MAC address for the PC's NIC card is displayed to the top right.

Further information about the PC (and other simulated devices) can be obtained by clicking the 🔍 icon found to the right of the main screen, and then clicking on the device. For the PC the only option is the ARP table and this is currently empty. (For routers and switches this is easily accessible information about the device – though the information can be obtained more 'conventionally' from the simulated object using the device interface!)

Before progressing return to the PCs Command Prompt (on the Desktop): the material you typed in is still there! The device behaves like a real device – the information is retained.

Now click on the IP Configuration tab. You will be taken to a window as shown in the following.

This is the PT equivalent to the GUI that is used by Windows to assign IP addresses etc.



Global Settings

Display Name PC0

Gateway/DNS

○ DHCP
● Static

Gateway

DNS Server

Gateway/DNS IPv6

○ DHCP
○ Auto Config
● Static

IPv6 Gateway

IPv6 DNS Server

Let us configure the PC using this GUI. (Strictly speaking we don't really need to use the form since our single computer is not connected to anything). Click on the IP Address box and input 1.0.0.2. Click

on the Subnet Mask; you will get a proposed mask – just accept this for the time being. Click on the Default Gateway and enter 1.0.0.1. Leave the DNS Server for the time being.

Come out of the PC and float the cursor over the icon again and you will see the information that you have input displayed.

Task

Introduce a printer , a telephone and a server into the logical workspace. Take a look at the Physical, Config and Desktop (server) interfaces to the devices. Try switching them On and Off (not the phone - no switch).

Note that all of the devices have options to assign IP addresses. A requirement for any **end** device on a network

Exit PT before starting the next activity. This ensures that any changes you have made will not be carried over into the next activity and the package starts in the standard mode.

Part 2 Creating a simple network

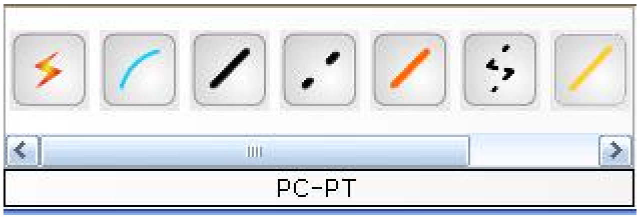
In this activity we will introduce two computers and then connect them up. We will check connectivity using the ping command. We will also introduce some new aspects of PT as we go; in particular, we will rename PCs and configure them with IP addresses.

Step 1: Configuring the network

Introduce two PCs into the workspace – click on the end devices icon (see Activity 1) then click on the workspace. Then repeat for the second PC. Make sure they are a couple of inches apart – note you can move them by: click, hold and drag the icon.

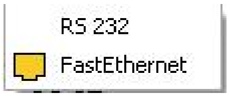
The two PCs will be named PC0 and PC1 We will rename the two PCs as ‘my comp’ and ‘your comp’. To do this click on the PC icon and select the Config tab. Just under the Global Settings header there is an input tool entitled Display Name. On one PC Type the name ‘my comp’ at the input tool (no inverted commas) and then name the other PC ‘your comp’ on the other machine.

To connect the two machines we need a copper crossover cable: click the ⚡ icon found in the bottom left group (this icon represents connectors). The box to the left will change to appear as follows. Note the icons represent different connection media, and there are more than are displayed as can be seen by using the slider bar.



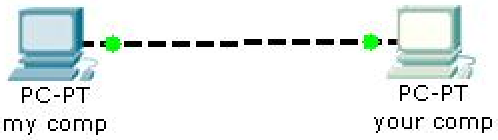
To select copper cross-over: move over the icons and note that the type of the connector is recorded in the text box at the bottom of this group, and note the type. The one we want is represented by ⋰ .

Click on the ⋰ icon and move onto the workspace. The cursor will change to a graphic representing a wire with a connector. To attach the wire to a computer click on it. The following box will appear next to the PC:



Click on the FastEthernet button (equivalent to attaching one end of the wire to the NIC on the PC). Now move the cursor over the other PC. (You will notice a wire graphic, extending from the first PC and moving with the cursor.) Click on the new PC and the same box as before will appear. Again, click on the FastEthenet button.

The current state of the window should have a network image in the logical workspace something like:

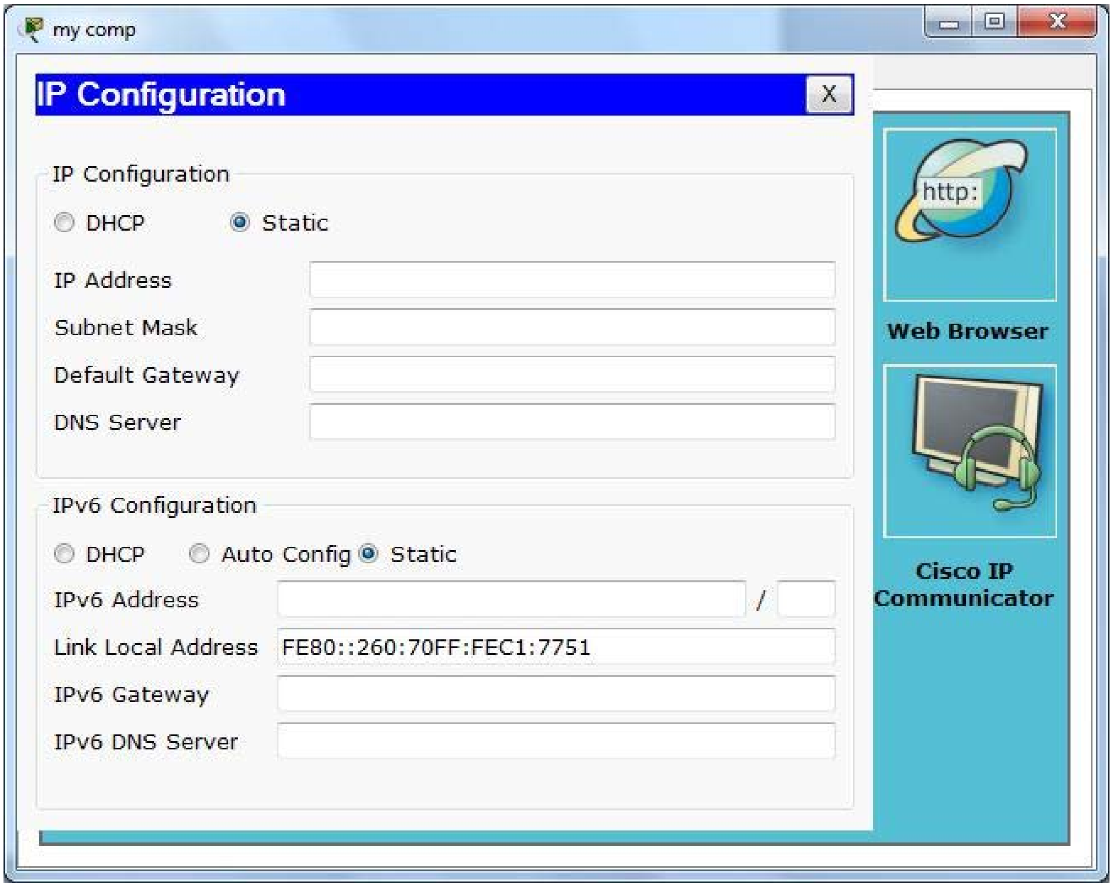


Representing two PCs connected by a copper cross-over cable via their FastEthernet ports.

Step 2 : Configuring IP addresses

The two PCs are connected but they cannot ‘speak’ to each other until they have IP addresses assigned.

Go into the Desktop of each PC and choose the IP configuration program which will bring up the following box.


my comp

IP Configuration

IP Configuration

○ DHCP ● Static

IP Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

Link Local Address FE80::260:70FF:FEC1:7751

IPv6 Gateway

IPv6 DNS Server

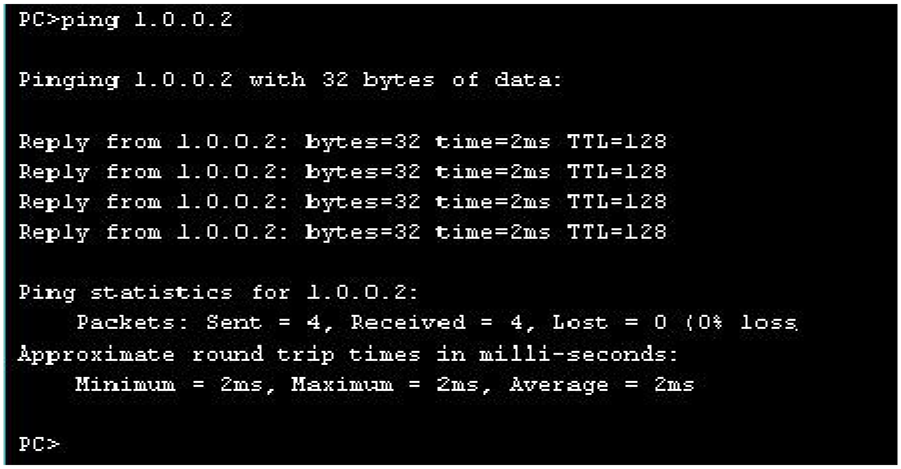
In the '*my comp'* input the IP address 1.0.0.1 and click in the Subnet Mask entry bar – this will automatically assign the mask 255.0.0.0. When this is done you exit the box by clicking the X at top right (opposite the IP Configuration header). Repeat the process on '*your comp*' PC, assigning address IP 1.0.0.2.

Step 3 : The Ping

To check that the two PCs are communicating, we will direct each PC to ping the other.

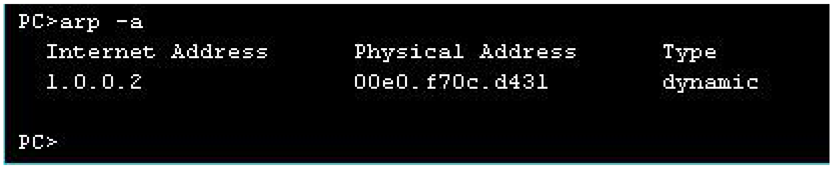
On '*my comp*' go into the Desktop and enter the Command Prompt. Enter on the active line (indicated by the prompt: PC>), ping 1.0.0.2 and observe the result. Repeat the process from '*your comp'*, remembering to use the correct IP address.

If you have successfully connected the machines up you will see a display like the following



```
PC>ping 1.0.0.2

Pinging 1.0.0.2 with 32 bytes of data:

Reply from 1.0.0.2: bytes=32 time=2ms TTL=128
Reply from 1.0.0.2: bytes=32 time=2ms TTL=128
Reply from 1.0.0.2: bytes=32 time=2ms TTL=128
Reply from 1.0.0.2: bytes=32 time=2ms TTL=128

Ping statistics for 1.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

PC>
```

We can also take a look at the ARP table for each computer by typing 'arp-a' at the command prompt. This contains the physical address required by the frame (don't worry about the particulars just now). This demonstrates further the nature of the simulation package.



```
PC>arp -a
  Internet Address      Physical Address      Type
  1.0.0.2               00e0.f70c.d431        dynamic

PC>
```

CONCLUSION A physical connection and an IP address is a necessary but not sufficient requirement for a device to be accessible on a network.

Exit PT before starting the next activity. This ensures that any changes you have made will not be carried over into the next activity and the package starts in the standard mode.

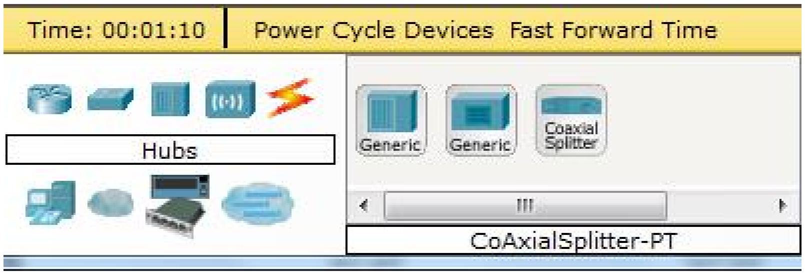
Part 3 Configuring the Network

In activity 2 we modelled the simplest possible network – two directly attached computers. The procedure described there is not sufficient when we increase the number of machines; an intermediate device is now required. In this activity we will simulate a network with 3 computers and an intermediate hub connecting them into a network.

Step 1: Constructing the network.

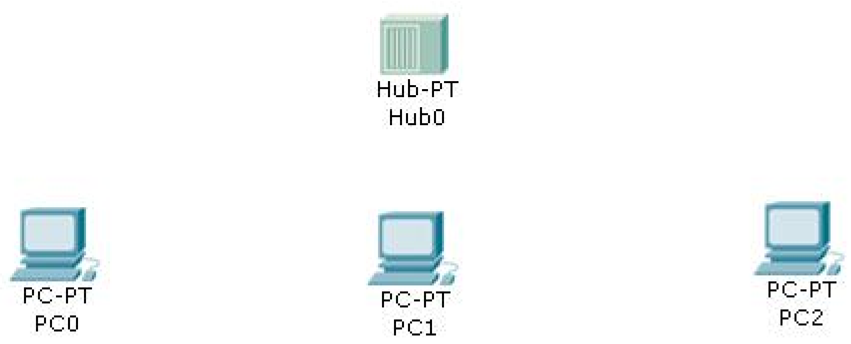
Introduce three PCs into the logical workspace (see Activity 2).

Introduce a hub. Move the cursor over the icons in the box bottom left. The types of objects represented by the icon will appear in the text box. Identify the icon representing Hubs and click. The box to the right will change indicating the available hubs (two in version 4.11) – see following.



Move the cursor over the three devices in the right hand box to see what the icon represents. Click on the generic icon for the Hub and drag into the logical workspace.

You should now have a work area something like the following (check that you have included a hub and not a repeater (look at name below the icon)).



You can rename the computers as before; and the hub by clicking on its icon – go to Config and changing the name there. This is up to you.

The network now has to be cabled. We use *copper straight* through cable in this situation (not the cross over version we used previously). Connect the FastEthernet ports on the PCs to available ports on the Hub (there are 6 ports on the Hub numbered 0 to 5)

Before progressing to A3 Step 2, let the cursor rest of the Hub icon. You will see a box appear in the logical workspace; it is attached to the Hub and contains information about it. In particular, the ports that are active are indicating that their link state is up. In general, information relating to devices in a simulation can be obtained by floating the cursor over the associated icon. Try this with the PCs.

Step 2 : Assigning IP addresses

We will address the 3 PCs simply as 1.0.0.1, 1.0.0.2 and 1.0.0.3. The Hub doesn't need an IP address (it simply takes packets in on one port and sends them out of all the other active ones). If you are unsure about assigning IP addresses review Activity 2 in this book.

Step 3: Investigating Connectivity with the Ping

From each PC ping each of the others and verify that they are connected. (Note that physically connected is not enough in the context of networking; they need to be in communication – see Activity 2).

Return to the command prompt on any of the PCs. Type help at the command prompt to see a list of the available commands – a limited but useful list.

Try the commands ipconfig (also try it as ipconfig /all) .

Try arp and arp –a.

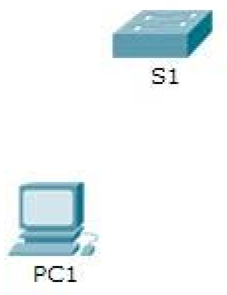
Try tracert to one of the other PCs (type tracert followed by the address eg tracert 1.0.0.2).

Exit PT before starting the next activity. This ensures that any changes you have made will not be carried over into the next activity and the package starts in the standard mode.

Lesson 2 Exploring a Network

Open file 2.1 Packet Tracer - Navigating the Internetwork Operating System (IOS)

Topology



Objectives

Part 1: Basic Connections, Accessing the CLI and Exploring Help

Part 2: Exploring EXEC Modes

Part 3: Setting the Clock

Background

In this activity, you will practice skills necessary for navigating the Cisco IOS, including different user access modes, various configuration modes, and common commands you use on a regular basis. You also practice accessing the context-sensitive Help by configuring the **clock** command.

Part 1: Basic Connections, Accessing the CLI and Exploring Help

In Part 1 of this activity, you connect a PC to a switch using a console connection and explore various command modes and Help features.

Step 1: Connect PC1 to S1 uses a console cable.

a. Click the **Connections** icon (the one that looks like a lightning bolt) in the lower left corner of the Packet Tracer window.

b. Select the light blue Console cable by clicking it. The mouse pointer will change to what appears to be a connector with a cable dangling off of it.

c. Click **PC1**; a window displays an option for an RS-232 connection.

d. Drag the other end of the console connection to the S1 switch and click the switch to bring up the connection list.

e. Select the Console port to complete the connection.

Step 2: Establish a terminal session with S1.

a. Click **PC1** and then select the **Desktop** tab.

b. Click the **Terminal** application icon; verify that the Port Configuration default settings are correct. What is the setting for bits per second? ________

c. Click **OK**.

d. The screen that appears may have several messages displayed. Somewhere on the display there should be a Press RETURN to get started! message. Press **ENTER**.
What is the prompt displayed on the screen? __________

Step 3: Explore the IOS Help.

a. The IOS can provide help for commands depending on the level being accessed. The prompt currently being displayed is called **User EXEC** and the device is waiting for a command. The most basic form of help is to type a question mark (?) at the prompt to display a list of commands.

S1> **?**

Which command begins with the letter ‘C’? ___________________

b. At the prompt, type **t**, followed by a question mark (**?**).

S1> **t?**

Which commands are displayed? ___________________________

c. At the prompt, type **te**, followed by a question mark (**?**).

S1> **te?**

Which commands are displayed? ___________________

This type of help is known as **context-sensitive** Help, providing more information as the commands are expanded.

Part 2: Exploring EXEC Modes

In Part 2 of this activity, you switch to privileged EXEC mode and issue additional commands.

Step 4: Enter privileged EXEC mode.

a. At the prompt, type the question mark (**?**).

S1> **?**

What information is displayed that describes the **enable** command?
____

b. Type **en** and press the **Tab** key.

S1> **en<Tab>**

What displays after pressing the **Tab** key? _________

This is called command completion or tab completion. When part of a command is typed, the **Tab** key can be used to complete the partial command. If the characters typed are enough to make the command unique, as in the case with the **enable** command, the remaining portion is displayed.

What would happen if you were to type **te<Tab>** at the prompt?

____
______

c. Enter the **enable** command and press **ENTER**. How does the prompt change?

____
______

d. When prompted, type the question mark (**?**).

S1# **?**

Previously there was one command that started with the letter 'C' in user EXEC mode. How many commands are displayed now that privileged EXEC mode is active? (**Hint**: you could type c? to list just the commands beginning with 'C'.)

____
______

Step 5: Enter Global Configuration mode.

a. One of the commands starting with the letter 'C' is **configure** when in Privileged EXEC mode. Type either the full command or enough of the command to make it unique along with the <**Tab**> key to issue the command and press **<ENTER>**.
S1# **configure**

What is the message that is displayed?

____
______

b. Press the **<ENTER>** key to accept the default parameter enclosed in brackets **[terminal]**.

How does the prompt change?
____

c. This is called global configuration mode. This mode will be explored further in upcoming activities and labs. For now exit back to Privileged EXEC mode by typing **end**, **exit** or **Ctrl-Z**.

```
S1(config)# exit

S1#
```

Part 3: Setting the Clock

Step 6: Use the clock command.

a. Use the **clock** command to further explore Help and command syntax. Type **show clock** at the privileged EXEC prompt.

```
S1# show clock
```

What information is displayed? What is the year that is displayed?

____

b. Use the context-sensitive Help and the **clock** command to set the time on the switch to the current time. Enter the command **clock** and press **ENTER**.

```
S1# clock<ENTER>
```

What information is displayed? ____

c. The % Incomplete command message is returned by the IOS indicating that the **clock** command needs further parameters. Any time more information is needed help can be provided by typing a space after the command and the question mark (?).

```
S1# clock ?
```

What information is displayed? ____

d. Set the clock using the **clock set** command. Continue proceeding through the command one step at a time.

```
S1# clock set ?
```

What information is being requested?

____

What would have been displayed if only the **clock set** command had been entered and no request for help was made by using the question mark?

____

e. Based on the information requested by issuing the **clock set ?** command, enter a time of 3:00 p.m. by using the 24-hour format of 15:00:00. Check to see if further parameters are needed.

```
S1# clock set 15:00:00 ?
```

The output returns the request for more information:

```
<1-31>   Day of the month

MONTH Month of the year
```

f. Attempt to set the date to 01/31/2035 using the format requested. It may be necessary to request additional help using the context-sensitive Help to complete the process. When finished, issue the **show clock** command to display the clock setting. The resulting command output should display as:

```
S1# show clock

*15:0:4.869 UTC Tue Jan 31 2035
```

g. If you were not successful, try the following command to obtain the output above:

```
S1# clock set 15:00:00 31 Jan 2035
```

Step 7: Explore additional command messages.

a. The IOS provides various outputs for incorrect or incomplete commands as experienced in earlier sections. Continue to use the **clock** command to explore additional messages that may be encountered as you learn to use the IOS.

b. Issue the following command and record the messages:

S1# **cl**

What information was returned? ____

S1# **clock**

What information was returned? ____

S1# **clock set 25:00:00**

What information was returned?

____

____

S1# **clock set 15:00:00 32**

What information was returned?

____

____

____

Tasks

Add another PC to the packet tracer work space and attempt to repeat the process above attaching it as a console to the switch.

Note that this isn’t possible. Why do you think that is?

Investigate network **switches** online. Here are some questions to help;

Define the term switch.

Compare a switch and a router.

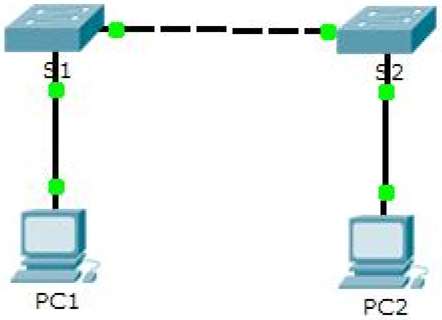
Find out how much a switch and a router cost.

Explain when you would recommend a switch or a router.

Lesson 3 Configuring Network Devices

Open file 3.1 Packet Tracer - Configuring Initial Switch Settings

Topology



Objectives

Part 1: Verify the Default Switch Configuration

Part 2: Configure a Basic Switch Configuration

Part 3: Configure a Message of the Day (MOTD) Banner

Part 4: Save configuration files to non-volatile RAM (NVRAM)

Part 5: Configure S2

Background

In this activity, you will perform basic switch configurations. You will secure access to the command-line interface (CLI) and console ports using encrypted and plain text passwords. You will also learn how to configure messages for users logging into the switch. These banners are also used to warn unauthorized users that access is prohibited.

Part 1: Verify the Default Switch Configuration

Step 1: Enter privileged mode.

You can access all switch commands from privileged mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use.

The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained.

a. Click **S1** and then the **CLI** tab. Press **<Enter>**.

b. Enter privileged EXEC mode by entering the **enable** command:

```
Switch> enable
Switch#
```

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Step 2: Examine the current switch configuration.

a. Enter the **show running-config** command.

```
Switch# show running-config
```

b. Answer the following questions (press space for more info):

How many FastEthernet interfaces does the switch have? _______

How many Gigabit Ethernet interfaces does the switch have? _______

What is the range of values shown for the vty lines? ______________

Part 2: Create a Basic Switch Configuration

Step 3: Assign a name to a switch.

To configure parameters on a switch, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the switch.

```
Switch# configure terminal

Switch(config)# hostname S1

S1(config)# exit

S1#
```

Step 4: Secure access to the console line.

To secure access to the console line, access config-line mode and set the console password to **letmein**. `S1#` **`configure terminal`**

```
Enter configuration commands, one per line. End with CNTL/Z.

S1(config)# line console 0

S1(config-line)# password letmein

S1(config-line)# login

S1(config-line)# exit

S1(config)# exit

%SYS-5-CONFIG_I: Configured from console by
console S1#
```

Why is the **login** command required?

Step 5: Verify that console access is secured.

Exit privileged mode to verify that the console port password is in effect.

```
S1# exit

Switch con0 is now available

Press RETURN to get started.


User Access Verification

Password:

S1>
```

Note: If the switch did not prompt you for a password, then you did not configure the **login** parameter as above.

Step 6: Secure privileged mode access.

Set the **enable** password to **c1$c0**. This password protects access to privileged mode.

Note: The **0** in **c1$c0** is a zero, not a capital O. This password will not grade as correct until after you encrypt it in Step 8.

```
S1> enable

S1# configure terminal

S1(config)# enable password c1$c0

S1(config)# exit

%SYS-5-CONFIG_I: Configured from console by
console S1#
```

Step 7: Verify that privileged mode access is secure.

a. Enter the **exit** command again to log out of the switch.

b. Press **<Enter>** and you will now be asked for a password:

```
User Access Verification
Password:
```

c. The first password is the console password you configured for **line console 0**. Enter this password to return to user EXEC mode.

d. Enter the command to access privileged mode – see above.

e. Enter the second password you configured to protect privileged EXEC mode.

f. Verify your configurations by examining the contents of the running-configuration file:

```
S1# show running-configuration
```

Notice how the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder.

Step 8: Configure an encrypted password to secure access to privileged mode.

The **enable password** should be replaced with the newer encrypted secret password using the **enable secret** command. Set the enable secret password to **itsasecret**.

```
S1# config t

S1(config)# enable secret itsasecret

S1(config)# exit

S1#
```

Note: The **enable secret** password overrides the **enable** password. If both are configured on the switch, you must enter the **enable secret** password to enter privileged EXEC mode.

Step 9: Verify that the enable secret password is added to the configuration file.

a. Enter the **show running-configuration** command again to verify the new **enable secret** password is configured.

   Note: You can abbreviate **show running-configuration** as

```
S1# show run
```

b. What is displayed for the **enable secret** password? ____

c. Why is the **enable secret** password displayed differently from what we configured?

Step 10: Encrypt the enable and console passwords.

As you noticed in Step 7, the **enable secret** password was encrypted, but the **enable** and **console** passwords were still in plain text. We will now encrypt these plain text passwords using the **service password-encryption** command.

```
S1# config t

S1(config)# service password-encryption

S1(config)# exit
```

If you configure any more passwords on the switch, will they be displayed in the configuration file as plain text or in encrypted form? Explain why?

Part 3: Configure a MOTD Banner

Step 11: Configure a message of the day (MOTD) banner.

The Cisco IOS command set includes a feature that allows you to configure messages that anyone logging onto the switch sees. These messages are called message of the day, or MOTD banners. Enclose the banner text in quotations or use a delimiter different from any character appearing in the MOTD string.

```
S1# config t

S1(config)# banner motd "This is a secure system. Authorized Access Only!"


S1(config)# exit


%SYS-5-CONFIG_I: Configured from console by
console S1#
```

When will this banner be displayed?

____

Part 4: Save Configuration Files to NVRAM

Step 12: Verify that the configuration is accurate using the show run command.

Step 13: Save the configuration file.

You have completed the basic configuration of the switch. Now back up the running configuration file to NVRAM to ensure that the changes made are not lost if the system is rebooted or loses power.

```
S1# copy running-config startup-config

Destination filename [startup-config]?[Enter]

Building configuration...

[OK]
```

_

Part 5: Configure S2

You have completed the configuration on S1. You will now configure S2. If you cannot remember the commands, refer to Parts 1 to 4 for assistance.

Configure S2 with the following parameters:

a. Name device: **S2**

b. Protect access to the console using the **letmein** password.

c. Configure an enable password of **c1$c0** and an enable secret password of **itsasecret**.

d. Configure a message to those logging into the switch with the following message:

```
Authorized access only. Unauthorized access is prohibited and
violators will be prosecuted to the full extent of the law.
```

e. Encrypt all plain text passwords.

f. Ensure that the configuration is correct.

g. Save the configuration file to avoid loss if the switch is powered down.

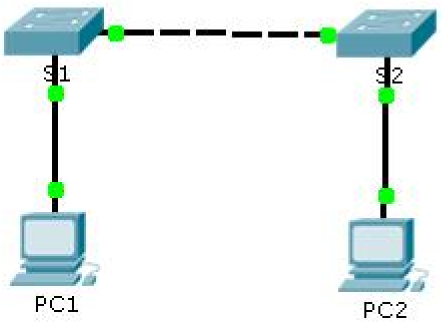
Tasks

Today you have had to use multiple logins to access different levels of control. Make a note of the key commands so that you can do this more easily in the future.

Lesson 4 Configuring Connectivity

Open file 4.1 Packet Tracer - Implement Basic Connectivity

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0

Objectives

Part 1: Perform a Configuration on S1 and S2

Part 2: Configure the PCs

Part 3: Configure the Switch Management Interface

Background

In this activity you will first perform basic switch configurations. Then you will implement basic connectivity by configuring IP addressing on switches and PCs. When the IP addressing configuration is complete, you will use various **show** commands to verify configurations and use the **ping** command to verify basic connectivity between devices.

Part 1: Perform a Basic Configuration on S1 and S2

Complete the following steps on S1 and S2.

Step 1: Configure S1 with a hostname.

a. Click **S1**, and then click the **CLI** tab.

b. Enter the correct command to configure the hostname as **S1**.

Step 2: Configure the console and privileged EXEC mode passwords.

a. Use **cisco** for the console password.

b. Use **class** for the privileged EXEC mode password.

Step 3: Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

____

____

____

Step 4: Configure a message of the day (MOTD) banner.

Use an appropriate banner text to warn unauthorized access. The following text is an example:

Authorized access only. Violators will be prosecuted to the full extent of the law.

Step 5: Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

____

____

Step 6: Repeat Steps 1 to 5 for S2.

Part 2: Configure the PCs

Configure PC1 and PC2 with IP addresses.

Step 7: Configure both PCs with IP addresses.

a. Click **PC1**, and then click the **Desktop** tab.

b. Click **IP Configuration**. In the **Addressing Table** above, you can see that the IP address for PC1 is 192.168.1.1 and the subnet mask is 255.255.255.0. Enter this information for PC1 in the **IP Configuration** window.

c. Repeat steps 1a and 1b for PC2.

Step 8: Test connectivity to switches.

a. Click **PC1**. Close the **IP Configuration** window if it is still open. In the **Desktop** tab, click **Command Prompt**. .

b. Type the **ping** command and the IP address for S1, and press **Enter**.

```
Packet Tracer PC Command Line
1.0 PC> ping 192.168.1.253
```

Were you successful? Why or why not?

Part 3: Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

Step 9: Configure S1 with an IP address.

Switches can be used as a plug-and-play device, meaning they do not need to be configured for them to work. Switches forward information from one port to another based on Media Access Control (MAC) addresses. If this is the case, why would we configure it with an IP address?

____

____

Use the following commands to configure S1 with an IP address.

```
S1 #configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

S1(config)# interface vlan 1

S1(config-if)# ip address 192.168.1.253 255.255.255.0

S1(config-if)# no shutdown

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to
up S1(config-if)#

S1(config-if)# exit

S1#
```

.

Step 10: Verify network connectivity.

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1’s and S2's IP address from PC1 and PC2.

a. Click **PC1**, and then click the **Desktop** tab.

b. Click **Command Prompt**.

c. Ping the IP address for PC2.

d. Ping the IP address for S1.

e. Ping the IP address for S2.

Note: You can also use the same **ping** command on the switch CLI and on PC2.

All pings should be successful. If your first ping result is 80%, retry; it should now be 100%. You will learn why a ping may fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.

Task

Go online shopping for the hardware in the network topology diagram shown at the beginning of the lesson.

Open file 4.2 Packet Tracer - Skills Challenge

Open the packet tracer lab file indicated above.

Topology

Addressing Table

.

Device	Interface	IP Address	Subnet Mask
Switch1	VLAN 1	192.168.2.253	255.255.255.0
Switch2	VLAN 1	192.168.2.254	255.255.255.0
PComp1	NIC	192.168.2.1	255.255.255.0
PComp2	NIC	192.168.2.2	255.255.255.0

Tasks

□ Change the Device names as indicated in blue in the table

□ Set the IP addresses indicated in blue in the table

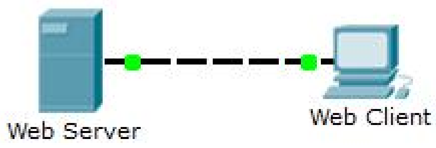
□ Correct the connection between the two PCs and the two switches.

□ Verify connectivity between the two PC end devices – remember to try this twice if necessary.

Lesson 5 Investigating TCP/IP and OSI

Open file 5.1 Packet Tracer - Investigating the TCP/IP and OSI Models in Action

Topology



Objectives

Part 1: Examine HTTP Web Traffic

Part 2: Display Elements of the TCP/IP Protocol Suite

Background

This simulation activity is intended to provide a foundation for understanding the TCP/IP protocol suite and the relationship to the OSI model. Simulation mode allows you to view the data contents being sent across the network at each layer.

As data moves through the network, it is broken down into smaller pieces and identified so that the pieces can be put back together when they arrive at the destination. Each piece is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer of the TCP/IP and OSI models. Packet Tracer simulation mode enables you to view each of the layers and the associated PDU. The following steps lead the user through the process of requesting a web page from a web server by using the web browser application available on a client PC.

Part 1: Examine HTTP Web Traffic

In Part 1 of this activity, you will use Packet Tracer (PT) Simulation mode to generate web traffic and examine HTTP.

Switch from Realtime to Simulation mode.

In the lower right corner of the Packet Tracer interface are tabs to toggle between **Realtime** and **Simulation** mode. PT always starts in **Realtime** mode, in which networking protocols operate with realistic timings. However, a powerful feature of Packet Tracer allows the user to "stop time" by switching to Simulation mode. In Simulation mode, packets are displayed as animated envelopes, time is event driven, and the user can step through networking events.

a. Click the **Simulation** mode icon to switch from **Realtime** mode to **Simulation** mode.

b. Select **HTTP** from the **Event List Filters**.

   1) HTTP may already be the only visible event. Click **Edit Filters** to display the available visible events. Toggle the **Show All/None** check box and notice how the check boxes switch from unchecked to checked or checked to unchecked, depending on the current state.

   2) Click the **Show All/None** check box until all boxes are cleared and then select **HTTP**. Click anywhere outside of the **Edit Filters** box to hide it. The Visible Events should now only display HTTP.

Generate web (HTTP) traffic.

Currently the Simulation Panel is empty. There are six columns listed across the top of the Event List within the Simulation Panel. As traffic is generated and stepped through, events appear in the list. The **Info** column is used to inspect the contents of a particular event.

Note: The Web Server and Web Client are displayed in the left pane. The panels can be adjusted in size by hovering next to the scroll bar and dragging left or right when the double-headed arrow appears.

a. Click **Web Client** in the far left pane.

b. Click the **Desktop** tab and click the **Web Browser** icon to open it.

c. In the URL field, enter **www.osi.local** and click **Go**.

   Because time in Simulation mode is event-driven, you must use the **Capture/Forward** button to display network events.

d. Click **Capture/Forward** four times. There should be four events in the Event List.

Look at the Web Client web browser page. Did anything change?

____

Explore the contents of the HTTP packet.

a. Click the first colored square box under the **Event List** > **Info** column. It may be necessary to expand the **Simulation Panel** or use the scrollbar directly below the **Event List**.

The **PDU Information at Device: Web Client** window displays. In this window, there are only two tabs (**OSI Model** and **Outbound PDU Details**) because this is the start of the transmission. As more events are examined, there will be three tabs displayed, adding a tab for **Inbound PDU Details**. When an event is the last event in the stream of traffic, only the **OSI Model** and **Inbound PDU Details** tabs are displayed.

b. Ensure that the **OSI Model** tab is selected. Under the **Out Layers** column, ensure that the **Layer 7** box is highlighted.

What is the text displayed next to the **Layer 7** label? ______________________________________

What information is listed in the numbered steps directly below the **In Layers** and **Out Layers** boxes?

____

c. Click **Next Layer**. Layer 4 should be highlighted. What is the **Dst Port** value? ____________________

d. Click **Next Layer**. Layer 3 should be highlighted. What is the **Dest. IP** value? ____________________

e. Click **Next Layer**. What information is displayed at this layer?

____

f. Click the **Outbound PDU Details** tab.

Information listed under the **PDU Details** is reflective of the layers within the TCP/IP model.

Note: The information listed under the **Ethernet II** section provides even more detailed information than is listed under Layer 2 on the **OSI Model** tab. The **Outbound PDU Details** provides more descriptive and detailed information. The values under **DEST MAC** and **SRC MAC** within the **Ethernet II** section of the **PDU Details** appear on the **OSI Model** tab under Layer 2, but are not identified as such.

What is the common information listed under the **IP** section of **PDU Details** as compared to the information listed under the **OSI Model** tab? With which layer is it associated?

____

What is the common information listed under the **TCP** section of **PDU Details**, as compared to the information listed under the **OSI Model** tab, and with which layer is it associated?

____

What is the **Host** listed under the **HTTP** section of the **PDU Details**? What layer would this information be associated with under the **OSI Model** tab?

____

g. Click the next colored square box under the **Event List** > **Info** column. Only Layer 1 is active (not grayed out). The device is moving the frame from the buffer and placing it on to the network.

h. Advance to the next HTTP **Info** box within the **Event List** and click the colored square box. This window contains both **In Layers** and **Out Layers**. Notice the direction of the arrow directly under the **In Layers** column; it is pointing upward, indicating the direction the information is travelling. Scroll through these layers making note of the items previously viewed. At the top of the column the arrow points to the right. This denotes that the server is now sending the information back to the client.

Comparing the information displayed in the **In Layers** column with that of the **Out Layers** column, what are the major differences?

____

i. Click the **Outbound PDU Details** tab. Scroll down to the **HTTP**

section. What is the first line in the HTTP message that displays?

____

j. Click the last colored square box under the **Info** column. How many tabs are displayed with this event and why?

____

Part 3: Display Elements of the TCP/IP Protocol Suite

In Part 2 of this activity, you will use the Packet Tracer Simulation mode to view and examine some of the other protocols comprising of the TCP/IP suite.

View Additional Events

a. Close any open PDU information windows.

b. In the Event List Filters > Visible Events section, click **Show All**. What additional Event Types are displayed?

____

____

____

____

____

____

These extra entries play various roles within the TCP/IP suite. If the Address Resolution Protocol (ARP) is listed, it searches MAC addresses. DNS is responsible for converting a name (for example, **www.osi.local**) to an IP address. The additional TCP events are responsible for connecting, agreeing on communication parameters, and disconnecting the communications sessions between the devices. These protocols have been mentioned previously and will be further discussed as the course progresses. Currently there are over 35 possible protocols (event types) available for capture within Packet Tracer.

c. Click the first DNS event in the **Info** column. Explore the **OSI Model** and **PDU Detail** tabs and note the encapsulation process. As you look at the **OSI Model** tab with **Layer 7** highlighted, a description of what is occurring is listed directly below the **In Layers** and **Out Layers** ("1. The DNS client sends a DNS query to the DNS server."). This is very useful information to help understand what is occurring during the communication process.

d. Click the **Outbound PDU Details** tab. What information is listed in the **NAME**: in the DNS QUERY section?

____

e. Click the last DNS **Info** colored square box in the event list. Which device is displayed?

____

What is the value listed next to **IP**: in the DNS ANSWER section of the **Inbound PDU Details**?

____

f. Find the first **HTTP** event in the list and click the colored square box of the **TCP** event immediately following this event. Highlight **Layer 4** in the **OSI Model** tab. In the numbered list directly below the **In Layers** and **Out Layers**, what is the information displayed under items 4 and 5?

____

TCP manages the connecting and disconnecting of the communications channel along with other responsibilities. This particular event shows that the communication channel has been ESTABLISHED.

g. Click the last TCP event. Highlight Layer 4 in the **OSI Model** tab. Examine the steps listed directly below **In Layers** and **Out Layers**. What is the purpose of this event, based on the information provided in the last item in the list (should be item 4)?

____

Challenge

This simulation provided an example of a web session between a client and a server on a local area network (LAN) . The client makes requests to specific services running on the server. The server must be set up to listen on specific ports for a client request. (Hint: Look at Layer 4 in the **OSI Model** tab for port information.)

Based on the information that was inspected during the Packet Tracer capture, what port number is the **Web Server** listening on for the web request?

____

____

What port is the **Web Server** listening on for a DNS request?

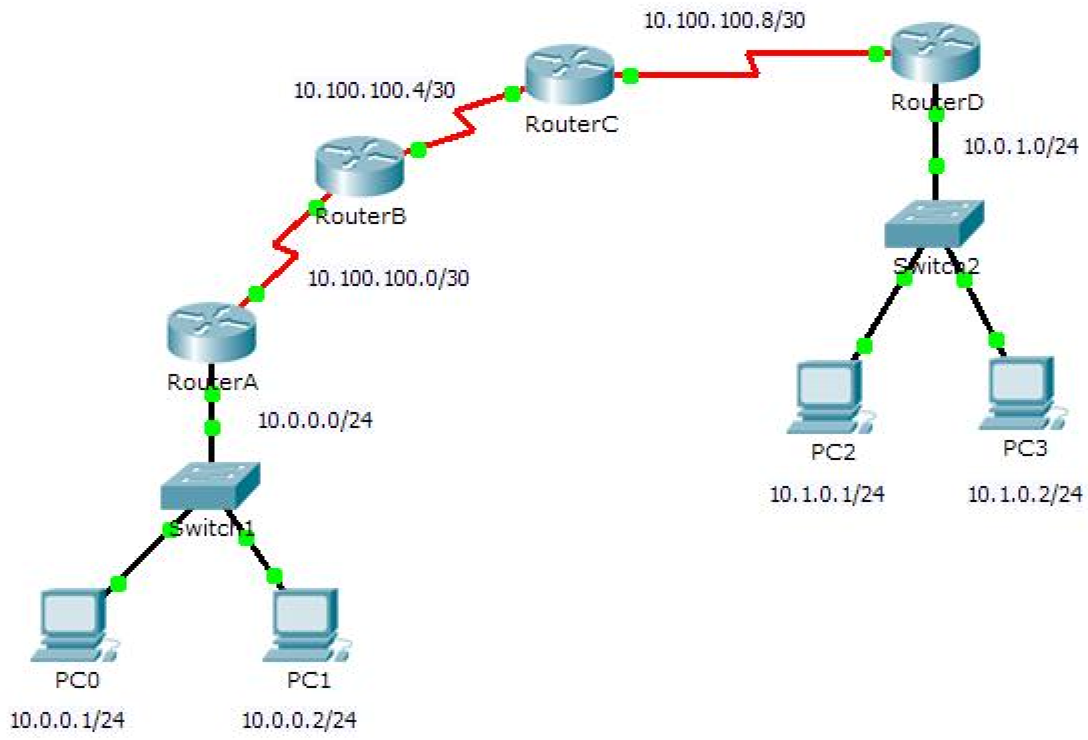
____

____

Part 4: Test End-to-End Connectivity with the tracert Command

Open file 5.2 Packet Tracer - Testing Connectivity with Traceroute

Topology



Objectives

Part 1: Test End-to-End Connectivity with the tracert Command

Part 2: Compare to the traceroute Command on a Router

Background

This activity is designed to help you troubleshoot network connectivity issues using commands to trace the route from source to destination. You are required to examine the output of **tracert** (the Windows command) and **traceroute** (the IOS command) as packets traverse the network and determine the cause of a network issue. After the issue is corrected, use the **tracert** and **traceroute** commands to verify the completion.

Step 1: Send a ping from one end of the network to the other end.

Click **PC1** and open the **Command Prompt**. Ping **PC3** at **10.1.0.2**. What message is displayed as a result of the ping?

Step 2: Trace the route from PC1 to determine where in the path connectivity fails.

a. From the **Command Prompt** of **PC1**, enter the **tracert 10.1.0.2** command.

b. When you receive the **Request timed out** message, press **Ctrl**+**C**. What was the first IP address listed in the **tracert** output?

c. Observe the results of the **tracert** command. What is the last address reached with the **tracert** command?

Step 3: Correct the network problem.

a. Compare the last address reached with the **tracert** command with the network addresses listed on the topology. The furthest device from the host 10.0.0.2 with an address in the network range found is the point of failure. What devices have addresses configured for the network where the failure occurred?

b. Click **RouterC** and then the **CLI** tab.

c. What is the status of the interfaces?

d. Compare the IP addresses on the interfaces with the network addresses on the topology. Does there appear to be anything extraordinary?

e. Make the necessary changes to restore connectivity; however, do not change the subnets. What is solution?

Step 4: Verify that end-to-end connectivity is established.

a. From the **PC1 Command Prompt**, enter the **tracert 10.1.0.2** command.

b. Observe the output from the **tracert** command. Was the command successful?

c. Click **RouterA** and then the **CLI** tab.

d. Enter the **traceroute 10.1.0.2** command. Did the command complete successfully?

e. Compare the output from the router **traceroute** command with the PC **tracert** command. What is noticeably different about the list of addresses returned?