Experiment-1

Aim: Study of different types of Network cables and Practically implement the cross-wired cable and straight through cable using clamping tool.

Apparatus (Components): RJ-45 connector, Climping Tool, Ethernet , LAN Tester

Procedure: To do these practical following steps should be done:

1. Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render is useless. Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.

2. Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than 1/2 of an inch of un-twisted wire.

3. You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end. Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated pics below.

Diagram shows you how to prepare Cross wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

Diagram shows you how to prepare straight through wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

Experiment - 2

Aim: Study of following Network Devices in Detail

- Hub
- Switch
- Router
- Gate Way

Procedure: Following should be done to understand this practical.

Apparatus (Components):Packet Tracer

1. **Hub:** An **Ethernet hub**, **active hub**, **network hub**, **repeater hub**, **hub** or **concentrator** is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

2. **Switch:** A **network switch** or **switching hub** is a computer networking device that connects network segments. The term commonly refers to a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.

3. **Router:** A **router** is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.

4. **Gate Way:** In a communications network, a network node equipped for interfacing with another network that uses different protocols.

- A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks.

Hub Networking in Cisco Packet tracer

In Cisco Packet Tracer, multiple computers can communicate through a hub.
First, add three computer equipment

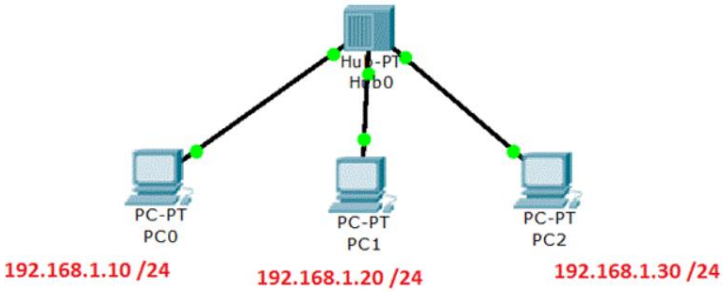
1. Follow the steps 1 and 2, and perform the 2 steps three times. Drag and drop the PC on the way. You can also hold down the Ctrl key and click the three blank spaces during the 2 steps to place the three computers.

Second. Add a hub to the picture

Third. Connect the PC device to the hub

1. Connect the hub and PC0.

Fourth, set the IP address of the PC



1. Click PC0, and a dialog box will pop up.
can select the IP segment according to your own situation.

2. Follow the steps to set the IP address and subnet mask of PC1 and PC2 as follows:

Fifth. Test that the three PCs can communicate with each other

Here ,we use the ping command to test the communication between PCs. It can also be tested by simulation.

select any one of the PCs, we assume that PC1 computer is selected here.

1. Click the icon, and a dialog box will pop up. The operation is as follows, and then command the terminal too early.

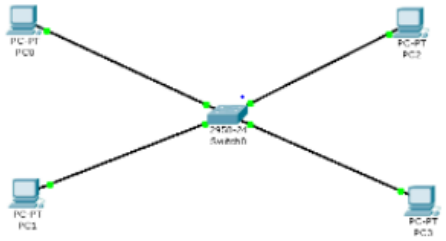
2, enter in the pop-up terminal:

Ping 192.168.1.2 and wait for the data packet to return the result

Ping 192.168.1.3 and wait for the data packet to return the result

If the result appears, it means that the communication is normal.

Connecting a Switch



Objectives

- Connect a switch to the network.
- Verify the configuration on the switch.

Background / Preparation

In this activity, you will verify the configuration on the customer Cisco Catalyst 2960 switch. The switch is already configured with all the basic necessary information for connecting to the LAN at the customer site. The switch is currently not connected to the network. You will connect the switch to the customer workstation, the customer server, and customer router. You will verify that the switch has been connected and configured successfully by pinging the LAN interface of the customer router.

Step 1: Connect the switch to the LAN.

a. Using the proper cable, connect the FastEthernet0/0 on Customer Router to the FastEthernet0/1 on Customer Switch.

b. Using the proper cable, connect the Customer PC to the Customer Switch on port FastEthernet0/2.

c. Using the proper cable, connect the Local Server to the Customer Switch on port FastEthernet0/3.

Step 2: Verify the switch configuration.

a. From the Customer PC, use the terminal emulation software to connect to the console of the customer Cisco Catalyst 2960 switch.

b. Use the console connection and terminal utility on the Customer PC to verify the configurations. Use cisco as the console password.

c. Verify IP connectivity between the Cisco Catalyst 2960 switch and the Cisco 1841 router by initiating a ping to 192.168.1.1 from the switch CLI.

d. Click the Check Results button at the bottom of this instruction window to check your work.

Configuring Wireless Router

Objectives:

Configure WEP security between a workstation and a Linksys wireless router.

Background / Preparation

You have been asked to go back to a business customer and install a new Linksys wireless router for the customer office. The company has some new personnel who will be using wireless computers to save money on adding additional wired connections to the building. The business is concerned about the security of the network because they have financial and highly classified data being transmitted over the network. Your job is to configure the security on the router to protect the data.

In this activity, you will configure WEP security on both a Linksys wireless router and a workstation.

Step 1: Configure the Linksys wireless router to require WEP.

a. Click the Customer Wireless Router icon. Then, click the GUI tab to access the router web management interface.

b. Click the Wireless menu option and change the Network Name (SSID) from Default to CustomerWireless. Leave the other settings with their default options.

c. Click the Save Settings button at the bottom of the Basic Wireless Settings window.

d. Click the Wireless Security submenu under the Wireless menu to display the current wireless security parameters.

e. From the Security Mode drop-down menu, select WEP.

f. In the Key1 text box, type 1a2b3c4d5e. This will be the new WEP pre-shared key to access the wireless network.

g. Click the Save Settings button at the bottom of the Wireless Security window.

Step 2: Configure WEP on the customer wireless workstation.

a. Click the Customer Wireless Workstation.

b. Click the Config tab.

c. Click the Wireless button to display the current wireless configuration settings on the workstation.

d. Change the SSID to CustomerWireless.

e. Change the Security Mode to WEP. Enter 1a2b3c4d5e in the Key text box, and then close the window.

Step 3: Verify the configuration.

After you configure the correct WEP key and SSID on the customer wireless workstation, notice that there is a wireless connection between the workstation and the wireless router.

a. Click the Customer Wireless Workstation.

b. Click the Desktop tab to view the applications that are available.

c. Click on the Command Prompt application to bring up the command prompt.

d. Type ipconfig /all and press Enter to view the current network configuration settings.

e. Type ping 192.168.2.1 to verify connectivity to the LAN interface of the customer wireless router.

f. Close the command prompt window.

g. Open a web browser.

h. In the address bar of the web browser window, type http://192.168.1.10. Press Enter. The Intranet web page that is running on the customer server appears. You have just verified that the customer wireless workstation has connectivity to the rest of the customer network.

i. Click the Check Results button at the bottom of this instruction window to check your work.