UMM AL-QURA UNIVERSITY

College of Computer and Information Systems

Computer Engineering Department

1403422

Computer Networks

Lab Manual

Student Name: _____

Student ID: _____

Section: _____ Group: _____

Session (Fall / Spring / Summer) _____

This page is intentionally left blank

TABLE OF CONTENTS

Prepared By:	Engr. Muhammad Saqib	2012
Revised By:	_____	_____
Reviewed By:	_____	_____
Approved By:	_____	_____

Umm Al-Qura University

Computer Engineering Department

LABORATORY SAFETY GUIDELINES

A. General Laboratory Safety Rules

1. Personal Safety

- Be familiar with the electrical and fire hazards associated with your workplace.
- Be as careful for the safety of others as for yourself. Think before you act.
- Be tidy and systematic.
- Avoid bulky, loose or trailing clothes. Avoid long loose hair.
- No one is allowed to enter in the lab area bare foot due to increased risk of electric shock.
- Remove metal bracelets, rings or watchstraps when working in the laboratories.
- Avoid working with wet hands and clothing.

2. Food, Beverages and Smoking

- Due to the increased risk of electric shock, no drinking of beverages, consumption or storage of any kind of food is allowed in the laboratory.
- Smoking is prohibited in all laboratories in all timings.

3. Soldering

- No one is allowed to do soldering in any of the computer engineering laboratories except the graduation project design laboratory.
- Anyone doing soldering in the graduation project design laboratory must wear appropriate apparel, socks, gloves, covered shoes and safety goggles to prevent the possibility of severe burns resulting from the splashing or dripping of hot liquefied solder into the face and eyes or on to the exposed skin on the chest, hands, legs, and feet.
- Students who are not so properly attired for these tasks will NOT be allowed to perform any type of soldering in the graduation project design laboratory.

4. Laboratory Operating Hours

- Students are never allowed to work alone in any lab area other than scheduled laboratory operating hours unless either a Lab T/A or Course Instructor is present inside that lab area.
- The laboratory operating hours for students are posted on the entrance doorway and on the notice board of computer engineering department.

5. Power Supply Related Safety

- Voltages above 50-VAC or 120-VDC are always dangerous.
- Extra precautions should be considered as voltage levels are increased.
- Never make any changes to circuits or mechanical layout without first isolating the circuit by switching off and removing connections to power supplies.

6. Laboratory Equipment

- Lab equipment may not be removed from the Computer Engineering lab areas without the permission of the Laboratory Supervisors.
- Laboratory bench equipment (except for some lab bench computers) must be turned off before closing down the lab area for the day.
- Never open (remove cover) of any equipment in the laboratories.
- Never "jump," disable, bypass or otherwise disengage any safety device or feature of any equipment in the laboratories.
- Laboratories shall be locked when unoccupied.

7. Waste Management Safety

- Know the correct handling, storage and disposal procedures for batteries, cell, capacitors, inductors and other high energy-storage devices.

8. Equipment Safety

- Before equipment is energized ensure, circuit connections and layout have been checked by a Teaching Assistant (TA) and all colleagues in your group has given their consent.
- Experiments left unattended should be isolated from the power supplies. If for a special reason, it must be left on, a barrier and a warning notice are required.
- Equipment found to be faulty in any way should be reported to the lab supervisor and taken out of service until inspected and declared safe.

9. Equipment Accessories

- Use extension cords only when necessary and only on a temporary basis.
- Request new outlets if your work requires equipment in an area without an outlet.
- Discard damaged cords, cords that become hot, or cords with exposed wiring.

B. Electrical and Fire Emergency Responses

1. Police, Fire or Medical Emergency

- Use the telephone located in the laboratory area and press 0-996 to notify police, fire, and ambulance for emergency help.
- Everyone present in the laboratory area shall be familiar with the locations and operation of safety and emergency equipment, including but not limited to, fire extinguishers, first aid kits, emergency power off system, fire alarm pull stations, and emergency telephones.

2. Electric Shock

- When someone suffers serious electrical shock, he may be knocked unconscious.
- If the victim is still in contact with electrical current, immediately turn off the electrical power source.
- If you cannot disconnect the power source, depress the Emergency Power Off switch.
- Do not touch a victim that is still in contact with a live power source; you could be electrocuted! Have someone call for emergency medical assistance immediately. Administer first-aid, as appropriate.

3. Electrical Fire

- If an electrical fire occurs, try to disconnect the electrical power source, if possible.
- If the fire is small and you are not in immediate danger; and if you have been properly trained in fighting fires, use the correct type of fire extinguisher to extinguish the fire.
- When in doubt, push in the Emergency Power Off button.
- NEVER use water to extinguish an electrical fire.

4. Emergency Power Off

- Every lab is equipped with an Emergency Power off System.
- When this switch is depressed, electrical power to the lab will shut off, except for lights.
- Only authorized personnel are permitted to reset power once the Emergency Power Off system has been engaged.

5. Building Evacuation in Emergency

- Everyone present in the laboratory should be familiar to emergency exits & way out plans.
- Use the nearest exit doorway from lab area closest to the stairwell to exit the building.
- Follow the Emergency Exit Signs posted in the hallways. Do not use elevators.
- Lab Teaching Assistants (T/As) or Instructor shall make sure all persons are out of the laboratory area and follow the directions posted at each doorway to the laboratory area.

The above general laboratory safety rules are designed to safeguard you and your co-workers, fellow students and colleagues and are a minimum requirement for individuals working in the computer engineering laboratories at Umm Al-Qura University, Makkah Al-Mukarramah. Specialized training and rules may apply depending on type and scope of activities involved.

This page is intentionally left blank

Lab 1: PC Network TCP/IP Configuration

In this lab we will learn about

- ✓ Computer Networks Configuration
  - Introduction to IP addressing
  - Identify tools used for discovering a computer's network configuration with various operating systems.
  - Gather information, including the connection, host name, MAC(Layer2) address, and TCP/IP Network(Layer 3)
  - Compare the network information to that of other PC's on the network.
  - Learn to use the TCP/IP packet Internet groper (ping) command from a workstation.
  - Learnt to use the trace route (tracert) command from a workstation.
  - Observe name-resolution occurrences using WINS and DNS servers.

Part A:Background/Preparation

This lab assumes that you are using Windows NT/2000/XP. This is nondestructive lab that you can perform on any host without changing the system configuration.

Ideally, you perform this lab in a LAN environment that connects to the Internet. You can use a single remote connection via a dial up modem or DSL. You will need the IP address information which the instructor should provide.

Introduction to IP addressing

Each Network Interface Card (NIC or Network card) present in a PC is assigned one Network address called as IP address [or Network address]. This IP address is assigned by the administrator of the network. No two PCs can have the same IP address.

There is a burned-in address on the NIC called as Physical Address [or MAC address or Hardware address]. The MAC address of a network card indicates the vendor of that card and a unique serial number.

Rules for IP 4 Addressing

1. Format of IP address IPv4 is made up of four parts, in the pattern as w.x.y.z. Each part has 8 binary bits and the values in decimal can range from 0 to 255.
2. IP address classes

IP addresses are divided into different classes. These classes determine the maximum number of hosts per network ID. Only three classes are actually used for network connectivity. The following table lists all of the address class.

3. Grouping of IP addresses into different classes.
   a) Class A, B, C, D, E
   b) Class A: first bit in w is 0 and others can be anything
      i. 0.0.0.0 to 127.255.255.255
      First bits are used for network part and the remaining for host part.
   c) Class B: First bit in w is 1 and second bit is 0.
      i. 128.0.0.0 to 191.255.255.255
      ii. First 16 bits for network part and remaining host part
   d) Class C: first bit in w is 1, second bit in w is 1 and third bit is 0
      i. 192.0.0.0 to 223.255.255.255
      ii. ii. First 24 bits for network part and last 8 bits for host part.
   e) Class D: first, second, third bits in w are 1 and fourth bit is 0; used for multicast.
      i. 224.0.0.0 to 247.255.255.255
   f) Class E: future use or experimental purposes.

4. Default Subnet mask it is used to identify the network part from the host part. Put binary one for the parts that represent network part and zero for the part that represent host part.
    a) Class A: 255.0.0.0
    b) Class B: 255.255.0.0
    c) Class C: 255.255.255.0
    d) We can't have mix of 1s and 0s in subnet mask. Only consecutive 1s is followed by consecutive 0s
5. Invalid IP address.
    a) If the network part is all 0s, the address belongs to class A. But this is an invalid ip address because for an ip address all the network or host part should not be all 1s or all 0s.
        i. 0.0.0.0 is not valid. Routers use it internally.
    b) If the network part is all 1s, this address belongs to class E. But due to presence of all 1s, it is not valid. This represent broadcast to all networks.
        i. 255.255.255.255 is not valid.
    c) If the host part is all 0s, this represents network address. This is not a valid ip address.
    d) If the host part is all 1s, this represents broadcast address. This is not a valid ip address.
    e) We can't use the ip address represented within private address range as part of public ip address.
        i. Class A: 10.0.0.0 to 10.255.255.255
        ii. Class B: 172.16.0.0 to 172.31.255.255
        iii. Class C: 192.168.0.0 to 192.168.255.255
    f) 127.0.0.0 network address is used for loop-back testing. This will help you to check the network card of your own PC [localhost].
    g) The validity of the IP address is also based on the subnet mask used provided.
6. Default subnet masks for standard IP address classes The following table lists the default subnet masks for each available class of TCP/IP networks.

Exercise

In this exercise, you will determine the correct class for a given IP address.

1. Write the address class next to each IP address.

2. Which address class (es) will allow you to have more than 1000 hosts per network?
3. Which address (es) will allow only 254 hosts per network?
4. Identify invalid IP address:

   Circle the portion of the IP address that would be invalid if it were assigned to a host, and then explain why it is invalid.

   a) 131.107.256.80

   b) 222.222.255.222

   c) 231.200.1.1

d) 126.1.0.0

e) 0.127.4.100

f) 190.7.2.0

g) 127.1.1.1

h) 198.121.254.255

i) 255.255.255.255

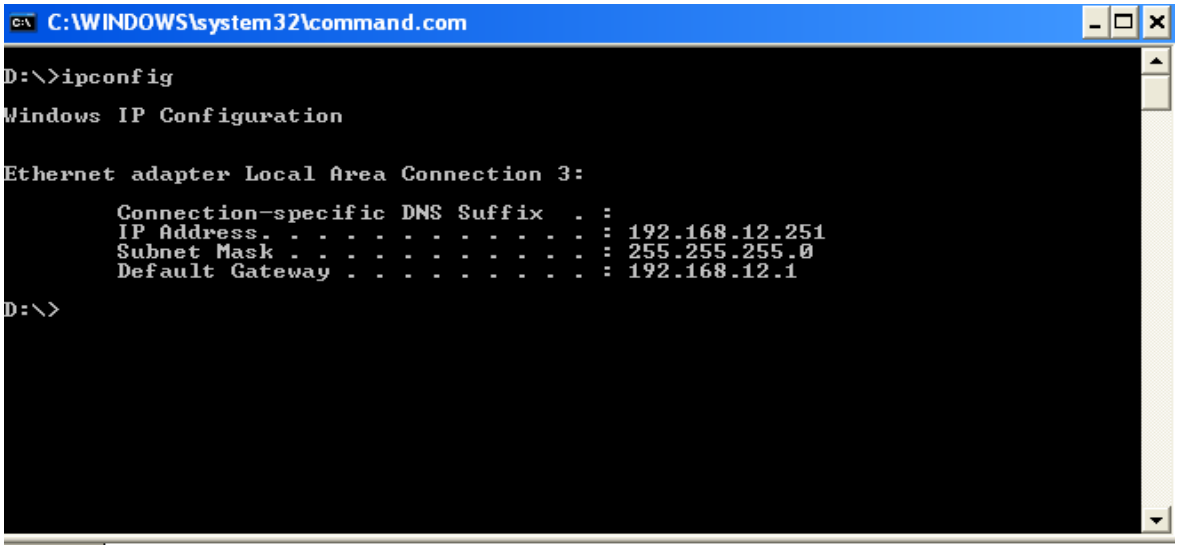
Network Configuration

Step 1. **Connect to the Internet.**

Establish and verify connectivity to the Internet. This step ensures the computer has an IP address.

Step 2. Gather TCP/IP configuration information.

a. Use the Start menu to open the command prompt (Start>Programs>Accessories>Command Prompt or Start>Programs>Command Prompt).
b. Type ipconfig and press Enter key. The spelling of the ipconfig is critical, but the case is not.



c. The screen shows the IP address, subnet mask and the default gateway. The IP address and the default gateway should be in the same network or subnet; otherwise this host wouldn't be able to communicate outside the network.

Step 3. Record the following TCP/IP information for this computer.

a. IP address:_____
b. Subnet mask:_____
c. Default gateway:_____

Step 4. Compare this computer's TCP/IP configuration to that of others on the LAN. If this computer is on a LAN, compare the information of several machines (Hosts).

a. Are there any similarities? _____
b. What is similar about the IP addresses? _____
c. What is similar about the default gateway? _____
d. Record a couple of the IP addresses (of your nearby hosts)

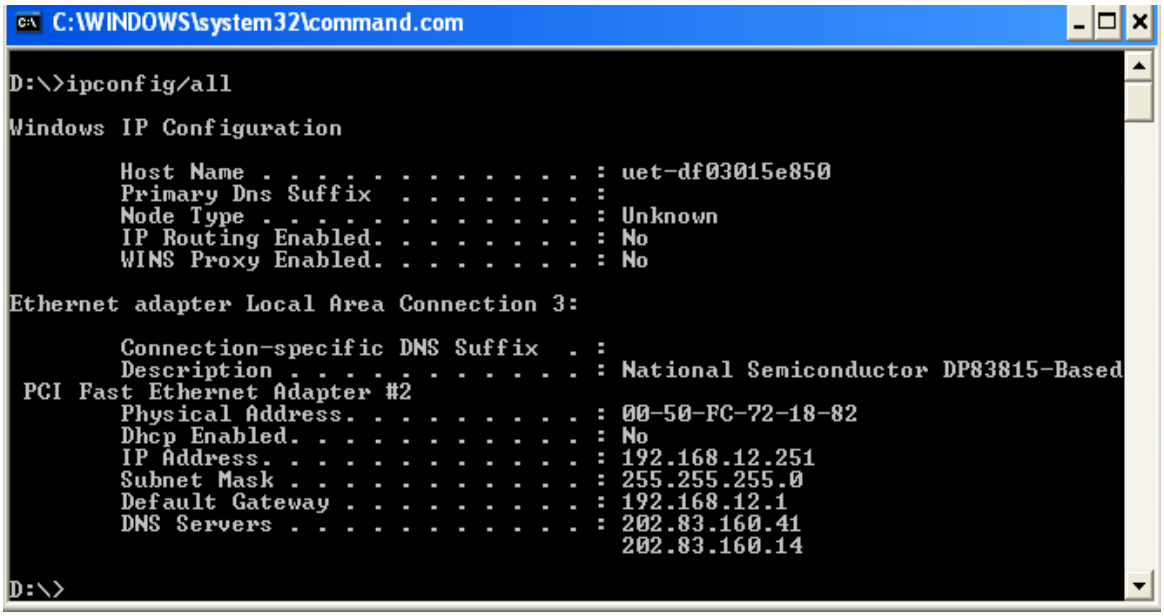
1._____

2._____

3._____

Step 5. Check additional TCP/IP configuration information.

a. To see more information, type ipconfig/all and press Enter key. The figure shows the detailed IP configuration of this computer on the screen.



b. You should see the following information: the host name (computer name), the Physical address of this machine, IP address, subnet Mask, Default Gateway and DNS Servers.

c. In the LAN, compare your result with a few nearby computers. What similarities do you see in the physical (MAC) address?

_____

d. Write down the computer's host name:_____

e. Write down the host names of a couple of other computer:

   a. _____

   b. _____

   c. _____

   d. _____

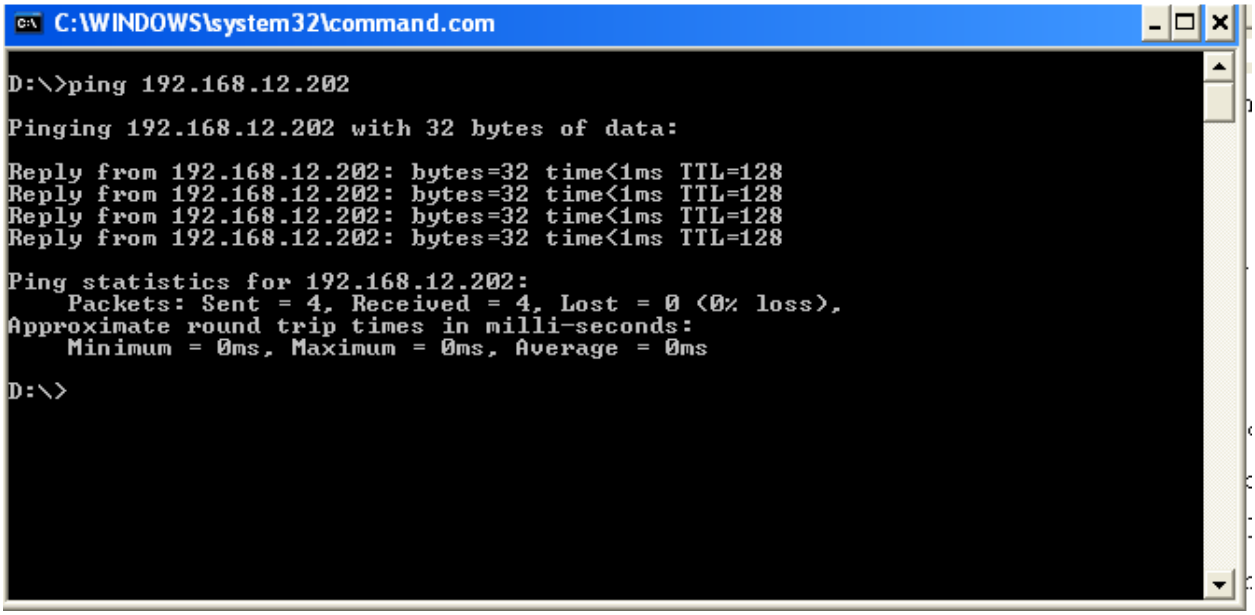
Step 6. Close the screen when finished.

Part B: Using PING TRACERT from a Workstation

Sept 1. Establish and verify connectivity to the Internet. This step ensures that the computer has an IP address.

Step 2. Open the Command prompt(MS-DOS). Ping the IP address of another computer.

a. In the window, type ping, a space, and the IP address of a computer recorded in the previous lab.



Ping uses the Internet Control Message Protocol(ICMP) echo-request and echo-reply feature to test physical connectivity. Because ping reports on four attempts, it gives an indication the reliability of the connection. Look over the result and verify that the ping was successful. Was the ping successful? If not, report to the instructor.

b. Ask the IP address of the nearby computers and ping. Note the result.

_____

c. Ping the IP address of Default gateway and DNS servers. Was the result successful?

_____

d. Ping the computer's loopback IP address. Type the following command:

ping 127.0.0.1

e. The address 127.0.0.1 is reserved for loopback testing. If the ping is successful, then TCP/IP is properly installed and functioning on this computer.

f. Was the ping successful for e._____

g. Ping the hostname of the computer that you recorded in lab 1.1.

h. Ping the Microsoft website(www.microsoft.com)

Step 3. Trace the route to the Umm-alqura university website: type tracert www.uqu.edu.sa and press Enter key.

The result shows the complete route to the site and the number of hops in path.

Trace a local host name or IP address in your local area network (LAN).

Record the output and interpret.

Step 4. Close the window. Also see "pathping ip or host" command. Which only shows path from source to destination.

Lab 2: Cable Construction

In this lab we will learn about

- ✓ Cable Construction and testing
  - Build a Category 5(CAT 5) Straight-Through Ethernet network cable
  - Test the cable for good connection
  - Build a Category 5(CAT 5) Cross-Over Ethernet network cable
  - Test the cable for good connection

Background/Preparation

This lab aim to construct straight through cable, used to connect computer to the Switch/Hub. It is used to connect dissimilar devices. While cross cable is used to connect to computers directly. It is also used when you connect to hubs/Switches with a normal port on both hubs/Switches. (In other words, the cross cable is used relatively in a rare case.). It is used to connect similar devices.

Straight through cable

Equipments/Tools: CAT 5 network cable, RJ-45 Connectors, Crimping tool, Cable tester.

Procedure

The wire has two sides. Let one side is Side A and the other side is Side B. Do the following steps with **Side A** of the wire.

Step 1. Remove the plastic cover from the cable up to two inches. You will see 4 twisted pairs (total 8 wires). In each twisted pair one wire will be colored and the other will be white. For example one will be Green and the other will be White having Green marks. The latter is called Green-White. Similarly there will be Brown wire twisted with Brown-White, Blue wire twister with Blue-White, Orange twisted with Orange-White.

Step 2. Untwist the wires and make them smooth(don't remove the plastic covers from the metal wires).

Step 3. Arrange the wires in the order: Orange-White, Orange, Green-White, Blue, Blue-White, Green, Brown-White, Brown.

Step 4. Cut the wires in straight fashion and insert in the RJ-45 Jack.

Step 5. Using the Crimping tool, punch it properly.

For Side B: Perform Step 1-5 for Side B.

Cross Over cable

Equipments/Tools: CAT 5 network cable, RJ-45 Connectors, Crimping tool, Cable tester.

Procedure

Side A

Repeat Steps 1 to 5 for side A similar to the process for straight through cable.

Side B

Arrange the wires as: green-white, green, orange-white, blue, blue-white, orange, brown-white, brown. And punch it properly.

Configuration table

Pin #	Side A	Side B	Pin #	Side A	Side B
1	orange-white	orange-white	1	orange-white	green-white
2	orange	orange	2	orange	green
3	green-white	green-white	3	green-white	orange-white
4	blue	blue	4	blue	blue
5	blue-white	blue-white	5	blue-white	blue-white
6	green	green	6	green	orange
7	brown-white	brown-white	7	brown-white	brown-white
8	brown	brown	8	brown	brown

For Straight cables *For Cross cables*

Lab 3: Building a Local Area Network

In this lab we will learn about

- ✓ Computer networks configuration
  - Understand difference between Repeater, Hub, Bridge, Switch
  - How Switch works
  - Building Peer to Peer network
  - Building Switch based network
  - Sharing File, Folder, and printer in a network

Theory

Repeater: With many networking terms, the name is indeed the recipe, and that's very true of a repeater. A repeater's job is to repeat an electrical signal, the form that our data has taken to be sent across a cable. Remember, "*it's all ones and zeroes!"*

The repeater takes an incoming signal and then generates a new, clean copy of that exact signal. This prevented maximum cable lengths from stopping transmissions, and also helped to ward off *attenuation - the gradual weakening of an electric signal as it travels*.

Hub: A hub is basically the same as a repeater, but the hub will have more ports. That's the only difference between the two. (Some hubs have greater capabilities than others, but a "basic" hub is simply a multiport repeater.)

Neither hubs nor repeaters have anything to do with the Data Link layer of the OSI model, nor do they perform any switching at all. Hubs and repeaters are strictly Physical layer devices, and that's where the trouble comes in. There are two major problems with hub

1. Only one PC at a time can send data so having one big collision domain. (Data sent by host can collide with another host) to prevent this host on shared network uses CSMA/CD.

2. One large broadcast domain.

Hubs vs. Switches.

1. With hubs, we've got one big collision domain consisting of all connected hosts. When hosts are connected to their own switch ports, they each have their own individual collision domain.

2. Hubs only allow one device to transmit at a time, resulting in shared bandwidth. Switches allow hosts to transmit simultaneously.

3. When one host connected to a hub sends a broadcast, every other host receives that broadcast and there's nothing we can do about it. When a host connected to a switch sends a broadcast, every other host receives it by default - but there *is something* we can do about that, as you'll see in the VLAN section of this course

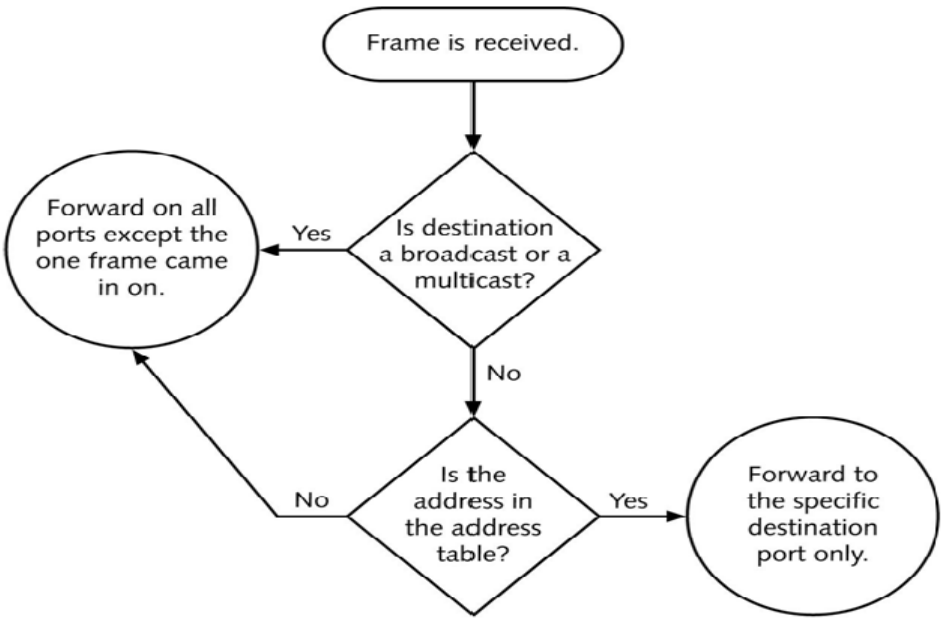
How Switch works: Cisco Switch will do one of the three things with an incoming frame

1. Forward it

2. Flood it

3. Filter it

To make this decision, the switch uses its MAC Address table to check if there's an entry for the destination MAC address - but first, the switch will actually check to see if there's an entry for the source MAC address of the frame, because it's that source MAC that the switch will use to actually build the table in the first place. How switch process frames shown below.



Flooding is performed when the switch has no entry for the frame's destination MAC address. When a frame is flooded, it is sent out every single port on the switch except the one it came in on. Unknown unicast frames are always flooded.

Forwarding is performed when the switch does have an entry for the frame's destination MAC address. Forwarding a frame means the frame is being sent out only one port on the switch.

Filtering is performed when the switch has an entry for both the source and destination MAC address, and the MAC table indicates that both addresses are found off the same port.

Peer to Peer network

In this lab you will learn how to connect two computers directly to each other. This is the simplest network you can imagine. The network having two directly computers connected is called peer to peer network. Later on you will learn that such a simple network is not “according to the definition of network.”

Equipment/Tools

Two computers having Windows XP/2000 and LAN Cards installed, one Cross-Over cable with appropriate length.

Procedure

Step 1.

Identify the proper Ethernet cable and connect the two PC's. Make sure that you are using the crossover cable constructed in the previous lab. Turn off both the computers. Attach one end of the cable in the Network Interface Card (NIC or LAN card) of one computer and the other end in the NIC of the other computer.

Step 2.

Plug in and turn on the computers. To verify the computer connections, ensure that the link lights on both NICs are lit.

Step 3.

Be sure to record the existing IP settings of both the computers, so that you can restore them ate end of the lab. The IP setting information includes IP address, subnet mask, default gateway and the DNS server information.

Step 4.

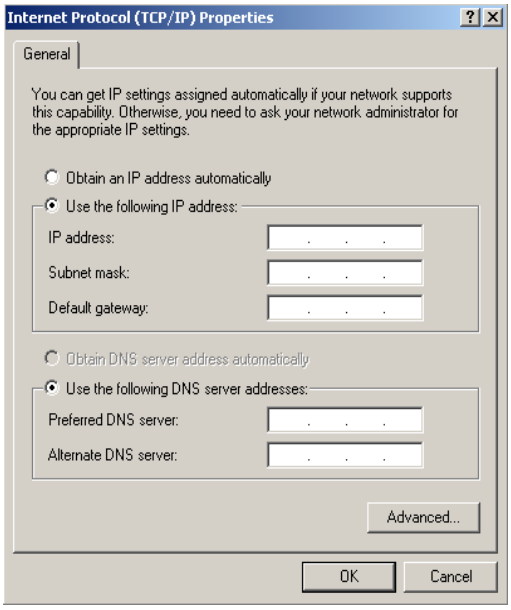
Perform on both computers. Click **Start>Control Panel> Network Connection**. Select the Local Area Network Connection and click **Change Settings of This Connection** on the left side window. You will see a figure showing the properties related to this connection.

Step 5.

Select **Internet Protocol(TCP/IP)** from the list and click the properties button. You will see a figure as shown in the following figure.

Step 6.

Set the IP address information for each of the PC. This information will be provided to you by the instructor.



Step 7.

Verify that the two computers can communicate. Use ping commands.

Step 8.

Restore the actual settings of both the computers you have recorded at the start of the lab.

You can share files, folders, printers and dialup network connection among these two computers.

Building a Switched based network

In this lab you will learn how to connect two or more than two computers in a Local Area Network (LAN) environment. The computers will be connected to one another via a central controller called switch (you can use a hub instead. Ask your instructor for the difference). The topology will be star.

Equipment/Tools

Three or more computers having Windows XP/2000 and LAN Cards installed, Layer 2 Switch, Straight-Through cables equal to the number of computers you want to connect with appropriate length.

Procedure

Identify the proper Ethernet cable and connect the two PC's. Make sure that you are using the crossover cable constructed in the previous lab. Turn off both the computers. Attach one end of the cable in the Network Interface Card (NIC or LAN card) of one computer and the other end in the NIC of the other computer.

Steps

1. Make sure that you have picked straight cables.
2. Power off all the computers and the switch.
3. Connect the computers to the switch.
4. Power On the computers and the switch.
5. Configure each computer with IP address and subnet masks.

On each of the computer apply the following settings:

Computer 1: IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0

Computer 2: IP Address: 192.168.1.2, Subnet Mask: 255.255.255.0

Computer 3: IP Address: 192.168.1.3, Subnet Mask: 255.255.255.0

Leave the other entries blank.

Verify the connections to all the systems using the ping command.

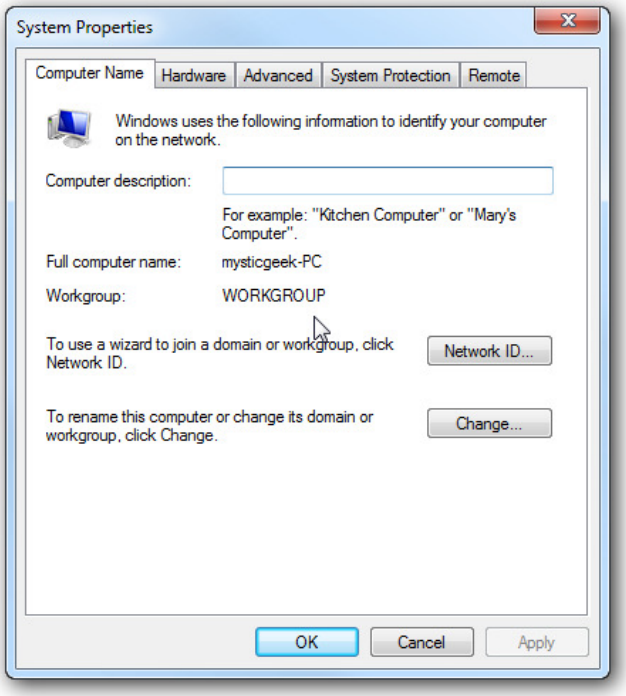
Part A: Share Files and Printers between Windows 7 and XP

If you have a home network and are running Windows 7 and have XP on other PC(s) you might want to share files between them. Today we will look at the steps to share files and hardware devices like a printer.

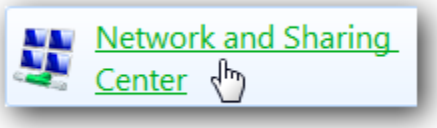
Sharing Files in Windows 7 and XP

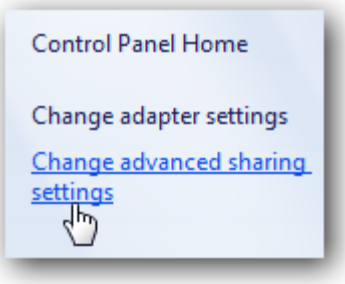
Sharing folders between two Windows 7 machines with the new HomeGroup feature is an easy process, but the HomeGroup feature is not compatible with Vista or XP. For this tutorial we are using Windows 7 x64 RC1 and XP Professional SP3 connected through a basic Linksys home wireless router.

First make sure both machines are members of the same Workgroup which by default is named Workgroup.

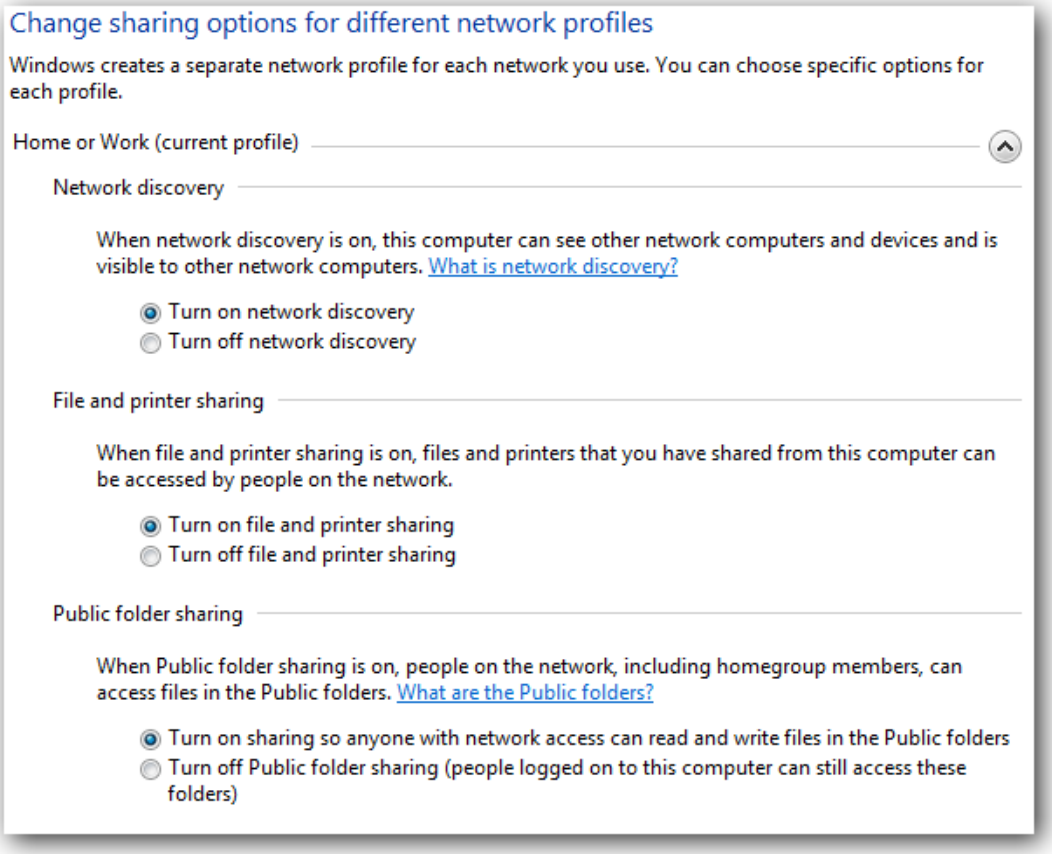


On the Windows 7 machine go into Control Panel \ All Control Panel Items \ Network and Sharing Center then click on Change advanced sharing settings

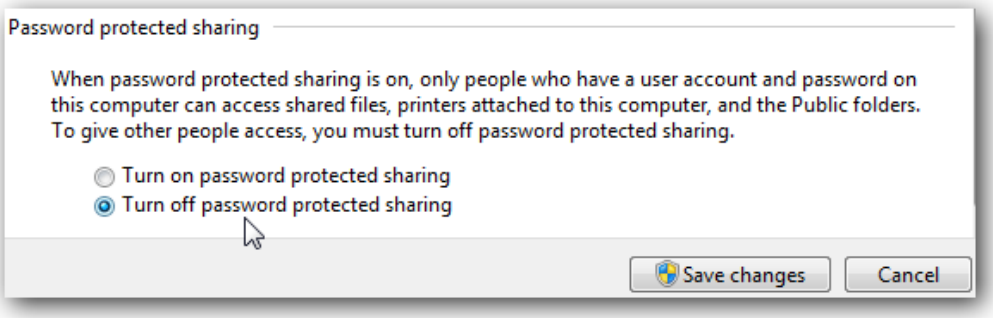




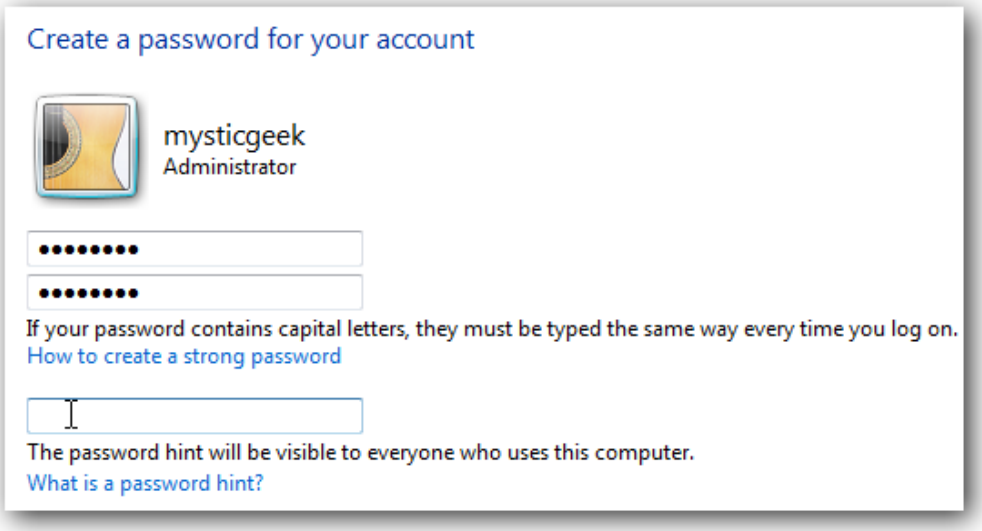
You will want to verify the following settings under Advanced Sharing Settings for the Home or Work and Public profile.



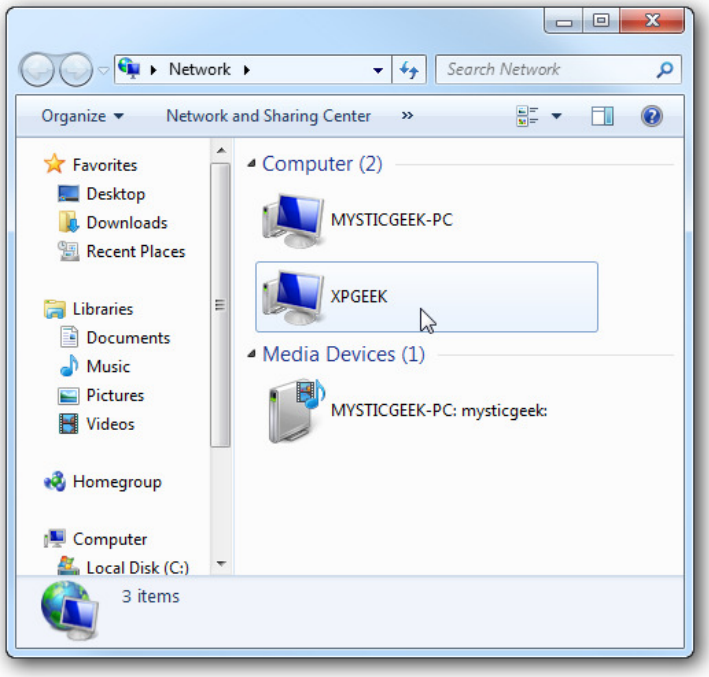
If you want any user to have access the public shares turn off password protection. This is located in Advanced Sharing Settings toward the bottom of the list.



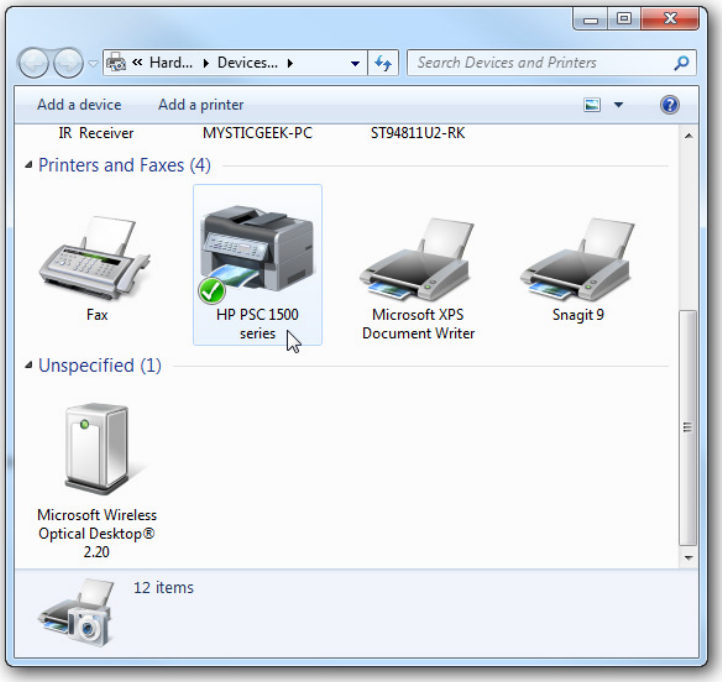
If you want to keep it enabled make sure there is a log in account for the other XP machines and they have a password.



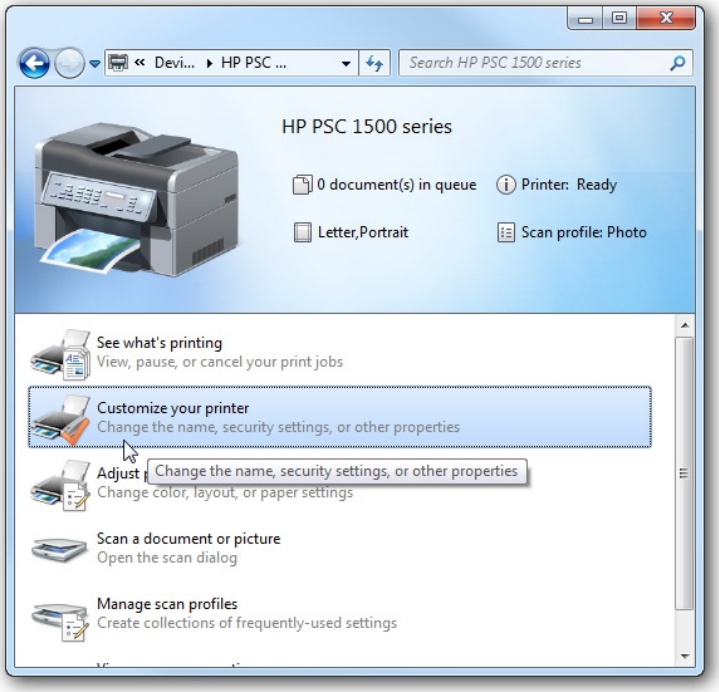
Now if you go into Network in Windows 7 you should see your XP machine and the Windows 7 as well which in this case is Mysticgeek-PC.



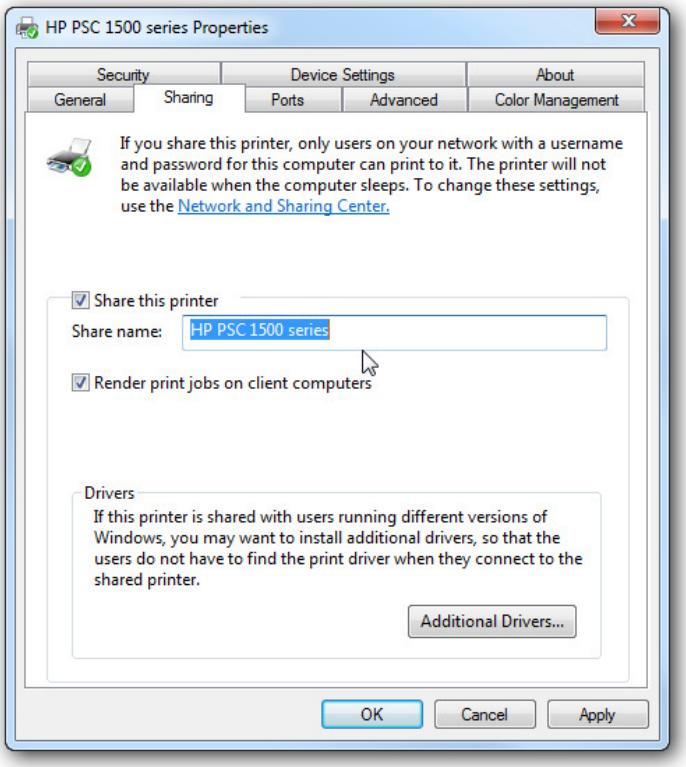
To share the printer on the Windows 7 machine go into Devices and Printers from the Start menu and double click on the printer icon.



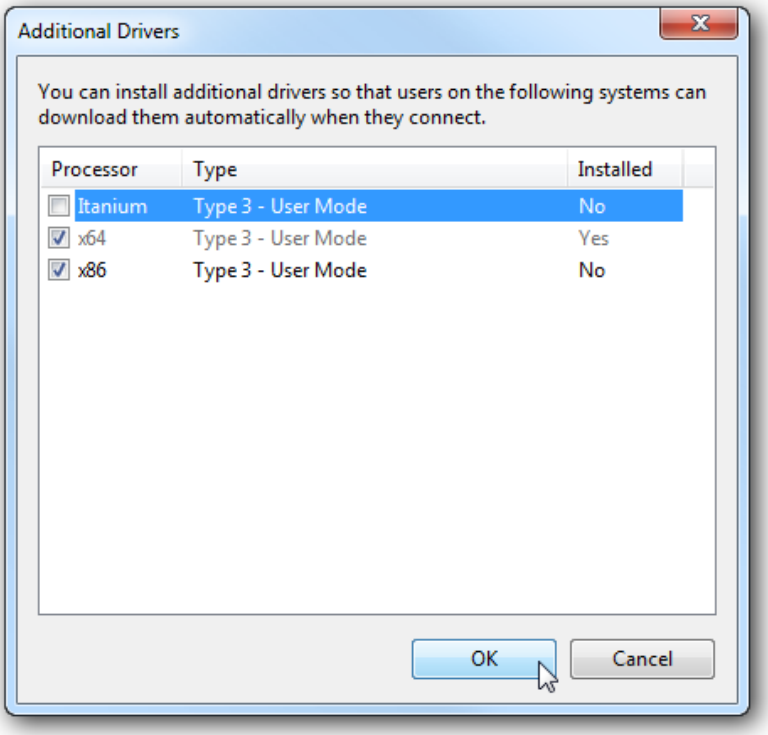
Next double click on *"Customize your printer"*.



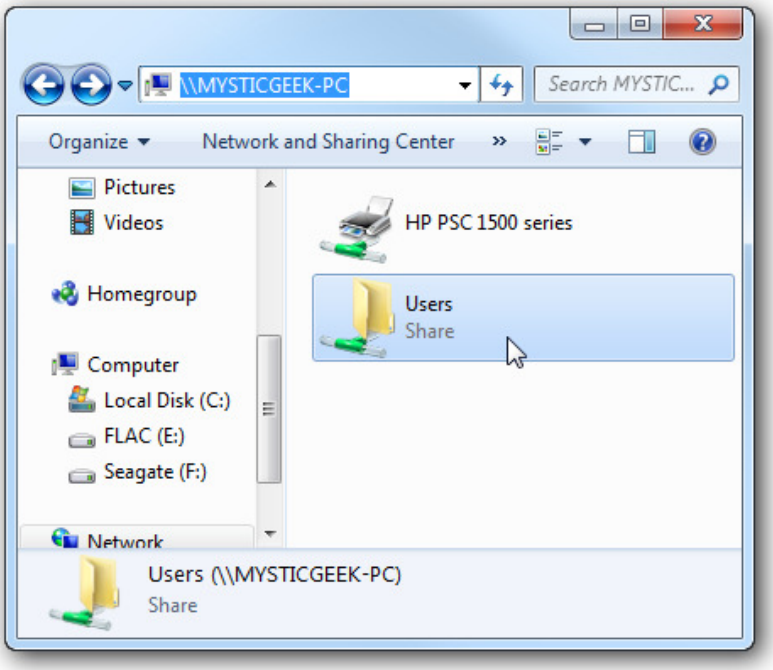
In the Properties screen click on the Sharing Tab and check the box to share the printer and type in its share name.



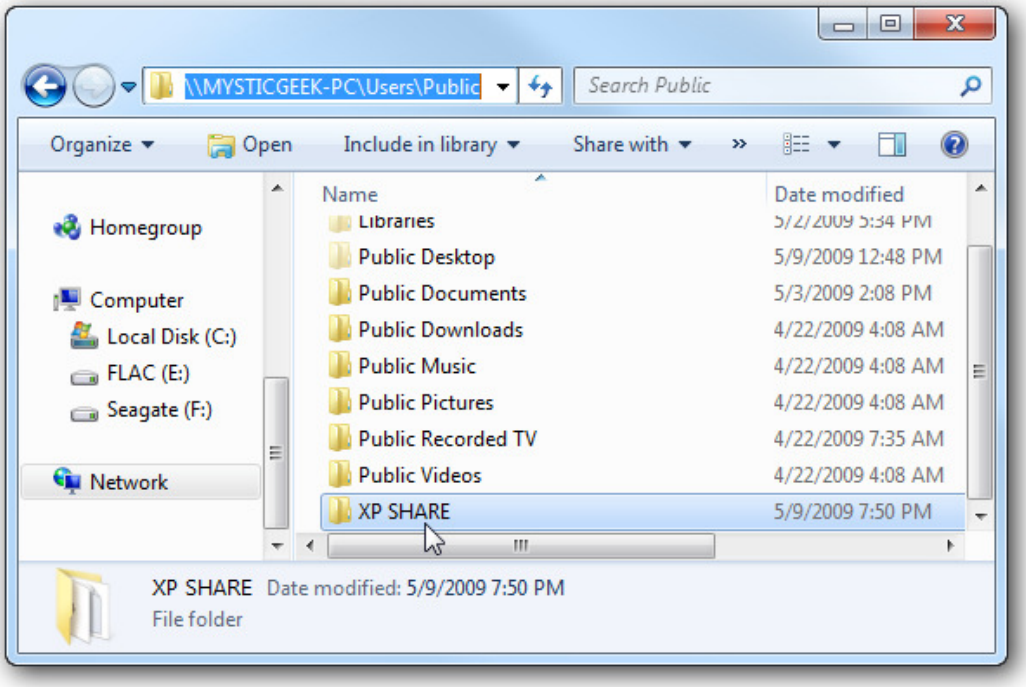
If your XP machine is an x86 OS you can install Additional Drivers before setting up the XP machine.



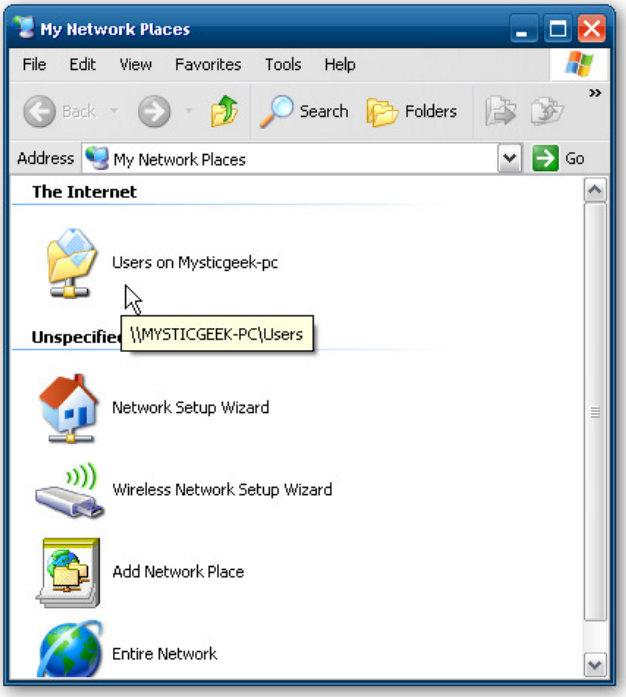
To find the shared folders and devices double click on the Windows 7 machine icon under Network. Here you can see the printer connected to my Windows 7 machine is shared and also the Users Folder.



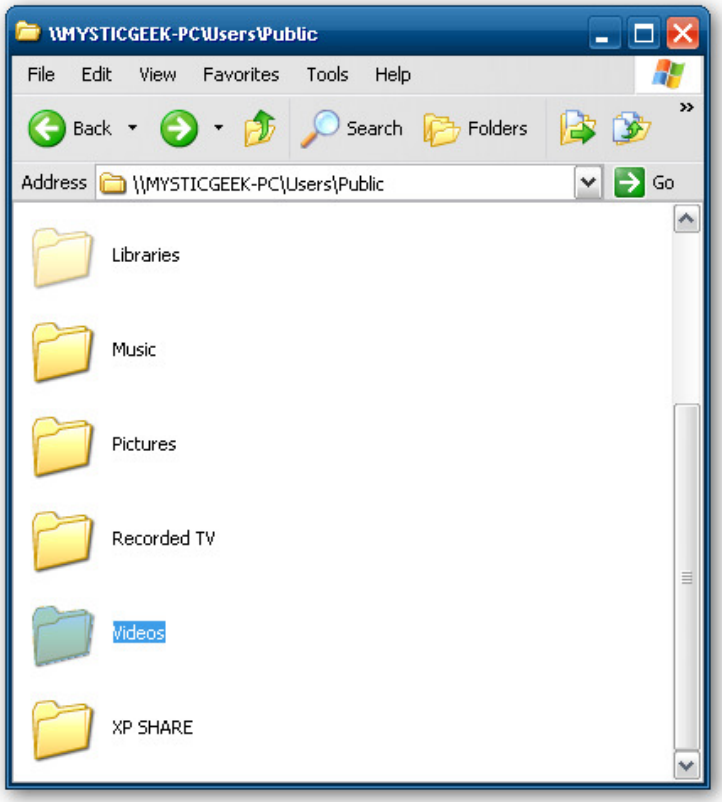
Continue into the Users folder and Public to see the shared folders, here I also created a folder called XP Share just to keep everything in central location.



Over on your XP machine open up My Network Places to find the Windows 7 *(mysticgeek-pc)* shared folder.

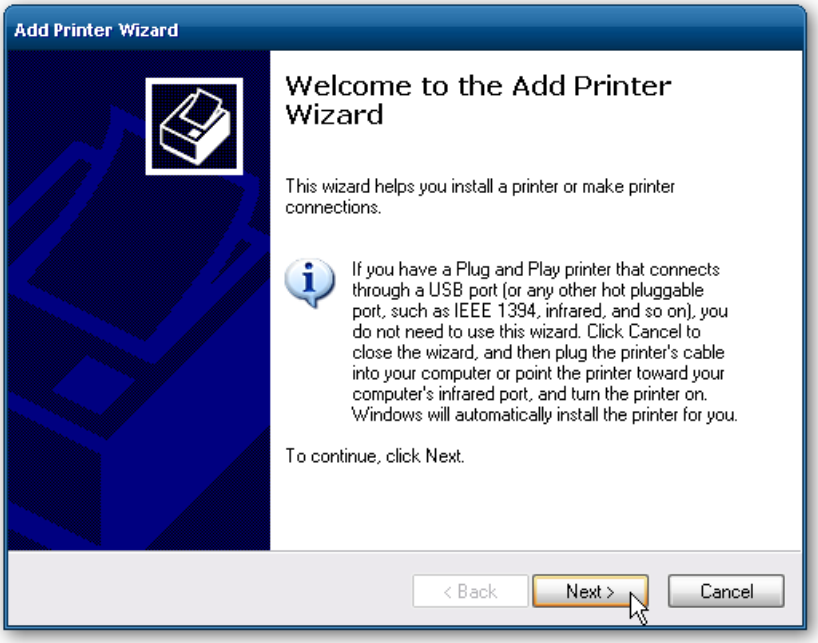


Double click on the Share folder to find a list of shared folders in the Public folder on Windows 7. If you have password protection enabled you will need to type in the username and password of the user account on the Windows 7 machine first.

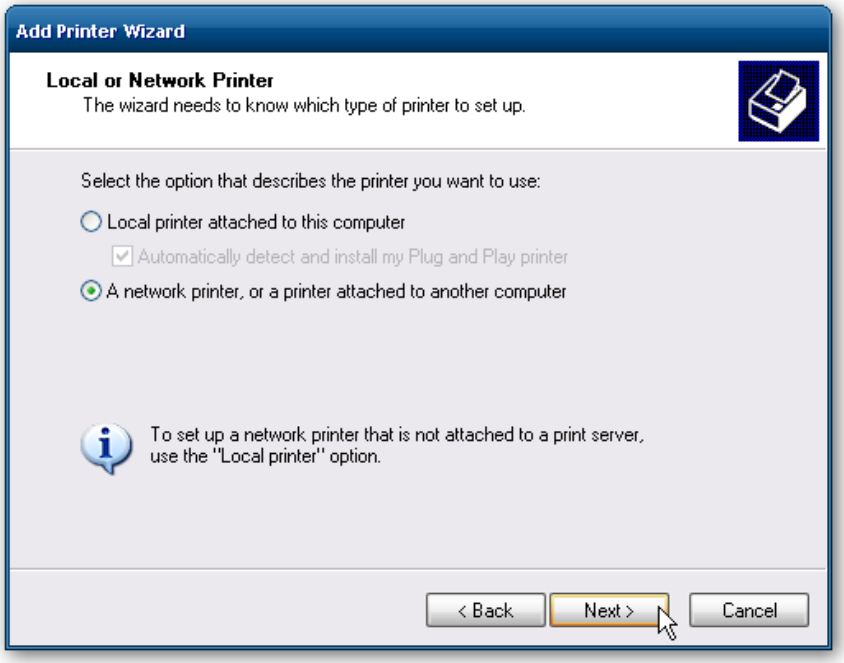


Setup XP With Shared Printer

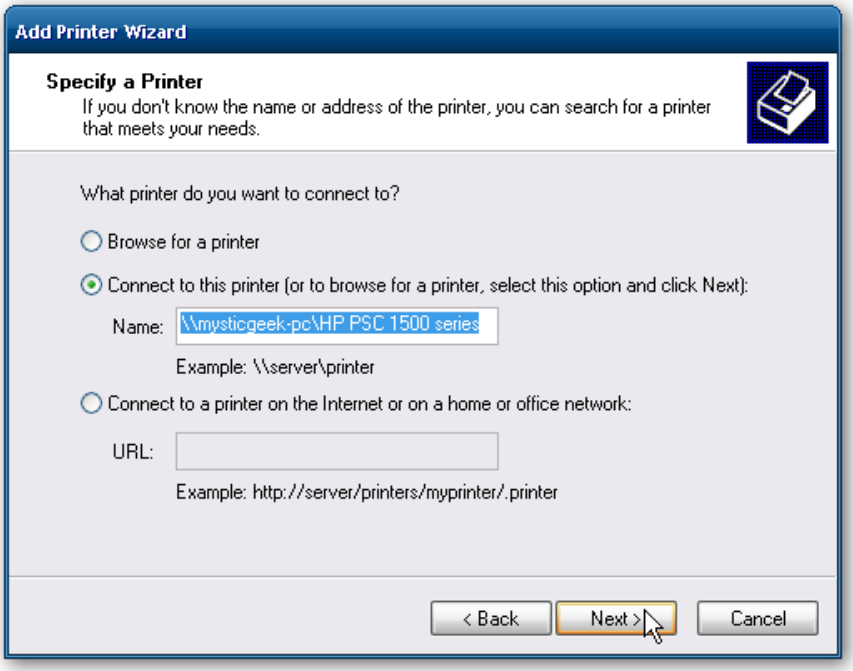
To set up the shared printer in XP you will need to go into Printers and Faxes from the Start menu and kick off the Add Printer Wizard.



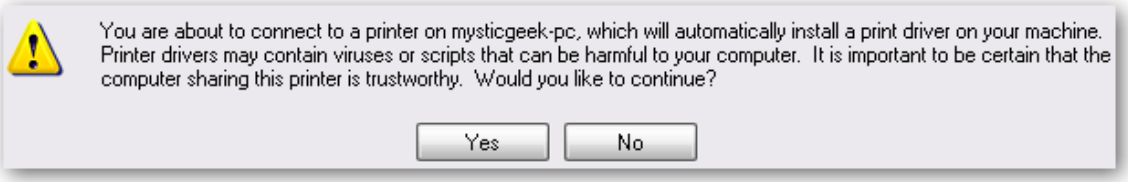
Now select *"A network printer, or a printer attached to another computer"* then hit Next.



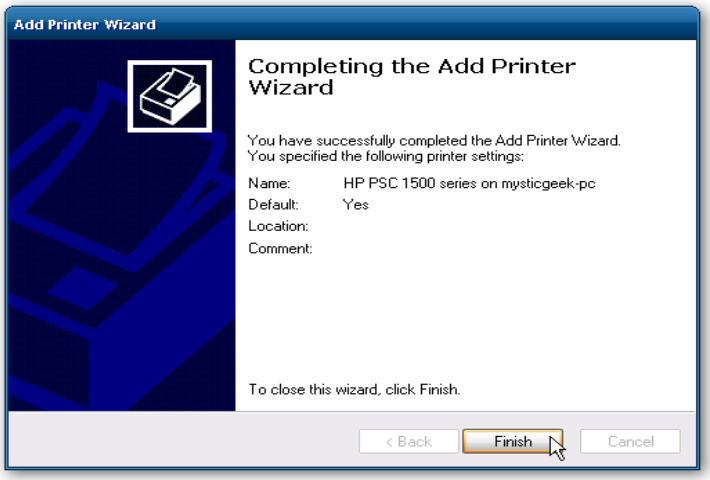
Next select *"Connect to this printer…"* and type in the path for the printer connected to the Windows 7 machine and click next.



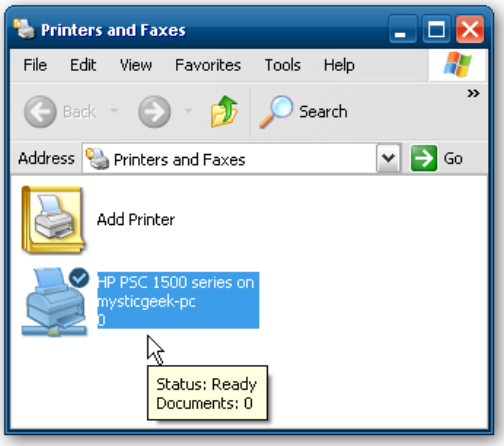
Now click Yes to the confirmation message.



Then click Finish the printer to install and complete the Wizard.



In some cases you will need to install the x86 XP drivers for the shared printer because the Windows 7 drivers are not compatible with XP. When everything is installed open up Printers and Faxes to find the shared printer.



This should help you get started with sharing your files and other devices with your Windows machine. When I first started I was able to see the printer on XP right away because I had a HomeGroup set up, but once I deleted it I needed to share the printer like you would for a workgroup. You might also have to do a couple restarts of the XP machine for it to see the shared resources on Windows 7.

Lab 4: Configuration of CISCO Catalyst Switch 3560

In this lab we will learn about

- ✓ Cisco catalyst switch 3560 configuration
  - Different configuration modes
  - Initial configuration of switch
  - Security for the switch at different level

Cisco uses IOS which stands for Internetwork operating system. IOS is command line interface for configuring switch and router. Following are steps for connecting to switch.

Connecting to Switch

1. Get a Consol Cable

2. Plug the serial end into the back of the computer

3. Put the RJ-45 into the consol port of Switch.

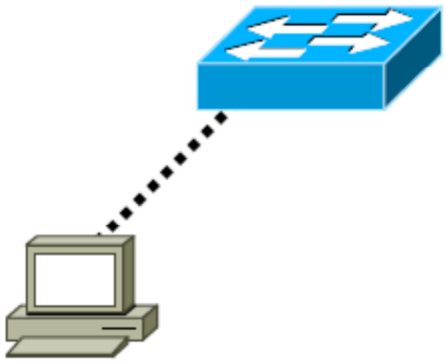
4. Get a terminal program

   - Hyperterminal

   - Tera term

   - Minicom

   - Securecrt



5. Set it to connect via com port with

Baud rate=9600

Data bits=8

Parity=None

Stop bits=1

Flow Control:None

Cisco is famous for its operating system, which uses command line interface for configuration of Switch and router. A lot of help is available to the user just by typing a question mark at the command prompt. Hyper terminal is no longer supported by windows, so we will use Tera term, which is free terminal program for connecting with switch.

Example: Using of help from Cisco IOS on setting a clock on a new switch

Steps: go to privileged configuration mode

Uqu_switch>enable

Type clock at the prompt followed by Question mark as follow

Uqu_switch#clock?

User is given a hint, how to complete a command

Uqu_switch#clock set ?

Uqu_switch#clock set 13:16:30 ?

Finally when <cr> is returned showing that the command is complete.

To see the current configuration file on switch use the following command

Uqu_switch#sh run

Which is a shortcut for Show running-configuration, we can use shortcuts for the Cisco commands only when they are unique.

Setting a hostname

Uqu_switch#configure terminal

Uqu_switch(config)#hostname saqib_switch

saqib_switch(config)#hostname Uqu_switch (for consistency throughout the Laboratory manual)

But switch should be named according to some convention like. 3rdF_R1_S1 meaning that switch is on 3rd floor room 1 having a number 1.

Assigning of IP address to the VLAN interface

By default switch have only one broadcast domain. By using VLAN, switch can be divided into multiple broadcast domains. For configuration purpose switch is assigned an IP address which is used for configuration of switch from remote place.

Assign IP address to the switch (User must be in global configuration mode)

Uqu_switch(config)#interface vlan1

Uqu_switch(config-if)#ip address 192.168.230.2 255.255.255.0

(Changing any setting will effect only the current interface e.g. vlan1)

Uqu_switch(config-if)#ip default-gatway 192.168.230.3

Uqu_switch(config-if)#end

Uqu_switch#show interfaces vlan1

Check the interfaces, if the interface is administratively down. Go again to global configuration mode and issue no shutdown command to make the interface running.

Uqu_switch(config)#

Uqu_switch(config)#interfaces vlan1

Uqu_switch(config-if)#no shutdown

Saving configuration to the start-up configuration

Uqu_switch(config)#copy running-config startup-config

Ctrl+z is command for getting into privileged mode

Uqu_switch#show startup-config

The following command shows the complete information about the version of IOS and other information about device.

Uqu_switch#show version

After initial configuration is done now it is time to lock it down, so need security.

Use of Telnet for remote connection

Go to command prompt and type telnet and then type IP address of the switch.

C:\telnet 192.168.230.2

Notice telnet will not work, because it requires password for it to work. By default it deactivated in Windows 7. Steps for activation are given below.

Go to control panel>programs and features>Turn windows features on or off>Telnet client

First step in security is to secure privileged Execution mode

Uqu_switch>enable

Uqu_switch#configure terminal

Uqu_switch(config)#enable password cisco

Uqu_switch(config)#exit

Uqu_switch#disable

Uqu_switch>

Now try the password set for privileged mode in the previous command

Uqu_switch>enable

Password:

Uqu_switch#show running-config

Notice: Problem with previous password is that, it can be seen in plain text in configuration file. Another password option is to use secret password, which cannot be seen in configuration file.

Using secret password to secure privileged execution mode

Uqu_switch(config)#enable secret cisco

Press Ctrl+Z

Now we have two passwords active on switch, secret password has higher preference over the plain text password. All configurations can be copied to notepad and can be pasted at once in global configuration mode.

Password for Console port

Now securing the console port

Uqu_switch(config)#line console 0

Uqu_switch(config-line)#password cisco

Uqu_switch(config-line)#login

Login command necessary so that user prompted for password.

But still telnet is not possible, for this we have to set virtual terminal lines in configuration file (vty 0-15). There are 15 virtual terminal lines in switch 3560, which can be used for connecting to switch from remote place. These 15 virtual terminal lines can be used simultaneously for connecting to switch. Let's check how many vty lines a switch has

Password for VTY Lines

Uqu_switch(config)#line vty ?

Setting a password for vty lines 0 and 1

Uqu_switch(config)#line vty 0 1

Uqu_switch(config-line)#login

Uqu_switch(config-line)#password cisco

Ctr+Z

Uqu_switch#

Now try the telnet session from DOS prompt.

All of the telnet transaction is being done in plain text which is the main security problem. Now we will check telnet transactions using packet sniffing software WireShark. Following are the steps

1. Open wireshark and select an interface, which is used for capturing the telnet traffic.

2. Start the telnet session. Also start the capturing process.

3. Stop the capturing and use the follow up TCP stream option from Wireshark. One can easily see all the telnet transactions from captured traffic.

Also the virtual terminal lines vty 0 1 password can be seen easily in configuration file. Another command can be used to encrypt the passwords.

Uqu_switch(config)#service password-encryption

Setting the Banner

Banner can be used for different copyright messages at the startup of switch or console. One such message is “Message of the Day (Motd)”.

Uqu_switch#configure terminal

Uqu_switch(config)#banner motd [press enter

Enter the text for the banner

End the banner with same sign [

Lab 5: Configuration of CISCO Router 2900

In this lab we will learn about

- ✓ Cisco Router 2900 configuration
  - Initial Configuration of Router
  - Configure Telnet, Consol password, privileged mode password and VTY lines password, Secure Shell
  - Configure serial interfaces DTE and DCE

Cisco uses IOS which stands for Internetwork operating system. IOS is command line interface for configuring switch and router. Following are steps for connecting to router.

Connecting to Router

1. Get a Consol Cable

2. Plug the serial end into the back of the computer

3. Put the RJ-45 into the consol port of Router.

4. Get a terminal program

   - Hyperterminal

   - Tera term

   - Minicom

   - Securecrt

5. Set it to connect via com port with

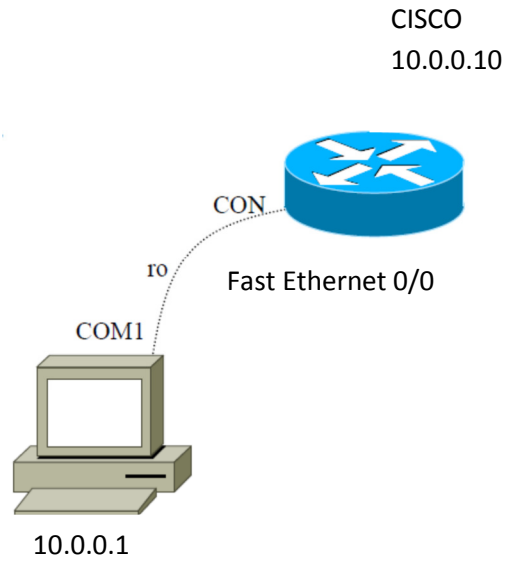
Baud rate=9600

Data bits=8

Parity=None

Stop bits=1

Flow Control:None



Configure IP Address on Fast Ethernet 0/1

Router(config)# hostname CISCO

CISCO(config)# int fastEthernet 0/1

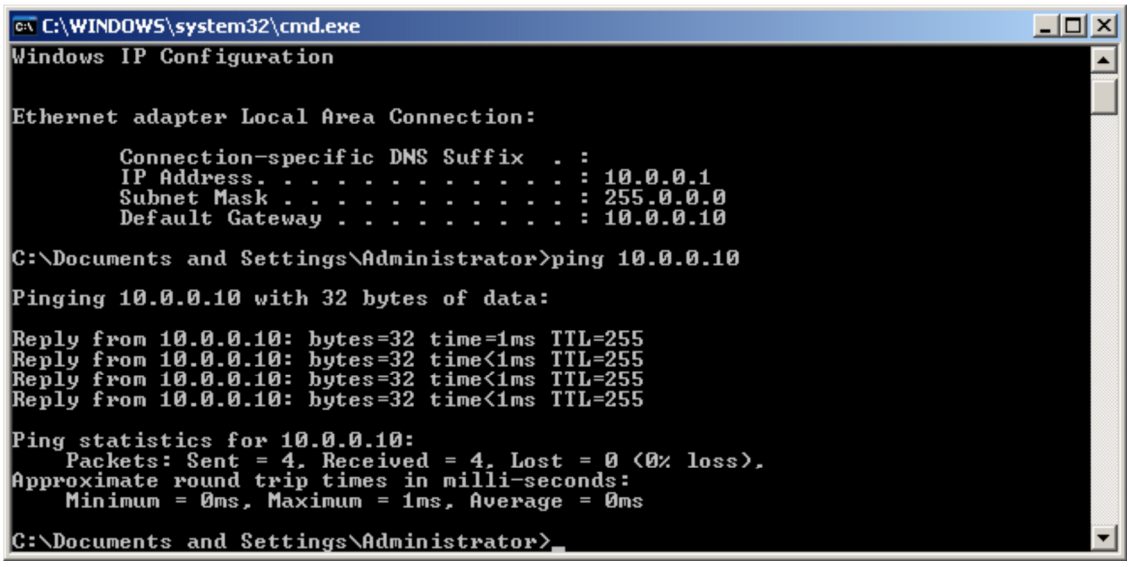
CISCO(config-if)# ip address 10.0.0.10 255.0.0.0

CISCO(config-if)# no shutdown

CISCO# sh ip int brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	10.0.0.10	YES	manual	up	up
Serial0/3/0	unassigned	YES	unset	administratively down	down
Serial0/3/1	unassigned	YES	unset	administratively down	down

!!! Make Sure the Connectivity established b/w 10.0.0.1 and 10.0.0.10 after assign ip.



Configure Telnet & privilege mode password

!!! Clear Text Password

CISCO(config)# enable password cisco

!!! Encrypted Password

CISCO(config)# enable secret cisco123

!!! Line Console Password

CISCO(config)# line console 0

CISCO(config-line)# password cttc

CISCO(config-line)# login

CISCO(config-line)# exit

!!! User Created so Telnet Session are authenticate with user id

CISCO (config)# username saqib password cisco

CISCO(config)# line vty 0 4

CISCO(config-line)# password cisco

CISCO(config-line)# login local

CISCO# sh line

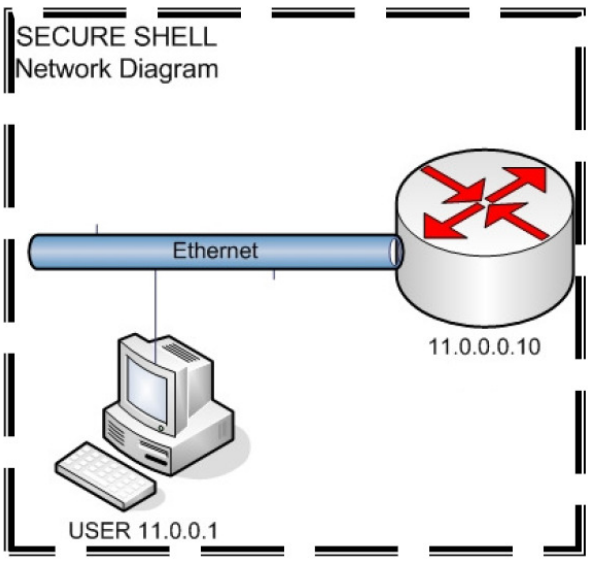
Configure SSH

User IP 11.0.0.1 and Connect to 11.0.0.10 fastEhernet0/1 On

To SSH Connectivity

Ping 11.0.0.1 to 11.0.0.10

!!!!! 100% Succeed



Uqu(config)# interface fastethernet 0/1

Uqu(config-if)# ip address 11.0.0.10 255.0.0.0

Uqu(config-if)# no shutdown

UQU

Uqu(config)# hostname uqu_router

uqu_router(config)# ip domain-name cisco.com

uqu_router(config)# crypto key generate rsa

The name for the keys will be: uqu.uqu.net

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]:

% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

uqu_router(config)# username student password saqib

uqu_router(config)# enable password cisco123

uqu_router(config)# line vty 0 4

uqu_router(config-line)# transport input ssh

uqu_router(config-line)# login local

!!! PC 11.0.0.1

!!! Open Putty.exe

!!! Type the fast Ethernet IP 11.0.0.100

Giving Username & Password

Configure Serial Connectivity between two routers

!!! Assign the IP address on R1

CISCO(config)# hostname R1

R1(config)# interface serial 0

R1(config-if)# ip address 15.0.0.1 255.0.0.0

R1(config-if)# no shutdown

R1(config-if)# clock rate 64000 (Clock Rate will set only DCE

Interface)

R1(config-if)# end

!!! Assign the IP address on R2

CISCO(config)# hostname R2

R2(config)# interface serial 0

R2(config-if)# ip address 15.0.0.2 255.0.0.0

R2(config-if)# no shutdown

R2(config-if)# end

R1# show interfaces serial 0

R1# show ip interface brief

R1# ping 15.0.0.2

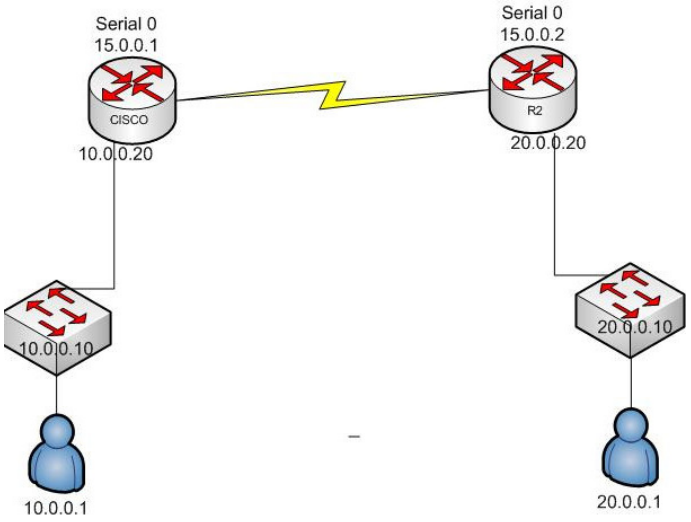
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 15.0.0.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

Configure Static Routes



CISCO(config)# interface serial 0

CISCO(config-if)# ip address 15.0.0.1 255.0.0.0

CISCO(config-if)# no shutdown

CISCO(config-if)# clock rate 64000 (Clock Rate will set only DCE Interface)

CISCO(config-if)# exit

CISCO(config)# interface ethernet 0

CISCO(config-if)# ip address 10.0.0.20 255.0.0.0

CISCO(config-if)# no shutdown

CISCO(config-if)# end

!!! Assign IP on R2

R2(config)# interface serial 0

R2(config-if)# ip address 15.0.0.2 255.0.0.0

R2(config-if)# no shutdown

R2(config-if)# end

R2(config)# interface ethernet 0

R2(config-if)# ip address 20.0.0.2 255.0.0.0

R2(config-if)# no shutdown

R2(config-if)# end

!!! ITS Shows Directly Connected Network

CISCO# sh ip route

C 10.0.0.0/8 is directly connected, Ethernet0

C 15.0.0.0/8 is directly connected, Serial0

R2# sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0

C 15.0.0.0/8 is directly connected, Serial0

!!! Static Route Define on CISCO

!!! 20.0.0.0 is the destination Network

CISCO(config)# ip route 20.0.0.0 255.0.0.0 15.0.0.2

!!! Static Route Define on R2

!!! 10.0.0.0 is the destination Network

R2(config)# ip route 10.0.0.0 255.0.0.0 15.0.0.1

!!! Static Entry now show on Routing Table

CISCO# sh ip route

S 20.0.0.0/8 [1/0] via 15.0.0.2

C 10.0.0.0/8 is directly connected, Ethernet0

C 15.0.0.0/8 is directly connected, Serial0

S means Static

20.0.0.0 mean network to reach

/8 means subnet

1 mean AD

0 Mean next hop

15.0.0.2 mean packet flow from here.

R2# sh ip route

C 20.0.0.0/8 is directly connected, Ethernet0

S 10.0.0.0/8 [1/0] via 15.0.0.1

C 15.0.0.0/8 is directly connected, Serial0

!!! Verfiy the connectivity

C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:

Reply from 20.0.0.1: bytes=32 time=20ms TTL=254

Reply from 20.0.0.1: bytes=32 time=20ms TTL=254

Ping statistics for 20.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 10ms, Maximum = 20ms, Average = 15ms

Lab 6: Design Problem using Router

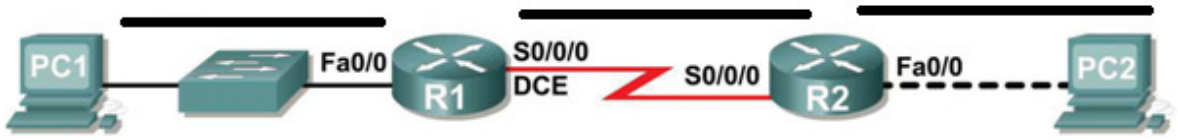
In this lab we will learn about

✓ Cisco Router 2900 configuration

- Different configuration modes
- Subnet an address space given requirements.
- Assign appropriate addresses to interfaces and document.
- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Perform basic configuration tasks on a router.
- Configure and activate Serial and Ethernet interfaces.
- Test and verify configurations.
- Reflect upon and document the network implementation.

Cisco uses IOS which stands for Internetwork operating system. IOS is command line interface for configuring switch and router. Following are steps for connecting to switch.

Topology Diagram



Addressing table

Device	Interface	IP Address	Subnet Mask	Def. Gateway
R1	Fa0/0			N/A
	S0/0/0			N/A
R2	Fa0/0			N/A
	S0/0/0			N/A
PC1	N/A			
PC2	N/A			

In this lab activity, you will design and apply an IP addressing scheme for the topology shown in the Topology Diagram. You will be given one class C address that you must subnet to provide a logical addressing scheme for the network. You must first cable the network as shown before the configuration can begin. Once the network is cabled, configure each device with the appropriate basic configuration commands. The routers will then be ready for interface address configuration according to your IP addressing scheme. When the configuration is complete, use the appropriate IOS commands to verify that the network is working properly.

Note: Use classful subnetting for this lab.

Task 1: Subnet the Address Space

Step 1: Examine the network requirements.

You have been given the 192.168.1.0/24 address space to use in your network design. The network consists of the following segments:

The network connected to router R1 will require enough IP addresses to support 20 hosts.

The network connected to router R2 will require enough IP addresses to support 20 hosts.

The link between router R1 and router R2 will require IP addresses at each end of the link.

(Note: Remember that the interfaces of network devices are also host IP addresses and are included in the above addressing scheme.)

Step 2: Consider the following questions when creating your network design.

How many subnets are needed for this network? _____

What is the subnet mask for this network in dotted decimal format? _____

What is the subnet mask for the network in slash format? _____

How many usable hosts are there per subnet? _____

Step 3: Assign subnetwork addresses to the Topology Diagram.

1. Assign the first subnet (lowest subnet) to the network attached to R1.

2. Assign the second subnet to the link between R1 and R2.

3. Assign the third subnet to the network attached to R2.

Task 2: Determine Interface Addresses

Step 1: Assign appropriate addresses to the device interfaces.

1. Assign the first valid host address in first subnet to the LAN interface on R1.

2. Assign the last valid host address in first subnet to PC1.

3. Assign the first valid host address in second subnet to the WAN interface on R1.

4. Assign the last valid host address in second subnet to the WAN interface on R2.

5. Assign the first valid host address in third subnet to the LAN interface of R2.

6. Assign the last valid host address in third subnet to PC2.

Note: The fourth (highest) subnet is not required in this lab.

Step 2: Document the addresses to be used in the table provided under the Topology Diagram.

Task 3: Prepare the Network

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces as shown in the topology.

Step 2: Clear any existing configurations on the routers.

Task 4: Perform Basic Router Configurations

Perform basic configuration of the R1 and R2 routers according to the following guidelines:

1. Configure the router hostname.

2. Disable DNS lookup.

3. Configure an EXEC mode password.

4. Configure a message-of-the-day banner.

5. Configure a password for console connections.

6. Configure a password for VTY connections.

Task 5: Configure and Activate Serial and Ethernet Addresses

Step 1: Configure the router interfaces.

Configure the interfaces on the R1 and R2 routers with the IP addresses from your network design. When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 2: Configure the PC interfaces.

Configure the Ethernet interfaces of PC1 and PC2 with the IP addresses and default gateways from your network design.

Task 6: Verify the Configurations

Answer the following questions to verify that the network is operating as expected.

From the host attached to R1, is it possible to ping the default gateway? _____

From the host attached to R2, is it possible to ping the default gateway? _____

From the router R1, is it possible to ping the Serial 0/0/0 interface of R2? _____

From the router R2, is it possible to ping the Serial 0/0/0 interface of R1? _____

The answer to the above questions should be yes. If any of the above pings failed, check your physical connections and configurations. If necessary, refer to Lab 1.5.2, “Basic Router Configuration.”

What is the status of the FastEthernet 0/0 interface of R1? _____

What is the status of the Serial 0/0/0 interface of R1? _____

What is the status of the FastEthernet 0/0 interface of R2? _____

What is the status of the Serial 0/0/0 interface of R2? _____

What routes are present in the routing table of R1?

_____

_____

What routes are present in the routing table of R2?

_____

_____

Task 7: Reflection

Are there any devices on the network that cannot ping each other?

_____

_____

What is missing from the network that is preventing communication between these devices?

_____

_____

Task 8: Document the Router Configurations

On each router, capture the following command output to a text (.txt) file and save for future reference.

Running configuration

Routing table

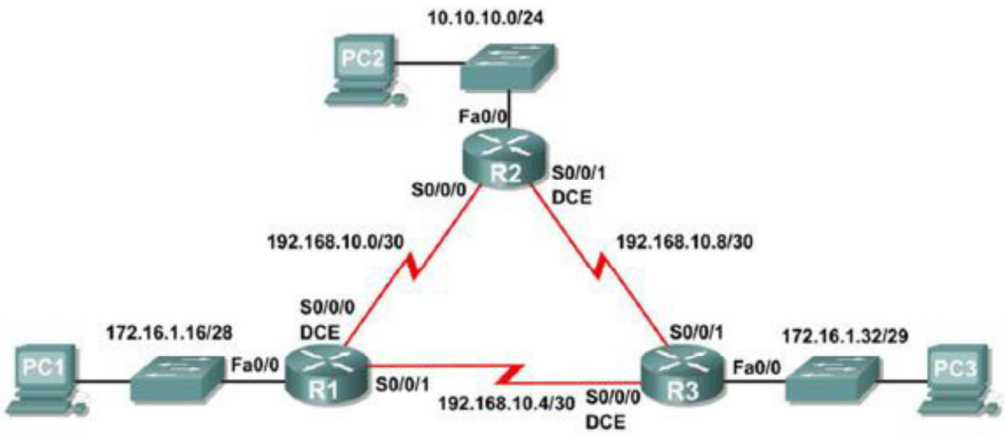
Summary of status information for each interface

Lab 7: Basic OSPF Configuration

In this lab we will learn about

✓ Basic OSPF Configuration on Cisco Router 2900

- Perform basic configuration tasks on a router.
- Configure and activate interfaces.
- Configure OSPF routing on all routers.
- Configure OSPF router IDs.
- Verify OSPF routing using show commands.
- Configure a static default route.
- Propagate default route to OSPF neighbors.
- Configure OSPF Hello and Dead Timers.
- Configure OSPF on a Multiaccess network.
- Configure OSPF priority.
- Understand the OSPF election process.
- Document the OSPF configuration.



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.17	255.255.255.240	N/A
	S0/0/0	192.168.10.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	10.10.10.1	255.255.255.0	N/A
	S0/0/0	192.168.10.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	Fa0/0	172.16.1.33	255.255.255.248	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC0	NIC	172.16.1.20	255.255.255.240	172.16.1.17
PC1	NIC	10.10.10.10	255.255.255.0	10.10.10.1
PC2	NIC	172.16.1.35	255.255.255.248	172.16.1.33

Task 1: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

Step 2: Clear any existing configurations on the routers.

Task 2: Basic Router Configurations

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

- Configure the router hostname
- Disable DNS lookup
- Configure the EXEC mode password as class

- Configure a password for console connections as cisco (case sensitive)
- Configure a password for VTY connections as cisco (case sensitive)

Task 3: Configure and Activate Serial and Ethernet Addresses

Step 1 Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the table.

Step 2 Configure the PCs with the IP addresses from the table.

Task 4: Configure OSPF on the R1 Router

Step 1 Configure OSPF with a process ID number of 1, advertise all networks.

Task 5: Configure OSPF on the R2 and R3 Routers

Step 1 Configure OSPF with a process ID number of 1, advertise all networks.

Task 6: Configure OSPF Router IDs

Step 1 Configure R1 with a Loopback0 interface of **10.1.1.1 255.255.255.255**.

Step 2 Configure R2 with a Loopback0 interface of **10.2.2.2 255.255.255.255**.

Step 3 Configure R3 with a Loopback0 interface of **10.3.3.3 255.255.255.255**.

Step 4 Copy all running-configs to the NVRAM and reload routers.

Task 7: Verify OSPF Operation

Step 1 Use the **show ip ospf neighbor** command to verify information about other routers was learned.

Step 2 Use the **show ip protocols** command to view information about the routing protocol.

Task 8: Examine OSPF Routes in the Routing Tables

Step 1 Use the **show ip route** command to view all learned networks via OSPF.

Task 9: Configure OSPF Cost

Step 1 Configure R1 serial interfaces with a bandwidth of 64.

Step 2 Configure R2 serial interfaces with a bandwidth of 64.

Step 3 Configure R3 serial interfaces with a cost of 1562.

Task 10: Redistribute an OSPF Default Route

Step 1 Configure a loopback address on the R1 router to simulate a link to an ISP.

Step 2 Create the loopback 1 **172.30.1.1 255.255.255.252** on the R1 router.

Step 3 Create a Default route directing traffic to the loopback interface.

Step 4 Redistribute the default route using OSPF.

Task 11: Verifying OSPF

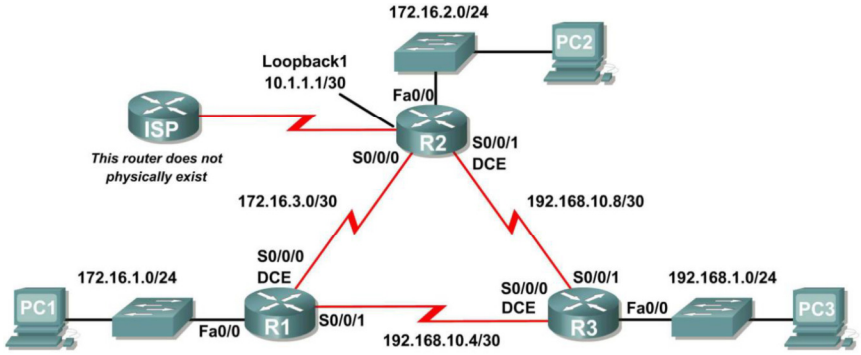
Step 1 Using the **show ip route** command verify that the default route was learned.

Lab 8: Basic EIGRP Configuration

In this lab we will learn about

✓ Basic EIGRP Configuration on Cisco Router 2900

- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Perform basic configuration tasks on a router.
- Configure and activate interfaces.
- Configure EIGRP routing on all routers.
- Verify EIGRP routing using show commands.
- Disable automatic summarization.
- Configure manual summarization.
- Document the EIGRP configuration.



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/0**	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	**Fa0/0**	172.16.2.1	255.255.255.0	N/A

	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
	Lo0	10.1.1.1	255.255.255.252	N/A
R3	**Fa0/0**	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	**NIC**	172.16.1.10	255.255.255.0	172.16.1.1
PC2	**NIC**	172.16.2.10	255.255.255.0	172.16.2.1
PC3	**NIC**	192.168.1.10	255.255.255.0	192.168.1.1

In this lab activity, you will learn how to configure the routing protocol EIGRP using the network shown in the Topology Diagram. A loopback address will be used on the R2 router to simulate a connection to an ISP, where all traffic that is not destined for the local network will be sent. Some segments of the network have been subnetted using VLSM. EIGRP is a classless routing protocol that can be used to provide subnet mask information in the routing updates. This will allow VLSM subnet information to be propagated throughout the network.

Task 1: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.
This activity begins with an initial network in the logical workspace.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations.

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections.

Task 3: Configure and Activate Serial and Ethernet Addresses.

Step 1: Configure the interfaces on the R1, R2, and R3 routers.
Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the Topology Diagram.

Step 2: Verify IP addressing and interfaces.
Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active. When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 3: Configure Ethernet interfaces of PC1, PC2, and PC3.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from the table under the Topology Diagram.

Task 4: Configure EIGRP on the R1 Router.

Step 1: Enable EIGRP.
Use the **`router eigrp`** command in global configuration mode to enable EIGRP on the R1 router. Enter 1 for the autonomous-system parameter.

```
R1(config)#router eigrp 1
```

Step 2: Configure classful network 172.16.0.0.
Once you are in the Router EIGRP configuration sub-mode, configure the classful network 172.16.0.0 to be included in the EIGRP updates that are sent out of R1.

```
R1(config-router)#network 172.16.0.0
```

The router will begin to send EIGRP update messages out each interface belonging to the 172.16.0.0 network. EIGRP updates will be sent out of the FastEthernet0/0 and Serial0/0/0 interfaces because they are both on subnets of the 172.16.0.0 network.

Step 3: Configure the router to advertise the 192.168.10.4/30 network attached to the Serial0/0/1 interface.
Use the wildcard-mask option with the network command to advertise only the subnet and not the entire 192.168.10.0 classful network.

Note: Think of a wildcard mask as the inverse of a subnet mask. The inverse of the subnet mask 255.255.255.252 is 0.0.0.3. To calculate the inverse of the subnet mask, subtract the subnet mask from 255.255.255.255:

  255.255.255.255
– 255.255.255.252 Subtract the subnet mask

---
0 . 0 . 0 . 3 Wildcard mask

```
R1(config-router)# network 192.168.10.4 0.0.0.3
```

When you are finished with the EIGRP configuration for R1, return to privileged EXEC mode and save the current configuration to NVRAM.

Task 5: Configure EIGRP on the R2 and R3 Routers.

Step 1: Enable EIGRP routing on the R2 router using the router eigrp command.
Use an autonomous system number of 1.

```
R2(config)#router eigrp 1
```

Step 2: Use the classful address 172.16.0.0 to include the network for the FastEthernet0/0 interface.

```
R2(config-router)#network 172.16.0.0
```

Notice that DUAL sends a notification message to the console stating that a neighbor relationship with another EIGRP router has been established.

What is the IP address of the EIGRP neighbor router?

_____

What interface on the R2 router is the neighbor adjacent to?

_____

Step 3: Configure the R2 router to advertise the 192.168.10.8/30 network attached to the Serial0/0/1 interface.

1. Use the wildcard-mask option with the network command to advertise only the subnet and not the entire 192.168.10.0 classful network.

2. When you are finished, return to privileged EXEC mode.

```
R2(config-router)#network 192.168.10.8 0.0.0.3
R2(config-router)#end
```

Step 4: Configure EIGRP on the R3 router using the router eigrp and network commands.

1. Use an autonomous system number of 1.

2. Use the classful network address for the network attached to the FastEthernet0/0 interface.

3. Include the wildcard masks for the subnets attached to the Serial0/0/0 and Serial 0/0/1 interfaces.

4. When you are finished, return to privileged EXEC mode.

```
R3(config)#router eigrp 1
R3(config-router)#network 192.168.1.0
R3(config-router)#network 192.168.10.4 0.0.0.3
R3(config-router)#network 192.168.10.8 0.0.0.3
R3(config-router)#
```

Notice that when the networks for the serial links from R3 to R1 and R3 to R2 are added to the EIGRP configuration, DUAL sends a notification message to the console stating that a neighbor relationship with another EIGRP router has been established.

Task 6: Verify EIGRP Operation.

Step 1: View neighbors.

On the R1 router, use the **show ip eigrp neighbors** command to view the neighbor table and verify that EIGRP has established an adjacency with the R2 and R3 routers. You should be able to see the IP address of each adjacent router and the interface that R1 uses to reach that EIGRP neighbor.

```
R1#show ip eigrp neighbors
```

Step 2: View routing protocol information.

On the R1 router, use the **show ip protocols** command to view information about the routing protocol operation. Notice that the information that was configured in Task 5, such as protocol, autonomous system number, and networks, is shown in the output. The IP addresses of the adjacent neighbors are also shown.

```
R1#show ip protocols
```

Notice that the output specifies the autonomous system number used by EIGRP. Remember, the autonomous system number must be the same on all routers for EIGRP to establish neighbor adjacencies and share routing information.

Task7: Examine EIGRP Routes in the Routing Tables.

Step1: View the routing table on the R1 router.

EIGRP routes are denoted in the routing table with a D, which stands for DUAL (Diffusing Update Algorithm), which is the routing algorithm used by EIGRP.

```
R1#show ip route
```

Notice that the 172.16.0.0/16 parent network is variably subnetted with three child routes using

either a /24 or /30 mask. Also notice that EIGRP has automatically included a summary route to Null0 for the 172.16.0.0/16 network. The 172.16.0.0/16 route does not actually represent a path to reach the parent network, 172.16.0.0/16. If a packet destined for 172.16.0.0/16 does not match one of the level 2 child routes, it is sent to the Null0 interface.

The 192.168.10.0/24 Network is also variably subnetted and includes a Null0 route.

Step 2: View the routing table on the R3 router.
The routing table for R3 shows that both R1 and R2 are automatically summarizing the 172.16.0.0/16 network and sending it as a single routing update. Because of automatic summarization, R1 and R2 are not propagating the individual subnets. Because R3 is getting two equal cost routes for 172.16.0.0/16 from both R1 and R2, both routes are included in the routing table.

Task 8: Configure EIGRP Metrics.

Step 1: View the EIGRP metric information.
Use the **`show ip interface`** `command` to view the EIGRP metric information for the Serial0/0/0 interface on the R1 router. Notice the values that are shown for the bandwidth, delay, reliability, and load.

```
R1#show interface serial0/0/0
```

Step 2: Modify the bandwidth of the Serial interfaces.
On most serial links, the bandwidth metric will default to 1544 Kbits. If this is not the actual bandwidth of the serial link, the bandwidth will need to be changed so that the EIGRP metric can be calculated correctly.

For this lab, the link between R1 and R2 will be configured with a bandwidth of 64 kbps, and the link between R2 and R3 will be configured with a bandwidth of 1024 kbps. Use the bandwidth command to modify the bandwidth of the Serial interfaces of each router.

R1 router:
```
R1(config)#interface serial0/0/0
R1(config-if)#bandwidth 64
```

R2 router:
```
R2(config)#interface serial0/0/0
R2(config-if)#bandwidth 64
R2(config)#interface serial0/0/1
R2(config-if)#bandwidth 1024
```

R3 router:
```
R3(config)#interface serial0/0/1
R3(config-if)#bandwidth 1024
```

Note: The bandwidth command only modifies the bandwidth metric used by routing protocols, not the physical bandwidth of the link.

Step 3: Verify the bandwidth modifications.
Use the **`show ip interface`** command to verify that the bandwidth value of each link has been changed.

Note: Use the interface configuration command **`no bandwidth`** to return the bandwidth to its default value.

Task 9: Examine Successors and Feasible Distances.

Step 1: Examine the successors and feasible distances in the routing table on R2.
`R2#show ip route`

Step 2: Answer the following questions:
What is the best path to PC1?

_____
_____

A successor is a neighboring router that is currently being used for packet forwarding. A successor is the least-cost route to the destination network. The IP address of a successor is shown in a routing table entry right after the word “via”.

What is the IP address and name of the successor router in this route?

_____

Feasible distance (FD) is the lowest calculated metric to reach that destination. FD is the metric listed in the routing table entry as the second number inside the brackets.

What is the feasible distance to the network that PC1 is on?

_____

Task 10: Determine if R1 is a Feasible Successor

for the Route from R2 to the 192.168.1.0 Network.

A feasible successor is a neighbor who has a viable backup path to the same network as the successor. In order to be a feasible successor, R1 must satisfy the feasibility condition. The feasibility condition (FC) is met when a neighbor’s reported distance (RD) to a network is less than the local router’s feasible distance to the same destination network.

Step 1: Examine the routing table on R1.
What is the reported distance to the 192.168.1.0 network?

_____

Step 2: Examine the routing table on R2.
What is the feasible distance to the 192.168.1.0 network?

_____

Would R2 consider R1 to be a feasible successor to the 192.168.1.0 network? _____

Task 11: Examine the EIGRP Topology Table.

Step 1: View the EIGRP topology table.
Use the **`show ip eigrp topology`** command to view the EIGRP topology table on R2.

Step 2: View detailed EIGRP topology information.

Use the [network] parameter of the **`show ip eigrp topology`** command to view detailed EIGRP topology information for the 192.16.0.0 network.

```
R2#show ip eigrp topology 192.168.1.0
```

How many successors are there for this network?

_____

What is the feasible distance to this network?

_____

What is the IP address of the feasible successor?

_____

What is the reported distance for 192.168.1.0 from the feasible successor?

_____

What would be the feasible distance to 192.168.1.0 if R1 became the successor?

_____

Task 12: Disable EIGRP Automatic Summarization.

Step 1: Examine the routing table of the R3 router.
Notice that R3 is not receiving individual routes for the 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24 subnets. Instead, the routing table only has a summary route to the classful

network address of 172.16.0.0/16 through the R1 router. This will cause packets that are destined for the 172.16.2.0/24 network to be sent through the R1 router instead of being sent straight to the R2 router.

Why is the R1 router (192.168.10.5) the only successor for the route to the 172.16.0.0/16 network?

_____
_____
_____
_____

Notice that the reported distance from R2 is higher than the feasible distance from R1.

```
R3#show ip eigrp topology
```

Step 3: Disable automatic summarization on all three routers with the `no auto-summary` command.

```
R1(config)#router eigrp 1
R1(config-router)#no auto-summary

R2(config)#router eigrp 1
R2(config-router)#no auto-summary

R3(config)#router eigrp 1
R3(config-router)#no auto-summary
```

Step 4: View the routing table on R1 again.

Notice that individual routes for the 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24 subnets are now present and the summary Null route is no longer listed.

Task 13: Configure Manual Summarization.

Step 1: Add loopback addresses to R3 router.

Add two loopback addresses, 192.168.2.1/24 and 192.168.3.1/24, to the R3 router. These virtual interfaces will be used to represent networks to be manually summarized along with the 192.168.1.0/24 LAN.

```
R3(config)#interface loopback1
R3(config-if)#ip address 192.168.2.1 255.255.255.0
R3(config-if)#interface loopback2
R3(config-if)#ip address 192.168.3.1 255.255.255.0
```

Step 2: Add the 192.168.2.0 and 192.168.3.0 networks to the EIGRP configuration on R3.

```
R3(config)#router eigrp 1
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
```

Step 3: Verify new routes.

View the routing table on the R1 router to verify that the new routes are being sent out in the EIGRP updates sent by R3.

Step 4: Apply manual summarization to outbound interfaces.

The routes to the 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24 networks can be summarized in the single network 192.168.0.0/22. Use the ip summary-address eigrp as-number network-address subnet-mask command to configure manual summarization on each of the outbound interfaces connected to EIGRP neighbors.

```
R3(config)#interface serial0/0/0
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
R3(config-if)#interface serial0/0/1
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
R3(config-if)#
```

Step 5: Verify the summary route.

View the routing table on the R1 router to verify that the summary route is being sent out in the EIGRP updates sent by R3.

Lab 9: Introduction to Wireshark

In this lab we will learn about

- ✓ Introduction to Wireshark and network traffic analysis
  - Introduction to Wireshark
  - Installation of Wireshark and basic usage
  - Network traffic analysis of HTTP, FTP protocol

What is wireshark

Wireshark is a network protocol analyzer, also known as a network sniffer. Formerly known as Ethereal, wireshark is computer application that captures and decodes packets of information from a network. "Wireshark can capture live network traffic or read data from a file and translate the data to be presented in a format the user can understand".

Why Wireshark

Wireshark is a valuable tool for administrators that allow them to monitor all traffic that passes on a network. It is very useful for analyzing, diagnosing and troubleshooting problems that may occur.

Some features of wireshark.

1. Data can be captured from a network connection or read from previous records of captured packets.
2. Live data can be read from Ethernet, FDDI, PPP, token ring, IEEE 802.11, classical IP over ATM, and loopback interfaces (at least on some platforms; not all of those types are supported on all platforms).
3. Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
4. Captured network data can be browsed via a GUI, or via the terminal((command line) version of the utility tshark.
5. Display filters can also be used to selectively highlight and color packet summay information.
6. Data display can be refined using a display filter
7. Hundreds of protocols can be dissected.

How to get Wireshark

Wireshark can be downloaded from website www.wireshark.org .

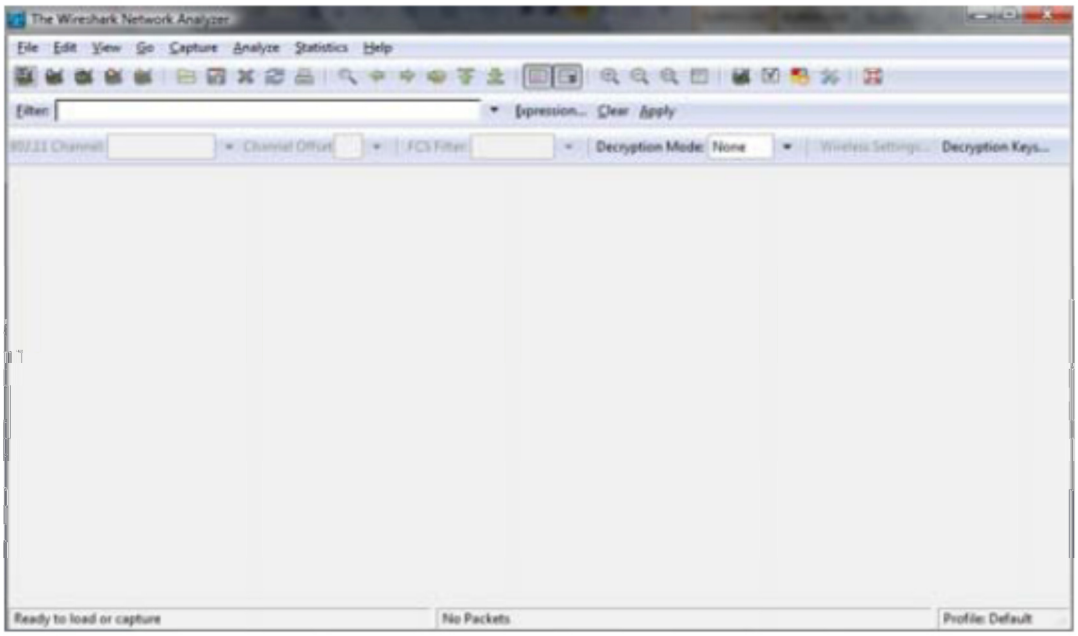
Getting started with Wireshark

Wireshark has a friendly graphical user interface that makes it easier for the to analyze and diagnose packets that passing throughthe network.

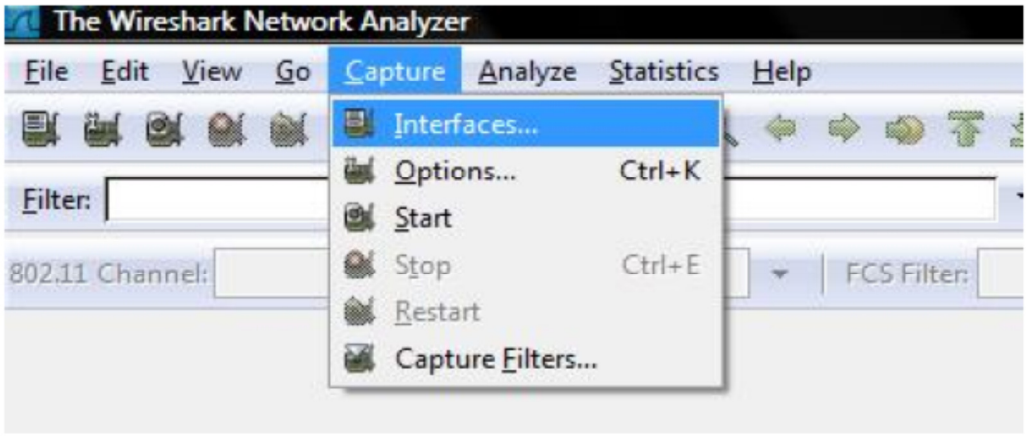
No data will initially be displayed when the user runs wireshark.

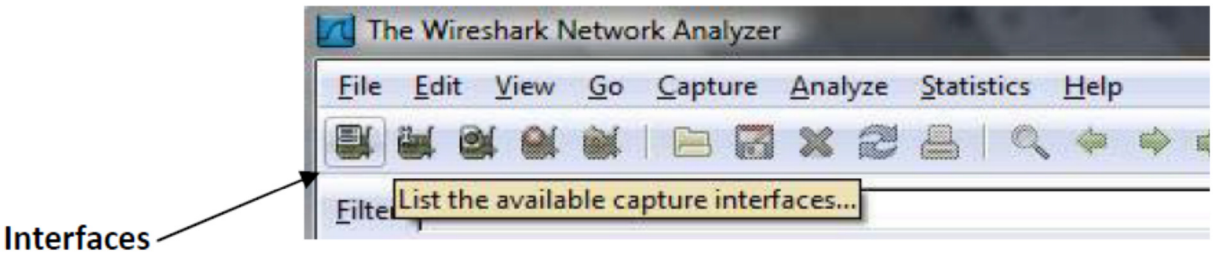
The environment and usage of wireshark will be explained further in this document.

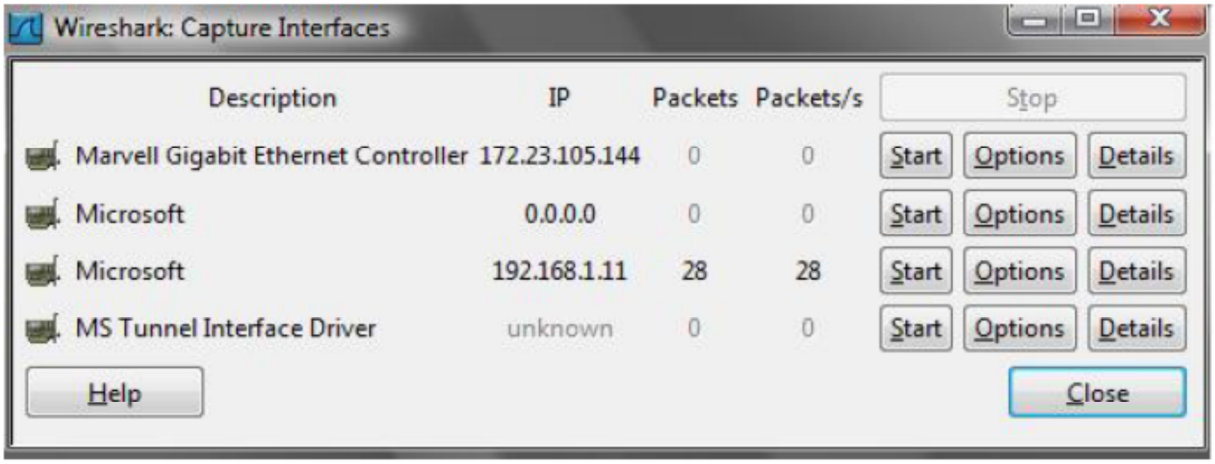
To start capturing packets you need to select the interface which is connected to the internet. This can be done by choosing Capture>>Interfaces from the Menu bar



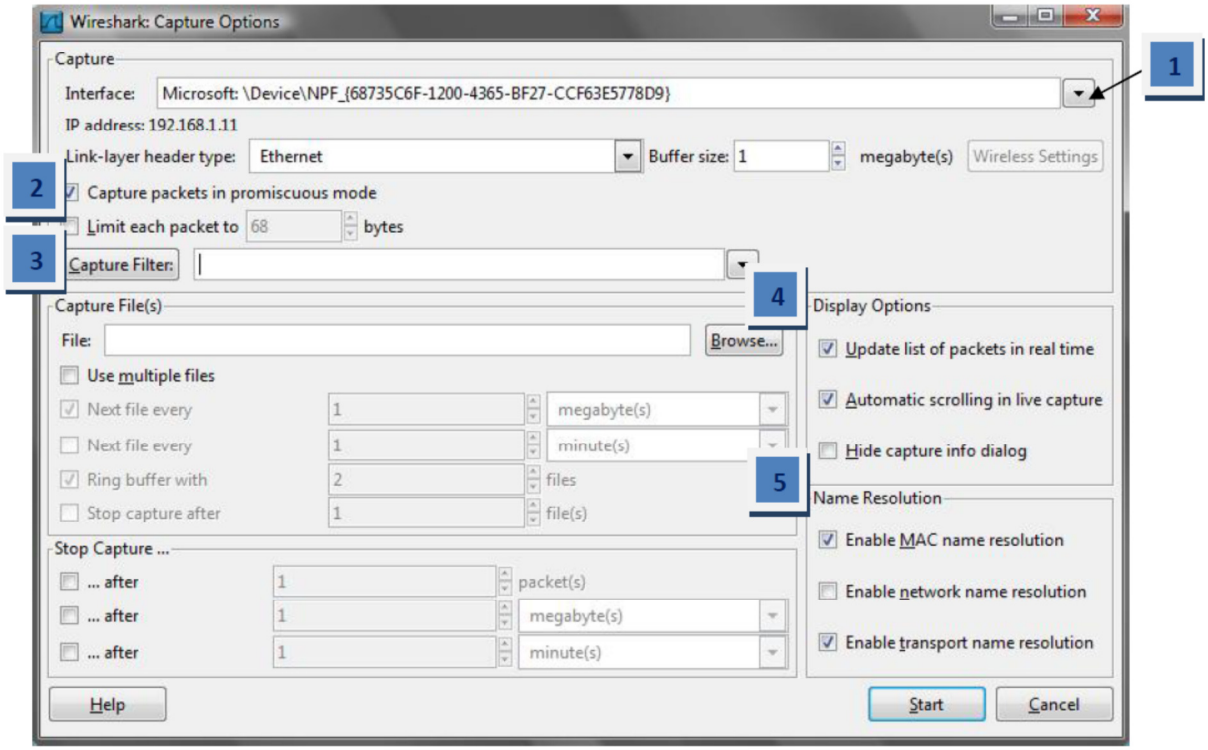
The different interfaces available that WinPcap driver sees in the machine are shown and you can either click start or click options for more options regarding capturing packets before starting the capture.







The following figure represents the Capture Option's Window



1 Switch between different interfaces. You can only capture on one of the interfaces that Wireshark found on the system at a time.

2 Capture packets in ***promiscuous*** mode checkbox allows Wireshark not only to capture the packets going to or from your computer, but also all packets on your LAN segment.

Limit each packet to n bytes field allows you to specify the maximum amount of data that will be captured for each packet, and is sometimes referred to as the snaplen[3].

3 Capture filters are to be explained thoroughly in the next document. The default is not choosing any filters when capturing.

4 Display Options:

Update list of packets in real time to display the packets right away once captured. If it is not chosen Wireshark will display the packets captured when you stop the capture. It is important to know that choosing this option decreases the ability to capture packets in high rates.

Automatic scrolling in live capture automatically scrolls down to the last packet captured. If this option is not chosen Wireshark adds new packets to the end of the list, but does not scroll to the end of the packets pane. You can toggle this off from the commands menu at any time as shown in the following page.

Hide capture info dialog: Toggle on/off to hide/show the capture info dialog while capturing.

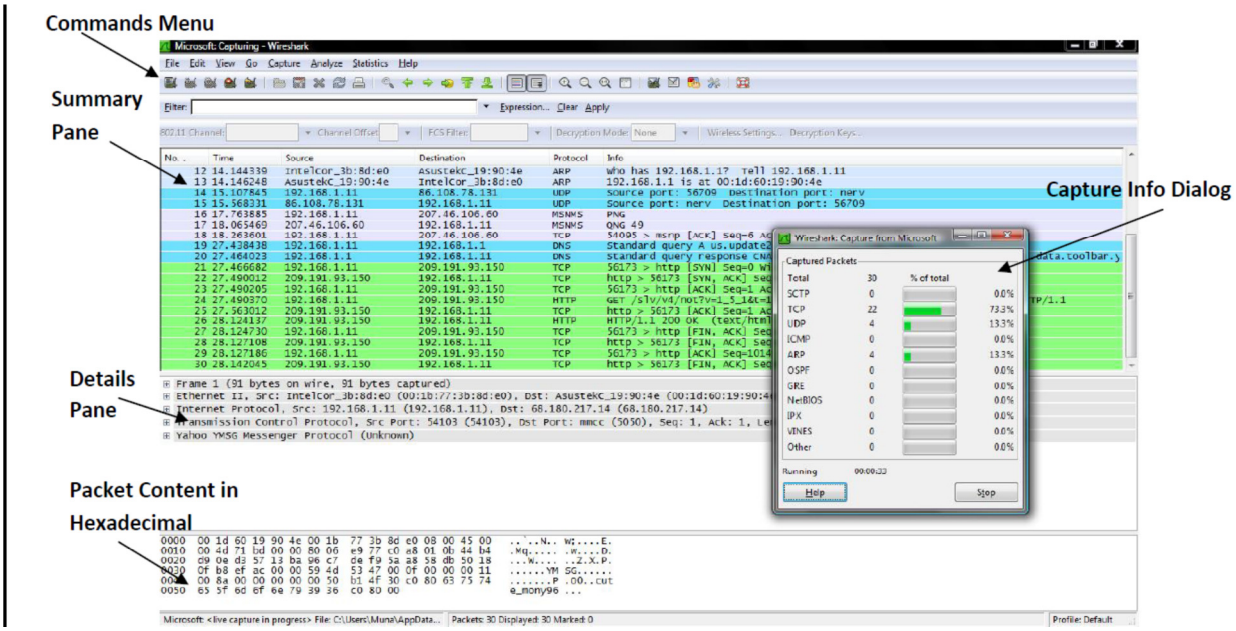
5 Name Resolution Options:

Enable MAC name resolution option: Toggle on/off to allow whether Wireshark translates MAC addresses into names or not.

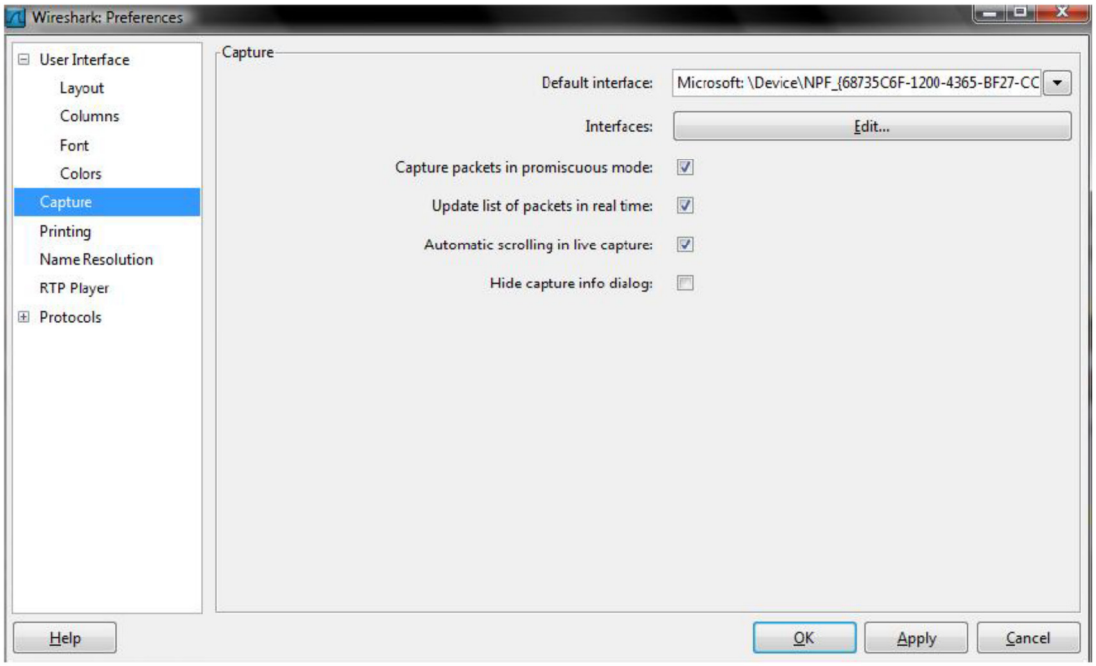
Enable network name resolution option: Toggle on/off to allow whether Wireshark translates network addresses into names or not.

Enable transport name resolution option: Toggle on/off to allow whether Wireshark translates transport addresses into protocols or not.

An interesting way to set up the environment in wireshark to a default interface and some default options instead of choosing them each and every time you run wireshark is by clicking the preferences icon from the commands menu and choosing the Capture tab.
Options similar to those found in the Capture options dialog box can be found.



1. List available capture interfaces
2. Show the capture options
3. Start a new live capture
4. Stop the running live capture
5. Restart the running live capture
6. Colorize packet list (Toggle button)
7. Auto scroll packet list in live capture (Toggle button)
8. Edit preferences
9. Show some help


Wireshark: Preferences
User Interface
Layout
Columns
Font
Colors
Capture
Printing
Name Resolution
RTP Player
Protocols
Capture
Default interface:
Microsoft: \Device\NPF_{68735C6F-1200-4365-BF27-CC
Interfaces:
Edit...
Capture packets in promiscuous mode:
Update list of packets in real time:
Automatic scrolling in live capture:
Hide capture info dialog:
Help
OK
Apply
Cancel