



**Lab**

**C1116**

كلية الهندسة – جامعة المنصورة

## **C1116      معمل شبكات الحاسب**

Computers and Control Systems Engineering Department

قسم هندسة الحاسبات ونظم التحكم

# **Laboratory Book**

**2021**

Computers and Control Systems Engineering Department

معمل شبكات الحاسب C1116

# Laboratory Book

---

# Table of Contents

1: Laboratory Basic Information.....	2
البيانات الأساسية للمعمل أولاً :	2
2: Laboratory Instruments.....	3
ثانياً: قائمة بالأجهزة والمعدات الموجودة بالمعمل	3
3: Laboratory Experimental List.....	4
ثالثاً: قائمة بالتجارب التي تؤدي داخل المعمل	4
4: Laboratory Beneficiaries.....	5
رابعاً: الخدمات المجتمعية التي يؤديها المعمل:	5
5: Laboratory Student Beneficiaries .....	6
خامساً: الخدمات الطلابية التي يؤديها المعمل:	6
6: Experimental Labs .....	7
سادساً: التجارب المعملية	7
Lab 1: PCs on a Network .....	8
Lab 2 : PCs on the Internet .....	17
Lab 3 : Wireless Networks and Mobile Systems .....	20
Lab 4 : In-class Lab Assignment Overview .....	21
<b>Laboratory Exercise: interference between Bluetooth and 802.11b</b> ..	26

## 1: Laboratory Basic Information

أولاً : البيانات الأساسية للمعمل

إسم المعمل:	معمل شبكات الحاسب الرقم الكودي : C1116
القسم العلمي:	هندسة الحاسبات ونظم التحكم
المشرف:	أ.د/ شريف السيد حسين أ.م.د/ عمرو محمد ثابت
أعضاء الهيئة المعاونة:	م/ مصطفى نصحي م/ حسام بلحة
أمين المعمل:	السيد/ محمد أبو بكر حامد محمد
التليفون:	داخلي 1297
الموقع بالنسبة للكلية:	الناحية البحرية
مساحة المعمل:	120 متر

## 2: Laboratory Instruments

ثانياً: قائمة بالأجهزة والمعدات الموجودة بالمعمل

Serial Number	العدد	إسم الجهاز	م
• MB MSI 945 (V+S+L)	10	CPU Intel P4 3GH	1
• MB Intel GB 915 (V+S+L)	4	CPU Intel P4 3 GHz	2
• MB MSI VIA	3	CPU Intel Celeron 2.1 GHZ	3
• MB Genix (V+S+L)	2	CPU Intel Celeron 2.1 GHZ	4
• MB MSI VIA	1	CPU Intel Celeron 2.1 GHZ	5

### 3: Laboratory Experimental List

ثالثاً: قائمة بالتجارب التي تؤدي داخل المعمل

<u>Experiment</u>	<u>Name</u>
<u>Lab 1 .....</u>	<u>PCs on a Network</u>
<u>Lab 2 .....</u>	<u>PCs on the Internet</u>
<u>Lab 3 .....</u>	<u>Wireless Networks and Mobile Systems</u>
<u>Lab 4 .....</u>	<u>In-class Lab Assignment Overview</u>
<u>Laboratory Exercise.....</u>	<u>interference between Bluetooth and 802.11b</u>

## 4: Laboratory Beneficiaries

رابعاً: الخدمات المجتمعية التي يؤديها المعمل:

- المستفيدين من المعمل: طلاب القسم بالإضافة إلى بعض طلاب البرامج النوعية
- الجهات التي تتعاون مع المعمل: لا يوجد
- الدخل السنوي للمعمل: لا يوجد
- الجهات الممولة لأنشطة المعمل: لا يوجد

المشاريع التنافسية التي يشارك فيها المعمل: مشاريع التخرج الخاصة بطلاب الصف الرابع – قسم هندسة الحاسبات و نظم التحكم.

## 5: Laboratory Student Beneficiaries

خامساً: الخدمات الطلابية التي يؤديها المعمل:

عدد الطلاب المستفيدين من المعمل	في خلال مده اسبوع 200 طالب
الأقسام العلمية المستفيدة من المعمل	قسم هندسة الحاسبات ونظم التحكم
الفرق الدراسية المستفيدة من المعمل	الفرقة الرابعة – الفرقة الثالثة من قسم هندسة الحاسبات ونظم التحكم.
المقررات الدراسية التي تستفيد من المعمل	معمار حاسب – تصميم رقمي و منطقي 2 – نظم تشغيل 2.
الأنشطة الطلابية داخل المعمل	ندوات طلابية- عقد جلسات مناقشة حلقات البحث لطلاب تمهيدى الماجستير و دبلومة الحاسبات – مناقشة مشاريع التخرج لطلاب قسم هندسة الحاسبات و نظم التحكم - عقد جلسات الامتحانات الشفوية لمادة نظم التشغيل – عقد الامتحانات العملية لمادة تصميم رقمي 1 و تصميم رقمي 2 – التدريب الصيفي لطلاب الصف الاول بقسم هندسة الحاسبات و نظم التحكم.
طلاب الدراسات العليا المستفيدين من المعمل	طلاب تمهيدى هندسة الحاسبات و دبلومة الحاسبات.
عدد الرسائل العلمية التي تمت في المعمل	تطبيق الجزء العملى لبعض الرسائل العلمية المتعلقة بالنظم الموزعة و أنظمة المتشابكات الحسابية والتي تعتمد على الأجهزة المتنقلة ذلك خلال الفترة من (2011 الى 2020).
عدد الدورات التدريبية التي تمت في المعمل	عقد دورتين تدريبيتين لتدريب طلاب القسم فى أنظمة قواعد البيانات
المسابقات العملية التي شارك فيها طلاب من المستفيدين من المعمل	مسابقات خاصة بمشاريع التخرج الخاصة بطلاب القسم ضمن يوم المهندس المصرى – مؤسسة مصر المحروسة – ايتيدا



# Experimental Labs

# Lab 1: PCs on a Network

## Objective

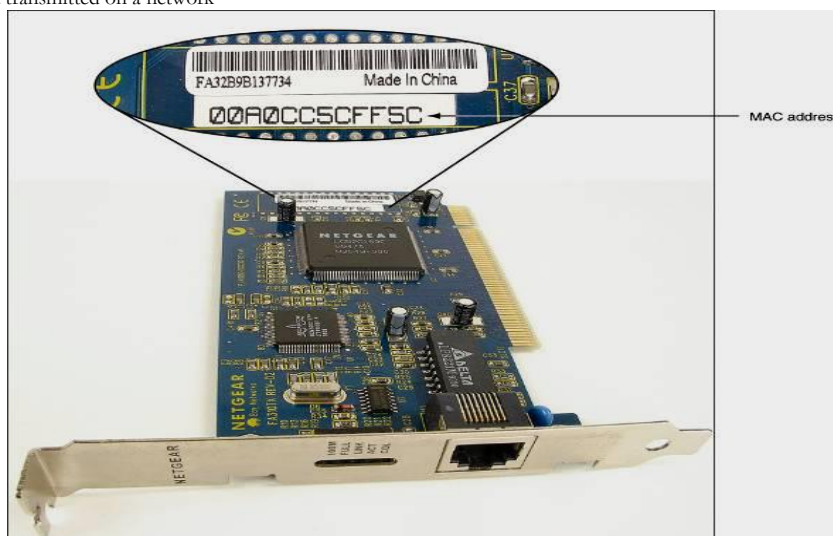
- Learn about different types of physical network architectures
- Learn how networking works with Windows
- Learn how to install a network card and connect to a network
- Learn about sharing resources on a network

## Sizes of Networks

- A network links two or more computers
- PAN (personal area network)
  - Consists of personal devices at close range
- LAN (local area network)
  - Covers a small local area such as a home, or office
- MAN (metropolitan area network)
  - Covers a large campus or city
- WAN (wide area network)
  - Covers a large geographical area; e.g., the Internet




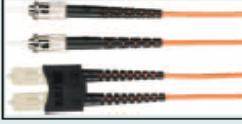
## Terms Used in Networking

- Node (host): one device on a network; e.g., server
- Network adapter: interfaces a PC with a network
  - Network interface card (NIC): fits in a PCI slot
- Adapter (MAC, physical, or hardware) address:
  - 48-bit (6-byte) id number hard-coded on card
  - Example: 00-0C-6E-4E-AB-A5
- Network protocols: rules of communication
- Packets (datagrams or frames)
- Basic unit of data transmitted on a network



*Ethernet network card showing its MAC address*

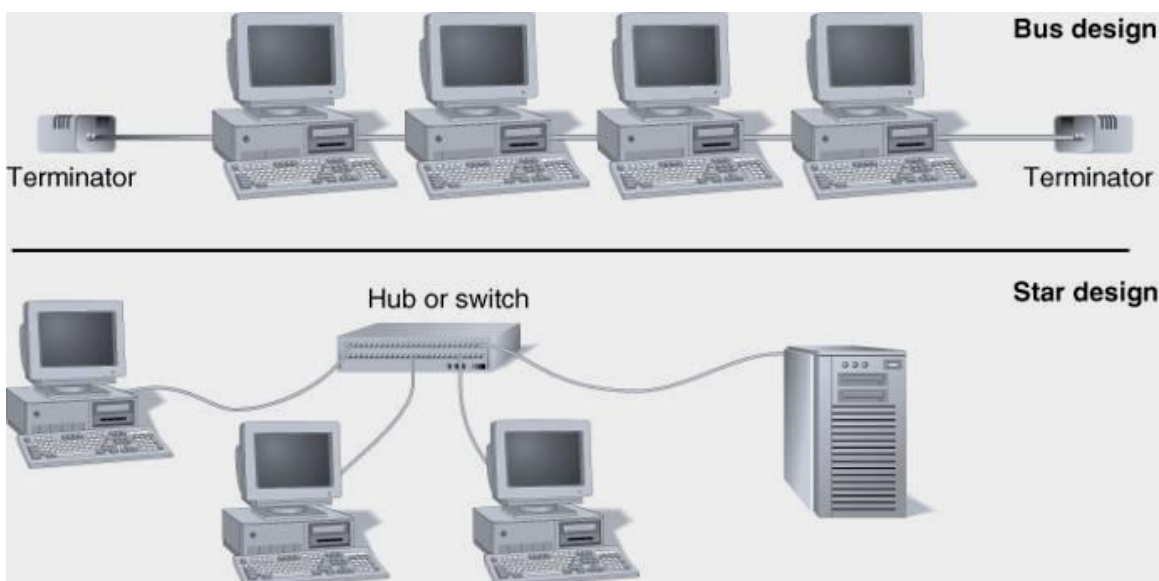
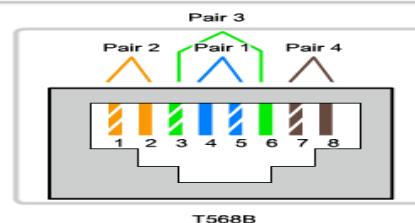
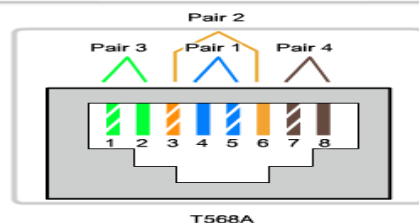
- Ethernet types (categorized by speed):
  - 10-Mbps Ethernet
  - 100-Mbps or Fast Ethernet
  - 1000-Mbps or Gigabit Ethernet
  - 10-Gigabit Ethernet
- Types of cabling used:
  - Two kinds of twisted-pair
    - Unshielded twisted pair (UTP): four pairs of twisted wire
    - Shielded twisted pair (STP): protected from EMI
  - Coaxial cable: single copper wire with braided shield
  - Fiber-optic: glass strands inside protective tubing

Cable System	Speed	Cables and Connectors	Example of Connectors	Maximum Cable Length
10Base2 (ThinNet)	10 Mbps	Coaxial uses a BNC connector		185 meters or 607 feet
10Base5 (ThickNet)	10 Mbps	Coaxial uses an AUI 15-pin D-shaped connector		500 meters or 1,640 feet
10BaseT, 100BaseT (Twisted-pair), and Gigabit Ethernet	10, 100, or 1,000 Mbps	UTP or STP uses an RJ-45 connector		100 meters or 328 feet
10BaseF, 10BaseFL, 100BaseFL, 100BaseFX, 1000BaseFX, or 1000BaseX (fiber-optic)	10, 100, or 1,000 Mbps	Fiber-optic cable uses ST or SC connectors (shown to the right) or LC and MT-RJ connectors (not shown)		500 meters up to 2 kilometers (6,562 feet)

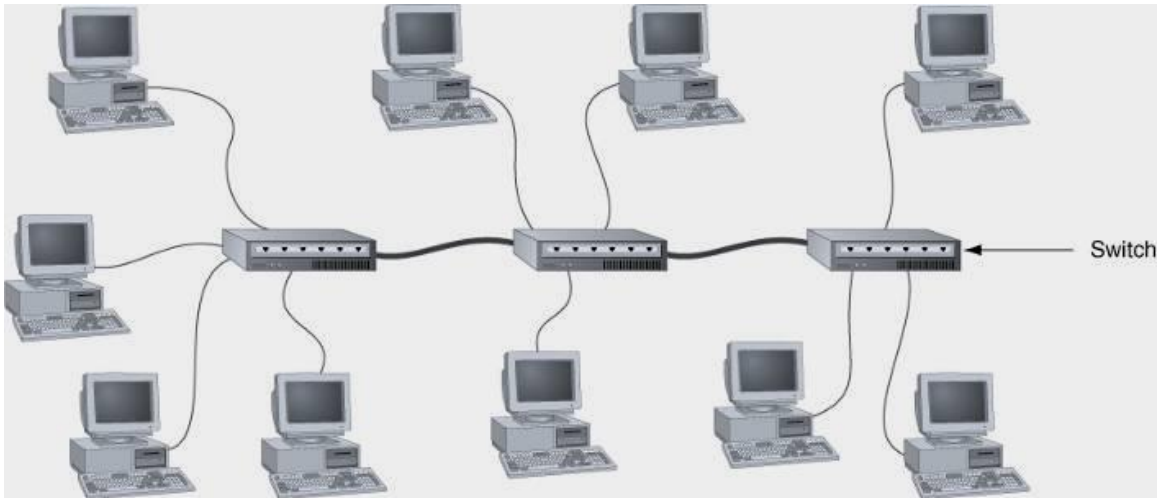
*Variations of Ethernet and Ethernet cabling*

**Straight-through, Crossover, and Rollover Cable Types**

Cable Type	Standard	Application
Ethernet Straight-through	Both end T568A or both end T568B	Connecting a network host to a network device such as a switch or hub.
Ethernet Crossover	One end T568A, other end T568B	Connecting two network hosts. Connecting two network intermediary devices (switch to switch, or router to router).
Rollover	Cisco proprietary	Connect a workstation serial port to a router console port, using an adapter.



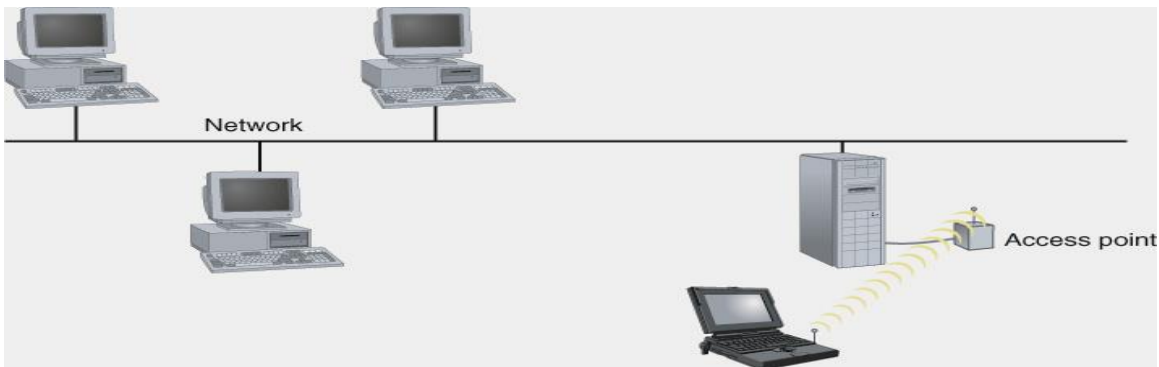
*Nodes on an Ethernet network can be connected to one another in a star or bus formation*



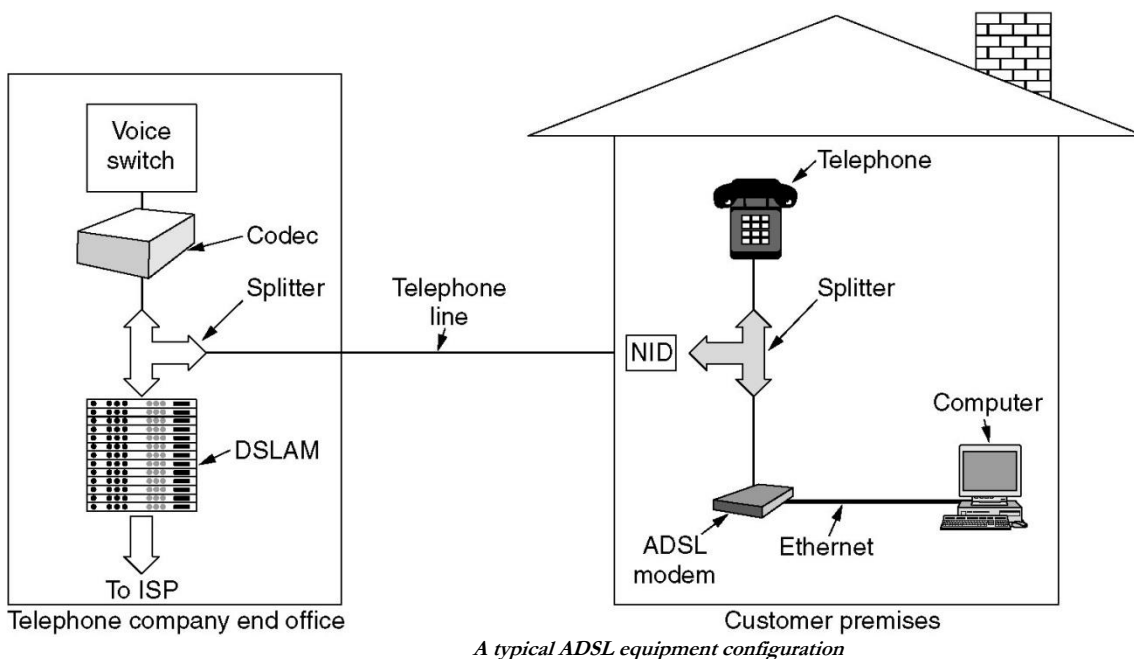
*A star bus network uses more than one switch*

## Wireless Networks

- Use radio waves or infrared light to connect PCs
- Popular in places where cables are difficult to install
- 802.11 wireless (Wi-Fi or Wireless Fidelity)
- Types: 802.11g (most popular), 802.11b, 802.11a
  - Two new standards: 802.11k and 802.11r
  - Ad hoc mode: directly links two wireless devices
  - Access point (AP): connects wireless device to LAN
- WiMAX (802.16 Wireless/802.16d and 802.16e)
- Used in public hot spots and as a last mile solution

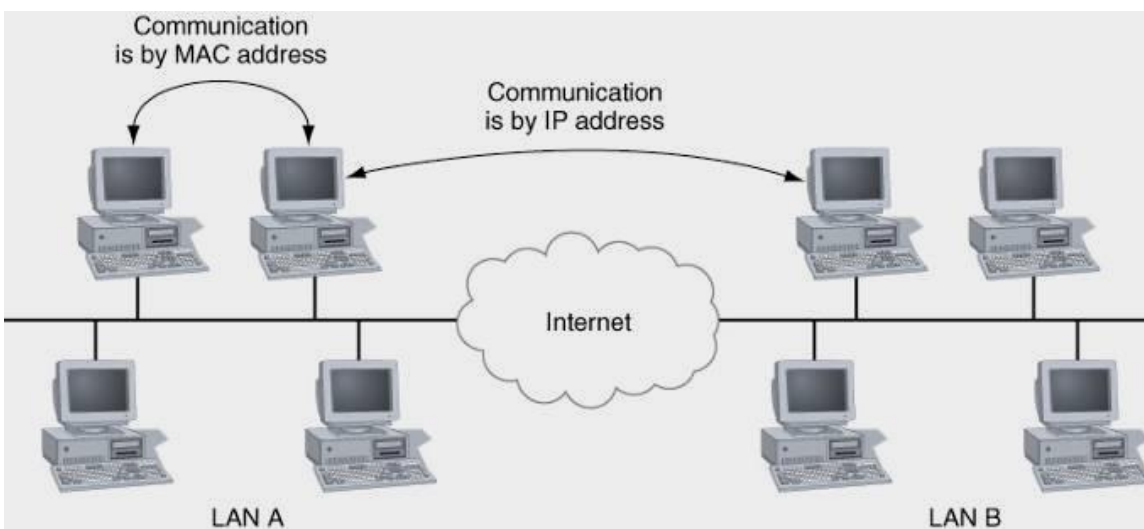


*Nodes on a wireless LAN connect to a cabled network by way of an access point*



## Addressing on a Network

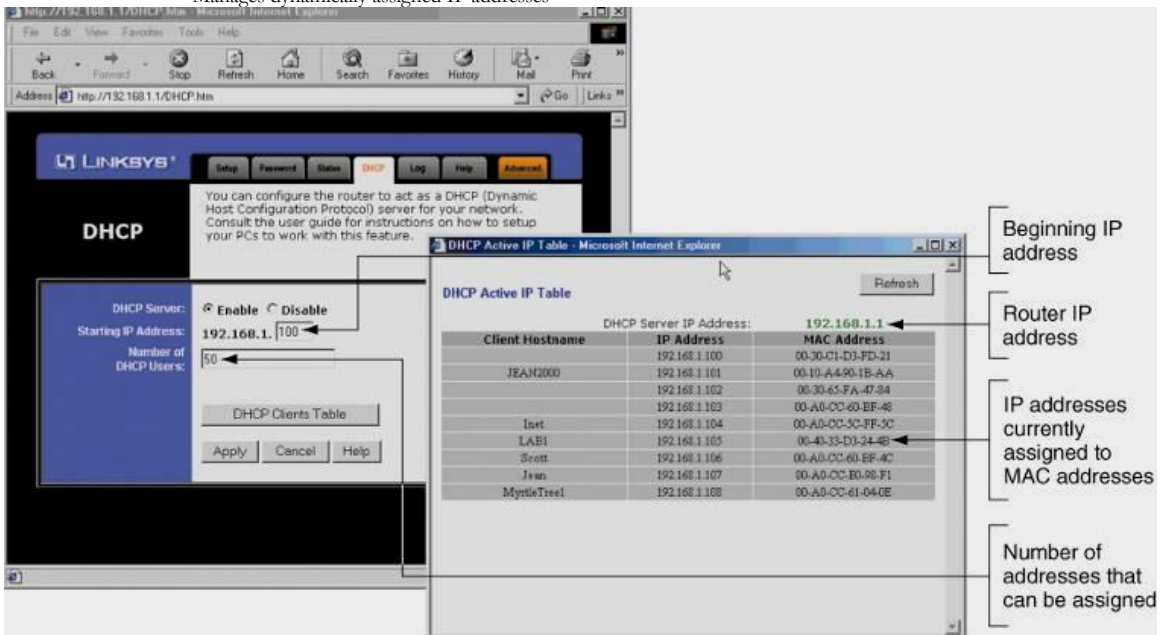
- Four methods used to identify devices and programs
  - Using a MAC address
  - Using an IP address
  - Using character-based names (host, domain, NetBIOS)
  - Using a Port address
- IP addresses
  - Used in TCP/IP to identify any device on the network
  - 4 bytes (octets) separated by dots; e.g., 190.180.40.120
  - System allows for up to 4.3 billion IP addresses
  - First part identifies network, last part identifies host



*Computers on the same LAN use MAC addresses to communicate, but computers on different LANs use IP addresses to communicate over the Internet*

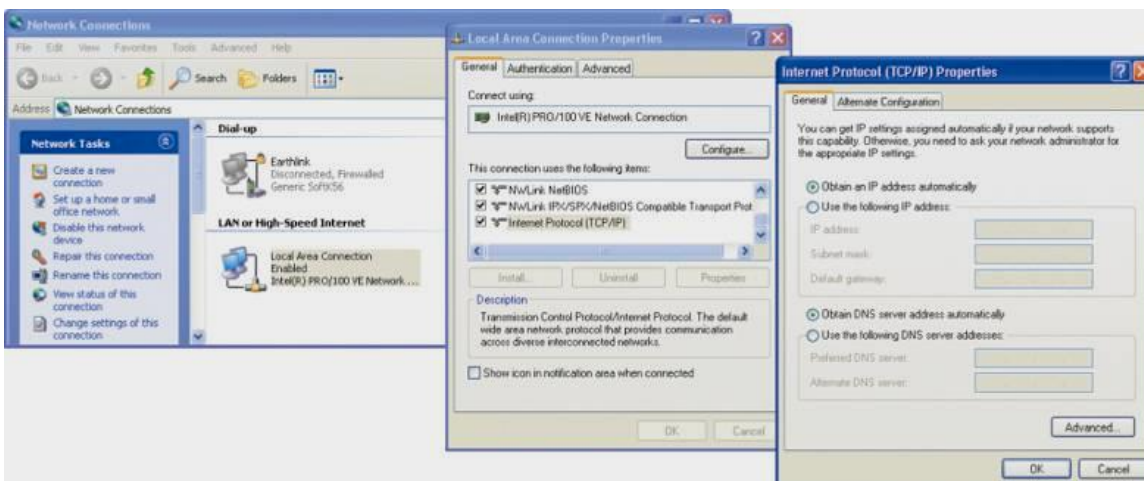
- IP address categories
  - Public IP address: available for use on the Internet
  - Private IP address: only used on a private intranet
  - Static IP address: permanently assigned to a node
  - Dynamic IP address: assigned for current session
- Solutions for IP address shortages

- 1. Private IP addresses
  - 2. Dynamic IP addressing (may be combined with 1)
- DHCP (Dynamic Host Configuration Protocol) server
  - Manages dynamically assigned IP addresses

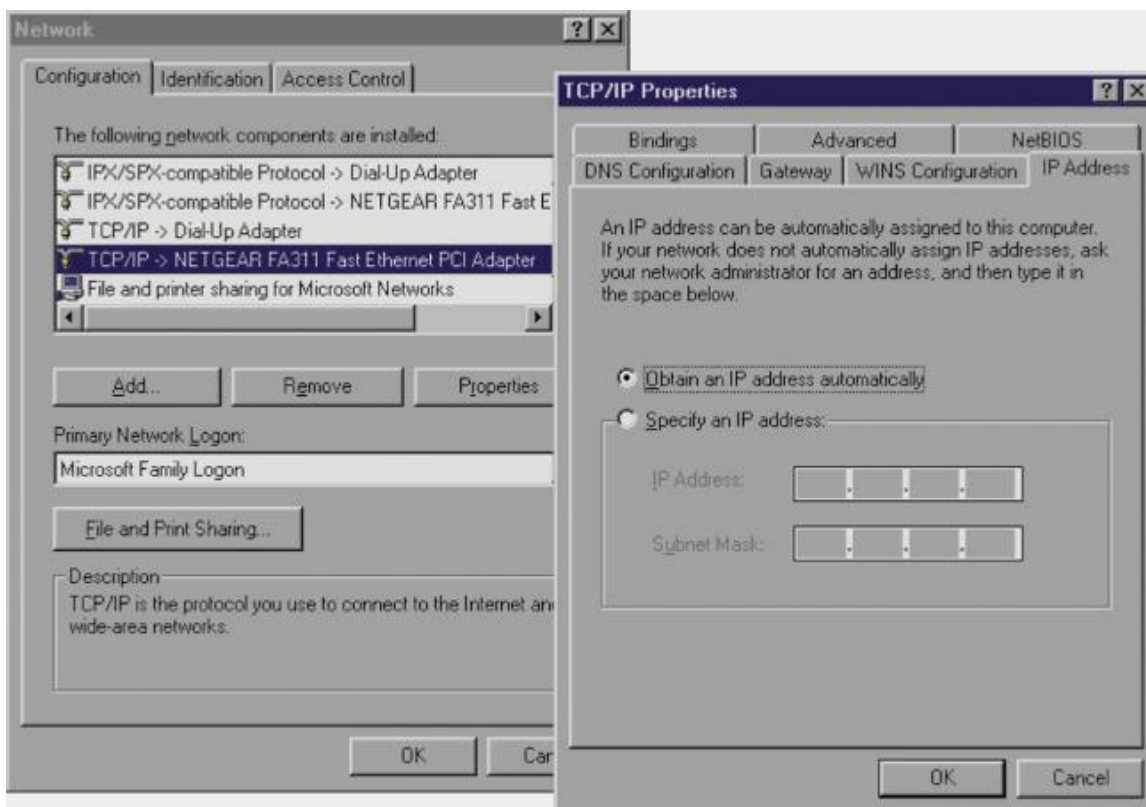


*A DHCP server has a range of IP addresses it can assign to clients on the network*

- Network address translation (NAT)
  - Presents public IP address for PC with private address
  - A proxy server makes the IP address substitutions
    - Proxy server: node between the network and the Internet
- Router can act as proxy server, DHCP server, firewall
- Name resolution: links a name to an IP address
- DNS (Domain Name System): tracks host names



*To configure TCP/IP under Windows XP, use the Internet Protocol (TCP/IP) Properties dialog box*



*To configure TCP/IP in Windows 98, select the binding and click Properties to view the TCP/IP Properties dialog box*

## Installing a Wireless Adapter in a Notebook

- Wireless adapter uses a USB port or PC Card slot
- Installation package includes a CD and accessories
- Overview of steps for installing a Linksys adapter
  - Install the software from the setup CD
  - Plug the wireless adapter into a USB port
  - Launch Found New Hardware and follow instructions
- Managing the issue of an unsigned driver
  - Find approved driver or continue installation



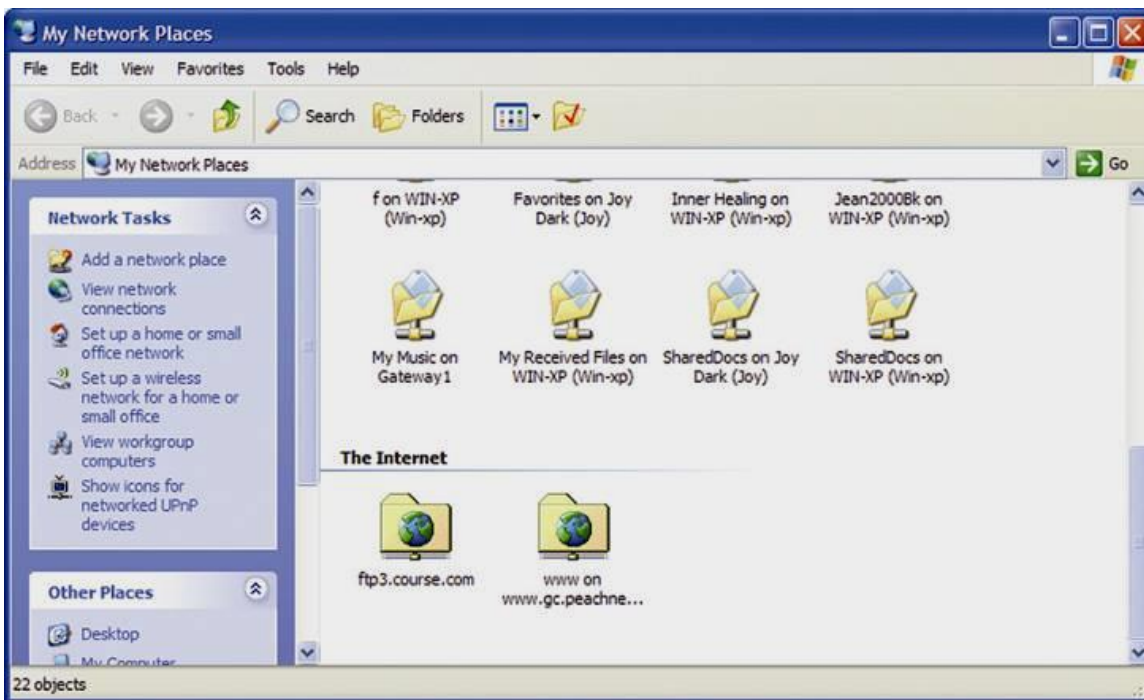


Plug the wireless USB adapter into the USB port

## Sharing Files, Folders, and Applications

- PCs in same workgroup or domain share resources
- How to makes network shares available
  - Use My Network Places in Windows 2000/XP
  - Use Network Neighborhood in Windows 9x/Me
- Windows components required for sharing resources
  - Client for Microsoft Networks
  - Printer Sharing for Microsoft Networks
- Creating a network share in Windows
  - Use Sharing tab in Properties dialog box of target

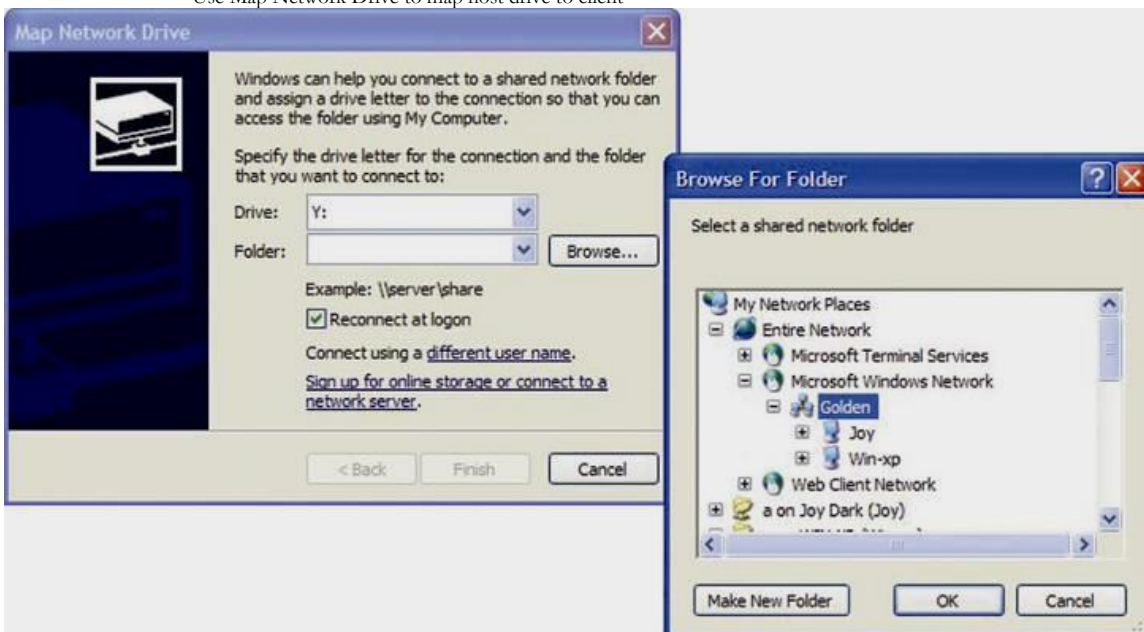




*View and access shared resources on the network using My Network Places in Windows XP*

## Network Drive Maps

- Make the client PC appear to have a new hard drive
  - Physical hard drive space is on the host (the server)
- Network File System (NFS)
  - Manages network drive maps between client and server
  - Is a type of distributed file system (DFS)
  - Provides more for highly reliable file sharing
- Overview of steps to create a network drive map:
  - Create a network share on the host
  - Access network using remote computer (client)
  - Use Map Network Drive to map host drive to client



*Mapping a network drive to a host computer*

- Define the main characteristics of the following network types (LAN-MAN-WAN-Internet)
- Specify why the portioning of the message within the network is bad solution?
- Network can be classified based on many parameters; State these parameters, for each specify the different types based on such parameter

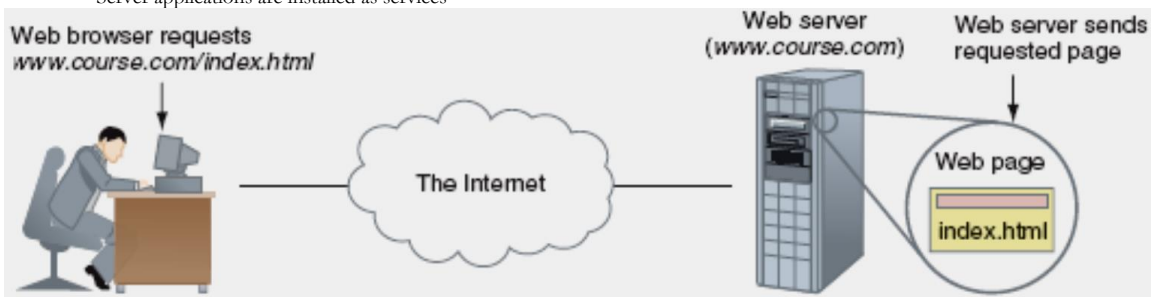
## Lab 2 : PCs on the Internet

### Objective

- Learn about the TCP/IP suite of protocols
- Learn how to connect to the Internet using cable modem, DSL, and dial-up connections and how to share those connections
- Learn how to use a router to enhance and secure a network connection to the Internet
- Learn about supporting common Internet clients such as Web browsers, e-mail clients, file transfer software, Internet telephone, and Windows XP Remote Desktop

### The TCP/IP Suite of Protocols

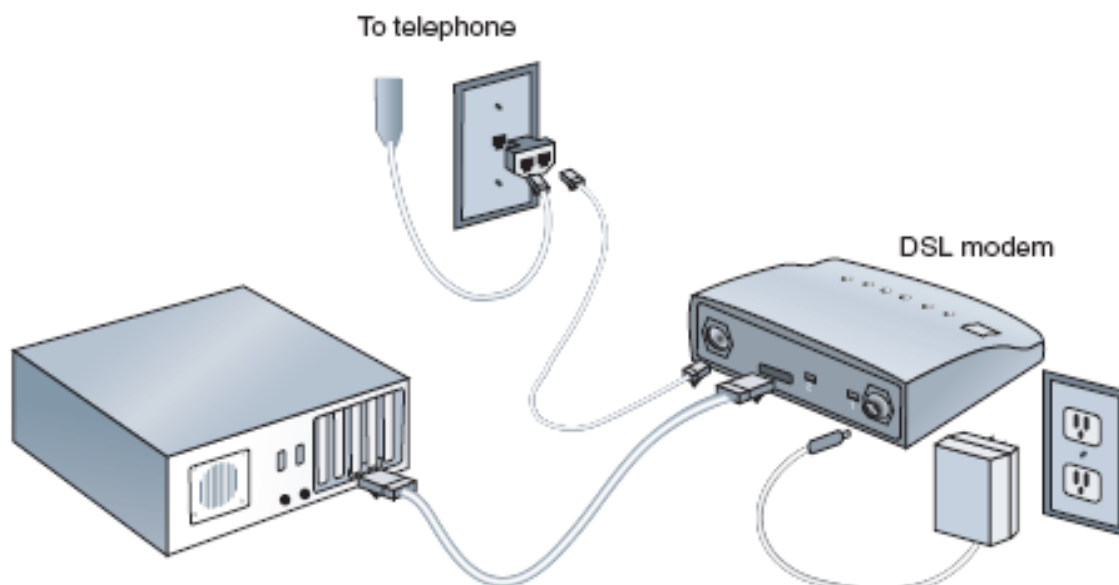
- Client/server application
  - Client application on one PC requests data from server
  - Server application on another PC returns data
- Example: World Wide Web
  - The client is a Web browser
  - The server is a Web server; e.g., Apache HTTP server
  - Requested data is a Web page
- Client applications are installed as programs
- Server applications are installed as services



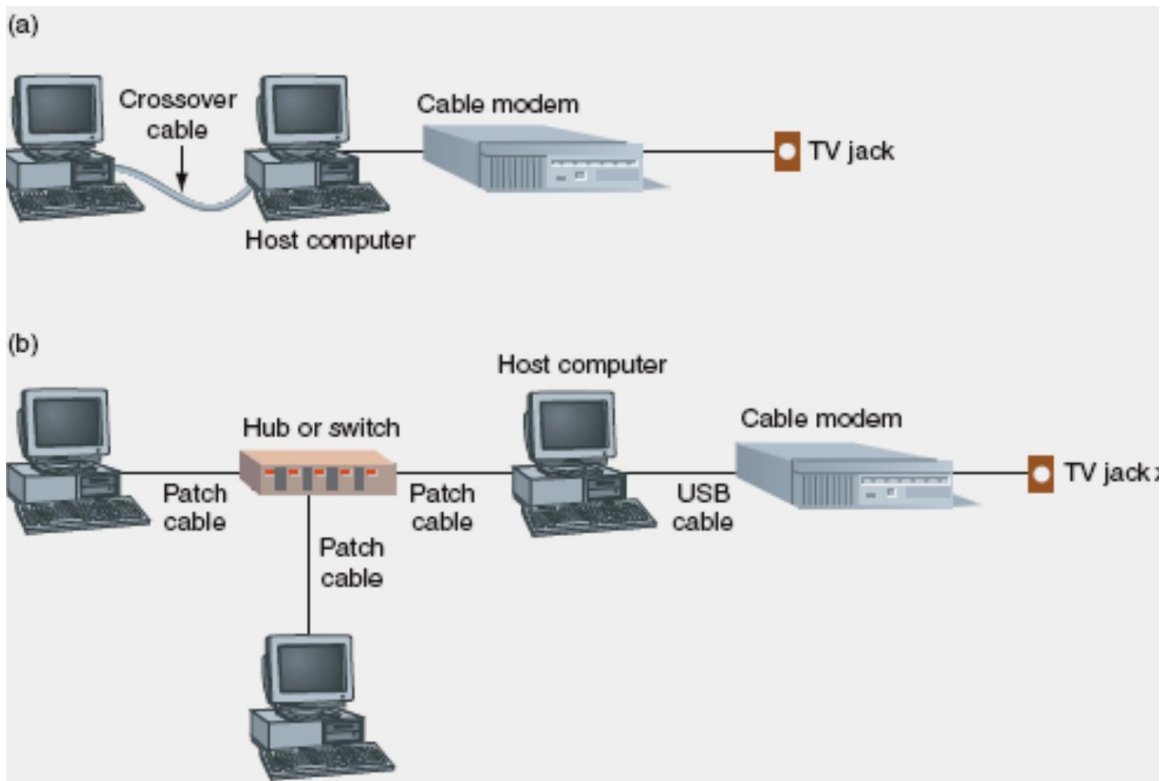
*A Web browser (client software) requests a Web page from a Web server (server software); the Web server returns the requested file or files to the client*

### DSL Connections

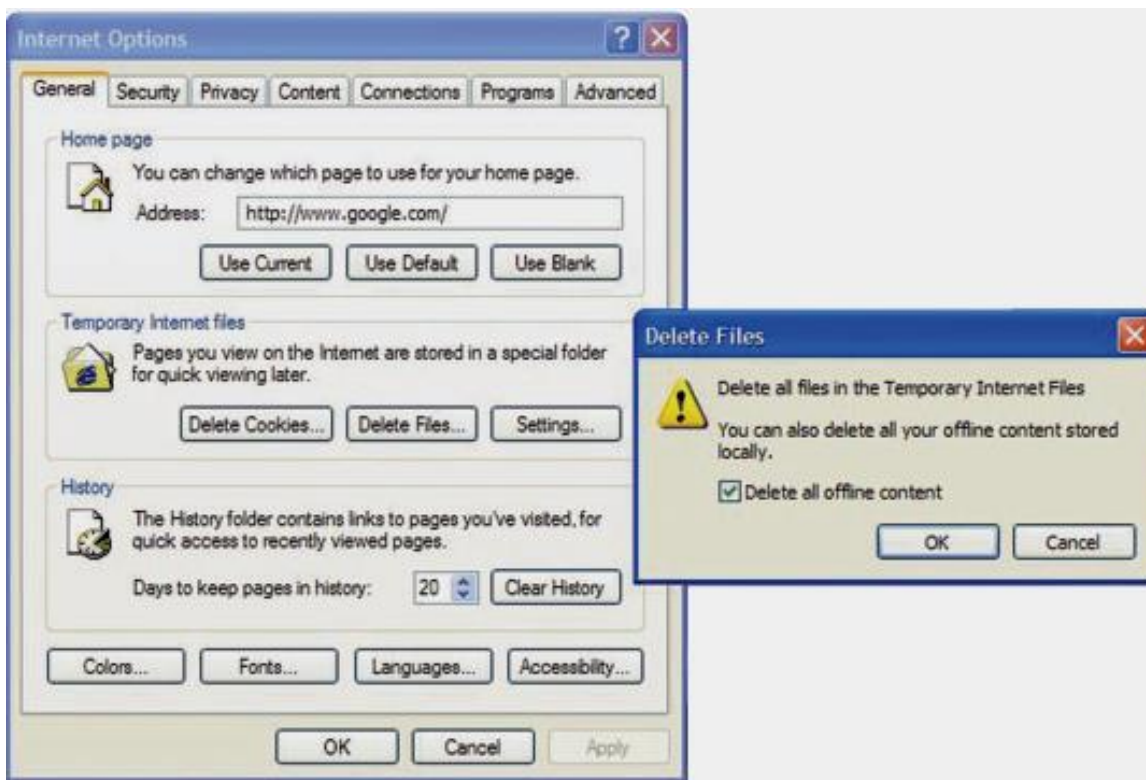
- Comparing communication media
  - Cable modem: TV cables shared by multiple users
  - DSL: dedicated phone lines
- Comparing service plans
  - Both: sliding-scale residential and business plans
- Comparing setup
  - Both: a modem interfaces PC and broadband jack
- Comparing installation services:
  - Both: will install equipment at additional cost



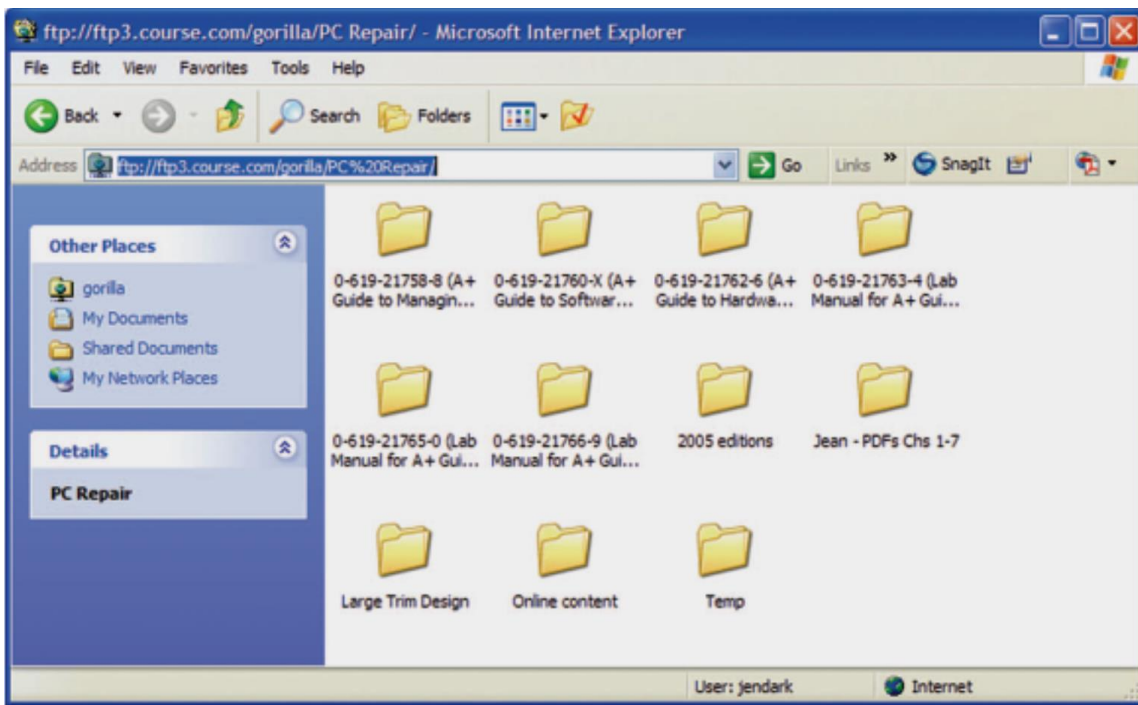
*Sample setup for DSL*



*Two or more networked computers can share a single Internet connection*



Use the Internet Options window to control the Internet Explorer environment



*Using Internet*

*Explorer as an FTP client*

# Lab 3 : Wireless Networks and Mobile Systems

## Part I – Objectives and Lab Materials Objective

The objectives of this lab are to:

- . Familiarize students with the operation of virtual private networks (VPN); and
- . Familiarize students with the operation of the Dynamic Host Configuration Protocol (DHCP) and IP masquerading, which is also known as network address translation (NAT).

After completing the assignment, the students should be able to:

- . Understand the operations of VPNs, DHCP, and NAT; and

☞ Setup VPN connections in Windows 2000 Professional systems.

### Hardware to be used in this lab assignment

Each group needs the following hardware.

☞ One (1) Dell Latitude C640 notebook computer (*with a fully charged battery*)

- . One (1) Xircom 802.11b wireless Ethernet adapter

☞ One (1) crossover Ethernet cable (*comes with the Intel Wireless Gateway*)

### Software to be used in this lab assignment

- . Microsoft Windows 2000 Professional operating systems

- . Ethereal network analyzer tool

## Part II – Pre-lab Assignment

This portion of the assignment should be completed **prior** to the in-class lab session.

- . Read the following overview of VPN in Windows 2000: “Virtual Private Networking in Windows

2000: An Overview,” available at

<http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remotaccess/vpnov erview.asp>.

## Lab 4 : In-class Lab Assignment Overview

The in-class lab assignment includes the following two tasks, Task A and Task B.

**Task A** – Teams of three groups will conduct the following tasks together. Setup VPN connections between two Windows 2000 Professional computers and monitor the operation and overhead of the VPN using Ethereal. The network scenario is illustrated in Figure 1.

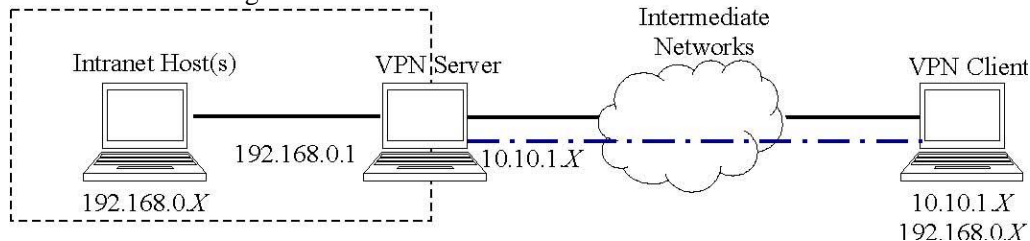


Figure 1. VPN network scenario.

ECE/CS 4984 Pre-lab and In-class Laboratory Exercise 10 Page 1 of 6

The VPN server is connected to a private intranet (192.168.0.0/24) and a “public” intermediate network (10.10.1.0/24). To access resources in the private network, the VPN client must connect to the VPN server with a secured tunnel through the public network. When connected, the VPN client is assigned a private IP address of 192.168.0.X. By forwarding IP packets between the VPN clients and the intranet hosts, the VPN server allows the VPN client to communicate with intranet hosts as if it is directly connected to the private network.

In this experiment, the VPN client will connect to the VPN server via an 802.11b access point that will be setup by the GTA. The intranet host will connect directly to the VPN server through an Ethernet interface. The intermediate networks are omitted in this experiment for simplicity. Each team will setup an intranet host, a VPN server and a VPN client.

**Task B** – Teams of two groups will conduct the following tasks together. Configure Internet Connection Sharing (ICS) and trace the operation of DHCP and NAT. The network scenario is illustrated in Figure 2.

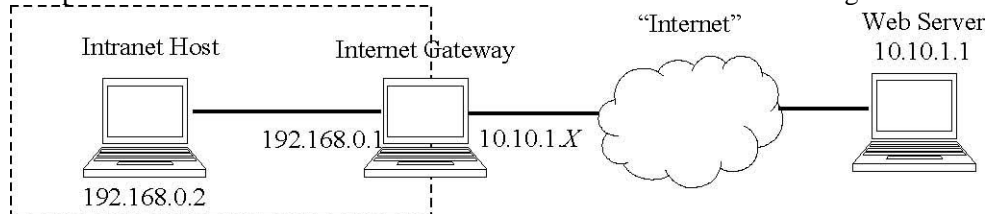


Figure 2. Network diagram for ICS.

In this scenario, the Internet gateway and the Web server are connected to the public “Internet” (the 10.10.1.0/24 network is assumed to be public in this experiment). The intranet (192.168.0.0/24) cannot access the “internet” directly and the private addresses 192.168.0.X are not reachable from the public Internet. Networking address translation (NAT) is used at the Internet gateway to provide connection to the Internet for hosts in the intranet. In Windows 2000, NAT and DHCP are used to enable Internet Connection Sharing (ICS).

In this lab experiment, the Internet gateway is connected to the public web server via an 802.11b access point. Each team will setup the intranet host and the Internet gateway. The GTA will setup the public web server and the access point.

### Details of Task A – Configure a VPN and Monitor Operation and Overhead

First, configure the network interfaces and setup an incoming connection on the **VPN server**. This is done with the following three steps.

1. On the notebook computer that will serve as the VPN server, boot into Windows 2000. If you have not done so, insert the Xircom 802.11b adapter into one of the PC Card slots. Launch the *Xircom Wireless Ethernet*



*Client Utility*, choose the “Commands->Edit Properties” menu. In the “System Parameters” tab, fill in **ECECS4984** as SSID1 and select **Infrastructure** as the network type. In the “Network Security” tab, check the **Enable WEP** option and enable **Shared Key Authentication**.

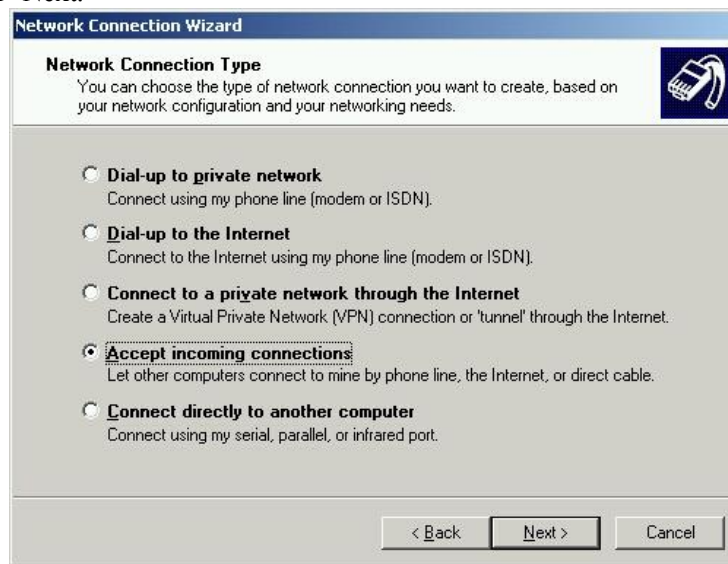
Use the *Xircom Client Encryption Manager* to enter the default WEP key **ABCDEF4984**.

- From the “Start” menu, open “Settings->Network and Dial-up Connections,” right-click on “Wireless LAN,” and then click “Properties.” Highlight the item “Internet Protocol (TCP/IP)” and then click “Properties.” In the “Internet Protocol Properties” dialog box, check “Obtain an IP address automatically” to enable DHCP. Then click “OK” to apply the changes. Open a command console, use the “ipconfig /all” command to verify that the “Wireless LAN” interface is properly configured. Check and record the assigned IP address, which will be the public address for your VPN server. Test the connection to the access point at IP address **10.10.1.1**.

In “Network and Dial-up Connections,” right-click “Local Area Network” and then click “Properties.” Highlight “Internet Protocol (TCP/IP)” and then click “Properties.” Set the IP address as **192.168.0.1** and the subnet mask as **255.255.255.0**.

- The following steps setup an incoming connection on the VPN server. In “Settings->Network and Dial-up Connections,” click “Make New Connection” to start the Network Connection Wizard. Click “Next.” (Note that if this is the first time for creating a VPN or dial-up connection, a “Location Information” dialog may appear. Input your area code to create the default location settings.)

On the “Network Connections Type” dialog box, select **Accept Incoming Connections** (as shown in the figure below), and then click “Next.”



On the “Devices for Incoming Connections” dialog box, do **NOT** select any device. Just click “Next.”

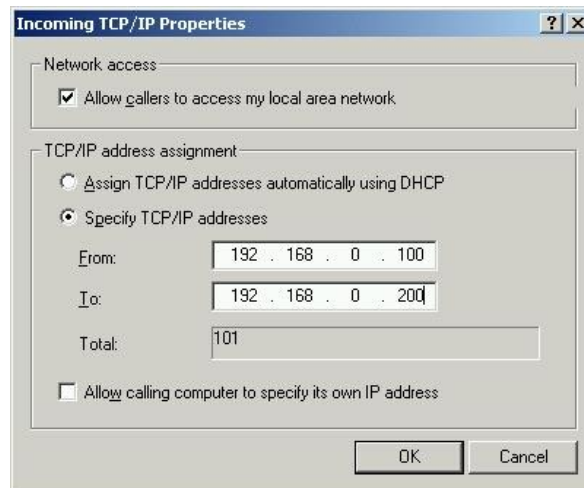
On the “Incoming Virtual Private Connection” dialog box, click **Allow Private Connections**, and then click “Next”.

On the “Allowed Users” dialog box, select **Administrator** to allow connection requests. Click “Next.”

On the “Networking Components” dialog box, select “Internet Protocol (TCP/IP)” and then click

“Properties.” Setup TCP/IP as shown in the following figure.





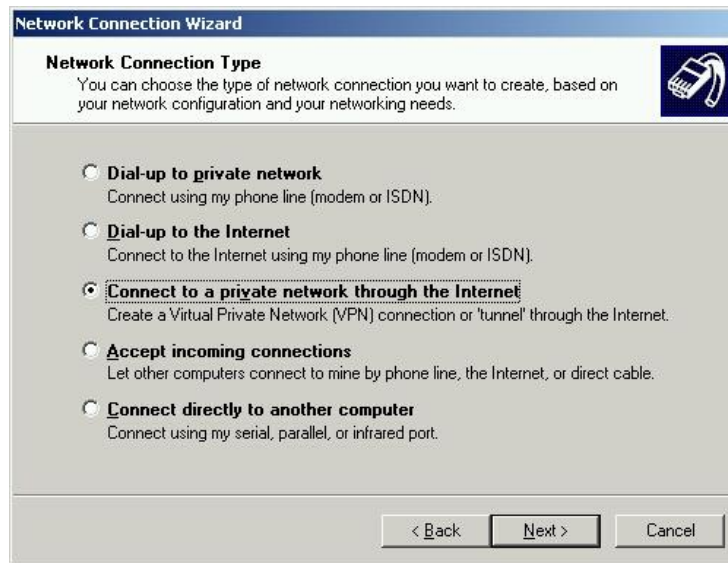
On the “Completing the Network Connection Wizard” dialog box, the default connection name is **Incoming Connections** and the name cannot be changed. Click “Finish” to close the dialog. The following two steps set up the **intranet host**.

- 1 On the notebook computer that serves as the intranet host, remove any wireless 802.11b card from the PC card slots. Use the crossover Ethernet cable to connect the intranet host and the VPN server via the wired Ethernet interface on each computer.
- 2 Boot Windows 2000, open “Settings->Network and Dial-up Connections,” right-click “Local Area Network,” and then click “Properties.” Highlight “Internet Protocol (TCP/IP)” and then click “Properties.” Setup the IP address as **192.168.0.2**, the default gateway as **192.168.0.1**, and the subnet mask as **255.255.255.0**. Click “OK” and close the dialog.

Setup the **VPN client** and create a VPN connection to the server according to the following four steps.

1. On the notebook computer that serves as the VPN client, boot Windows 2000. If you have not done so already, insert the Xircom 802.11b adapter into one of the PC Card slots. Launch the *Xircom Wireless Ethernet Client Utility*, choose the “Commands->Edit Properties” menu. In the “System Parameters” tab, fill in **ECECS4984** as SSID1 and choose **Infrastructure** as the network type. In the “Network Security” tab, check the “Enable WEP” option and enable **Shared Key Authentication**.  
Use the *Xircom Client Encryption Manager* to enter the default WEP key **ABCDEF4984**.
- 2 Open “Settings->Network and Dial-up Connections,” right-click “Wireless LAN,” and then click “Properties.” Highlight “Internet Protocol (TCP/IP)” and click “Properties.” Configure TCP/IP to use DHCP. Use the *ipconfig /all* command to verify that the “Wireless LAN” interface is properly configured and record the assigned IP address. Use the *ping* command to test the connection to the VPN server (10.10.1.X) of your team.
- 3 In “Network and Dial-up Connections,” double-click “Make New Connections” to start the “New Connection Wizard.” Click “Next.” (Note that if this is the first time creating a VPN or dial-up connection on this computer, a “Location Information” dialog may appear. If so, input your area code to create the default location settings.)

On the “Network Connection Type” dialog box, select **Connect to Private Network through Internet** as shown below and then click “Next”.



If the “Public Network” dialog appears, select “Do not dial the initial connection” option and then click “Next.”

In the “Destination Address” dialog box, type in the public IP address of the VPN server (10.10.1.X) to which you are attempting to connect and then click “Next.”

On the “Connection Availability” dialog box, check **Only for Myself** and then click “Next.”

On the “Completing the Network Connection Wizard” dialog box, accept **Virtual Private Connection** as the default connection name and then click “Finish.” The “Connect Virtual Private Connection” dialog will appear.

4. The “Connect Virtual Private Connection” dialog will appear. Click “Properties” to display the VPN settings dialog. In “Security” tab, check **Advanced (custom settings)** and click “Settings.” Select **No encryption allowed** for the “Data encryption” options. Click “OK” to close the dialog boxes. Encryption is an essential feature of a VPN, but we are disabling encryption here in order to analyze the operations in the VPN with Ethereal.

Use Ethereal network analyzer to trace the operation and overhead of VPN according to the following four steps.

1. Launch Ethereal on the VPN client, use menu “Capture->Start” to open the “Capture Options” dialog box. Select the 802.11b wireless interface (Cisco 340 Series Wireless LAN Adapter). Disable the **Capture packets in promiscuous mode** and **Enable network name resolution** options. Click “OK” to start tracing packets.

2. In the “Connect Virtual Private Connection” dialog box, enter **Administrator** as the user name and **wireless** as the password. Then click “Connect” to establish the VPN connection. An icon for the VPN connection will appear in the system tray when connected.

Use the `ipconfig /all` command to check the assigned IP address for the VPN client. The VPN client will have a virtual interface with a private IP address in the range of 192.168.0.100–192.168.0.200. Test the connection to the intranet gateway (with IP address 192.168.0.1) and the intranet host (with IP address 192.168.0.2).

2. Start Windows Explorer and enter “\\192.168.0.2\” in the address bar. You should be able to find the shared resources on that computer (printers, scheduled tasks, shared folders, etc.).

3. Close the VPN connection. Stop tracing with Ethereal. Examine the packets transferred between the VPN client and the intranet host and answer the following questions.

- 1) What tunneling protocol is used to establish the VPN connection, PPTP, L2TP, or IPSec?
- 2) Identify the sequence of packet exchanges that establish the VPN connection.
- 3) Examine some IP packets (such as ping request/reply) between the VPN client and the intranet host. Explain how these IP packets are encapsulated. Calculate the overhead (total bytes of the extra headers) of the VPN connection.

Have the GTA verify your results.

## Details of Task B – Configure ICS and Trace the Operations of DHCP and NAT

Two notebook computers are used in the following procedures.

1. On the notebook computer that will serve as the **Internet gateway**, boot into Windows 2000. Insert the Xircom 802.11b adapter into one of the PC Card slots. Launch the *Xircom Wireless Ethernet Client Utility*, choose the “Commands->Edit Properties” menu. In the “System Parameters” tab, fill in **ECECS4984** as SSID1 and select **Infrastructure** as the network type. In the “Network Security” tab, check the **Enable WEP** option and enable **Shared Key Authentication**. Use the *Xircom Client Encryption Manager* to enter the default WEP key **ABCDEF4984**.
2. Connect the **Internet gateway computer** to the **intranet host** via a crossover Ethernet cable. On the Internet gateway computer, open “Settings->Network and Dial-up Connections,” click on “Local Area Network,” and select “Properties.” In the settings dialog, highlight “Internet Protocol (TCP/IP)” and then click “Properties.” Check “Obtain an IP address automatically” to enable DHCP. Click “OK” to close the dialog boxes. Reboot the computers if prompted. On the **intranet host**, remove any wireless 802.11b card from the PC card slots and configure the “Local Area Network” interface to use DHCP in the same way.
3. On the **Internet gateway**, open “Settings->Network and Dial-up Connections,” right-click “Wireless LAN,” and then click “Properties.” Click on the “Sharing” tab in the “Wireless LAN Properties” dialog, check **Enable Internet Connection Sharing for this connection**, and then click “OK.” When prompted for confirmation, click “OK.” The wizard will automatically setup the wired Ethernet interface with IP address 192.168.0.1. DHCP and NAT will be enabled on this interface at the same time.
- 2 On the **Internet gateway**, open “Settings->Network and Dial-up Connections,” right-click “Local Area Network,” and then click “Properties.” Highlight “Internet Protocol (TCP/IP)” and then click “Properties.” Verify that the interface was assigned a fixed IP address of **192.168.0.1** and a subnet mask of **255.255.255.0**.
- 3 On the **Intranet host**, start Ethereal and begin tracing packets on the “Local Area Network” interface (3Com EtherLink PCI). On the **Internet gateway**, start Ethereal Network Analyzer and begin tracing packets on the 802.11b wireless interface (Cisco 340 Series Wireless LAN Adapter). Remember to enable the **Capture packets in promiscuous mode** and **Enable network name resolution** options.
- 4 On the intranet host, open a command console and execute the *ipconfig /renew* command to send a DHCP request to the internet gateway. Test the connection to the web server (with IP address 10.10.1.1) in the “internet.” Start Internet Explorer and browse the web page **http://10.10.1.1**.
- 5 On the intranet host, stop tracing with Ethereal. Examine the packet trace to locate and examine the following messages from the packet trace.
  - 1) The DHCP request message and the corresponding reply message. Record the fields in the reply message, such as client IP address, subnet mask, router, DNS server, lease time, etc.
  - 2) The TCP connections for the HTTP session. Record the source and destination IP addresses. What are the source and destination ports used for this HTTP session? Note that there may be multiple TCP connections.
8. On the internet gateway, stop tracing with Ethereal. Examine the packet trace and answer the following questions.
  - 1) Locate the TCP connection for the HTTP session. Record the source and destination IP addresses. What are the source and destination ports used for this HTTP session?
  - 2) Compare the TCP packets from the intranet host and the TCP packets captured on the internet gateway. How does NAT work for the HTTP session?

*Hint:* You may want to repeat steps 5, 6 and 7 to understand the operation of NAT. Clear the cache for the Internet Explorer before you repeat these steps.

# Laboratory Exercise: interference between Bluetooth and 802.11b

## Part I – Objectives and Lab Materials

### Objective:

The objectives of this lab are to: □ Illustrate the set up of a Bluetooth Piconet. □ Identify the potential interference between Bluetooth and 802.11b.

After completing the assignment, you should be able to: □ Set-up a Bluetooth connection between two or more nodes; □ Mitigate the interference of Bluetooth on 802.11b.

### Hardware to be used in this lab assignment:

☞ Xircom credit card Bluetooth adapter ☞ Xircom 802.11b adapter ☞ Dell Notebook

### Software to be used in this lab assignment:

□ Bluetooth connection manager □ Intellisync software □ *netperf* running on the notebooks

## Part II – Pre-lab Assignment

- Read the *netperf* manual installed in /root/WMSD/labs/lab\_6/netperf\_manual.pdf. Read sections 3,4,7 and 8. You will use *netperf* to measure the throughput. Alternatively, the *netperf* manual can also be obtained from <http://www.netperf.org/netperf/training/Netperf.html>.
- Write a script in Linux that invokes the netperf client (*netperf\_client*) to transfer UDP segments for 15 seconds. Ensure that the segment size is so chosen to avoid any IP fragmentation. Save the script in the /root/WMSD/labs/lab\_6 folder.
- Read the article by J. del Prado and S. Choi, “Experimental study on co-existence of 802.11b with alien devices,” Proceedings of the IEEE Vehicular Technology Conference, Atlantic City, October 2001.

## Part III – In-class lab assignment

We will study interference between Bluetooth and 802.11b. Students will form teams consisting of four groups (eight students). Two groups will be involved in the establishment of a Bluetooth Piconet and other two groups will be involved in the set-up of an ad-hoc network. We will study the difference in throughput for an ad-hoc connection in the presence of a Bluetooth piconet. The configuration is as shown in Figure 1:



Figure 1 - Experiment Set-up.

- The first task is to set-up the experiment. For this purpose, the two groups responsible for the set-up of an ad-hoc network will form the source and the receiver of the ad-hoc link. One group will be the *src* and the other will be the *dest*.
- Boot the two notebooks in Linux with the 802.11b cards in the PCMCIA slots. Use the *iwconfig* command in Linux to set the mode of operation to Ad-Hoc, ESSID to *wmsdgroupnumber* where *groupnumber* is the number of the group acting as *src*. Set the transmission power to 1mW or 0 dBm. Make a note of your settings. Set the IP address of the *src* and *dest* as 169.254.1.id\_of\_notebook where *id\_of\_notebook* is the id associated with your notebook. Set the channel of operation as assigned by the GTA to you.
- Establish an ad-hoc connection between the *src* and *dest*. Ping the *src* machine from the *dest* and capture a screen shot of the ping output, thereby validating the ad-hoc connection.

To introduce interference, we now establish a Bluetooth piconet around *dest* as shown in Figure 1.

- . Start by inserting the Xircom Bluetooth cards in the notebooks. One of the groups will act as the “master” of a Bluetooth Piconet and the other group will be the “slave.” After inserting the Bluetooth adapter in the PCMCIA slot, click on the “Bluetooth places” icon in the task bar. When the manager appears on your screen, check the properties of your card. This can be done by right clicking on the icon corresponding to the name of your notebook and clicking on the “Properties” button.
- . The properties of the Bluetooth device include name of the device, 48-bit MAC address of the Bluetooth adapter, device class and connection profile. Ensure that the encryption is off for the connection between the communicating devices. Note the MAC address of your device.
- . A Bluetooth device can be either in non-pairable mode or in pairable mode. In pairable mode the Bluetooth device accepts paring – i.e. creation of bonds – initiated by the remote device, and in non-pairable mode it does not. Set the pairable mode to “Bondable” on your device. After confirming the settings on the notebooks involved in the set up of the Bluetooth link, the group that is acting as master of the piconet should right-click on the “New” icon and click on the “Discover all” option (see Figure 2). The group acting as “slave” should right-click on the icon corresponding to the notebook name and

click on the “Discoverable” icon (see Figure 3). With this, the “slave” makes itself available to be discovered by the “master.” When the “slave” device is discovered, the details about it are displayed at the “master” under the “New” icon.

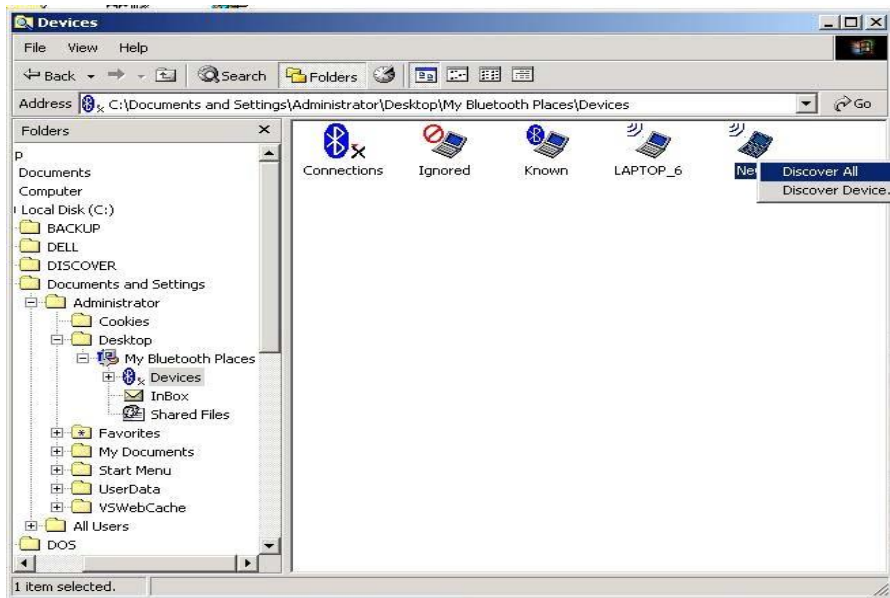


Figure 2- Snapshot of the master device’s “Bluetooth places” window.

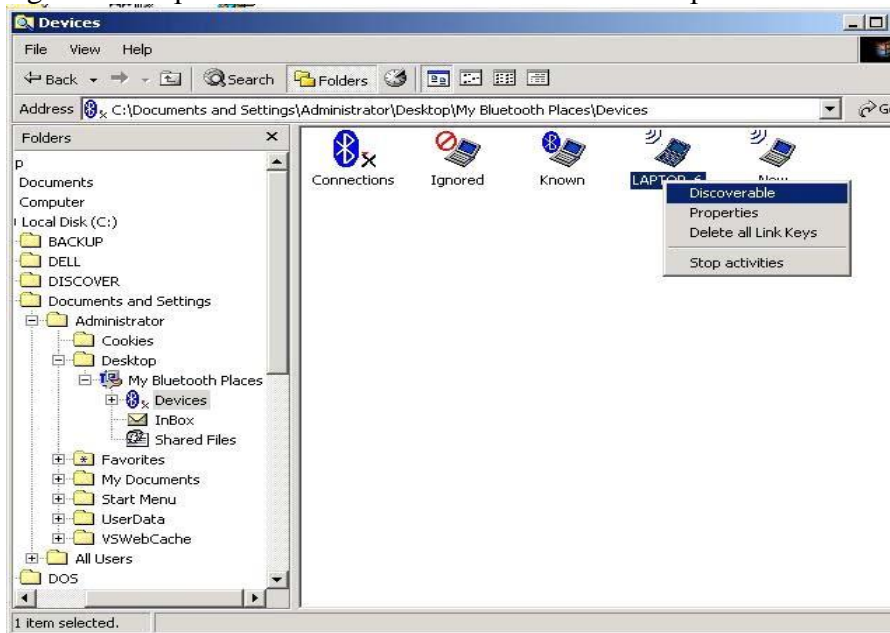


Figure 3- Snapshot of the slave device’s “Bluetooth places” window.


Double-click the “New” icon to display the discovered “slave.” Double-click on the “slave” and there will be a list of profiles available on that “slave.” Double-click on the “Intellisync” profile and there will be an option of establishing a one-time or a permanent connection. Establish a permanent connection between the “master” and the “slave” such that in the event of a



disconnection, the two devices will be connected again. Select the “permanent” radio button and click ok.

One of the main applications of Bluetooth is essentially looked as a “cable-replacement” technology; it provides emulation of serial data transfer between two devices. The Bluetooth devices that you have provide the emulation of serial ports. When you use the synchronization software, Intellisync, you make use of port COM 12. You have now established a Bluetooth piconet. The set-up of the experiment is now complete.

### Throughput measurements

- We will measure the throughput of the ad-hoc connection in the absence and then in the presence of Bluetooth interference using *netperf*. The *netperf* binary is located in `/usr/local/netperf` and is linked at `/usr/local/bin`, so it can be executed from any folder in Linux.
- . Stop the Bluetooth radio on both, the “master” and the “slave” devices. To stop the Bluetooth radio, right-click on the  icon in the task bar and then uncheck the “Radio on” option.
- Start the *netperf* server on the *dest* node by typing *netserver* in the terminal window. *netserver* is configured to listen to connections on port 12865. Run the *netperf* client script (*netperf\_client*) saved in the `/root/WMSD/labs/lab6` folder by typing `./netperf_client` in the terminal window on the *src* node.
- Measure the throughput returned by *netperf* for a data rate of 1Mbps. The data rate can be varied by using *iwconfig*. The signal level can be read by typing *iwconfig* in the terminal window. Take the measurement at a signal level of -60dBm at the *src* node. Perform three such data transfers using *netperf* and note down the throughput values for each such transfer.
- Capture a screen shot of the *netperf* terminal window for the report. The screen shot should be taken for only one of the three readings of throughput. In order to take a snapshot on Linux, click on the “K” icon in the taskbar and go to graphics>KSnapshot. Use KSnapshot to take a screen shot of the *netperf* window.

We now introduce interference in the form of a data transfer in the Bluetooth piconet.

- . Start the Bluetooth radio on the “master” and the “slave” device by clicking on the red icon in the task bar, as done above for stopping the Bluetooth radio. Right - click on the same red

icon in the task bar after your radio is “on” and click on “Open my Bluetooth places.” When the manager appears on your screen, on the “master” device, double-click on the “Connections” icon in the left hand frame. You will see the permanent connection being displayed as shown in Figure 4 below.

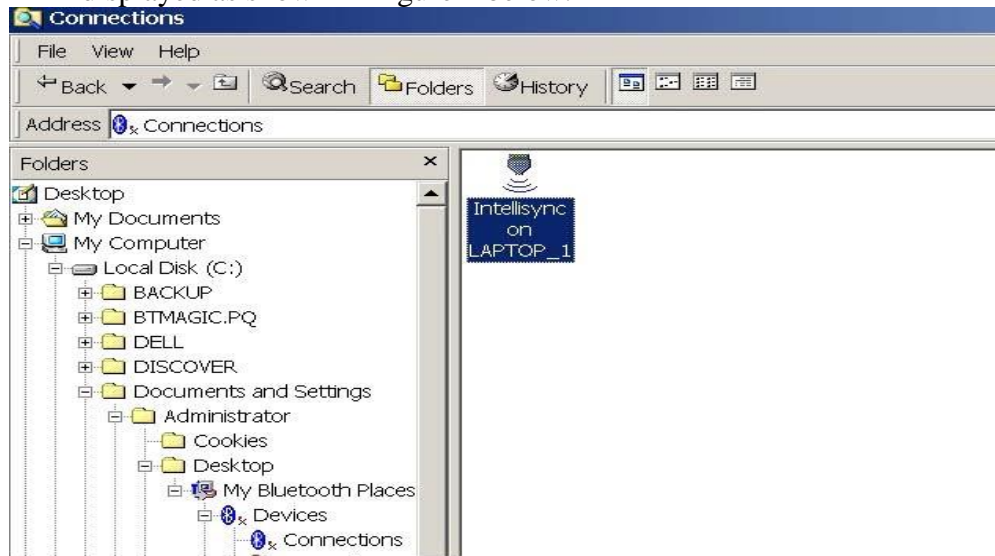


Figure 4- Snapshot of the “Connections” window under “My Bluetooth places”

- The “master” connects to the slave using Intellisync software. Start the Intellisync agent on both devices by going to Start>Programs>Intellisync>Intellisync agent. Using the Intellisync agent on the desktop, select ‘File Transfer’ icon on both the notebooks as shown in Figure 5.



Figure 5- Snap shot of the Intellisync agent

- . A connection will be established between the two Bluetooth devices with an accompanying sound. A security window will appear on the screen if the connection is being established for the first time. Under this security setting, select the “Security” tab and allow the remote user to access your inbox only. Select the “Inbox transfer only” button as shown in Figure 6.



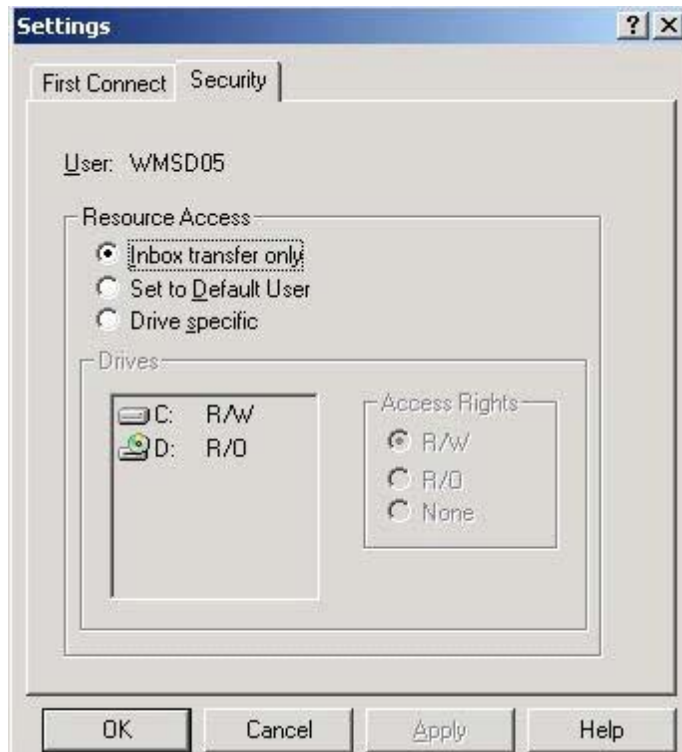


Figure 6- Snap shot of the security settings for Intellisync

- In order to start the data transfer, on the “slave” system, select the file “pockettvsetup-0.9.4.exe” in C:\WMSD\iPAQ and start its transfer to the “master” device. The file can be chosen from the right-hand side explorer window. Right click on the file and select the “master” as shown in Figure 7.

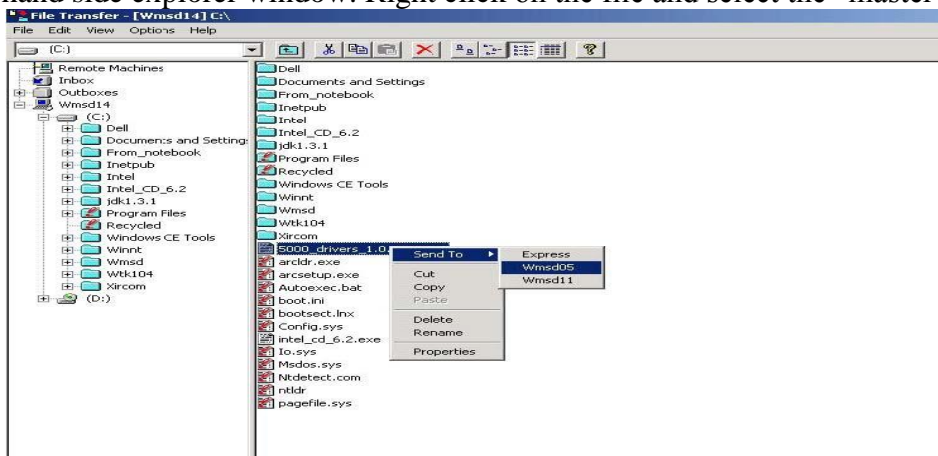


Figure 7- Snap shot of the File transfer explorer window.

- Here, Bluetooth interference is present in the form of data transfer between two devices. Now measure the throughput of IEEE 802.11b connection using *netperf*. Start the *netperf\_client* at the *src* and measure the throughput. While you measure the IEEE 802.11b throughput, ensure that the Bluetooth

devices are transferring data. Perform three such data transfers using *netperf* and note down the throughput values for each such transfer.

- Report the throughput for the adhoc connection. Capture a screen shot of the *netperf* terminal window, to be included in this week's report. The screen shot should be taken for only one of the three readings of throughput. In order to take a snapshot on Linux, click on the "K" icon in the taskbar and go to graphics>KSnapshot. Use KSnapshot to take a screen shot of the *netperf* window. Also take a snapshot of the Bluetooth data transfer.

Note: While transferring Bluetooth data for different data rates, delete the file being transferred after it is transferred to the "master" device and re-transfer the same file for different data rates.

- Repeat the above procedure of throughput measurements for different IEEE 802.11b data rates of 2Mbps and *auto*. Do this in the absence and in the presence of a Bluetooth connection. In order to change the data rate of the ad-hoc connection use *iwconfig*.

Note: *auto* data rate means that the IEEE 802.11b link will try to maintain a theoretical bandwidth of 11Mbps; however it may reduce to a bandwidth less than 11Mbps, depending on current channel conditions.

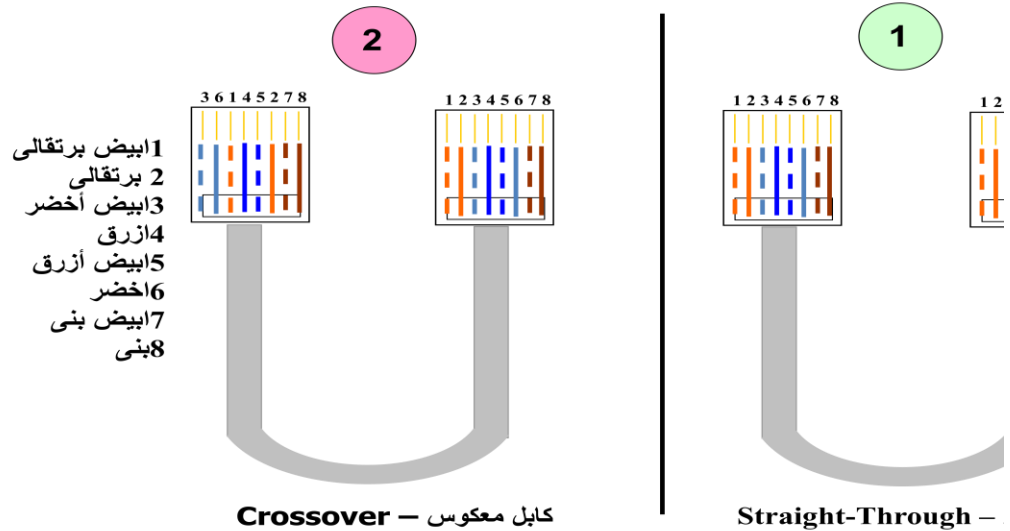
جربة (1) بطاقة الشبكة والكابلات المجدولة غير المغلفة

ولاً: التعرف على وظيفة وخصائص بطاقة مواجهة الشبكة NIC  
.....

ثانياً: الكابلات المجدولة غير المغلفة (UTP)، ووصلات (RJ-45)  
  
ثالثاً: تركيب وصلات RJ45 إلى كابلات UTP  
.....

إبعاً: تركيب كابل (UTP) نوع (Cross Cable)، ونوع (Drop Cable) .....  
  
خامساً: فحص كابلات UTP بعد تجهيزها  
.....

## Types of UTP cabling links in terms of the linking functionality



Crossover is used to

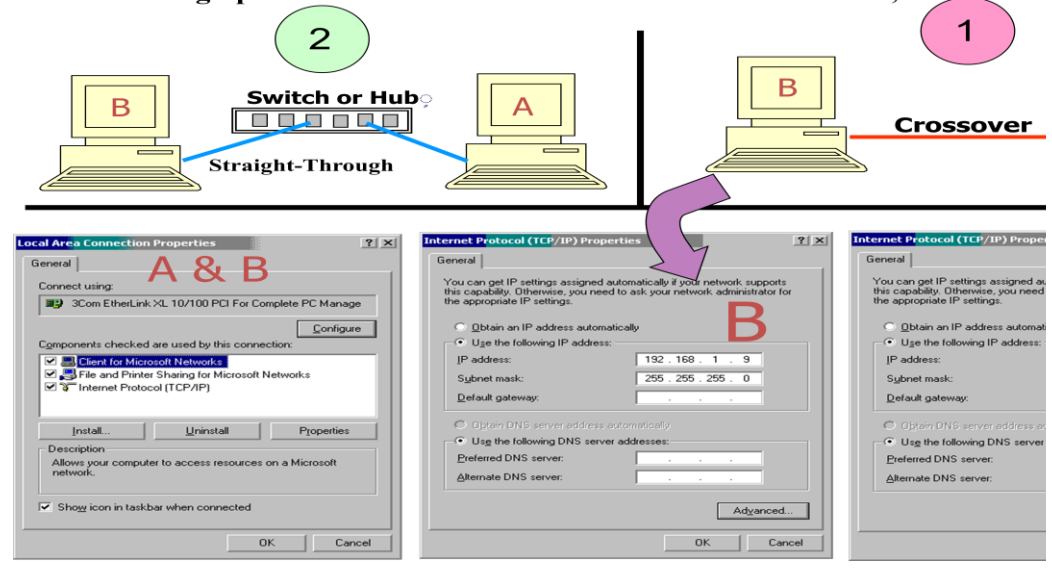
- 1 - Connect two computers with each other directly.
- 2 - Linking with the hop-hop.
- 3 - Switch link with the switch.
- 4 - Connect the router with the router.
- 5 - Hop link with the switch.

Straight – through U

- 1 - connect a compu a hop or switch.
- 2 - Connect with the or switch hop.

## Setting up a home network on the two devices in the home, in two different ways

Setting up a home network on the two devices in the home, in two diff



#### جربة (2) بناء شبكة بين جهازين وعناوين IP

ولاً: بناء شبكة مكونة من جهازي حاسب

.....

انئاً: عناوين IP وطرق الحصول عليها

.....

الئاً: استعراض أجهزة الحاسب المرتبطة بمجموعة العمل

.....

#### جربة (3) بناء شبكة نجمية نوع مجموعة عمل

ولاً: التعرف على وظيفة جهاز التوصيل المركزي Hub Switch

.....

انئاً: التعرف على طريقة بناء شبكة نجمية بين مجموعة أجهزة

.....

الئاً: التعرف على طريقة إنشاء مجموعات العمل

.....

إبعاً: البحث عن أجهزة الحاسب المرتبطة بمجموعة عمل

.....

#### جربة (4) الشبكات النجمية الخطية

ولاً: توسيع الشبكة المحلية باستخدام Hub Switch

.....

انئاً: ربط مجموعتي عمل باستخدام أقنعة شبكة متشابهة

.....  
ثالثاً: ربط مجموعتي عمل باستخدام أقتعة شبكة مختلفة  
.....

إبعاً: إرسال رسالة وحدة لتحكم  
.....

#### جربة (5) حسابات المستخدمين المحليين

ولاً: التعرف على حسابات المستخدمين المحليين المعدة مسبقاً  
.....

ثانياً: إنشاء حساب مستخدم محلي جديد  
.....

ثالثاً: إدارة حسابات المستخدمين المحليين  
.....

#### جربة (6) المجموعات المحلية وتعيين حقوق المستخدمين

ولاً: التعرف على المجموعات المحلية المعدة مسبقاً وصلاحياتها  
.....

ثانياً: إنشاء مجموعة محلية جديدة  
.....

ثالثاً: إضافة حسابات مستخدمين محليين إلى مجموعة محلية  
.....

إبعاً: تعيين حقوق المستخدمين من خلال المجموعات المحلية  
.....

خامساً: إعادة تسمية وحذف مجموعة محلية  
.....

#### جربة (7) بيئة تشغيل Windows XP Prof. متعددة المستخدمين

ولاً: دراسة التشكيل الجانبي لحسابات المستخدمين في ويندوز

.....

ثانياً: أمن وسرية مجلدات التشكيل الجانبي لحسابات المستخدمين المحلية .

ثالثاً: علاقة حسابات المستخدمين مع مجلدات التشكيل الجانبي الخاصة بها

.....

#### جربة (8) المشاركة على الأقراص و المجلدات

ولاً: إنشاء مشاركات على الأقراص المحلية والمجلدات باستخدام المعالج

.....

ثانياً: إلغاء المشاركات عن الأقراص المحلية والمجلدات باستخدام المعالج

.....

ثالثاً: طريقة أخرى لإنشاء المشاركات على الأقراص المحلية والمجلدات

.....

إبعاً: طريقة أخرى لإلغاء المشاركات على الأقراص المحلية والمجلدات

.....

خامساً: الوصول إلى المشاركات على حاسبات مجموعة العمل

.....

#### جربة (9) تثبيت وتشغيل خدمة DHCP على خادم Windows 2000 Server

ولاً: التعرف على وظيفة خدمة DHCP .....

ثانياً: التعرف على طريقة تثبيت خدمة DHCP .....

..... التعرف على طريقة تفعيل خدمة DHCP

جربة (10) ضم محطة عمل إلى شبكة نطاق

ولاً: خطوات ومتطلبات ضم محطة عمل (الحاسب) للعمل ضمن شبكة النطاق ....

ثانياً: كيفية الحصول على عناوين IP تلقائياً باستخدام بروتوكول DHCP .....

ثالثاً: التعرف على طريق استعراض محطات العمل الأعضاء في النطاق .....

إبعاً: أوامر بيئة التشغيل الخطية DOS في التعامل مع شبكة النطاق .....