

Department of CSE/IT
LAB MANUAL OF DATA COMMUNICATION
(DC)

Subject: DC
Semester: 4th

Code: CS-214
Branch: CSE

S No.	List of Practical	Page No.
1.	Familiarization with computer hardware	1-3
2.	Introduction with network Computing.	4-9
3.	Study of Peer to Peer networking	10-13
4.	Study the different Topologies used in LAN TCP/IP.	14-17
5.	Client/Server Architecture.	18
6.	Familiarization with transmission media viz coaxial cable, twisted pair cable, optical cable, connectors.	19-26
7.	Configuring Network Neighborhood.	27-34
8.	Sharing of resources with two connected nodes.	35-37
9.	Implementation of protocol & their configuration services.	38-42

EXPERIMENT NO. 5

NAME : CLIENT/SERVER ARCHITECTURE.

OBJECTIVE : TO UNDERSTAND CLIENT/SERVER ARCHITECTURE.

Centralized Computing -

Here the application operates on the server and all clients interact with the central application through client side interface terminals - dumb terminals when a client requests data from a database, the system moves all the data across the network to the client this causes the network to slow down for other clients

The Client –

The front end client runs an application that presents an interface to the user (this doesn't reside on the server at all) formats requests for data displays data it receives from the server. The user uses an on-screen form, called a search key to specify search requests the data can be presented to the user in various ways - different users access the same database to present information in a way that suits them Front End Tools query tools user applications e.g. Excel provides front end access to back end databases program development tools. Visual Basic is used to develop front end tools to access backend data.

The Server -

usually dedicated to STORING and MANAGING data most of the database activity happens on the server sorting data updates, additions, deletions, and protection .Stored procedures short, pre-written data-processing routines used by client applications stored on the server and can be used by any client one stored process can be called by any number of client applications instead of having to incorporate the same routine into the code of each program

Client / Server Architecture

- Single server
- Multiple servers with special tasks
- Distributed server arrangements

Servers across a WAN link synchronized to endure they all have the same data in common Data Warehouse. One server stores large amounts of data and forwards the most sought after data to intermediate servers that format the data. This off loads some of the processing from the intermediate servers that are contacted by clients

Advantages of the Client / Server Environment:-

Less network traffic => only results of query are sent over the network

The server is more powerful than the client and does most of the processing

More RAM and storage space on server means you don't have to spend as much MONEY on each client Back end data is more easily secured and BACKED UP

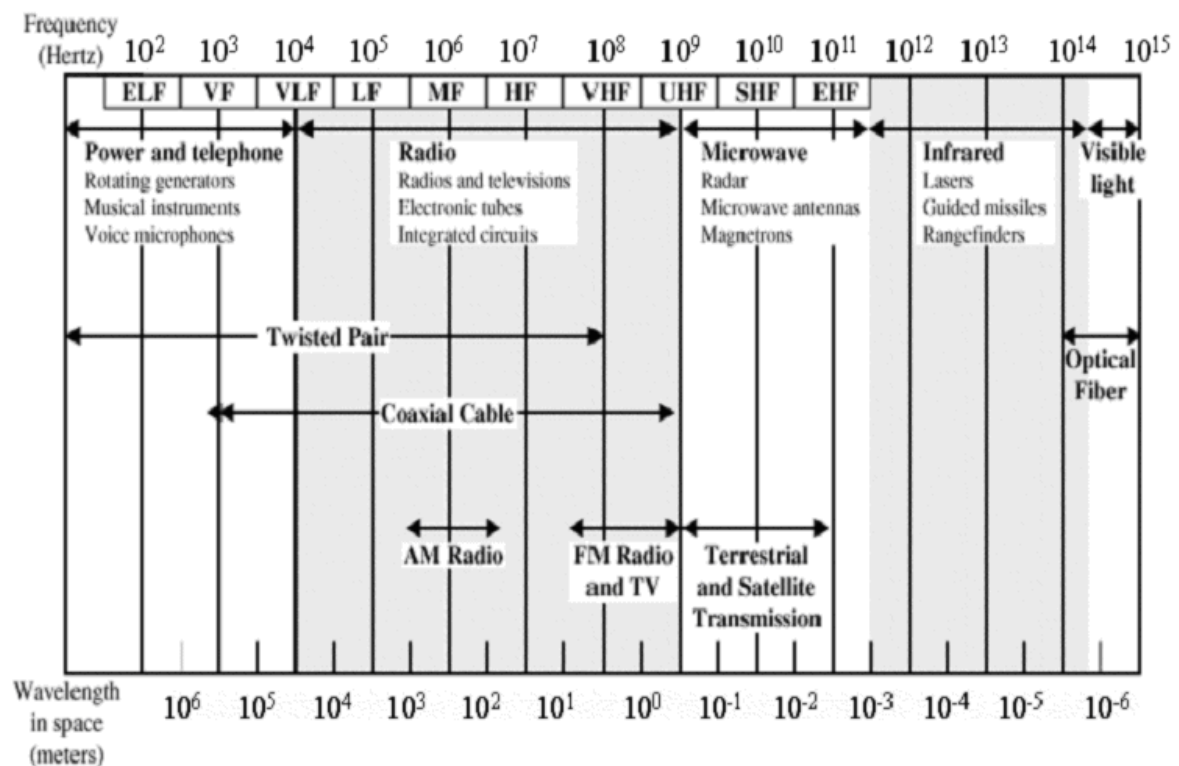
EXPERIMENT NO. 6

NAME : FAMILIARIZATION WITH TRANSMISSION MEDIA VIZ COAXIAL CABLE, TWISTED PAIR CABLE, OPTICAL CABLE, CONNECTORS.

OBJECTIVE :TO UNDERSTAND DIFFERENT TYPES OF TRANSMISSION MEDIA AND THEIR CONNECTORS.

The Electromagnetic Spectrum

All electronic communication operates within the electromagnetic spectrum travelling, theoretically, at the speed of light. That is 2.997925×10^8 metres per second. We have already seen that the velocity and strength over distance of electronic signals is affected by the transmission media and as such this media has to be selected carefully.



Electromagnetic Spectrum for Telecommunications

Media used for communication can be classified as guided or unguided.

Network Cabling:-

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will

utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

Unshielded Twisted Pair (UTP) Cable

Shielded Twisted Pair (STP) Cable

Coaxial Cable

Fiber Optic Cable

Wireless LANs

Cable Installation Guides

Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See fig. 1).

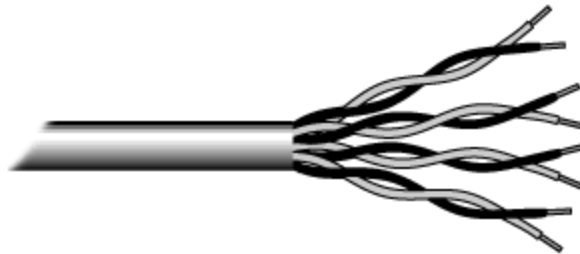


Fig.1. Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated five categories of wire.

Categories of Unshielded Twisted Pair

Type	Use
Category 1	Voice Only (Telephone Wire)
Category 2	Data to 4 Mbps (LocalTalk)
Category 3	Data to 10 Mbps (Ethernet)
Category 4	Data to 20 Mbps (16 Mbps Token Ring)
Category 5	Data to 100 Mbps (Fast Ethernet)

Buy the best cable you can afford; most schools purchase Category 3 or Category 5. If you are designing a 10 Mbps Ethernet network and are considering the cost savings of buying Category 3 wire instead of Category 5, remember that the Category 5 cable will provide more "room to grow" as transmission technologies increase. Both Category 3 and Category 5 UTP have a maximum segment length of 100 meters. In Florida, Category 5 cable is required for retrofit grants. 10BaseT refers to the

specifications for unshielded twisted pair cable (Category 3, 4, or 5) carrying Ethernet signals. Category 6 is relatively new and is used for gigabit connections.

Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

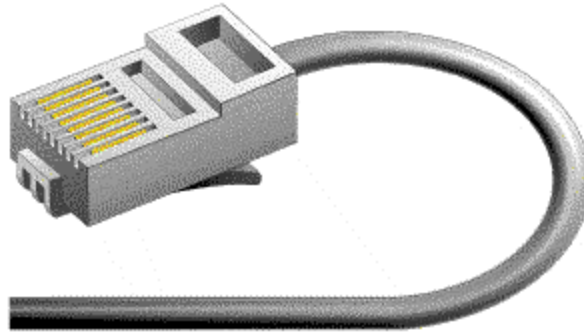


Fig. 2. RJ-45 connector

Shielded Twisted Pair (STP) Cable

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair (STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology.

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

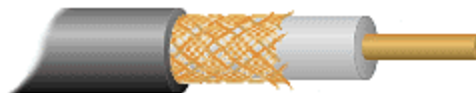


Fig. 3. Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable is popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayonet-Neill-Concelman (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather than screw, onto the cable.

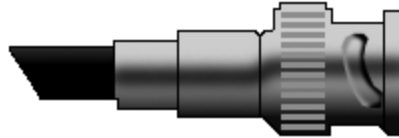


Fig. 4. BNC connector

Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 5). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

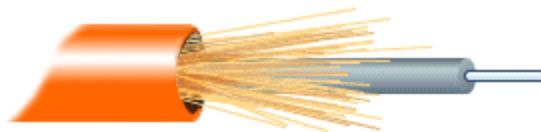


Fig.5. Fiber optic cable

Facts about fiber optic cables:

Outer insulating jacket is made of Teflon or PVC.

Kevlar fiber helps to strengthen the cable and prevent breakage.

A plastic coating is used to cushion the fiber center.

Center (core) is made of glass or plastic fibers.

Fiber Optic Connector

The most common connector used with fiber optic cable is an ST connector. It is barrel shaped, similar to a BNC connector. A newer connector, the SC, is becoming more popular. It has a squared face and is easier to connect in a confined space.

Ethernet Cable Summary

Specification	Cable Type	Maximum length
10BaseT	Unshielded Twisted Pair	100 meters
10Base2	Thin Coaxial	185 meters
10Base5	Thick Coaxial	500 meters
10BaseF	Fiber Optic	2000 meters
100BaseT	Unshielded Twisted Pair	100 meters
100BaseTX	Unshielded Twisted Pair	220 meters

Wireless LANs

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

Wireless networks are great for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Wireless LANs have several disadvantages. They provide poor security, and are susceptible to interference from lights and electronic devices. They are also slower than LANs using cabling.

Installing Cable - Some Guidelines

When running cable, it is best to follow a few simple rules:

Always use more cable than you need. Leave plenty of slack.

Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.

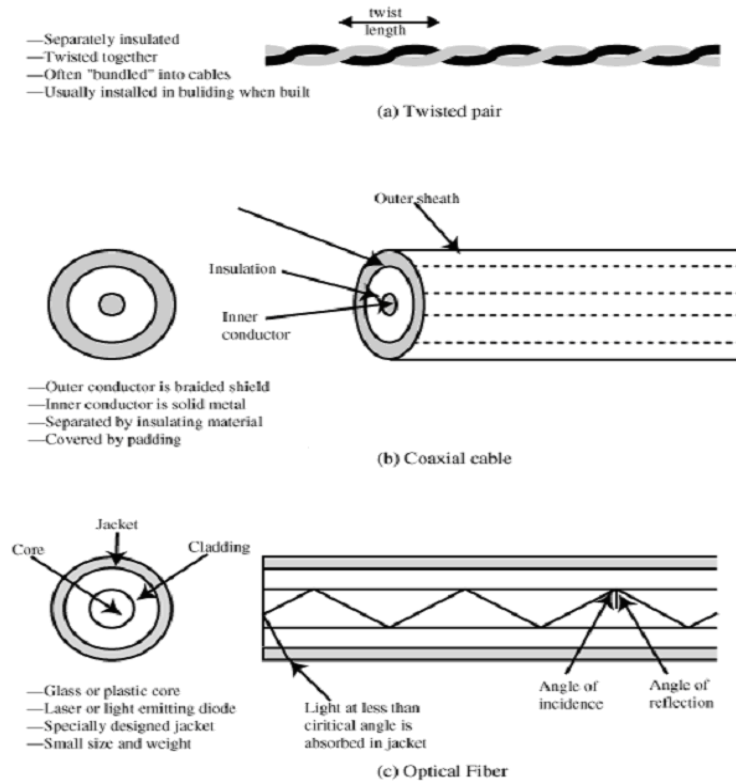
Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.

If it is necessary to run cable across the floor, cover the cable with cable protectors.

Label both ends of each cable.

Use cable ties (not tape) to keep cables in the same location together.





Guided Transmission Media

Unguided media - wireless transmission

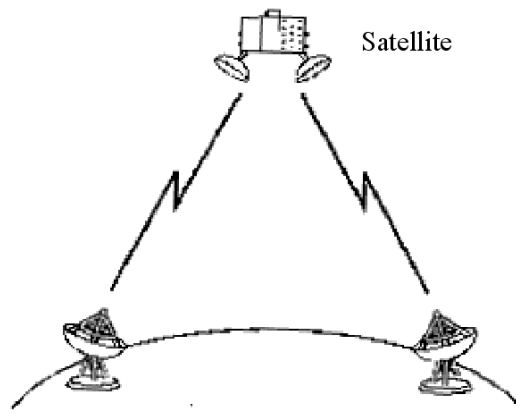
Wireless transmission radiates electromagnetic energy from antennae.

This can be directional - in a beam - or omnidirectional i.e. all around radiation.

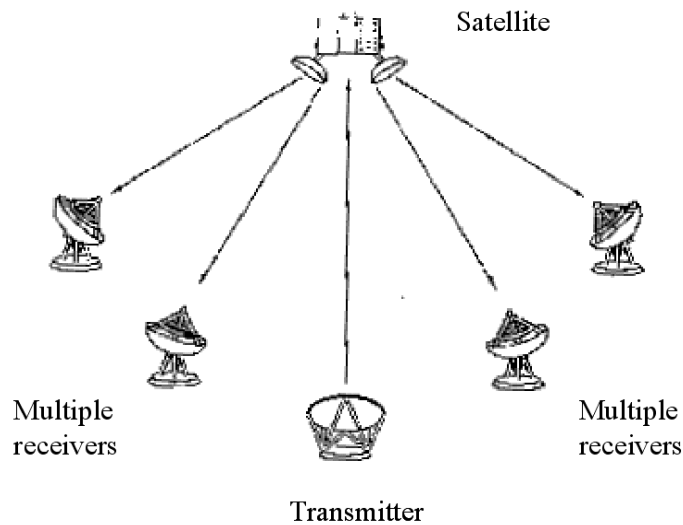
Terrestrial Microwave Communication is accomplished through line of sight parabolic dish antenna located on elevated sites.

Satellite Microwave

Overcomes the line of sight problems of terrestrial microwave and can be used for point to point or broadcast transmission. Uses an uplink and downlink frequency, a common frequency set is referred to as the 4/6 range which uses a downlink frequency of 4GHz and an uplink frequency of 6GHz.



Point-to-point link via satellite microwave



Broadcast link via satellite microwave

Typical uses of satellite microwave - television distribution, long distance telephone transmission, private business networks for global organisations.

Suffers the same attenuation problems as terrestrial microwave.

Broadcast radio transmission

Broadcast radio is omnidirectional and does not require complex dish antenna but allows a great deal of flexibility and is tolerant of alignment needs.

Covers the frequency range 3KHz to 1GHz. The concepts of broadcast radio are well known to the general public. Lower frequency signals are reflected off the ionosphere and this helps bounce signals between the atmosphere and the earth for wide reception coverage. Frequencies above 30MHz are not reflected from the atmosphere and rely on line of sight transmission.

Low frequencies are less susceptible to attenuation from atmospheric conditions but are affected by ionospheric changes.

Higher frequencies can be affected by reflection of signals.

Infrared transmission

Infrared communication is now common as a means of wireless communication between devices. It will not penetrate buildings and therefore is secure.

Used for very short line of sight transmission, remote car locking systems, wireless security alarms, remote TV channel changes etc.

EXPERIMENT NO. 7

NAME : CONFIGURING NETWORK NEIGHBORHOOD.

OBJECTIVE : TO UNDERSTAND HOW TO CONFIGURE NETWORK.

Configuring the Network:

1. Under Control panel/Network/identification make sure each computer has a unique name.
2. Make sure that workgroup is same for all computers.
3. Do not have any spaces in either the computer or workgroup names. Keep them simple.
4. Select different IP addresses for each computer. Use same subnet mask. If you are connecting to internet enter in gateway & DNS IP addresses.
5. Click on the file & print sharing button & check off whether you want to share files or Printers.

After configuring the Networking card on each computer, it is necessary to know how many systems have to be configured on network. If there are two systems on n/w then they have to be connected through cross cable otherwise a HUB or Switch have to be used to connect more than two computers.

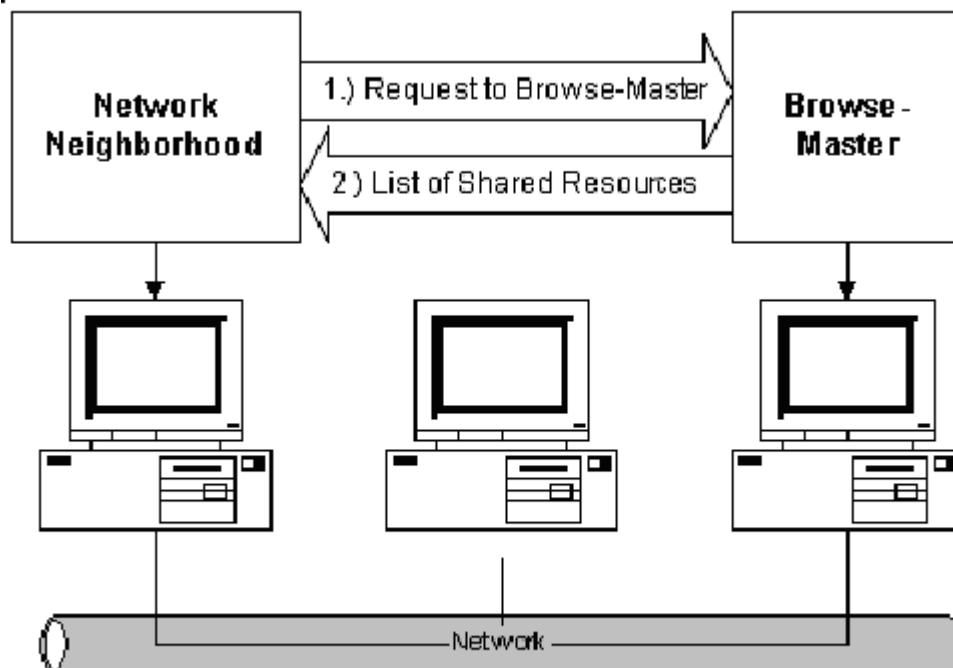
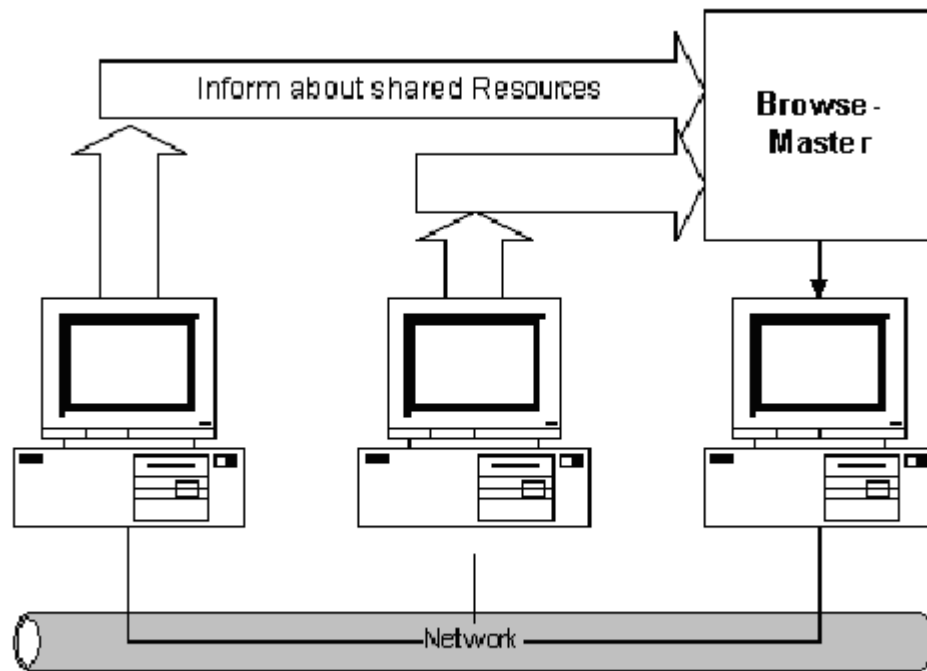
Trouble Shooting of NIC:

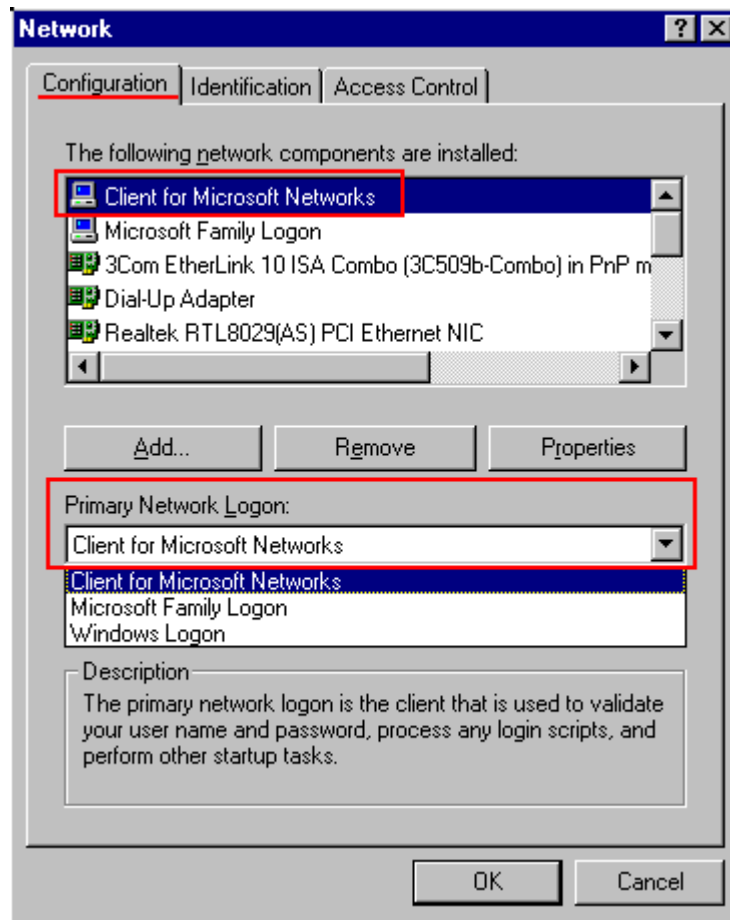
To check whether NIC is properly configured or not, open command prompt & type.

How does the "Network Neighborhood"/"My Computer Places" work ?

Please, spend the time to learn about this, it explains the sometimes strange behavior. On a network based on Microsoft networking, there MUST be for each workgroup one system acting as the book-keeper, this system is called the "*Browse-Master*". When you have a network of Windows95/98/ME/2000/XP systems and you switch on these systems, one of first things done by the network-software is to check on the network for the presence of a Browse-Master:

- If no Browse-Master is found, then a Browse-Master is elected.
- Only a system with "File-and-Printer Sharing" installed can be elected to become a Browse-Master
- On a network with a mixture of Windows95/98/ME and Windows NT/2000/XP systems, the "strongest system" wins the election and becomes the Browse-Master.
strength of Windows Versions :
 - Windows 3.x ----- > "weakest system"
 - Windows 95
 - Windows 98
 - Windows ME
 - Windows NT4 Workstation
 - Windows 2000 Workstation (internal name : NT 5.0)
 - Windows XP (internal name : NT 5.1) -----> "Strongest system"
- On a network with a Windows NT or 2000 server, the server becomes the Browse-Master, (a server is always "stronger" than a workstation)
- each system sends the list of available shared resources to the Browse-Master:

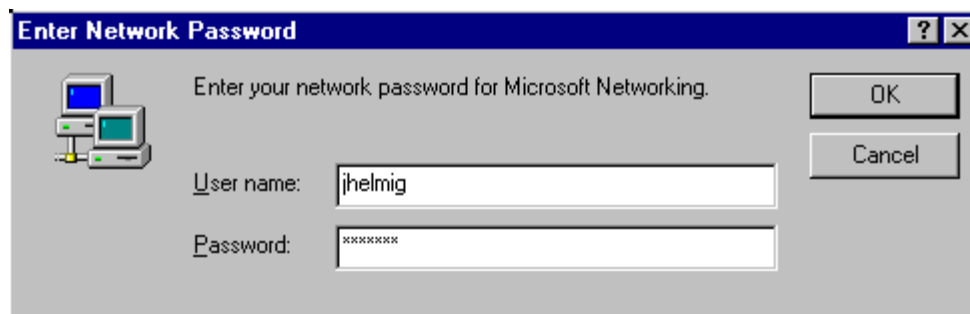




Important :
to be able to use
the network, it is
required on
Windows95/98/ME
to have as part of
the
Network
configuration the
"Client for
Microsoft
Networks"

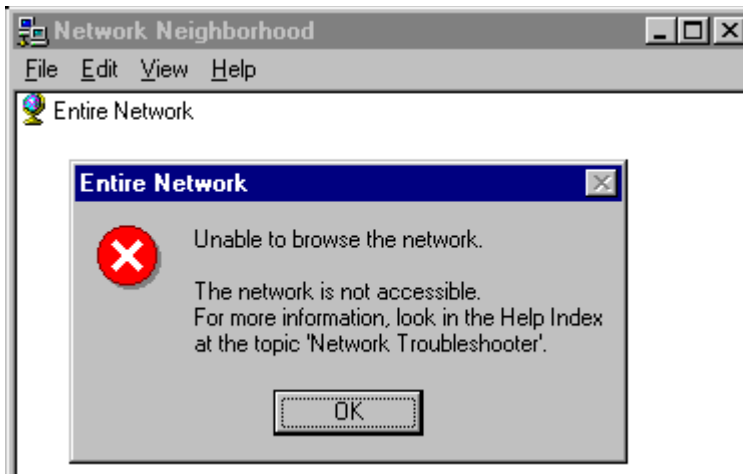
and you must
define as
"Primary Network
Logon" to use the
"Client for
Microsoft
Networks"

and when powering on / starting up your system , you must "Logon" to the system using the Network login ("Enter Network Password") :

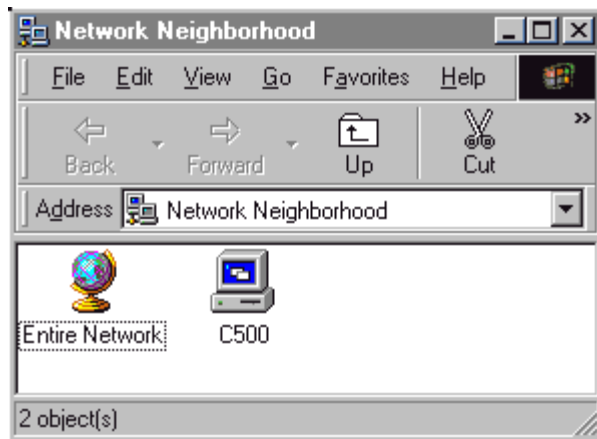


If you press the *ESC*-key or click on "Cancel" then you did NOT validate your network Username and will not have access to the network , i.e. you can not use the "Network Neighborhood"/"My Computer Places" !

This "Master Browser" configuration and its election process explains now some of the "strange" behavior of the Network-Neighborhood:



Your own system does NOT have "File-and-Printer Sharing" installed:
Your system could not find a "Browse-Master" on the network.



Your own system has "File-and-Printer Sharing" installed:
Only your own system is displayed, not any other system on the network.

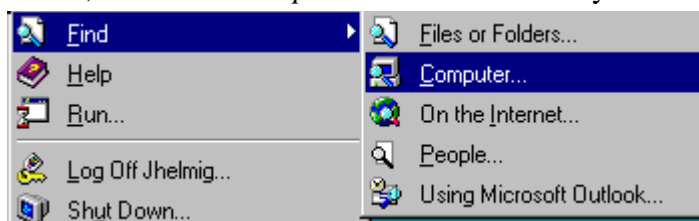
First: after switching on Windows, it can take a few minutes to elect the Browse-Master, it may help to close the "Network Neighborhood" and open it again after a few minutes.
Second: when a system is switched on or off later, it can take up to 15 minutes before the display-list of the Browse-Master is updated (for details, see the Resource-kit)

If you are still not getting a proper display, then check the following:

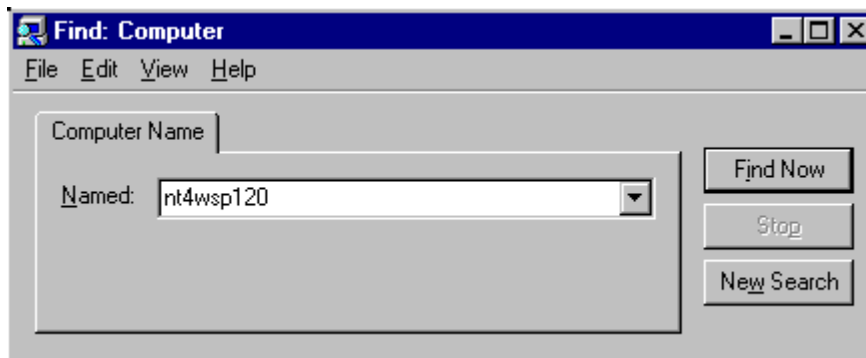
- verify, that all systems are defined to use the SAME workgroup.
- only systems with "File-and-Printer Sharing" installed and SOMETHING shared are displayed.
- test the network connection

There are some network configurations, where you can not use the Network Neighborhood, like on some Dialup-Network connections (via modem) or when using a Direct-Cable connection.

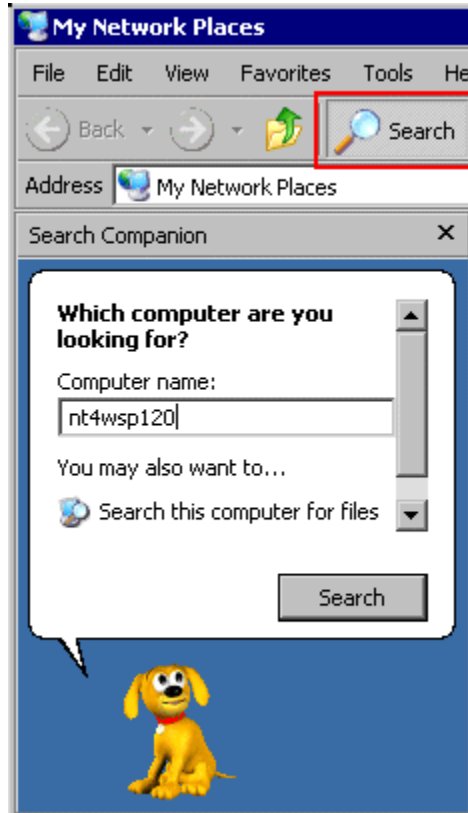
In such cases, use "*Find Computer*" to access other systems.



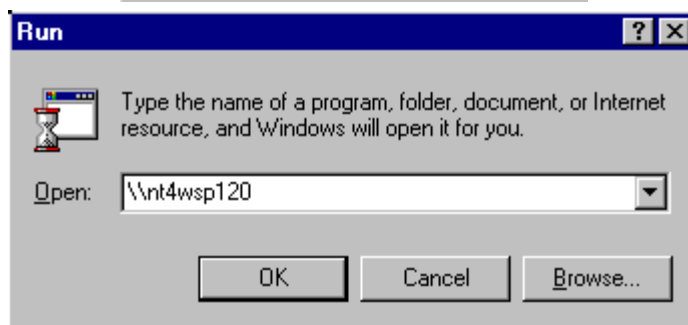
Select in the Windows menu "*Find*", then "*Computer*",



and enter the computername of the system to access , then use "Find Now". It will search the network, (not asking the Master Browser)



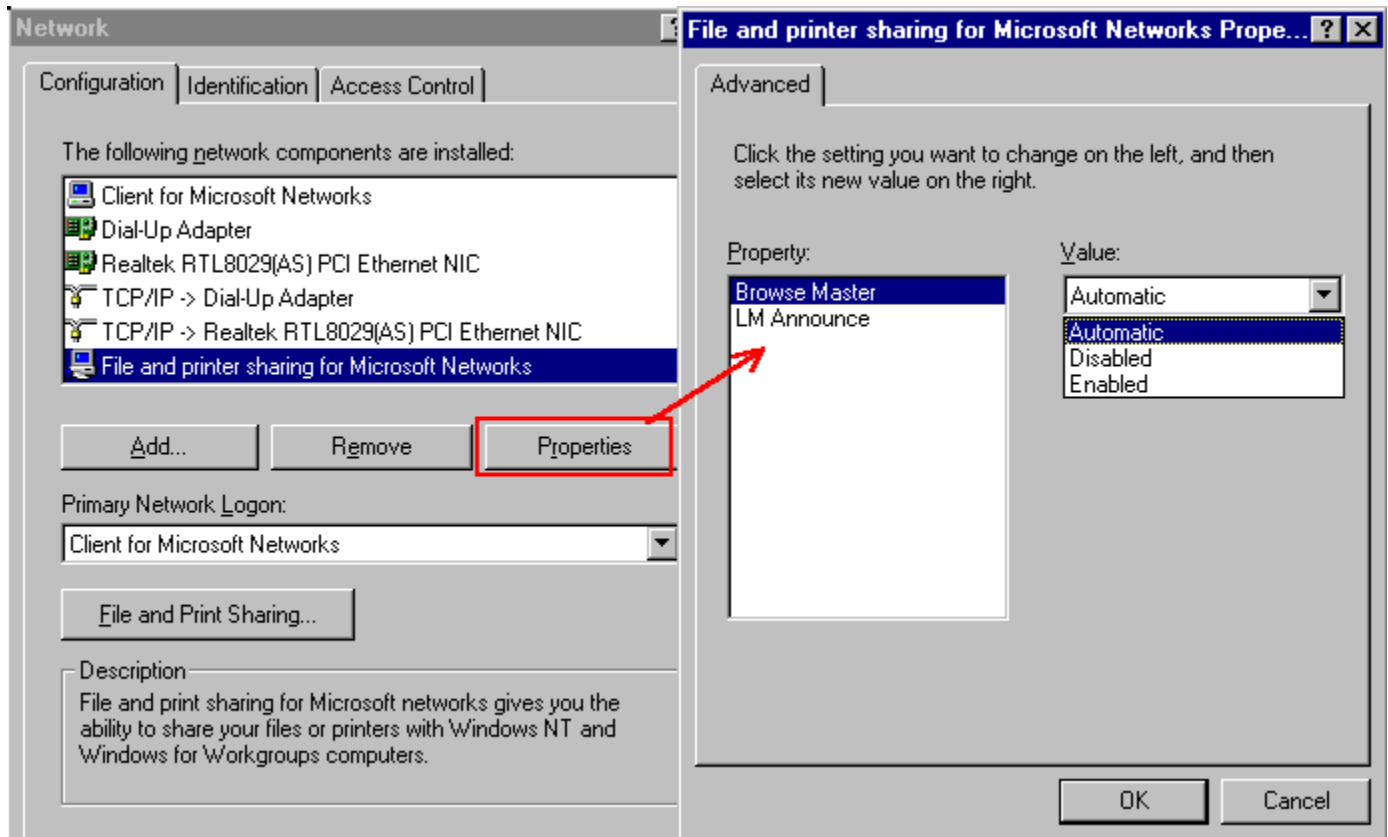
When using "My Network Places", use the "Search" button and then enter the system, which you like to access (with or without the help of Fido/Rover, the animated dog)



(all WIndows versions)

You can also search for a system by entering in the RUN- windows (on the windows menu) the computer-name preceded by double-backslash, like: \\nt4wsp120

On networks using TCP/IP-protocol, you can find out which system is acting as Browse-Master. If you like to control yourself, which system is acting as the Browse-Master :



view the "Properties" of the "File and Printer Sharing": by default, the setting for "Browse Master" is "Automatic", which is causing the systems to elect a Browse-Master.

You can name a system to be the Browse-Master by changing the "Browse Master" value to "Enabled", but then you MUST on ALL other systems in this workgroup change the value to "Disabled".

EXPERIMENT NO. 8

NAME :SHARING OF RESOURCES WITH TWO CONNECTED NODES.
OBJECTIVE:TO UNDERSTAND SHARING OF RESOURCES OF NETWORK.

COMPONENTS NEEDED:

1. A Computer with an operating system capable of peer-to-peer such as windows 95/98/XP/2000 Professional.
2. Communication protocols such as TCP/IP OR Net BEUI.
3. A physical interface for each computer.
4. Physical connectivity components such as cables & connections.
5. Three 10 Mbs Hubs.
6. A printer and printer cable.
7. Introduction to networking text.

(1). Setup at least two isolated groups of computer and have each of these computer share files with other members of their own group through a 10 Mbs Hub. Record the transfer times of these exchanges in order to document throughput. Then connect all the groups together into a shared central 10 Mbs hub to transfer files & compare the level of throughput with first configuration.

Begin by noting the hardware of our n/w ready to share resources via the Ethernet peer-to-peer connected. Now configure the Windows 98 software to allow sharing of hard disk 2 CD-ROM drives so that peers will have access to each.

a). Double-click on the My Computer Icon. Then right click the c: drive icon scroll half down the box & select sharing by clicking on it.

b). Now click the sharing tab at the right of this window. Select the shared as radio buttons & enter a share name in the text box as follows: h disk #where# is the same as the number following the last "." In your machine IP address. In other words name your shared hard drive as "h disk" followed by the host ID portion of m/c's IP address.

c). Now move down to the Access type area & select "full". Leave the Full Access password" text box blank in the password sections and click O.K. password confirmation window is displayed leave the entry blank & select OK at the top right position of the window.

d). The hard disk drive on computer should now be available to other members of the network. Note the c: drive icon has a hand under it to denote it is shared. Double-click on one of the icons that depicts other members of n/w. This should bring up a folder labeled as that node's hard disk.

(2). Now setup the CD-ROM Drive for sharing but allow read only access rather than full.

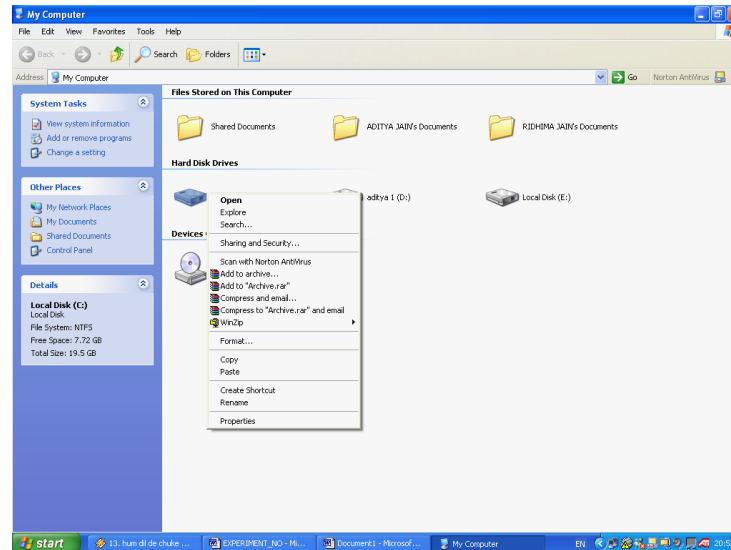
a). Double-Click on My Computer icon displayed on your computer screen. Then right click on D : drive icon. Scroll half-way down the box and select sharing by clicking on it.

b). Now click the sharing tab at the right of this window. Select the shared as radio button & enter a share name in the text box as follows: CD-ROM #where# is the same as no. following the last "." In

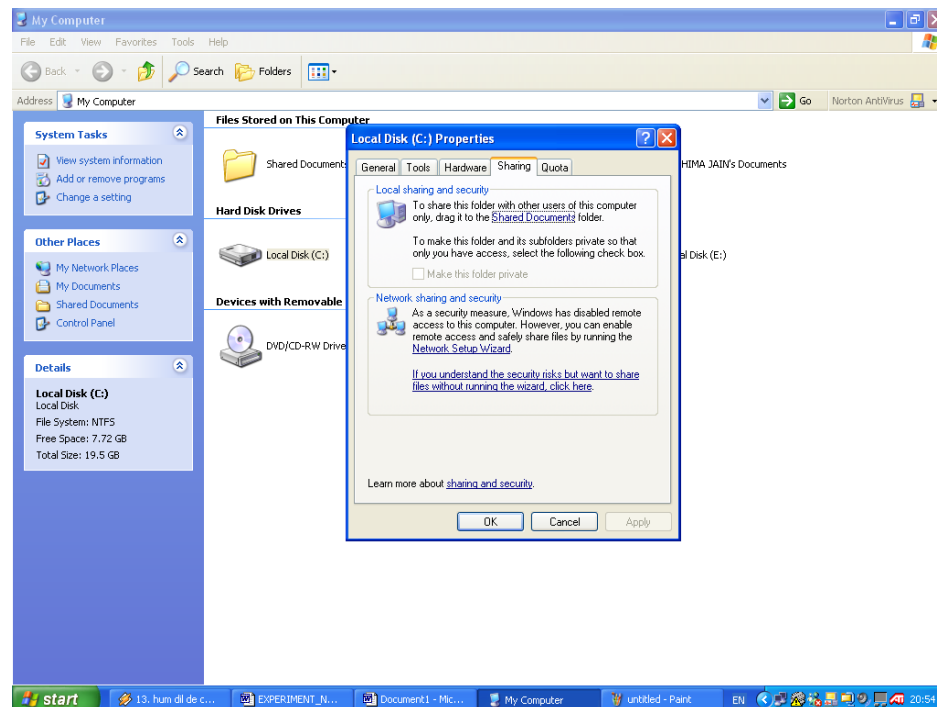
m/c's IP address. In Other words name your shared hard drive as "CD-ROM" followed by the host ID portion of the machines IP address.

c).Now move down Access type area & select read only. Leave the Read only password: text box blank in the password section & click O.K. If a password configure confirmation window is display leave the entry blank & select OK at the top right portion of the window.

d).CD-ROM Drive is the shared resources on the network. It is important to note that purpose of configuring desktop Operating System to allow for sharing of CD-ROM drive was to reinforce the procedure of sharing a resource.



Sharing is like this in XP
Then



this is how sharing can be done in XP

EXPERIMENT NO.9

NAME :IMPLEMENTATION OF PROTOCOL & THEIR CONFIGURATION SERVICES.

OBJECTIVE : TO UNDERSTAND HOW TO IMPLEMENT PROTOCOL AND THEIR SERVICES.

Services are the basic method of connecting to the server from any host or server .In general, a service is required on the server before any job.

Network Protocol:

A network protocol describes the data connected in Ethernet packet. The n/w protocol provided by server is completely different other than use of Ethernet of data layer. The following steps are followed to implement the protocol.

To add a protocol:

Select the adapter that will use the protocol from the display list, and then select add protocol.

To modify protocol configuration:

Select the protocol to modify from the displayed list, then select protocol configuration. Enter new configuration parameters as you did when adding protocols.

To view protocol configuration:

Select the protocol to view from displayed list, then select protocol view protocol configuration.

To remove a protocol configuration:

Select the protocol to remove from the displayed list, and then select protocol-to remove. We will be prompted to confirm choice & informed when the operation is completed.

Configuring & Implementation of TCP/IP protocol.

TCP/IP overview

Transmission Control Protocol/Internet Protocol (TCP/IP) is the most popular network protocol and the basis for the Internet. Its routing capabilities provide maximum flexibility in an enterprise-wide network. In Windows XP TCP/IP is automatically installed.

On a TCP/IP network, you must provide IP addresses to clients. Clients may also require a naming service or a method for name resolution. This section explains IP addressing and name resolution for Network Connections on TCP/IP networks. It also describes the FTP and Telnet tools that are provided by TCP/IP.

Assigning IP addresses to dial-up and virtual private network (VPN) connections

Each remote computer connecting to a remote access server on a Windows TCP/IP network is provided an IP address by the remote access server.

If you use a specific IP address, the remote access server must be configured to permit users to request a specific address.

Name resolution for network and dial-up connections

In addition to requiring an IP address, network and dial-up connections on a TCP/IP network may require a mechanism to map computer names to IP addresses. Four name resolution options are available: DNS, WINS, broadcast name resolution, and the Hosts files. In small networks where IP addresses do not change, network and dial-up connections can use a Hosts file for name resolution. By using these files on the local drive, you do not need to transmit name resolution requests to a WINS or DNS server and wait for the response. Internet tools/IP provides File Transfer Protocol (FTP) and Telnet. FTP is a character-based utility that permits you to connect to FTP servers and transfer files. Telnet is graphical application that lets you log in to remote computers and issue commands as if you were at the keyboard of the computer. Multiple variations of FTP, Telnet, and other programs based on earlier Internet standards are also available on the Internet or commercially.

For information about configuring a connection, see To configure a connection. For information about configuring TCP/IP, see To configure TCP/IP settings.

To configure TCP/IP settings

Open  Network Connections.

Click the connection you want to configure, and then, under Network Tasks, click Change settings of this connection.

Do one of the following:

If the connection is a local area connection, on the General tab, under This connection uses the following items, click Internet Protocol (TCP/IP), and then click Properties.

If this is a dial-up, VPN, or incoming connection, click the Networking tab. In This connection uses the following items, click Internet Protocol (TCP/IP), and then click Properties.

Do one of the following:

If you want IP settings to be assigned automatically, click Obtain an IP address automatically, and then click OK.

If you want to specify an IP address or a DNS server address, do the following:

Click Use the following IP address, and in IP address, type the IP address.

Click Use the following DNS server addresses, and in Preferred DNS server and Alternate DNS server, type the addresses of the primary and secondary DNS servers.

To configure DNS, WINS, and IP Settings, click Advanced.

To open Network Connections, click Start, click Control Panel, click Network and Internet Connections, and then click Network Connections.

You should use automated IP settings (DHCP) whenever possible, for the following reasons:

DHCP is enabled by default.

If your location changes, you do not have to modify your IP settings.

Automated IP settings are used for all connections, and they eliminate the need to configure settings such as DNS, WINS, and so on.

To install Simple TCP/IP Services

Open  Add or Remove Programs in Control Panel.

Click Add/Remove Windows Components.

In Components, click Networking Services, and then click Details.

In Subcomponents of Networking Services, click Simple TCP/IP Services, and then click OK.

Click Next.

If prompted to do so, type the path where the Windows XP distribution files are located, and then click OK.

Click Finish and then click Close.

To open Add or Remove Programs, click Start, click Control Panel, and then click Add or Remove Programs.

You must be logged on as an administrator or a member of the Administrators group in order to complete this procedure. If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.

Simple **TCP/IP** Services for Windows XP provides support for the optional **TCP/IP** protocol services listed in the following table.

Protocol	Description	RFC
Character Generator (CHARGEN)	Sends data made up of the set of 95 printable ASCII characters. Useful as a debugging tool for testing or troubleshooting line printers.	864
Daytime	Returns messages containing the day of the week, month, day, year, current time (in <i>hh:mm:ss</i> format), and time-zone information. Some programs can use the output from this service for debugging or monitoring variations in system clock time or on a different host.	867
Discard	Discards all messages received on this port without response or acknowledgment. Can serve as a null port for receiving and routing TCP/IP test messages during network setup and configuration or, in some cases, can be used by programs as a message discard function.	863
Echo	Echoes back data from any messages it receives on this server port. Can be useful as a network debugging and monitoring tool.	862
Quote of the Day (QUOTE)	Returns a quotation as one or more lines of text in a message. Quotations are taken at random from the following file: <code>systemroot\System32\Drivers\Etc\Quotes</code> . A sample quote file is installed with the Simple TCP/IP Services. If this file is missing, the quote service fails.	865

All of these protocol services are classified as elective Internet standards and are defined and described in the specified Request for Comments (RFC) document listed in the table. For more information on these protocol services, see the RFCs.

Do not install Simple TCP/IP Services unless you specifically need this computer to support communication with other systems that use these protocol services.

After Simple TCP/IP Services are installed, you cannot enable or disable the separate services individually.

To force a network adapter to acquire an IP address

Open  Network Connections.

Click the icon for the adapter that connects this computer to the Internet or to other network computers.

Under Network Tasks, click Repair this connection.

To open Network Connections, click Start, click Control Panel, click Network and Internet Connections, and then click Network Connections.

Internet Connection Sharing, Internet Connection Firewall, Discovery and Control, and Network Bridge are not available on Windows XP 64-Bit Edition.

If you are having difficulty connecting the Internet Connection Sharing (ICS) host to the Internet, you can use Repair to obtain refreshed IP address configurations from your Internet service provider (ISP).

If a computer on your network is unable to communicate with other network computers, you can use Repair to force the connection to refresh its IP address configuration from the ICS host.


If the icon for the shared Internet connection does not automatically appear on a client computer (and the Allow other network users to control or disable the shared Internet connection check box has not been disabled), it may be because ICS has not assigned an IP address to your network adapter. An IP address is required in order for a client computer to use ICS Discovery and Control features, connect with to the Internet, or to communicate with other computers on the network.

When ICS is enabled, it automatically provides an IP address for the ICS host's private connection. The ISP assigns an IP address to the shared Internet connection.

Before using the Repair menu command on the ICS host computer, ensure that you have plugged in the adapter that is used for the Internet connection.

Before using the Repair menu command, ensure that the client computer is plugged into the network and that the ICS host is running, configured, and connected to the network.

To test a TCP/IP configuration by using the ping command

To quickly obtain the TCP/IP configuration of a computer, open  Command Prompt, and then type ipconfig. From the display of the ipconfig command, ensure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.

At the command prompt, ping the loopback address by typing ping 127.0.0.1.

Ping the IP address of the computer.

Ping the IP address of the default gateway.

If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.

Ping the IP address of a remote host (a host that is on a different subnet).

If the ping command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.


Ping the IP address of the DNS server.

If the ping command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

To open command prompt, click Start, point to All Programs, point to Accessories, and then click Command Prompt.

If the ping command is not found or the command fails, you can use Event Viewer to check the System Log and look for problems reported by Setup or the Internet Protocol (TCP/IP) service.

The ping command uses Internet Control Message Protocol (ICMP) Echo Request and Echo Reply messages. Packet filtering policies on routers, firewalls, or other types of security gateways might prevent the forwarding of this traffic.

The ipconfig command is the command-line equivalent to the winipcfg command, which is available in Windows Millennium Edition, Windows 98, and Windows 95. Windows XP does not include a graphical equivalent to the winipcfg command; however, you can get the equivalent functionality for viewing and renewing an IP address by opening  Network Connections, right-clicking a network connection, clicking Status, and then clicking the Support tab. Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

To run ipconfig, open the command prompt, and then type ipconfig.

To open Network Connections, click Start, click Control Panel, click Network and Internet Connections, and then click Network Connections.