**Introduction**

\*What is communication.

\*Mode of communication(simplex,half-duplex,duplex).

\*Component of communication(sender, receiver , message , protocol). What is networking.

\*Types of networking, etc.

**Familiarization with different networking device**

**1. Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

**2. Hub** –  A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.  In other words, [collision domain](https://en.wikipedia.org/wiki/Collision_domain) of all hosts connected through Hub remains one.  Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

• Active Hub :- These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.

• Passive Hub :- These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend distance between nodes.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

• Transparent Bridges :- These are the bridge in which the stations are completely unaware of the

bridge’s existence i.e. whether or not a bridge is added or deleted from the network , reconfiguration of

the stations is unnecessary. These bridges makes use of two processes i.e. bridge forwarding and bridge learning.

• Source Routing Bridges :- In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a specical frame called discovery frame, which spreads through the entire network using all possible paths to destination.

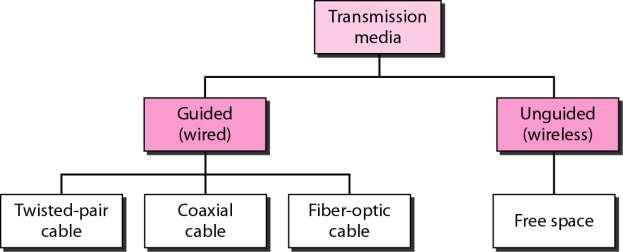
4. Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

**TRANSMISSION MEDIA**

Transmission media can be divided into two broad categories:



Guided media is the one which provides a conduit from one device to another; include twisted pair cable, co-axial cable and fiber optic cable.

Twisted and co-axial use metallic (Cu) conductor that transport signals in the form of electric current, whereas optical fiber is a glass or plastic cable and transport signal in the form of light.

Twisted Pair Cable (100 Hz to 5 MHz

Frequency range of Twisted Pair Cable is 100 Hz to 5 MHz. Twisted pair cable comes in two forms:

1>Unshielded Twisted Pair (UTP), 2> Shielded Twisted Pair (STP).

**Unshielded Twisted Pair (UTP)**

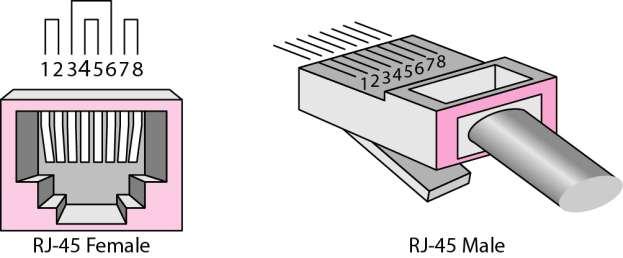
UTP is the most common type of telecomm. Medium and is use in telephone system, which consists of two conductor (Cu), each with of different plastic color insulation to identify specific conductor.

**Advantage of UTP**

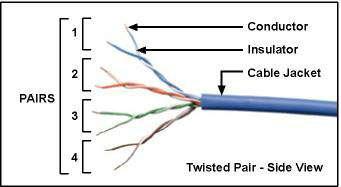
UTP is cheap, flexible and easy to install, higher grade of UTP are used in many LAN technologies.

UTP cable standards

**UTP connector**



UTP is most commonly connected to n/w devices via a snap-in plug like RJ45 connector with 8 conductors.



**Shielded Twisted Pair(STP)**

STP has a metal foil or braided-mesh covering that encases each pair of insulated conductors. The metal casing prevents the penetration of electromagnetic noise.

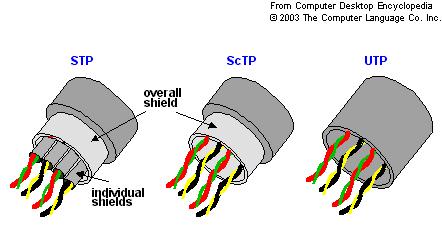
Through the use of STP we can eliminate the phenomenon called ***crosstalk.***

STP has the same quality consideration as UTP.

STP is more expensive than that of UTP but less susceptible to noise.

**STP connector**

STP Uses same connectors as UTP but shield must be connected to groun



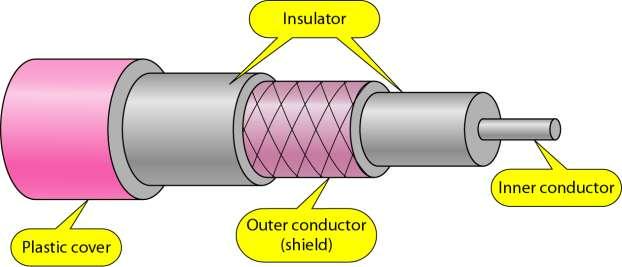
**Co-axial cable (100 KHz to 500 MHz)**

Coaxial cable carries signal of higher frequency ranges (100 KHz – 500 MHz) Introduction

Coax has a central core conductor of solid or stranded wire enclosed in an insulating sheath, which in turn, encased in an outer conductor of metal foil, braid, or a combination of two (usually copper).

The outer metallic wrapping serves both as a shield against noise and second conductor which completes the circuit.

The outer conductor is also enclosed in an insulating sheath and the whole cable is protected by a plastic cover.



Coaxial cable standards

Different coaxial cable designs are categorized by the Radio Government (RG) ratings. Each denotes a unique set of physical specifications, including wire gauge, the thickness and type of inner insulator.

The following are:

RG – 8, RG – 9, RG – 11: Used in thick Ethernet.

RG – 58:00 Used in thin Ethernet.

RG – 59: Used for TV.

**Coaxial cable connectors**

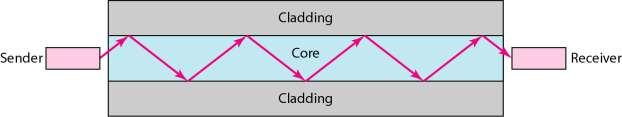
There are number of connectors available for coax some of them are

***BNC*** *(bayonet n/w connector)*

***T-connectors*** which allow secondary cable to branch off from main line

***Terminators*** used in Bus topologies.

**OPTICAL FIBER**



Optical fiber is made of glass or plastic and transmits signals in the form of light.

A core is surrounded by cladding, forming the fiber. Fiber is covered by a buffer layer that protects it from moisture; finally the entire cable is encased in an outer jacket.

Both core and cladding can be made either of glass or plastic but must be of different densities. The inner core must be completely regular in size and shape.The outer jacket can be made either of Teflon coating, plastic coating, fibrous plastic, metal tubing etc. each of which has its own purpose and depends on where the cable is to be installed.

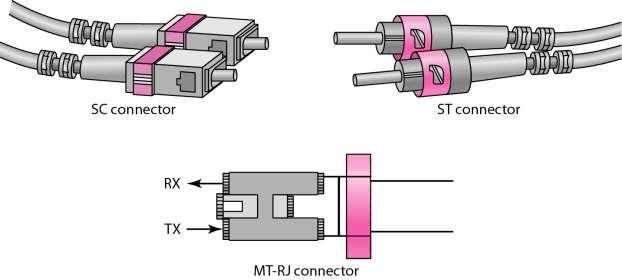
Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic.

The difference in density of the two materials must be such that a beam of light through the core is reflected off the cladding instead of being refracted into it.

There are two types of Propagation Modes:

The purpose of fiber optic cable is to contain & direct a beam of light from source to target. For transmission, the sending device must be equipped with a light source & the receiving device with a photosensitive cell.

The light source can be either LED or ILD (Injection Laser Diode)



***Advantages of Optical fiber***

Noise Resistance

Less signal attenuation

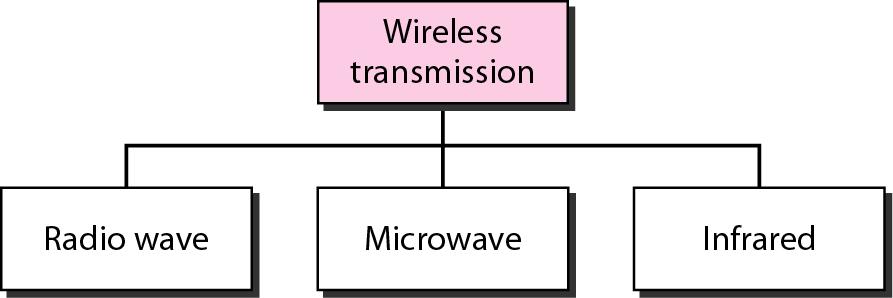
Higher Bandwidth

***Disadvantages of Optical fiber***

Cost

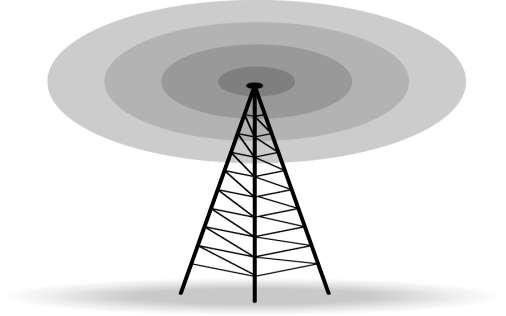
Installation/maintenance

Fragility or delicate



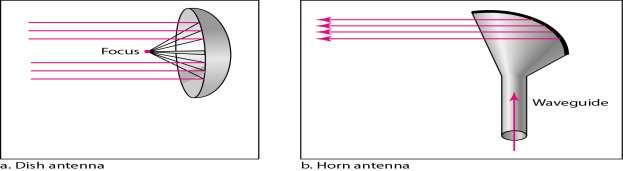
**RADIO WAVES**

Radio waves are used for multicast communications, such as radio and television, and paging systems. They can penetrate through walls. Highly regulated. Use omni directional antennas.



**MICROWAVES**

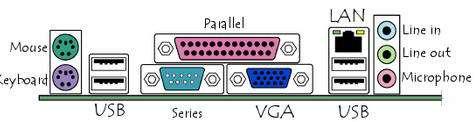
Microwaves are used for unicast communication such as cellular telephones, satellite networks,and wireless LANs.Higher frequency ranges cannot penetrate walls.Use directional antennas -point to point line of sight communications.



**INFRARED**

Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

**The input-output connectors.**



The motherboard has a certain number of input/output sockets found on

the rear panel.

Most motherboards have the following connectors:

A serial port for connecting old peripherals.

A parallel port manily for connecting old printers;

Usb Ports (1.1 -low speed, or 2.0, high-speed), for connecting more

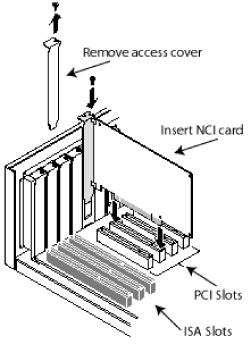
recent peripherals;

**RJ45 connector** (called*LAN*or*ethernet port*) used forconnecting thecomputer to a network. It corresponds to a network card integrated into the motherboard;

**VGA connector** (called*SUB-D15*), for connecting a monitor. Thisconnector interfaces with the built-in graphics card;

**Audio plugs** (*Line-In*,*Line-Out*and*microphone*), for connecting soundspeakers or a hi-fi system, as well as a microphone. This connector interfaces with the built-in

**Different types of slots-**PCI slots are white, ISA slots are black.



Lab-5: LAN CONFIGURATION

Use the following steps to setup your LAN connection in Windows XP,

when your computer is the device plugged in to your wireless radio or POE.

Note: - You will need your static IP settings and DNS settings before you

continue. If you don't have your settings, call into support so we can

provide them to you.

1. First, go to the start menu and into Control Panel.



2.Once in Control Panel, if you are in Category view, click on "Switch to

Classic View" in the top left



3. Now that you are in classic view, find and double click on Network

Connections.

4. Now that you are in Network Connections, right click on your Local Area

Connection, and left click on properties.

5. In the Local Area Connections properties window, highlight Internet

Protocol, and click on the properties button.

6. In the Internet Protocol (TCP/IP) Properties window, you will need to

select "Use the following IP address" and "Use the following DNS server

addresses:"

Enter in the corresponding settings per their section. If you don't have the

settings, or need help with them, call into tech support so we can provide

them to you.

7. Once the settings have been entered in, click ok on the Internet Protocol

(TCP/IP) Properties window, then click on close on the Local Area

Connections properties window.

At this point the Local Area Connection should say connected. See if you

can browse to a web site at this time. If you are able to, your setup is

complete. If you are not able to browse, call us here at tech support, so we

can verify your settings are correct.

**LAN SETUP AND MONITORING**

Objectives

� Learn to create a simple LAN with two PCs using an Ethernet hub

and two straight-through cables to connect the workstations

� Learn to configure and verify the network connectivity.

� Learn about various network related commands

Setting up a simple networkIn this experiment, we will learn how to connect two PCs to create a simple

Peer-to-Peer network. The instructions for this Lab focus on the Windows

2003 operating system. You will share a folder on one workstation and

connect to that folder from the other workstation. This Lab is divided into

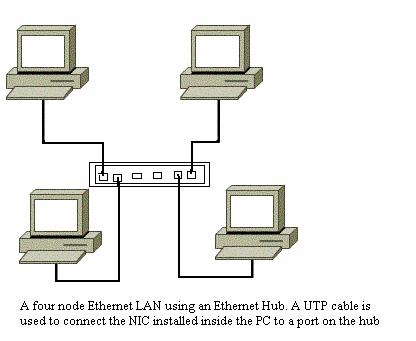
two exercises as follows:

Exercise: The two PCs will be connected with a hub between them [Refer

Figure ]. Using a hub allows for more than just two workstations to be

connected depending on the number of ports on the hub. Hubs can have

from 4 to 32 ports.



**Network Connection via Hub**

**Tools / Preparation:** The workstations should have Network Interface

Cards (NIC) installed with the proper drivers. The following resources will

be required:

1. Two Pentium-based workstations with a NIC in each (NIC drivers

should be available)

2. An Ethernet hub (4 or 8 port) and two CAT5 straight-wired cables.

**Check Local Area Network Connections**

Task: Verify the cables.Explanation: You should check the cables to verify that you have good

layer 1 physical connections.

Exercise: Check each of the two CAT 5 cables from each workstation to

the hub. Verify that the pins are wired straight through by holding the two

RJ-45 connectors for each cable side by side with the clip down and

inspect them. All pins should have the same color wire on the same pin at

both ends of the cable. (Pin 1 should match pin 1 and pin 8 should match

pin 8 etc.)

**Plug in and connect the equipment**

Task: Check the workstations and hub for exercise.

Exercise: Check to make sure that the NICs are installed correctly in each

workstation. Plug in the workstations and turn them on. Plug the straight

through cable from workstation 1 into port 1 of the hub and the cable from

workstation 2 into port 2 of the hub. After the workstations have booted,

check the green link light on the back of each NIC and the green lights on

ports 1 and 2 of the hub to verify that the are communicating. This also

verifies a good physical connection between the Hub and the NICs in the

workstations (OSI Layers 1 and 2). If the link light is not on it usually

indicates a bad cable connection, an incorrectly wired cable or the NIC or

hub may not be functioning correctly.

**Network Adapters and Protocols**

Task: Check the Network Adapter (NIC): Use the Control

Panel**--->**System-->Device Manager utility to verify that the Network Adapter

(NIC) is functioning properly for both workstations. Double click on Network

Adapters and then right click the NIC adapter in use. Click Properties to

see if the device is working properly.

Explanation: If there is a problem with the NIC or driver, the icon will show

a yellow circle with an exclamation mark in it with (possible resource

conflict) or a red X indicating a serious problem (device could cause

Windows to lock up).

**Check the TCP/IP Protocol Settings**

Task: Use the Control Panel/Network Connections (or Properties in

Context Menu of My Network Places) to display Network Connections

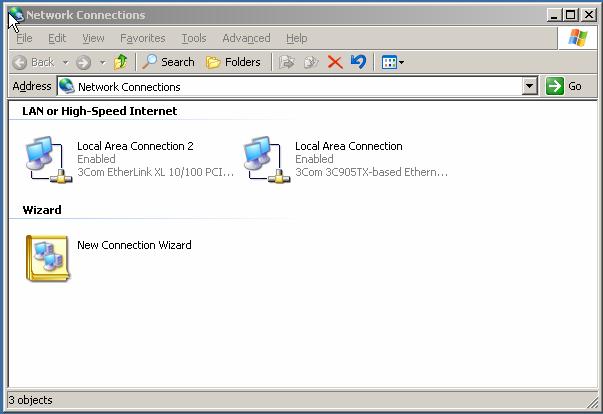
Window. Then use Properties in Context Menu of Local Area Connection to

display Local Area Connection Properties Window. Select the TCP/IP

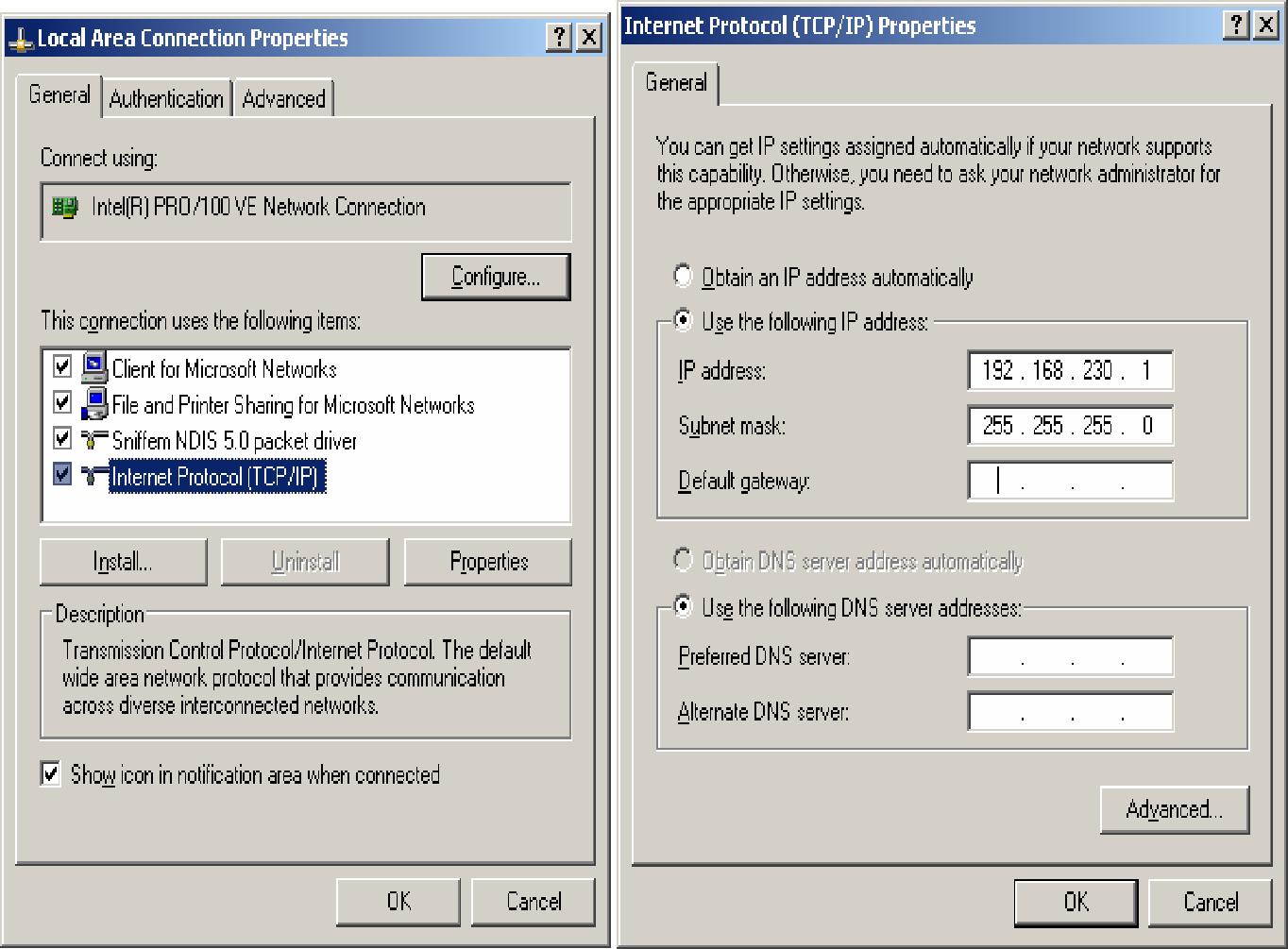
protocol from the Configuration Tab and click on properties. Check the IP

Address and Subnet mask for both workstations on the IP Address Tab.

Network Connections Window



TCP/IP Properties Window



Explanation: The IP addresses can be set to anything as long as they are

compatible and on the same network. Record the existing settings before

making any changes in case they need to be set back (for instance, they

may be DHCP clients now). For this lab, use the Class C IP network

address of 192.168.230.0 and set workstation 1 to static IP address

192.168.230.1 and set workstation 2 to 192.168.230.2. Set the default

subnet mask on each workstation to 255.255.0.0. For the purpose of this

lab, you can leave the Gateway and DNS Server entries blank.

**NETWORKING COMMANDS OF UNIX**

The following information consists of various UNIX networking and system

administration commands that you may wish to learn. This is not a formal

homework, itis just something I suggest you investigate at least a little for your own

edification.

Please read the man pages and try to experiment with the commands

when possible. You

need root access to do some of the commands, but you can at least look at

the man pages

to see how the programs operate. For example, use

> man arp

to read the man page on arp.

For now I just want you to be aware of the commands and have an idea of

what they do.

If you need to learn a program in more detail you at least have a place to

start. Being a

sysadmin is tough and it can take a long time to really learn how everything

works.

Most of the programs for the UAA math system (i.e. saturn, mazzy) are

stored in

/usr/sbin.

This will be different for other operating systems. For example, SunOS

stores most of

these in /usr/etc instead.

You might want to add /usr/sbin to your path if you can‟t execute them. If

you

are using saturn with bash, then add :/usr/sbin to the end of your PATH in

your .profile

file.

Common System Administrator files and commands

Network Status commands

running error stats + counts on config interface every N seconds

–a

socket ports and state

-s

protocol (tcp etc.) counts and errors

-r

routing table dump

–i

list of interfaces and gives 3 letter interface namesIf you use the –n flag, host addressed will be numeric and avoid a DNS

lookup,

which might be faster in some cases. Combine with the other switches.

Network interfaces commands

–a

Show all interfaces

setup for a particular interface, e.g. ln0

Set params of the interface. Root only. Typically IP address, subnet,

are set upon bootup in /etc/rc\*

ROOT ONLY

Connectivity

send an ICMP echo message (one packet) to a host.

This may go continually until you hit Control-C.

Ping means a packet was sent from your machine via ICMP, and echoed at

the IP level. ping tells you if the OS is up; but doesn't tell you if inetd or

other daemons are running.

talk to "hosts" at the given port number. By default, the telnet

port is port 23. See the file /etc/services for a list of what

services are in use at what ports. A few samples:

7 – echo port, use control-] to get out

25 – SMTP, use to send mail

79 - Finger

-number

Can tell if inetd is functioning. With telnet you can use the ip number

instead of the host name. If ip-number as opposed to telnet hostname

works, you have problems with the name server. If you can ping, but you

can't telnet, you have problems with getting processes running and

possibly inetd configuration problems.

Routing

–r

Print routing tables. The routing tables are stored in the kernel and used

by ip to route packets to non-local networks.

The route command is used for setting a static (non-dynamic by handroute) route path in the route tables. It is typically used at boot in the

/etc/rc scripts. It can be used for setting a default route; i.e., when in doubt

send all packets to a particular local gateway. Generally ROOT ONLY.

The BSD daemon that does dynamic routing. Started at boot. This runs

the RIP routing protocol. ROOT ONLY. You won‟t be able to run this

without root access.

Gated is an alternative routing daemon to RIP. It uses the OSPF, EGP,

and RIP protocols in one place. ROOT ONLY.

Useful for tracing route of IP packets. The packet causes message to be

sent back from all gateways in between the source and destination.

Arp

–a

Print the arp table. Arp is used to translate IP addresses into Ethernet

addresses. Root can add and delete arp entries. Deleting them can be

useful if an arp entry is malformed or just wrong. Arp entries explicitly

added by root are permanent -- they can also be by proxy. The arp table is

stored in the kernel and manipulated dynamically. Arp entries are cached

and will time out and are deleted normally in 20 minutes.

NFS/NIS

Network file system/yellow pages

Shows your filesystem and mount for the current directory

-t nfs

Show nfs mounts.

Use to mount a file system, ROOT ONLY.

/etc/fstab contains the mounts done at boot time.

/etc/exports contains mount points exported on a suste,/

/etc/mtab contains the mount table built by mount.

Other Useful Commands

List of processes in action, usage varies from system to system.

“ps -aux | grep <string> “ often useful to filter output by string

List your processes in the foreground.

Makes queries to the DNS server to translate IP to a name, or vice versa.Transfer files to host. Often can use login=“anonymous” , p/w=“guest”

Rcp performs a remote copy from one system to another, and is used

much

like Unix cp. Rcp and rsh use rshd which is controlled by inetd. The rshd

security protocol is very weak, and uses the .rhosts and /etc/hosts.equiv

files. Since security is so weak these protocols are often banned from

systems (e.g., add “\*” to rhosts and anyone could log into your account).

BSD remote shell.

-l <login>

Logs into the host with a virtual terminal like telnet.

Important Files

/etc/hosts - names to ip addresses

/etc/networks - network names to ip addresses

/etc/protocols - protocol names to protocol numbers

/etc/services - tcp/udp service names to port numbers

Not all programs use these services.

ROOT ONLY

daemons started at boot:

inetd

inetd is the BSD mother daemon that listens on the apps in /etc/inetd.conf

and makes connections for these other daemons.

sendmail

Sendmail runs the SMTP mail protocol on tcp port 25. If you telnet

to port 25, you are talking directly to sendmail. Some old configurations

allowed forgeries to be made in this fashion (mail relaying) but that has

been mostly disabled today.

**Installation and working of Telnet (TerminalNetwork)**

Hardware Required:

LAN Card, LAN drivers, 2-computers, Modem, Cables

Theory:

Its an abbreviation for ―Terminal Network‖. Telnet is a protocol that allows a user to

log on to other computers. You use an IP address or domain name to log on. Bulletin

boards are still available to play games, download files or read information. In addition,

you can play games with your friends over this type of network. Telnet is not as

common as it once was. Nevertheless, it is a simple method of connecting to different

friends or online communities.

Telnet is a user command and an underlying TCP/IP protocol for accessing remote

computers. Through Telnet, an administrator or another user can access someone

else's computer remotely. On the Web, HTTP and FTP protocols allow you to request

specific files from remote computers, but not to actually be logged on as a user of that

computer. With Telnet, you log on as a regular user with whatever privileges you may

have been granted to the specific application and data on that computer. A Telnet

command request looks like this (the computer name is made-up):

telnet the.libraryat.whatis.edu

The result of this request would be an invitation to log on with a user-id and a prompt for

a password. If accepted, you would be logged on like any user who used this computerevery day. Telnet is most likely to be used by program developers and anyone who has

a need to use specific applications or data located at a particular host computer.

Procedure:

1. Go to “My Computer” right click and select properties.

2. Then go to Manage. In the opened window select “Services and Application” then

select ―Telnet‖ from right hand side of window.

3. In property window of telnet set “start-up” box to “Automatic”

4. Go to Start->All Programe->Accessories->Command prompt

5. In “C:” prompt(C:\>) type telnet and type the IP of the 2nd computer after space.

Eg: telnet 192.27.24.1

6. Enter username and password of 2nd computer when prompted.

7. To quit type “exit”

Properties of Telnet:

net works on password protected system

Telnet service must be “ON” on both the system

Result:

The experiment completed successfully accessing of system which is for possible

telnet.