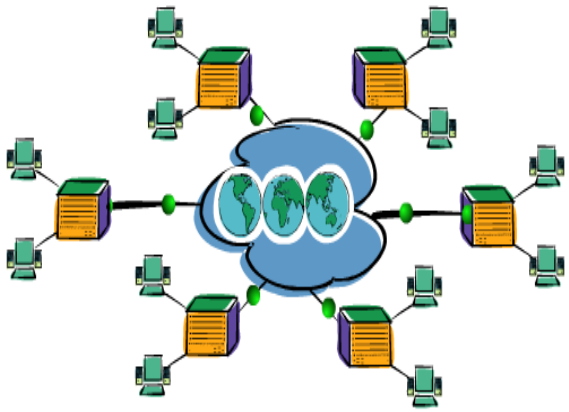
King Fahd University of Petroleum and Minerals

Department of Electrical Engineering

EE 400

TELECOMMUNICATIONS NETWORKS



Laboratory Manual

July 2003

Preface

A set of experiments will be carried out to demonstrate and complement the course material. Network design principles and influential factors are emphasized throughout the lab work. A network design package (ConfigMaker) is utilized is two experiments to design simple and core networks. Many network design architecture (peer-to-peer, client/server, point-to-point) are demonstrated/implemented. After carrying out all the experiments, the student is expected to acquire a good hands-on experience in network design, configuration and troubleshooting.

TABLE OF CONTENTS

Experiment # 1

Sampling and Quantization

Objective:

Study sampling, quantization and re-construction of a signal using Matlab Simulation.

Sampling Theorem and Quantization:

The sampling theorem states that if the highest frequency in the signal spectrum is B (Hz), the signal can be reconstructed from its samples, taken at a rate not less than 2B samples per second. This means that in order to transmit the information in a continuous-time signal, we need only transmit its samples as shown in figure 1. Unfortunately, the sample values are still not digital because they lie in a continuous range and can take on any one of the infinite values in the range. This difficulty is resolved by a process called "**quantization**", where each sample is approximated, or rounded off to the nearest quantized level, as shown in figure 1. Amplitudes of the signal m(t) lie in the range (-mp, mp), which is partitioned into L intervals, each of magnitude $\Delta v = 2m_p / L$. Each sample amplitude is approximated to the midpoint of the interval in which the sample value falls. Each sample is now approximated to one of the L numbers. The information is thus digitized.

The quantized signal is an approximation of the original one. We can improve the accuracy of the quantized signal to any desired degree by increasing the number of levels L.

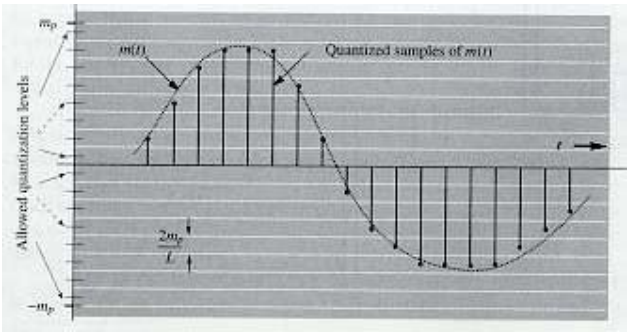


Figure 1: Sampling of a Signal.

MATLAB functions used in this Simulation:

The details for the matlab commands and functions that may be useful in this simulation experiment are given below.

zeros

ZEROS Zeros array.

ZEROS(N) is an N-by-N matrix of zeros.

ZEROS(M,N) or ZEROS([M,N]) is an M-by-N matrix of zeros.

ones

ONES Ones array.

ONES(N) is an N-by-N matrix of ones.

ONES(M,N) or ONES([M,N]) is an M-by-N matrix of ones.

filter

FILTER One-dimensional digital filter.

Y = FILTER(B,A,X) filters the data in vector X with the filter described by vectors A and B to create the filtered data Y. The filter is a "Direct Form II Transposed" implementation of the standard difference equation:

a(1)*y(n) = b(1)*x(n) + b(2)*x(n-1) + ... + b(nb+1)*x(n-nb)
- a(2)*y(n-1) - ... - a(na+1)*y(n-na)

If a(1) is not equal to 1, FILTER normalizes the filter coefficients by a(1).

plot

PLOT Linear plot.

PLOT(X,Y) plots vector Y versus vector X. If X or Y is a matrix, then the vector is plotted versus the rows or columns of the matrix, whichever line up. If X is a scalar and Y is a vector, length(Y) disconnected points are plotted.

stem

STEM Discrete sequence or "stem" plot.

STEM(Y) plots the data sequence Y as stems from the x axis terminated with circles for the data value.

STEM(X,Y) plots the data sequence Y at the values specified in X.

quant

QUANT Discretize values as multiples of a quantity.

QUANT(X,Q) takes these inputs,

X - Matrix, vector or scalar.

Q - Minimum value.

and returns values in X rounded to nearest multiple of Q

fft

FFT Discrete Fourier transform.

FFT(X) is the discrete Fourier transform (DFT) of vector X. For matrices, the FFT operation is applied to each column. For N-D arrays, the FFT operation operates on the first non-singleton dimension.

FFT(X,N) is the N-point FFT, padded with zeros if X has less than N points and truncated if it has more.

ifft

IFFT Inverse discrete Fourier transform.

IFFT(X) is the inverse discrete Fourier transform of X.

IFFT(X,N) is the N-point inverse transform.

IFFT(X,[],DIM) or IFFT(X,N,DIM) is the inverse discrete Fourier transform of X across the dimension DIM.

Exercise:

The following Signal is given:

$X = \cos(2\pi f_1 T)+(2/3)*\cos(2\pi f_2 T)-(2.5/3)*\cos(2\pi f_3 T)$

using Matlab;

(1) Generate a train of pulses, use the impulse response of a comb filter H(z)=1/(1-(z)^-4)

(2) Sample the given signal

(3) Quantize the sampled signal

(4) Use a low pass filter to reconstruct the original signal.

Submit the hard copy with figures and soft copy of the program.

Experiment # 2
Transmission Media & Networking Components

Objectives:
Study different types of networking cables, connectors and other network components.

Transmission Media (refer to text book, sec 3.7)
Computers communicate data in a network over a medium. The choice of the medium is very critical since it affects the network cost, maximum operating speed, and error rates. Network media should be durable, rodent-proof, reliable, inexpensive, immune to noise, and easy to install, maintain, and reconfigure. The longer the transmission distance, the lower the maximum speed.

Transmission Media Types:

***Air*:** The transmission of data is performed using radio waves, infrared, or laser light. The advantage of this medium is that it eliminates cabling. The disadvantages are:

- Need of an unobstructed line-of-sight path between nodes.
- Light signal are susceptible to interference from fog, and smoke.
- Data can be intercepted (security problems).

***Twisted-Pair (TP)*:** It consists of two insulated wires twisted together. Most of the telephone lines use TP. The twisting tends to expose each wire in the pair to the interference uniformly. Wires have an American Wire Gauge (AWG) number based on their diameter. For network purposes, 22-and 24-gauge are two most common types of twisted-pair cabling. Twisted-pair cable is bundled in groups of pairs, many LANs use 25 pairs. The advantages of TP is that they are:

- Available in many forms at low prices.
- Relatively easier to install.
- Used extensively in telephone lines.

***Shielded Twisted-Pair (STP)*:** It has improved noise immunity and crosstalk and has better system security.

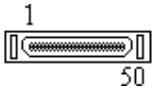
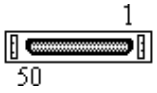
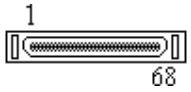
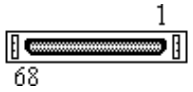
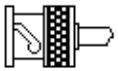
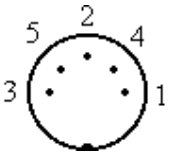
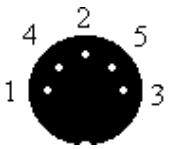
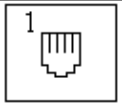
***Coaxial Cable (CO)*:** It is used in commercial TV networks. It is the third mostly used cable (power lines, TP) with a bandwidth second only to that of fiber-optic cable. A coaxial cable is composed of a copper conductor surrounded by insulation. An outer jacket composed of copper or aluminum acts as conductor, and also provides protection, While more expensive than TP, it can transmit data significantly faster over a much longer distance.

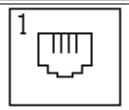
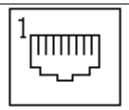
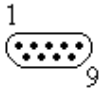
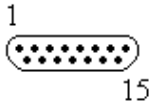
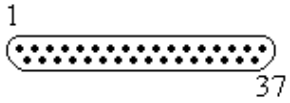
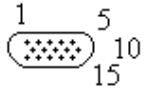
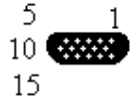
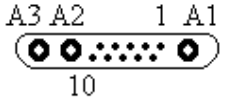
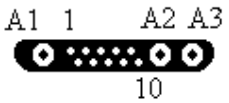
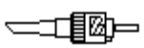
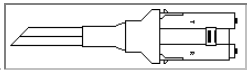
***Fiber-optic*:** It has extremely low rates of signal loss and high immunity to radiation, crosstalk, lighting, and corrosion. The transmission capability of fiber-optic cable is virtually unlimited. Its bandwidth is constrained only by its ability to generate light signals of uniform frequency. The light is generated by lasers or by LEDs. The cabling can consist of a single fiber (monomode), several fibers (multimode), or a variation of multimode (graded index) in which the index of refraction drops slowly from the center of the fiber towards the outside.

Physical-Layer Media Specifications

Specifications	10Base5	10Base2	10Base-T	10Base-TX (Fast Ethernet)	10Base-TX (Gigabit Ethernet)	FDDI
Cable Type	Thick coaxial cable	Thin coaxial cable	Twisted-pair	Twisted-pair (two pairs)	Twisted-pair (four pairs)	Fiber optic
Cable Impedance	50 ohms	50 ohms	85-110 ohms	85-110 ohms	85-110 ohms	-
Signaling techniques	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Baseband
Data Rate	10 Mbps	10 Mbps	10 Mbps	100 Mbps	1 Gbps	100 Mbps
Maximum cable segment length	500 m	185 m	100 m	205 m	200 m	2 km
Maximum network length	2500 m	925 m	2500 m	2500 m	2500 m	10 km
Attachments per segment	100	30 (29 with a repeater)	1	1	1	-
Attachments spacing	2.5 m	0.5 m				-
Connector type	DB-15 connector	BNC	RJ 45 (8 pin)	RJ 45 (8 pin)	RJ 45 (8 pin)	MIC, ST
Topology	Linear Bus	Linear Bus	Star-wired bus	Star-wired bus	Star-wired bus	Ring
Maximum number of stations per network	1024	1024	1024	1024	1024	1000

Connector Reference Chart

Description	Male	Female	Side View	Common Applications
Amphenol 50 Pin				Telco, SCSI
Half Pitch Centronics 50 pin				SCSI
Half Pitch Centronics 68 pin				SCSI
BNC				LAN, Video
DIN 5 Pin				AT Keyboard, Audio, MIDI
Mini-DIN 4 Pin				Apple Destop Bus, SVHS, S-Video
Mini-DIN 6 Pin				PS/2 Keyboard/Mouse
RJ10				Telephone

RJ11				Telephone
RJ45				ISDN, LAN
Sub-D 9 Pin				RS232, RS449, EGA, CGA
Sub-D 15 Pin				X.21, Mac Video
Sub-D 25 Pin				RS232, Centronics
Sub-D 37 Pin				RS449
Sub-D 50 Pin				SCSI
Sub-D 15 Pin High-Density				VGA, SVGA, XGA
13C3				Sun Work Station
ST				FDDI
MIC				FDDI

Cabling Categories:

- *Category 1*: suitable for voice only (1950s)
- *Category 2*: suitable for voice and low data rates (less than 4 Mbps). (1960s)
- *Category 3:* suited for voice and data rates up to 10 Mbps (frequency bandwidth 16 MHz). Uses 4 twisted-pairs. May support data rates up to 100 Mbps like 100Base-T4. Standard for most telephone installations. (1991)
- *Category 4:* consists of 4 twisted-pairs. Suitable for data rates up to 16 Mbps (frequency bandwidth 20 MHz). Support fast Token Ring networks. (1993)
- *Category 5:* consists of 4 twisted-pairs. Suitable for data rates up to 100 Mbps (frequency bandwidth 100 MHz). Supports 100Base-TX. (1994)
- *Category 6:* consists of 4 twisted-pairs. Suitable for data rates up to 1 Gbps). Supports 1000Base-TX. (1994)

Topologies:

Bus: All devices connect to a common, shared cable (or backbone).

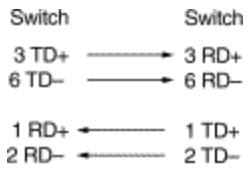
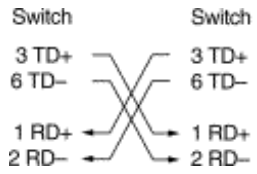
Ring*:* Nodes are wired in circle. Each node is connected to its neighbors on either side and data passes around the ring in one direction only.

Star*:* All devices connect to a central hub. The hub receives signals from other networks devices and routes the signals to the proper destinations.

Straight-Through and Crossover Cable Pin outs:

Cables ending in RJ45's may be wired up in two ways: straight through and crossover. A straight through cable connects pins N at both ends, whereas a crossover cable has the various pairs crossed over. Whether a straight through or crossover cable is required will depend on the types of network equipment and how they are interlinked.

The schematics of crossover and straight-through cables are shown in below.

Straight-Through Cable Schematic	Crossover Cable Schematic
	

LAN Devices:

Network Interface Cards (For further reading on the subject, refer to Text book, sec 6.2)

Network interface cards, commonly referred to as NICs, are used to connect a PC to a network. The NIC provides a physical connection between the networking cable and the computer's internal bus. NICs come in three basic varieties: 8-bit, 16-bit, and 32-bit. The larger the number of bits that can be transferred to the NIC, the faster the NIC can transfer data to the network cable.

Many NIC adapters comply with Plug-n-Play specifications. On these systems, NICs are automatically configured without user intervention, while on non-Plug-n-Play systems, configuration is done manually through a setup program and/or DIP switches.

Cards are available to support almost all networking standards, including the latest Fast Ethernet environment. Fast Ethernet NICs are often 10/100 capable, and will automatically set to the appropriate speed. Full duplex networking is another option, where a dedicated connection to a switch allows a NIC to operate at twice the speed.

Repeaters :

A repeater is a device used to extend the network length and topology beyond what can be achieved by a single cable segment. It is used to re-time and amplify the individual signals and has no concept of packets.

Repeaters, also called hubs or concentrators, are bit level devices. What this means that they do not examine the data packets that travel through them. They have no knowledge of addresses associated with the source or the destination. The basic operation of a repeater is to repeat traffic. Any data arriving on one port will be amplified and repeated out all ports (except the port on which it was received).

Repeaters were originally designed with only two ports and were used to increase the size of coax cable-based networks. This way, different lengths of coax cable coulds be attached to the repeater to extend the size of the network. This would allow the network to reach all areas of large or tall buildings. Data would be repeated from one cable segment to the other.

When the coax cabling was replaced by concentrators or hubs, the concentrators were, in fact, just repeaters with many more ports. Now, data reeived on one port would be replicated anywhere from twice to hundreds of times and transmitted to attached stations. The repeater also had the ability to track how much traffic was crossing through it.

Repeaters may also be linked together for even greater distances, but it is recommended that the data should not need to cross more than four repeaters. This is because each time the data gets repeated it may be slightly distorted. If there are too many distortions, original signal may be unreadable.

A very important fact to note about hubs is that they only allow users to shared Ethernet. A network of hubs/repeaters is termed a "shared Ethernet," meaning that all members of the network are contending for transmission of data onto a single network (collision domain).

This means that individual members of a shared network will only get a percentage of the available network bandwidth

Repeaters support all standard LAN protocols and cabling types, and a repeater can translate between different cabling. Today, repeaters are being replaced called a bridge.

Bridges :

A bridge operates at layer 2 of the OSI model and offers several functions, including expansion of networks beyond normal physical limitation, overcoming station count limitations, packet storage and forwarding, and keeping local traffic local by building an address table (SAT) of where devices are located within the network.

Bridges offer several advantages over repeaters, including:

- **Expansion of network** - because of regeneration issues, packets can only be repeated a limited number of times. Bridges eliminate the problem by copying and recreating new packets before forwarding them.
- **Overcoming station count limitations** - each type of LAN (Ethernet, token ring, FDDI) has a maximum number of users allowed on one segment. Bridges allows for the creation of multiple bridging segments.
- **Packet storage and forwarding** – bridges receive the packet, examine it, and then determine where it needs to go. If there is other traffic on the destination port, the bridge buffers (stores) the packet until the port is able to accept more traffic.
- **Keeping local traffic local** – the bridge's ability to read packets and identity addresses enables it to determine where a destination is located. This eliminates sending packets to segments that do not contain the destination.
- **Translating between different speeds** – bridges are required to interface between networks of different speeds (e.g., Ethernet's 10, 100, and 1000 Mbps)

- **Translating traffic between LAN protocols** – bridges, acting as interpreters, have the ability to translate packets between other LAN protocols such as Ethernet, token ring, FDDI, and ATM.

Bridges fit into the network in a similar fashion as repeaters and they support all the capabilities of repeaters (amplifications of signals, etc.) However, bridges have increased intelligence and can perform additional functions.

The repeater repeats all traffic that goes through it, so if I had a 24-port repeater and a packet came in one port, it would be repeated out 23 other ports. This is because the repeater does not know where to send it. A bridge, though, is aware of the individual packets and the addressing that is used. A bridge that receives that same packet examines it and resends it only to the port that has the diestination address attached to it. Obviously, this is a better way to handle traffic.

Besides having the ability to examine packets and forward based on addresses, bridges have the ability to learn where the different addresses are located on the network. This means the bridge will learn which PC is located on which port, and it also keep track of this address if

the PC is moved. Bridges can also be used to separate repeated networks.Bridges support all protocol and media types, and even have the ability to translate one LAN protocol to another.

Routers :

Routers perform their function at layer 3 of the OSI Model and are used to forward messages across an extended network based on network layer addresses (logical addressing), not MAC layer addresses. They route messages from end-station to end station, allowing multiple paths between them. Routeres can also be used to provide better traffic isolation and security by using access lists that control who can communicate through the router. Routers are used to forward traffic on the internet.

Routers offers several advantages over repeaters and bridges. These include:

- **Isolation of broadcast traffi**c – routers prevent the flow of broadcast traffic from one LAN to another.
- **Path selection** – routers can use the best path that physically exists between source and destination. Some routers allows for load balancing over redundant paths.
- **Flexibility** – routers can support any desired protocol or network topology.
- the total size of the network interconnected with routers is, for all practical purposes, unlimited (e.g., the Internet)
- Routers supports layer 1,2,and 3 functionality.

Note : Routers are more intelligent than bridges, but they are not plug-and –play- routers must be configured by a human.

Routers are designed to separate different parts of the network into what are called sub-nets, which are subdivisions of the the total network. This division of the network is done to support the different requirements of the organization, and it allows a network manager to separate and control traffic in the different sub-nets. Routers are often used to separate the network for the purpose of security. Doing this allows a network manager to keep some traffic inside a sub-net and allows other traffic to cross sub-net boundaries. An example of using routers and sub-nets would be a large company that has divided their network up based on departments. Sales might be one sub-net, marketing on another sub-net, and engineering on another sub-net. All these sub-nets would form the complete network, and within each sub-net is a collection of users connected to bridges or repeaters.

Routers support all the capabilities of bridges and repeaters along with network layer (layer3) protocols.

Switches :

Networks started as a collection of computers connected by a single cable.

The next evolution of networks was the introduction of the repeater. The repeater allowed the larger networks (Distance and size) and eliminated the cable as a single point of failure. The problem was that traffic was flooded everywhere.

The next evolution was the bridge. Originally, bridges were designed to separate networks into different sections, and this cut down on the amount of flooded traffic. Bridges could then used to interconnect groups of users connected to repeaters.

Next came the router. With the routers, logical groupings could be defined, traffic could be better controlled. Now you had networks with users connected to repeaters, the repeater connected to bridges and the bridges connected to routers, with each network network device doing its own thing.

A switch operates at layer 1, layer 2, and layer 3 (sometimes layer 4) and allows users to use a single device to support multiple capabilities. Now, using one device, some traffic can be repeated, some bridged, and some routed, all based on where the traffic needs to go. This is called switching.

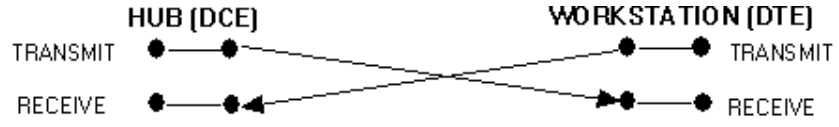
Switches combine the intellegence of repeaters, bridges, and routers into one networking device. Some of the advantages to using single box for all three functions are listed as follows:

- Save time – one device to manage
- Single device reqiured for spare
- Reconfigure instead of move/replace
- Single version of software need for uipgrading network.

Switches look like repeaters or bridges and allow direct connection to the PCs or to other switches, bridges, or routers, These devices are designed with much more intelligence built in, and the netwirk manager can configure any port, or groups of ports , to act as repeaters, bridges, or routers. the idea here is that you do not need to purchase and manage three different types of devices in your network – you can purchase one type of device and configure it the way you need it.

MDI / MDI-X ports:

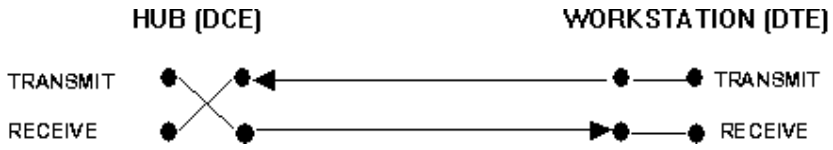
Consider the connection between a hub (DCE) and a workstation (DTE), shown in the figure below



The connection between a DCE and a DTE using a crossover cable.

There must be a point of crossover between the DCE and DTE for data to be successfully exchanged. Figure above shows a cable with the transmit and receive pairs crossed over. On a hub most of the ports will connect to DTE's (workstations, PCs etc.) and at some point a signals crossover must be effected. Equipment manufacturers are aware of this situation so the industry accepted standard is that all ports on hubs and switches which do not have a

media conversion capability have crossovers already built in. In such cases (the vast majority) only a straight-through cable is required to connect to a DTE. Figure below shows the DCE (hub) with a built in crossover port. Visually it is not easy to distinguish between straight-through and crossover cables so it is preferable to avoid having both types of cable in an installation. Using hubs and switches with crossover ports built in is a way of eliminating the need for crossover cables altogether. Ports on such equipment are often marked MDI-X. Uplink ports (e.g. 100BaseT) will not usually have built-in crossover and may be marked MDI.



The connection between a DCE and DTE using a straight through cable because the port of the DCE is already crossed over internally. Many hubs and switches feature ports which are switchable between crossover for DTE connection and straight-through for cascading or uplinking, all others being MDI-X only, or unmarked

MODEMS

The modem is a device that converts digital information to analog by MODulating it on the sending end , and DEModulating the analog information into digital information at the receiving end. They act as textual and voice mail systems, facsimiles, and are connected or integrated into cellular phones and in notebook computers enabling sending data from anywhere. Modem speeds are not expected to be increased much over today's 56 kbps. Further dramatic speed increases will require digital phone technology such as ISDN, xDSL and fiber optic lines.

xDSL

DSL stands for Digital Subscriber Line:

- ***Digital*** - means a line able to carry data traffic in its original form, as opposed to analog (see below)
- ***Subscriber Line*** - the line connecting the individual subscriber (e.g. a household) to the local exchange

The use of digital lines makes transmission of computer information faster and more reliable. It also allows much faster connect and disconnect, eliminating the slow process required for modems to establish a connection and start handling traffic. Over time its expected that all future telephony will be digital. The "x" in xDSL simply means there are several variations, eg ADSL, VDSL

DSL Summary Table

DSL Type	Description	Data Rate Down/Upstream	Distance Limit	Application
G.Lite (same as DSL Lite)	"Splitterless" DSL "	From 1.544 Mbps to 6 Mbps , depending on the subscribed service	18,000 feet on 24 gauge wire	The standard ADSL; sacrifices speed for not having to install a splitter at the user's home or business
HDSL	High bit-rate Digital Subscriber Line	1.544 Mbps duplex on two twisted-pair lines; 2.048 Mbps duplex on three twisted-pair lines	12,000 feet on 24 gauge wire	T1/E1 service between server and phone company or within a company; WAN, LAN, server access
SDSL	Symmetric DSL	1.544 Mbps duplex (U.S. and Canada); 2.048 Mbps (Europe) on a single duplex line downstream and upstream	12,000 feet on 24 gauge wire	Same as for HDSL but requiring only one line of twisted-pair
ADSL	Asymmetric Digital Subscriber Line	1.544 to 6.1 Mbps downstream; 16 to 640 Kbps upstream	1.544 Mbps at 18,000 feet; 2.048 Mbps at 16,000 feet; 6.312 Mpbs at 12,000 feet; 8.448 Mbps at 9,000 feet	Used for Internet and Web access, motion video, video on demand, remote LAN access
RADSL	Rate-Adaptive DSL from Westell	Adapted to the line, 640 Kbps to 2.2 Mbps downstream; 272 Kbps to 1.088 Mbps upstream	Not provided	Similar to ADSL
VDSL	Very high Digital Subscriber Line	12.9 to 52.8 Mbps downstream; 1.5 to 2.3 Mbps upstream; 1.6 Mbps to 2.3 Mbps downstream	4,500 feet at 12.96 Mbps; 3,000 feet at 25.82 Mbps; 1,000 feet at 51.84 Mbps	ATM networks; Fiber to the Neighborhood

Experiment # 3

Peer to Peer and Client Server Network Models

Objectives:

Build a small network using Windows-2000 operating system networking features. This includes:

1. Writing the network parameters used in the lab
2. Install TCP/IP protocol
3. Manually configure TCP/IP parameters
4. Use *ipconfig* utility to view configured TCP/IP parameters.
5. Use *ping* utility to test TCP/IP communications.
6. Share a folder
7. Assign shared folder permissions to users and groups
8. Connect to the shared folder
9. Stop sharing a folder.
10. Using *arp* command
11. Using *netstat* command to view the established and listening connections to the computer.

1. Write the network parameters used in the lab.

Network Architecture:

Cable Type:

Connector Type to Network Card:

Network Card brand name:

2. Peer to Peer Networking:

Network Addresses Settings

1. Log on computer as a local *administrator*
2. Go to **Settings**, then **Network and Dial-up Connections**, then check the properties of **Local Area Network**
3. First we will remove all the protocols, Click on **Internet Protocol (TCP/IP)** and then click on **uninstall** and *restart* the computer.

4. After restarting your computer, you log on again as local *administrator*, and again go to *Local Area Network Properties*, you will see there is no protocol installed and you can not access any network resources.
5. To add protocols, Click on **install**, select on *Protocol*, click on **Add**, select *Internet Protocol (TCP/IP)* and then click ***ok***.
6. In *Local Area Connection Properties* window, select *Internet Protocol (TCP/IP)* then click **Properties**.
7. Either you check on *Obtain an IP address automatically* the IP address would be assigned to your computer automatically by DHCP server, or if you check on *Use the following IP address* then you would have to enter the static IP address with proper subnet mask and gateway address. (The lab instructor will tell you the static IP address of the computer, subnet mask and default gateway).
8. Check *Use the following DNS server addresses*, Enter **196.15.32.126** in the *preferred DNS server* (Primary DNS server) and enter **196.15.32.192** in the *Alternate DNS server* (Secondary DNS server).
9. Click on **Advanced**, in *IP settings* tab you will see the computer IP address and gateway address, if there is no gateway address present, then click **Add**, enter the *default gateway address* and click **Add** again.
10. Click **DNS** tab, you will see the DNS server addresses.
11. Click **WINS** tab, if there is no WINS addresses, click on **Add**, and enter **196.15.32.158**, click **Add**.
12. Now click **OK**, click **OK** again on TCP/IP properties window.
13. Click close on Local Area Connection Properties window.

Network Identification Settings:

1. Right click on **My Computer** icon on desktop, click on **Properties**, Click on **Network Identification** tag, click on **Properties**.
2. Type computer name **ee400pcX** (where **X** is the number of computer, ask the instructor the number of your computer).
3. In peer-to-peer networking, the computer is standalone or a part of any Workgroup. Check *Workgroup* and type **ee400** in workgroup.
4. Click **OK**, and click **OK** again and restart your computer for new settings to take effect.

Now the TCP/IP and network settings have been completed, in the next exercise we will verify these settings by using *ping* and *ipconfig* DOS commands.

3. Using *ping* and *ipconfig*:

1. Log on as normal *user*. (ask instructor the username and password of the computer)
2. Start *command prompt*, click on **Start**, click **RUN**, and type **cmd** and press enter, you will enter in the DOS command prompt.
3. Type **ping 127.0.0.1** and then press enter. This internal loop-back test should give you four replies if TCP/IP is bound to the Network Adaptor.
4. Now we will test the TCP/IP connectivity, **ping** the EE-400 lab server (the server IP address would be provided by the lab instructor). Four replies messages from server should appear.
5. Try **ping** other computers in the lab. (The IP addresses of other computers would be provided by the lab instructor)
6. To verify the TCP/IP parameters, type **ipconfig/all** and press enter, now you will see the host name of your computer, IP address of your computer, subnet mask, default gateway, DNS servers, WINS and etc.

4. Sharing a Folder

1. Log on as Local *Administrator*, and right click on **Start** button and then click on **Explorer** to start the Windows-2000 Explorer.
2. Create the folder named **Public** at the root directory level of drive D.
3. Right-click the newly created **Public** folder to display the menu and then click on **properties** option.
4. In folder properties window, click on **Sharing** tab. Click on **Share** this folder.
5. There is one option, **User limit**, you can limit the number of users to access this folder, and you can **allow maximum users** to access this shared folder.
6. Now click on **apply** and click **OK**. You will see hand symbol on the Public folder, that shows the sharing of Public folder.

5. Assigning Shared Folder Permissions:

1. Go to Windows-2000 explorer, right-click the **Public** folder, then click **sharing**, Click **Permissions**

2. Permissions for Public window will appear and you will see the permissions are assigned to Everyone. By default the permissions are assigned to Everyone that is all users can access this folder. Now we will modify the permissions settings.
3. Select **Everyone** and Click **Remove**.
4. Click **Add,** and select the **users** and **groups** to whom you want to assign the permission to access this public folder.
5. To assign permissions administrators group, select **Administrators**, then click **Add**.
6. To assign permissions to users group, select **Users**, then click **Add**.
7. Now click **OK**.
8. You will see the *Administrators* and *Users* group in the permissions window. Select *Administrators* and see the permissions assigned to this group. You will see the *Read* permission is assigned to the Administrator group by default. Here you can change the permissions to the administrator group, Check **Full Control** and click **Apply**.
9. Now select the *Users* group and see the permissions assigned to the Users group. By default Users group has Read permissions.
10. You can change the permissions for Users group and you can also assign permissions to a specific user with the same procedure.

6. Connecting to a Shared Folder using RUN command

1. Log on as a normal *user*.
2. Click **Start**, and then click **Run**
3. In the open box, type **\\ee400pc1** and then click **OK**. The **EE400PC1** window appears and only the folders that are shared appear to network users.
4. Close the **ee400pc1** window.

7. Connecting to a Shared Folder using MAP Network Drive

1. On the desktop, Right-click **My Network Places**, then click on **Map Network Drive**.
2. Select Drive letter as **Z**. (You can select any available drive letter E through Z).
3. In Folder option, type the correct path as **\\ee400pc1\Public**.
4. Uncheck the option of *Reconnect at logon*. If you will check this option, the drive will be mapped whenever the computer re-starts.
5. Then click **Finish**.
6. Now Start the Windows Explorer and view the drives under *My Computer*. You will see a directory has been added as Public on ee400pc1.

8. Disconnecting the Mapped Network Drive

1. Start the Windows Explorer, and right-click on the drive letter **Z**. (the drive letter which is mapped with network drive).
2. Click **Disconnect**. The mapped network drive would be removed from the left pane of the Windows Explorer.

9. Stopping a Shared Folder

1. Log on as local *administrator*, then Start Windows Explorer.
2. Locate the *Public* Folder, and right-click on the folder and click **Sharing**.
3. In the *Sharing* tab of Public Properties, Click on *Do not Share this folder*.
4. Then click on **Apply** and click **OK**.
5. Now you can delete the *Public* folder.

10. ARP Cache

1. Log on as a Local **Administrator**.
2. Start the command prompt, type **arp –a** and then press **Enter** to view the ARP cache.
3. Write the entries in ARP cache below:

_____

_____

_____

_____

4. **Ping** the IP address of any computer in the lab. (ask the Instructor which IP address to be pinged). This will add an entry to the arp cache.
5. View the new entry in arp cache.
6. To remove the any entry in the ARP cache, type **arp –d** IP_address. (where the IP_address is the one to be removed from the ARP cache).

11. Using *netstat* DOS command

The *netstat* utility queries a host about its TCP/IP network status. It can also find the state of the routing table in a host, which TCP/IP server processes are active in the host, and which TCP connections are active.

1. Start DOS command prompt, type **netstat** and then press **Enter**. You will see the list of established connections with your computer.
2. Now type **netstat –a**, it will display all the connections and listening ports.
3. Now create a **Public** folder on your computer and make **sharing** the Public folder and assign permission to Everyone.
4. Ask your neighboring friend to map Public folder.
5. When your friend has mapped the Public folder of your computer, then Start DOS command prompt and type **netstat –a**. You will see the computer name of your friend who mapped the Public folder of your computer.

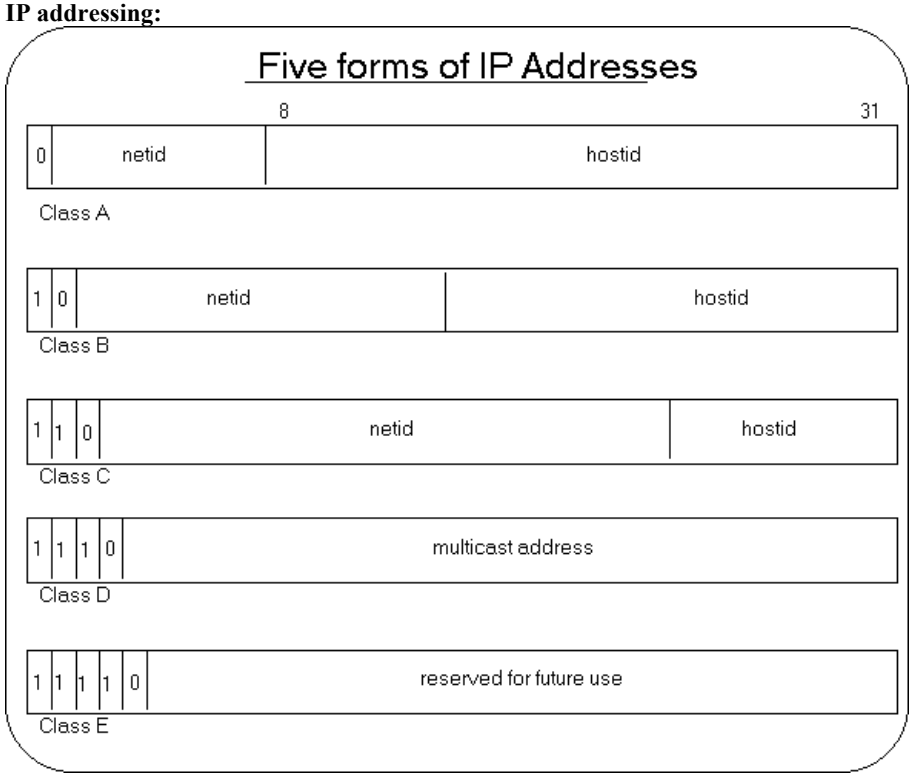
Experiment # 4

IP Addressing and Subnetting

Objectives:

After this experiment, the students should be able to configure for networking, assign IP address, and subnet mask to any of the host running on windows 98 OS. They should be able to test the connectivity of the host to the network and check the network status.

IP addressing:



	Net ID	First Host	Last Host	Net ID (bytes)	Host ID (bytes)	Size of Net
Class A				**1**	**3**	Huge # of Host, Less # of NW
First Network	1.0.0.0	1.0.0.1	1.255.255.254			
Last Network	126.0.0.0	126.0.0.1	126.255.255.254			
Class B				**2**	**2**	# of Host = # of NW
First Network	128.1.0.0	128.1.0.1	128.1.255.254			
Last Network	191.254.0.0	191.254.0.1	191.254.255.254			
Class C				**3**	**1**	Huge # f NW, Less # of Hosts
First Network	192.0.1.0	192.0.1.1	192.0.1.254			
Last Network	223.255.254.0	223.255.254.1	223.255.254.254			

Class D: a multicast address. (224.0.0.0 - 240.0.0.0)

Class E: reserved for future use. (241.0.0.0 - 248.0.0.0)

Special forms of INTERNET Addresses

For class C address, only 254 hosts can be supported because

- 0 is reserved for boot process
- 255 reserved for broadcast e.g.

0.0.0.0 - This host.

0.host_number - host on this net.

255.255.255.255 - Limited broadcast (local net).

net_number.255 - Directed broadcast for the specified net. (e.g 196.15.32.255 broadcast to all hosts of the local network.)

127.anything - Loop back (should never appear on the net).

IP Subnetting

Subnetting is a Technique used to allow a single IP network address to span multiple physical networks. IP hosts should support subnetting. Subnetting is done by using some of the bits of the host-id part of the IP address as a physical network identifier. The subnet mask is used to determine the bits of the network identifier. All hosts on the same network should have the same subnet mask.

An example of Subnetting:

The Class B network 128.10.0.0 can be subnetted using the first 8 bits of the host-id, to span 254 different physical networks. The subnet mask for this case is 255.255.255.0 The subnetworks are: 128.10.1.0, 128.10.2.0, ..., 128.10.254.0 . Each of the subnetworks can have up to 254 different hosts:

128.10.XXX.1, 128.10.XXX.2, ..., 128.10.XXX.254 .

If there is a need for less physical nets and more hosts in each one, less host-id bits can be used for subnetting. For example: With the subnet mask 255.255.254.0, 126 different subnets are available with up to 510 hosts in each one.

Many Class A and B networks do not contain as many hosts as they could. This situation causes a lot of address space waste. Subnetting better utilizes the address space by dividing these big networks to smaller ones.

IP Subnetting examples

Class C subnetting example.

In Host ID, 3 bits are used for subnet, 5 are used for Hosts

Only $(2^5 = 32) - 2 = 30$ Host are allowed for each subnet because

- 31 used for broadcast
- 0 used for bootup

Only $(2^3 = 8) - 1 = 7$ subnets are allowed because

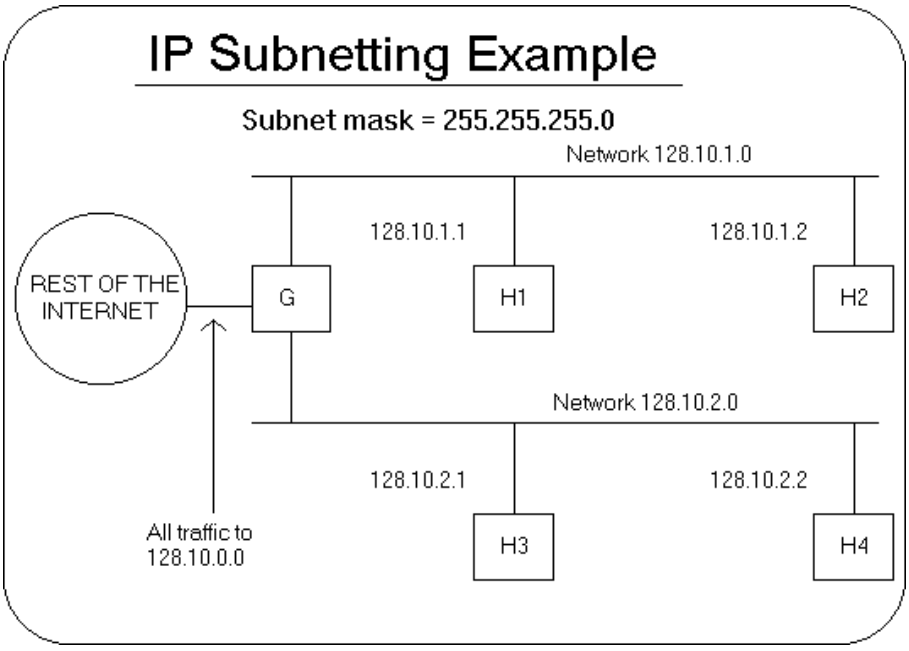
- 0 is not allowed

Subnet mask for Host ID field will be $(1110\ 0000)_b = (224)_d$

Thus full Subnet mask will be 255.255.255.224

Class B subnetting example.

Dividing a single Class B network into two subnetworks:



Configuring the HOSTS File:

You will add host name/IP address mappings to your HOSTS file, and then use the file to resolve host names.

Pinging local hostname:

You will ping the name of local host to verify that Microsoft TCP.IP can resolve local host names without entries in the HOSTS file.

1. Type **ping** *hostname* (where hostname is the name of your computer) and then press Enter. See what was the response?
2. Type **ping** *hostname* (where hostname is the name of another computer) and then press Enter. See what was the response?

Pinging Remote hostname:

1. Type **ping** *vlsi* and then press Enter. (vlsi is the remote computer name). See what was the reponse?

Editing HOSTS File:

1. Start command prompt, and then change the directory to
   cd d:\winnt\system32\drivers\etc
2. You will now use a text editor to modify a file called **HOSTS**. Type **edit hosts** and then press Enter.
3. Add the following entry to the HOSTS file:
   196.1.64.70 vlsi
4. Press **Alt** key, then **Save** the file, and then **Exit**.

Using HOSTS file for name resolution:

1. Type **ping vlsi** and then press Enter. See what was the response.

Domain Name System (DNS)

The Domain Name System protocol provides a mapping between cryptic IP address and, easier to remember, host names. Host names are used because they are easier for humans to remember. For example, telnet itc.itc.kfupm.edu.sa is easy to remember than telnet 196.15.32.8

The Internet Domain Name System (DNS) is an attempt to decentralize administration of the mapping of host names to host addresses by the use of name-servers, each of which controls part of name space. This becomes necessary partly because the static host table formerly used for that purpose most of the hosts in the Internet are on networks local to particular organizations. It is desirable to allow the local administration to control that mapping. The DNS also implements a hierarchical naming scheme and provides protocols for communication with the name-servers. A set of top-level domains is administered by the Internet and is defined in the basic DNS specifications.

Top Level Domains:

The top level domains can be categorized as Organizational and Geographic:

com	Commercial
edu	Educational
gov	Governmental
mil	Military
net	Administrative organizations for network such as CSNET, BITNET etc.
org	Other Organizations
XX	two letter country code, e.g., sa for Saudi Arabia.

DNS Naming Convention:

- Besides the root, each node in DNS database has a name of up to 63 characters.
- Each sub domain must have a unique name within its parent domain.

Domains-Subtrees of the Entire Database:

Root-Level Domain: Top of the hierarchy is called the root domain.

Top-Level Domain: First level domain contains second level domains and hosts. Top Level domains include .com and .net. This is a child of the root.

Second-Level Domain: It contains hosts and other domains called "subdomains". Microsoft.com and Compaq.com are second level domains. Second level domains are children of First-Level Domains.

Third-Level Domain: It contains hosts and other domains called "subdomains". mspress.microsoft.com is a subdomain and a third-level domain. A third-level domain is a child of a second-level domain.

DNS Operation:

DNS uses a client/server model, in which DNS servers (name servers) contain information about the DNS database and make this information available to clients (resolvers).

DNS name servers perform name resolution by interpreting network information to find a specific IP address. Let see how DNS operates using the example of widget.universal.com

1. A resolver (or client) passes a query to its local name server.
2. The local name server sends an iterative request to one of the DNS root servers, requesting resolution of the domain name. The DNS root server returns a referral to the name servers that are authoritative for the com DNS domain.
3. The local name server sends an iterative request to one of the com name servers, which responds with a referral to the "universal" name servers.
4. The local name server sends an iterative request to one of the "universal" name servers.
5. When the universal name server receives the request from the local name server, it passes the widget piece of the DNS name to its local WINS server for resolution, WINS returns the IP address for widget to the universal name servers, which returns the IP address of the domain name to the local DNS server, which then send it back to the client resolver.

Experiment # 5

Point to point local communication and Remote Access Service (RAS)

Objective:

Connecting two computers through Modems, Parallel and Serial Cables. Remote Access Service Setup and Configuration.

Connecting Computers through Parallel/Serial Cables:

1. Log on computer as **Administrator**.
2. Connect two computers with Parallel Cable or Serial Cable. One computer would be configured as Host (Server) and other as Guest (Client).
3. Specify the *DNS Servers IP addresses*, *WINS Server IP address*, *Gateway IP address* and *domain name* in the network settings.
4. Go to **Start**, **Settings**, **Network and Dial-up Connections**, open **Make New Connection**, then Click **Next**.
5. Check *Connect directly to another computer* option, then Click **Next**.
6. For Server; Check *Host*,
   For Client; Check *Guest*
   Guest computer can access the shared resources on the Host computer.
7. Select *Connection Device* that is Direct Parallel (LPT1) or Communication Port (COM1) or Communication Port (COM2). Then Click **Next**. Note: The data transfer rate of LPT Port is very much faster than COM Port.
8. For Host computer; Select *usernames* to give privilege to login from Client machine,
   For Guest computer; Select either *For all users* or *only for myself*
   then click **Next**.
9. Click **Finish**. Hence the Guest computer can connect to Host computer and can access the shared resources on the Host computer.

Connecting Computers through Twisted-Pair Cross-over Cable:

1. Log on computer as **Administrator**.
2. Connect two computers with twisted-pair crossover cable.
3. Here both computers can access each other's shared resources.

RAS Setup:

1. Log on computer as **Administrator**.
2. Specify the *DNS Servers IP addresses*, *WINS Server IP address*, *Gateway IP address* and *domain name* in the network settings.
3. If you have an external modem, connect it to serial port of computer then switch the modem ON. If you have internal modem, then first switch the computer OFF, open computer case, install the modem in any free slot on the motherboard, after hardware installation switch your computer ON.
4. If computer does not detect modem automatically, go to **Start**, **Settings**, **Control Panel**, **Phone and Modem Options**. Click **Add**, check option *Don't detect my modem; I will select it from a list*, click **Next**.
5. Click **Have Disk**, Click **Browse**, Go to drive **E**, go to folder **modemdrv**, then select the driver files and install modem driver.
6. After modem installation, you can configure your computer as *RAS Server* or *RAS Client* or *both* but you can use one service (Server/Client) at one time.

RAS Server Setup:

1. Go to **Start**, **Settings**, **Network and Dial-up Connections**, open **Make New Connection**, then Click **Next**.
2. Check *Accept incoming Connections* option, then Click **Next**.
3. Check *modem*, click **Next**, Click **Next** again.
4. Select *usernames* to give privilege of RAS service, then click **Next**.
5. Click **Next** and Click **Finish**. Hence the client machine can connect to server machine and can access the local area network of server machine. If accessing local area network is stopped by the server machine, then client can only access the shared resources on the RAS server. For this purpose, go to *Incoming Connections* **Properties**, go to **Networking**, check *TCP/IP properties*, if you uncheck the option *Allow callers to access*

my local area network then client machine can not access local area network of RAS server.

RAS Client Setup:

1. Go to **Start**, **settings**, **Network and Dial-up Connections**, open **Make New Connection**, then Click **Next**.
2. Check *Dial-up to Private Network* option, then Click **Next**.
3. Enter phone number of RAS Server, click **Next**, and then type *dial up* name like RAS EE-400 or anything you like, then click **Finish**.
4. A small window will appear connect to RAS EE-400, click on **Properties** and go to **Networking** and assign *TCP/IP* settings, like *DNS IP addresses, WINS IP address*, and *gateway IP address*.
5. Click on **Dial**, after get connected to the RAS Server, the client machine will be treated as if it is on the local area network of RAS server machine.

Experiment # 6
Data Traffic Capture and Protocol Analysis

Objective:

Introduction to data packet capturing and analysis of individual packet contents including the details associated with the protocols used.

Introduction:

Ethereal is a GUI network protocol analyzer. It lets you interactively browse packet data from a live network or from a previously saved capture file. Like other protocol analyzers, Ethereal's main window shows 3 views of a packet.

1. It shows a summary line, briefly describing what the packet is.
2. A protocol tree is shown, allowing you to drill down to exact protocol or field that you interested in.
3. Finally, a hex dump shows you exactly what the packet looks like when it goes over the wire.

In addition, Ethereal has some features that make it unique. It can assemble all the packets in a TCP conversation and show you the ASCII (or EBCDIC, or hex) data in that conversation (TCP stream). Display filters in Ethereal are very powerful; more fields are filterable in Ethereal than in other protocol analyzers, and the syntax you can use to create your filters is richer

Important Menu Items:

File:Open, File: Close, File: Reload

Open, close, or reload a capture file. The *File:Open* dialog box allows a filter to be specified; when the capture file is read, the filter is applied to all packets read from the file, and packets not matching the filter are discarded.

File: Print Packet

Print a fully-expanded protocol tree view of the currently-selected packet. Printing options can be set with the *Edit: Preferences* menu item.

File: Quit

Exits the application.

Edit: Capture Filters

Edits the saved list of capture filters, allowing filters to be added, changed, or deleted.

Edit: Display Filters

Edits the saved list of display filters, allowing filters to be added, changed, or deleted.

Edit: Protocols

Edits the list of protocols, allowing protocol dissection to be enabled or disabled.

Capture: Start

Initiates a live packet capture (see Capture Options below). A temporary file will be created to hold the capture. The location of the file can be chosen by setting your TMPDIR environment variable before starting **Ethereal**. Otherwise, the default TMPDIR location is system-dependent, but is likely either */var/tmp* or */tmp*.

Capture: Stop

In a capture that updates the packet display as packets arrive (so that Ethereal responds to user input other than pressing the ``Stop'' button in the capture packet statistics dialog box), stops the capture.

Display: Options

Allows you to sets the format of the packet timestamp displayed in the packet list window to relative, absolute, absolute date and time, or delta, to enable or disable the automatic scrolling of the packet list while a live capture is in progress or to enable or disable translation of addresses to names in the display.

Display: Match

Creates a display filter, or adds to the display filter strip at the bottom, a display filter based on the data currently highlighted in the protocol tree, and applies the filter.

If that data is a field that can be tested in a display filter expression, the display filter will test that field; otherwise, the display filter will be based on absolute offset within

the packet, and so could be unreliable if the packet contains protocols with variable-length headers, such as a source-routed token-ring packet.

The **Selected** option creates a display filter that tests for a match of the data; the **Not Selected** option creates a display filter that tests for a non-match of the data. The **And Selected**, **Or Selected**, **And Not Selected**, and **Or Not Selected** options add to the end of the display filter in the strip at the bottom an AND or OR operator followed by the new display filter expression.

Display: Prepare

Creates a display filter, or adds to the display filter strip at the bottom, a display filter based on the data currently highlighted in the protocol tree, but doesn't apply the filter.

Display: Collapse All

Collapses the protocol tree branches.

Display: Expand All

Expands all branches of the protocol tree.

Tools: Follow TCP Stream

If you have a TCP packet selected, it will display the contents of the data stream for the TCP connection to which that packet belongs, as text, in a separate window, and will leave the list of packets in a filtered state, with only those packets that are part of that TCP connection being displayed. You can revert to your old view by pressing ENTER in the display filter text box, thereby invoking your old display filter (or resetting it back to no display filter).

The window in which the data stream is displayed lets you select whether to display:

whether to display the entire conversation, or one or the other side of it;

whether the data being displayed is to be treated as ASCII or EBCDIC text or as raw hex data; and lets you print what's currently being displayed, using the same print options that are used for the *File: Print Packet* menu item, or save it as text to a file.

Tools: Decode As

If you have a packet selected, this menu item will present a dialog allowing you to change which dissectors are used to decode this packet. The dialog has one panel each

for the link layer, network layer and transport layer protocol/port numbers, and will allow each of these to be changed independently. For example, if the selected packet is a TCP packet to port 12345, using this dialog you can instruct Ethereal to decode all packets to or from that TCP port as HTTP packets.

WINDOWS

Main Window

The main window is split into three panes. You can resize each pane using a ``thumb'' at the right end of each divider line. Below the panes is a strip that shows the current filter and informational text.

Top Pane

The top pane contains the list of network packets that you can scroll through and select. By default, the packet number, packet timestamp, source and destination addresses, protocol, and description are displayed for each packet; the *Columns* page in the dialog box popped up by *Edit: Preferences* lets you change this (although, unfortunately, you currently have to save the preferences, and exit and restart Ethereal, for those changes to take effect).

If you click on the heading for a column, the display will be sorted by that column; clicking on the heading again will reverse the sort order for that column.

An effort is made to display information as high up the protocol stack as possible, e.g. IP addresses are displayed for IP packets, but the MAC layer address is displayed for unknown packet types.

The right mouse button can be used to pop up a menu of operations.

The middle mouse button can be used to mark a packet.

Middle Pane

The middle pane contains a *protocol tree* for the currently-selected packet. The tree displays each field and its value in each protocol header in the stack. The right mouse button can be used to pop up a menu of operations.

Bottom Pane

The lowest pane contains a hex dump of the actual packet data. Selecting a field in the *protocol tree* highlights the corresponding bytes in this section. The right mouse button can be used to pop up a menu of operations.

Current Filter

A display filter can be entered into the strip at the bottom. A filter for HTTP, HTTPS, and DNS traffic might look like this:

```
tcp.port == 80 || tcp.port == 443 || tcp.port == 53
```

Selecting the *Filter:* button lets you choose from a list of named filters that you can optionally save. Pressing the Return or Enter keys, or selecting the *Apply* button, will cause the filter to be applied to the current list of packets. Selecting the *Reset* button clears the display filter so that all packets are displayed.

Preferences

The *Preferences* dialog lets you control various personal preferences for the behavior of **Ethereal**.

Column Preferences

The *Columns* page lets you specify the number, title, and format of each column in the packet list.

The *Column title* entry is used to specify the title of the column displayed at the top of the packet list. The type of data that the column displays can be specified using the *Column format* option menu. The row of buttons on the left perform the following actions:

TCP Streams Preferences

The *TCP Streams* page can be used to change the color of the text displayed in the TCP stream window. To change a color, simply select an attribute from the ``Set:'' menu and use the color selector to get the desired color. The new text colors are displayed in a sample window.

User Interface Preferences

The *User Interface* page is used to modify small aspects of the GUI to your own personal taste:

Capture Preferences

The *Capture* page lets you specify various parameters for capturing live packet data; these are used the first time a capture is started.

The *Interface:* combo box lets you specify the interface from which to capture packet data, or the name of a FIFO from which to get the packet data. You can specify whether the interface is to be put in promiscuous mode or not with the *Capture packets in promiscuous mode* check box, can specify that the display should be updated as packets are captured with the *Update list of packets in real time* check box, and can specify whether in such a capture the packet list pane should scroll to show the most recently captured packets with the *Automatic scrolling in live capture* check box.

Protocol Preferences

There are also pages for various protocols that Ethereal dissects, controlling the way Ethereal handles those protocols.

The *Edit Capture Filter List* dialog lets you create, modify, and delete capture filters, and the *Edit Display Filter List* dialog lets you create, modify, and delete display filters.

The *Capture Filter* dialog lets you do all of the editing operations listed, and also lets you choose or construct a filter to be used when capturing packets.

The *Display Filter* dialog lets you do all of the editing operations listed, and also lets you choose or construct a filter to be used to filter the current capture being viewed.

The *Read Filter* dialog lets you do all of the editing operations listed, and also lets you choose or construct a filter to be used to as a read filter for a capture file you open.

The *Search Filter* dialog lets you do all of the editing operations listed, and also lets you choose or construct a filter expression to be used in a find operation.

In all of those dialogs, the *Filter name* entry specifies a descriptive name for a filter, e.g. **Web and DNS traffic**. The *Filter string* entry is the text that actually describes the filtering action to take, as described above. The dialog buttons perform the following actions:

Capture Options

The *Capture Options* dialog lets you specify various parameters for capturing live packet data.

The *Interface:* field lets you specify the interface from which to capture packet data or a command from which to get the packet data via a pipe.

The *Limit each packet to ... bytes* check box and field lets you specify a maximum number of bytes per packet to capture and save; if the check box is not checked, the limit will be 65535 bytes.

The *Capture packets in promiscuous mode* check box lets you specify whether the interface should be put into promiscuous mode when capturing.

The *Filter:* entry lets you specify the capture filter using a tcpdump-style filter string as described above.

The *File:* entry lets you specify the file into which captured packets should be saved, as in the *Printer Options* dialog above. If not specified, the captured packets will be saved in a temporary file; you can save those packets to a file with the *File: Save As* menu item.

The *Use ring buffer* check box lets you specify that the capture should be done in ``ring buffer" mode; the *Number of files* field lets you specify the number of files in the ring buffer.

The *Update list of packets in real time* check box lets you specify whether the display should be updated as packets are captured and, if you specify that, the *Automatic scrolling in live capture* check box lets you specify the packet list pane should automatically scroll to show the most recently captured packets as new packets arrive.

The *Stop capture after ... packet(s) captured* check box and field let you specify that Ethereal should stop capturing after having captured some number of packets; if the check box is not checked, Ethereal will not stop capturing at some fixed number of captured packets.

If ``ring buffer" mode is not specified, the *Stop capture after ... kilobyte(s) captured* check box and field let you specify that Ethereal should stop capturing after the the file to which captured packets are being saved grows as large as or larger than some specified number of kilobytes (where a kilobyte is 1000 bytes, not 1024 bytes). If the check box is not checked, Ethereal will not stop capturing at some capture file size

(although the operating system on which Ethereal is running, or the available disk space, may still limit the maximum size of a capture file).

If ``ring buffer" mode is specified, that field becomes the *Rotate capture file very ... kilobyte(s)* field, and specifies the number of kilobytes at which to start writing to a new ring buffer file; the check box is forced to be checked, as ``ring buffer" mode requires a file size to be specified.

The *Stop capture after ... second(s)* check box and field let you specify that Ethereal should stop capturing after it has been capturing for some number of seconds; if the check box is not checked, Ethereal will not stop capturing after some fixed time has elapsed.

The *Enable MAC name resolution*, *Enable network name resolution* and *Enable transport name resolution* check boxes let you specify whether MAC addresses, network addresses, and transport-layer port numbers should be translated to names.

Display Options

The *Display Options* dialog lets you specify the format of the time stamp in the packet list. You can select ``Time of day" for absolute time stamps, ``Date and time of day" for absolute time stamps with the date, ``Seconds since beginning of capture" for relative time stamps, or ``Seconds since previous frame" for delta time stamps. You can also specify whether, when the display is updated as packets are captured, the list should automatically scroll to show the most recently captured packets or not and whether addresses or port numbers should be translated to names in the display on a MAC, network and transport layer basis.

Exercise:

1. Connect your computer to a port on HP Ethernet switch.
2. Launch Ether Real Protocol Analyzer software.
3. Go to **Capture Menu** and click on **Start**. Another small window will open.
4. Uncheck the options ***Capture packets in promiscuous mode, Enable MAC name resolution, Enable network name resolution, Enable transport name resolution***.
5. Check the options ***Update list of packets in real time and Automatic scrolling in live capture.***
6. Click **OK**.

7. Capturing process will start immediately. Start a TELNET session.
8. Stop the capturing process and analyze the packets.
9. Repeat the same process for a HTTP session.
10. Connect your computer to a port on 3Com Ethernet hub and repeat the above.

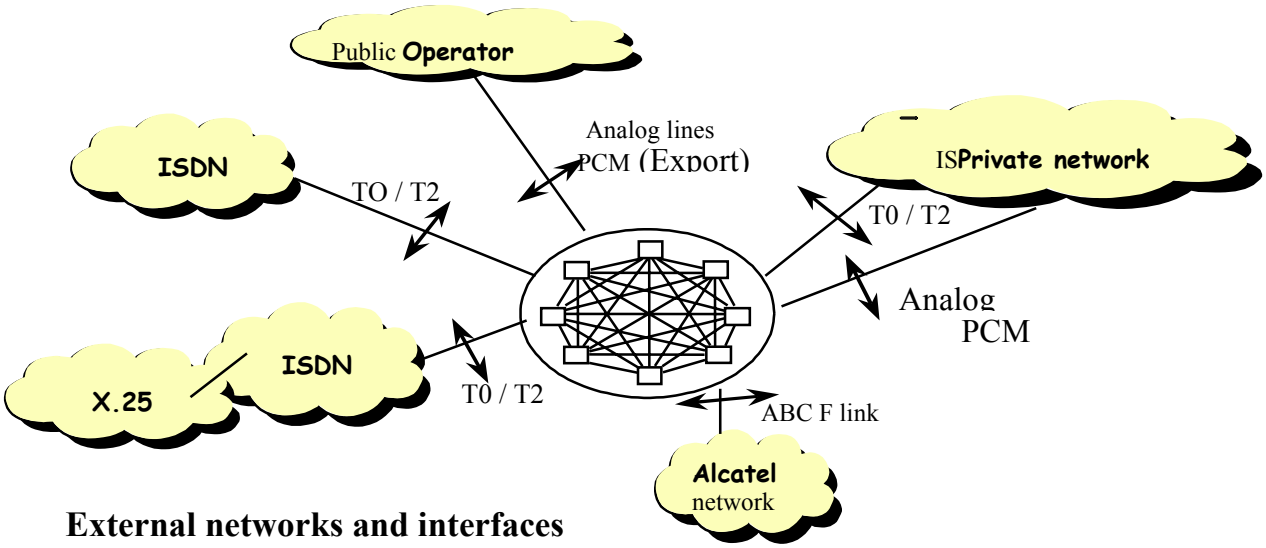
Experiment # 7
Intersystem Links - A visit to KFUPM Voice Network

Objectives:

After this experiment, the students should be able identify different types of voice and data network links.

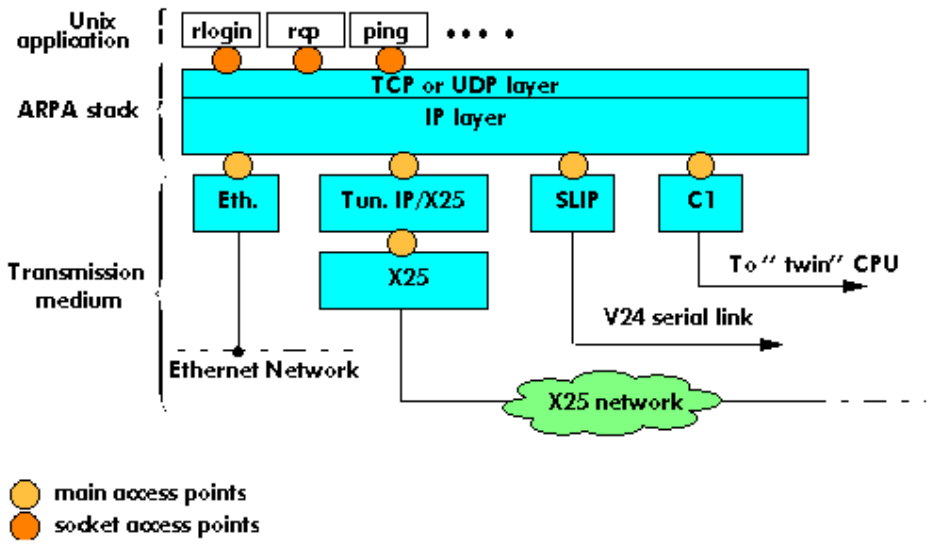
Type of private voice networks:

1. Homogenous (ABC-F2 or E1 protocol)
2. Alcatel Heterogeneous (ABC_F1 protocol)
3. Heterogeneous (QSIG protocol)



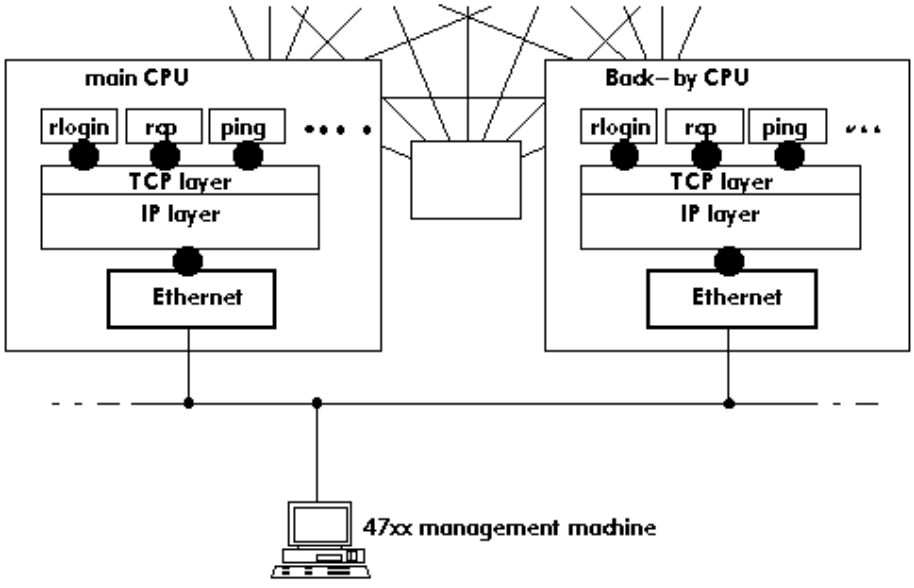
External networks and interfaces

The IP facilities use the following transmission media: - Ethernet network - X25 network - V24 serial links - Inter ACT link.



1. ETHERNET INTERFACE

The Ethernet interface enables the PABX to be connected to an Ethernet network.

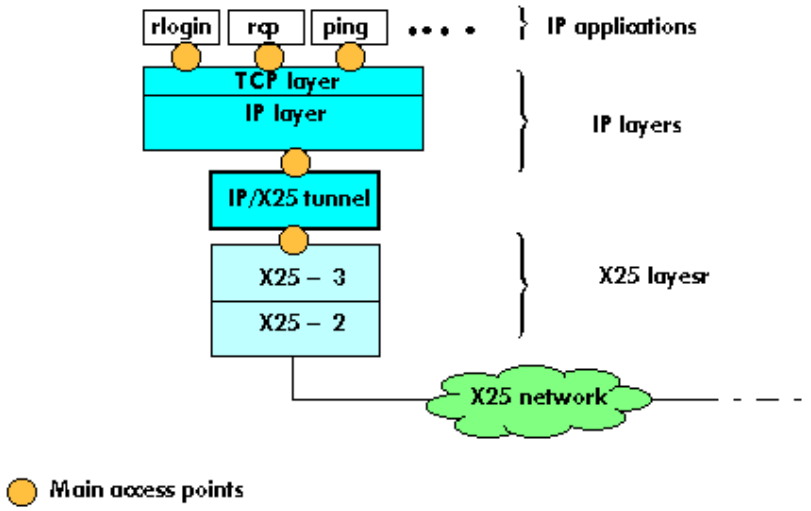


2. IP/X25 TUNNEL INTERFACE

The tunnel enables the internal X25 network between the PABXs to act as a communications medium. The function of the IP/X25 tunnel is to transform the datagrams which leave the IP layer into X25 packets. The IP/X25 tunnel also

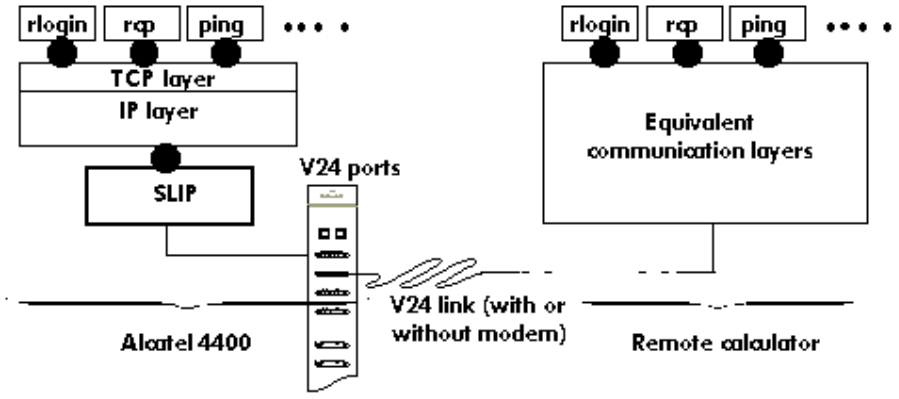
controls the transforming of the off-line IP protocol into on-line X25 protocol. For this, it establishes and releases the X25 connections.

The IP/X25 tunnel only works on ABC links.



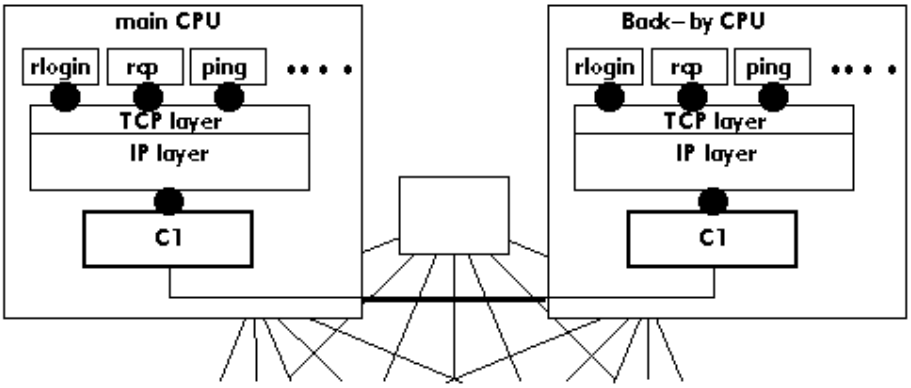
3. SERIAL LINK

The management equipment or other equipment of the PABX may be connected by a V24 type serial link. For this mode of communication, two protocols are suggested: the SLIP protocol and the PPP protocol

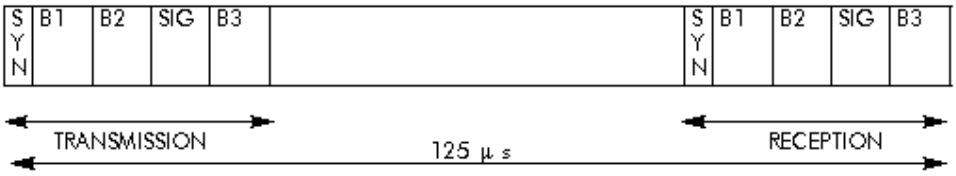


4 C1 Link

The C1 link allows the master and slave CPU to communicate with each other via the ACT.



UA link The terminal adapters (TA) and dedicated sets are connected to the system via this UA link, which carries 4 x 64Kbit/s channels (3 B channels and one signaling channel). It is used to multiplex voice and data on the same physical link. The UA link presents a 125 micro second frame with the following format:



For example, in the case of a V24 terminal connected behind a UA set, the multiplexing is carried out as follows: - the SIG channel carries the UA signaling exchanged between the set and system, - one B channel caries voice, - one B channel carries the V24 terminal data.

ISDN interfaces ACT boards

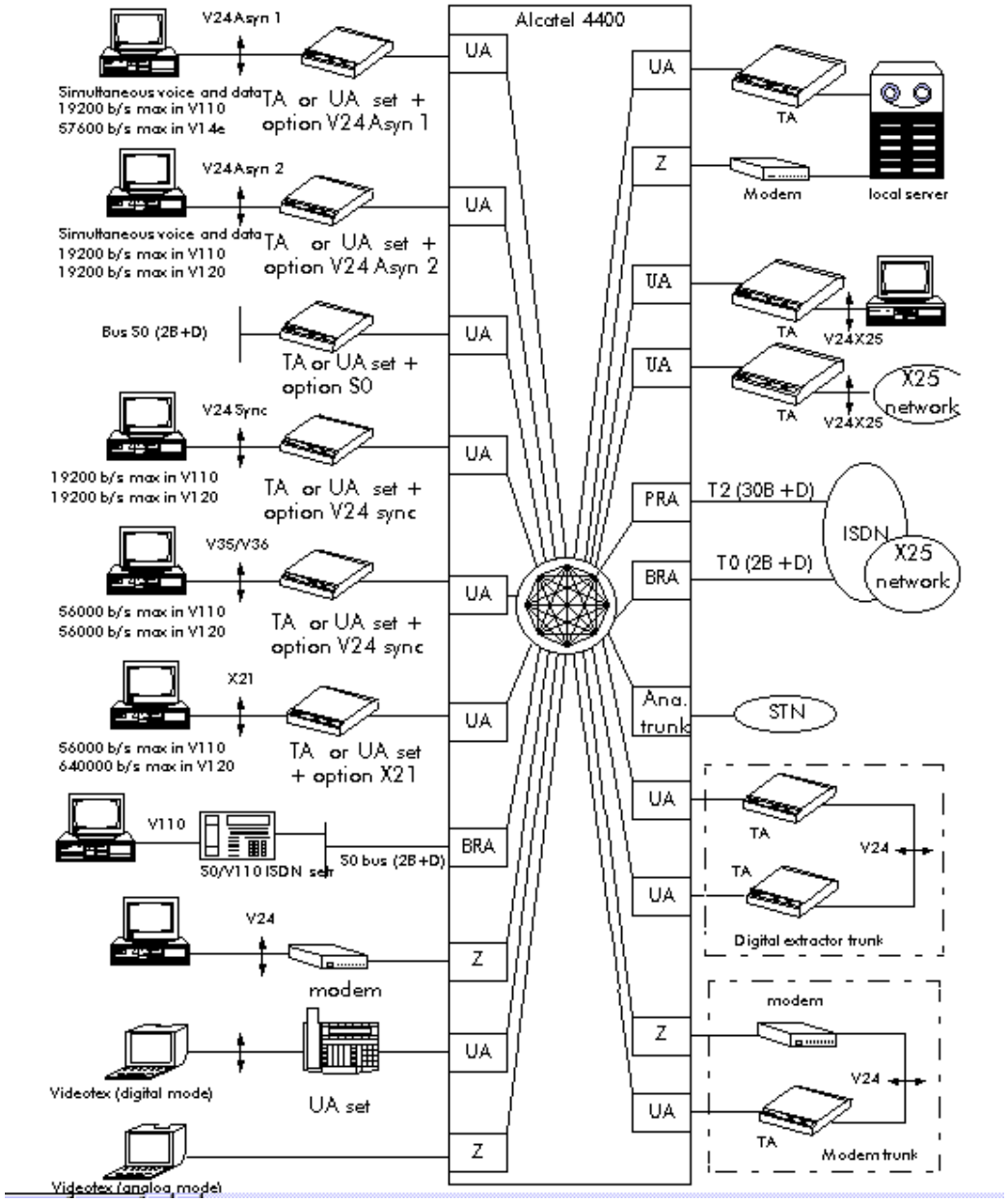
The ISDN boards that can be connected on the ACT backplane are of the following types: - --

BRA board offering 8 E0 bus interfaces

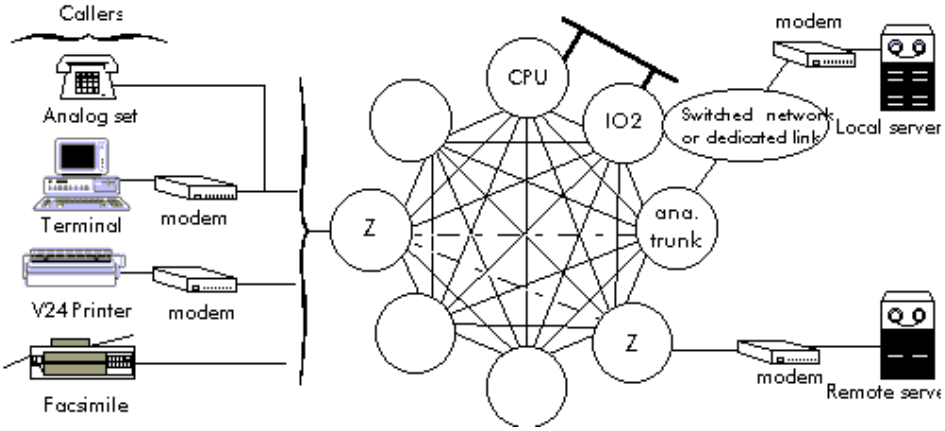
PRA board offering 1 E1 interface.

BPRA board offering 1 E1 interface and 3 E0 bus interfaces

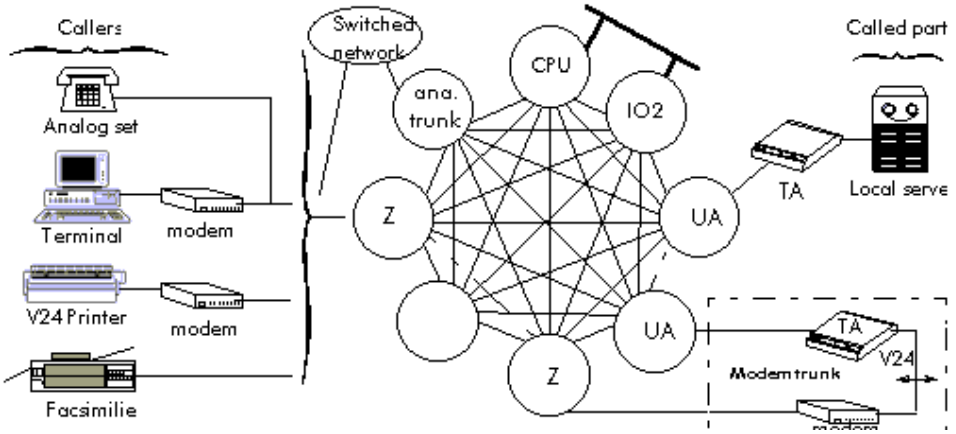
Terminal connection This takes place using interfaces behind the UA set or TA adapters: - asynchronous V24 interface, - synchronous V24/V35/V36 interface, - X21 interface, - S0 interface.


Alcatel 4400
V24Asyn 1
Simultaneous voice and data
19200 b/s max in V110
57600 b/s max in V14e
TA or UA set + option V24Asyn 1
V24Asyn 2
Simultaneous voice and data
19200 b/s max in V110
19200 b/s max in V120
TA or UA set + option V24 Asyn 2
Bus S0 (2B+D)
TA or UA set + option S0
V24Sync
19200 b/s max in V110
19200 b/s max in V120
TA or UA set + option V24 sync
V35/V36
56000 b/s max in V110
56000 b/s max in V120
TA or UA set + option V24 sync
X21
56000 b/s max in V110
640000 b/s max in V120
TA or UA set + option X21
V110
S0/V110 ISDN set
S0 bus (2B+D)
V24
modem
Videotex (digital mode)
UA set
Videotex (analog mode)
UA
Z
BRA
TA
Modem
local server
V24X25
X25 network
PRA
T2 (30B +D)
ISDN
T0 (2B +D)
Ana. trunk
STN
Digital extractor trunk
Modem trunk

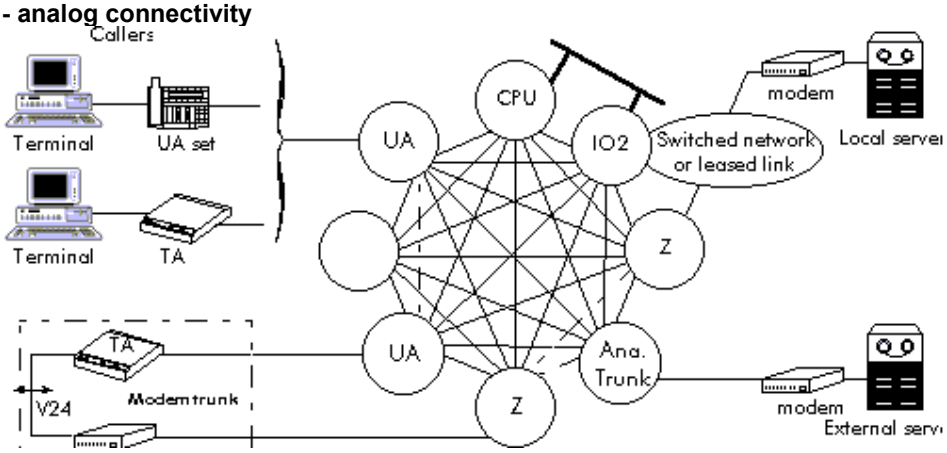
Analog - analog connectivity



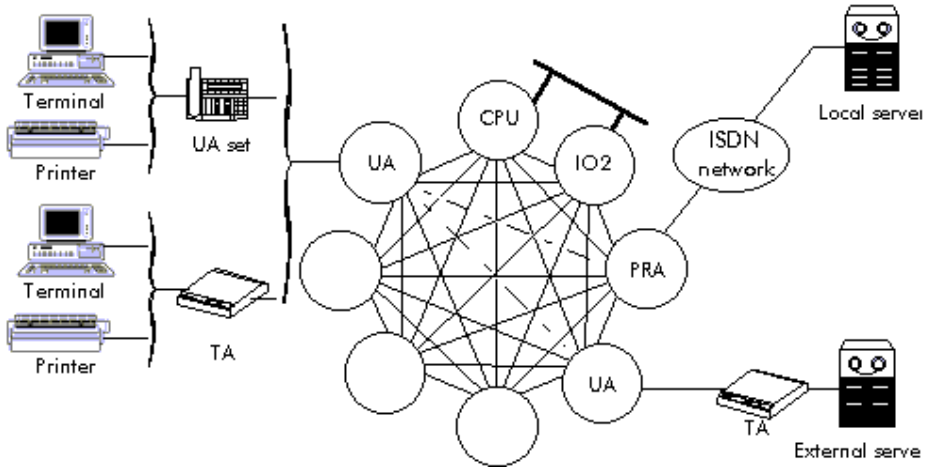
Analog - digital connectivity



Digital - analog connectivity



Digital - digital connectivity



Configuration of Inter-system links (E1/T2):

- PCM link is E1 link (uses PCM boards)
- ABC link is special link for inter-node connection (uses PRA boards)
- T2 is ISDN link used for public network connection (uses PRA board)

Time slot 0 is used for alarms, Time slot 16 is used for signaling.

ABC Link management (Inter node links):

- PRA coupler management
- Link configuration
- Channel assignments
- IP/X25 Tunnel management

ABC Trunk Group management (Links b/w heterogeneous systems):

- Trunk group creation
- **Coupler management**

QSIG Protocol:

QSIG is a modern, powerful and intelligent inter-PINX (Private Integrated services Network Exchange) signaling system designed specifically to meet the requirements for sophisticated communications services. It provides:

- a platform for future development supported by international standards organizations;

- a harmonized method for interconnecting multi-vendor equipment;
- a mechanism for manufacturers to provide innovative features within a heterogeneous environment;
- a flexible and cost efficient method of linking PINX equipment;

Experiment # 8
Design of Simple Networks using CISCO ConfigMaker

Objectives:

In this experiment students will learn CISCO ConfigMaker software tool and use it to design elementary networks using hosts, hubs, switches and routers.

Introduction:

Cisco ConfigMaker is an easy-to-use Windows 98/Me/NT/2000 application that configures Cisco routers, switches, hubs, and other devices. Using a graphical user interface (GUI), you draw your network, and then Cisco ConfigMaker creates the Cisco IOS configuration files for the devices on your network without requiring you to know the Cisco IOS command-line interface (CLI). You can also use Cisco ConfigMaker as an off-line tool. Without having the devices on-hand, you can draw and configure your entire network until you are ready to deliver the configuration to them.

To start Cisco ConfigMaker, select ***Start>Programs>Cisco ConfigMaker V2.5.1*** from the Windows Start menu.

Salient Features Overview:

Feature	**Cisco ConfigMaker Support**
Devices	• Routers-Cisco 800, 1000, 1600, 1700, 2500, 2600, 3600, and 4000 (excluding routers with Token Ring) • Switches-Cisco 1548, 1548M Micro Switch 10/100 • Hubs-Cisco 1538, 1538M Micro Hub 10/100, Cisco FastHub 412, 412M, 424, 424M • Stacks-Cisco Micro Hub Stack, Cisco FastHub Stack • Other-Cisco Cache Engine (only configures Web Cache Communication Protocol (WCCP) version 1 on the router)
LAN connections	Ethernet, Fast Ethernet
WAN connections	• ISDN BRI, ISDN PRI, ISDN leased line (Cisco 1603 and 1604 only) • Frame relay, Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), asynchronous, PPP over Ethernet (PPPoE) for Cisco 1700 series routers, and voice line • POTS (for the 800 routers)
Routing protocols	EIGRP, RIP version 2, Static Routing (IP only)

Virtual Private Network (VPN)	• Configures IPSec and Internet Key Exchange (IKE) • Uses pre-shared key method for authentication; configure hashing method, encryption method, security association (SA) timeout values • Draws VPN connections between point-to-point sites
Quality of service (QoS)	• Configures QoS settings on WAN interfaces to prioritize voice traffic • Configures Committed Access Rate (CAR) to limit bandwidth for certain sites and applications
Voice	• Supports voice-over-IP (VoIP) connection to telephones, facsimiles, Private Branch Exchanges (PBXs), and Public Switched Telephone Networks (PSTNs) • Supports an analog telephone connection to the Cisco 803 and 804 routers • Supports 2BRI-NT/TE voice interface cards (VICs) on Cisco 1751 router only • Configures QoS settings on WAN interfaces to prioritize traffic • Caller ID capability on VIC-2FXO-M1, VIC-2FXO-M2, VIC-2DID/FXS, and VIC-2FXS (1700 series only) • Direct Inward Dialing (DID) capability on VIC-2DID/FXS
Backup	Backs up a Frame Relay, PPP, HDLC, or an ISDN leased line connection with a dial up, an ISDN, or another serial connection
Simple Network Management Protocol (SNMP)	• Configures read community string and read/write community string. • Configures SNMP trap manager
Dynamic Host Control Protocol (DHCP)	Configures DHCP server or DHCP relay
CSU/DSU	Configures CSU/DSU module (not supported on ISDN PRI network modules)
Other features	• AutoDetect Device Wizard-automatically identifies your device • IP Subnet Calculator-calculates IP and subnet masks • Ping Device-pings any address on your network • Issue show commands-runs **show** commands on your router • WAN Configuration Worksheets-assists in gathering data for your connection • Instant Upgrade-easily upgrades Cisco ConfigMaker • Cisco ConfigMaker Tutorial-guide to using Cisco ConfigMaker

System requirements	• 80486 or Pentium-class computer • Windows 98, Windows Me, Windows 2000, or Windows NT 4.0 with at least Service Pack 3 • 16 MB RAM • 20 MB disk space • 800 x 600 display with at least 256 colors

Practice:

- Designing network of a lab using hosts and a hub
- Designing network of a building using hosts, hubs, and a switch.
- Designing network of two buildings connected with each other by a router.

Note: Network details including device type and IP address ranges will be specified in the lab by the instructors.

Experiment # 9
Point-to-point LAN extension by bridges and LAN connectivity over a WAN by routers using DSL link

Objective:

In this experiment students will learn the connectivity and configuration issues for a Point-to-point LAN extension by bridges and LAN connectivity over a WAN by routers using DSL link. Students will have hands-on practice for the configuration of the involved network components i.e. DSL equipment, bridges and routers.

Introduction:

The campus HDSL system provides connection between geographically distributed Ethernet Local Area Networks (LANs) in a campus environment. To provide the connection, the campus-REX performs MAC bridging or static IP routing over a HDSL line. Telephone-grade copper wiring can be used as the HDSL transmission medium.

When LANs are distributed over a large physical area (such as within a metropolitan area) or cabling is not available between sites, unloaded pair of coppers may be leased from a local carrier for LAN connectivity.

Digital Subscriber Line (DSL) technology is a modem technology that uses existing twisted-pair telephone lines to transport high-bandwidth data, such as multimedia and video, to service subscribers. The term *xDSL* covers a number of similar yet competing forms of DSL technologies, including ADSL, SDSL, HDSL, HDSL-2, G.SHDL, IDSL, and VDSL. xDSL is drawing significant attention from implementers and service providers because it promises to deliver high-bandwidth data rates to dispersed locations with relatively small changes to the existing telco infrastructure.

xDSL services are dedicated, point-to-point, public network access over twisted-pair copper wire on the local loop (last mile) between a network service provider's (NSP) central office and the customer site, or on local loops created either intrabuilding or intracampus

Routing is the act of moving information across an internetwork from a source to a destination. Along the way, at least one intermediate node typically is encountered. Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing

to the casual observer. The primary difference between the two is that bridging occurs at Layer 2 (the link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). This distinction provides routing and bridging with different information to use in the process of moving information from source to destination, so the two functions accomplish their tasks in different ways.

Exercise:

A. Point-to-point LAN extension by bridges using HDSL link

1. Connect the campus-REX unit1 to the console using COM1.
2. Log on the HyperTerminal utility. Press Spacebar and you will be asked to enter password. Hit Enter to skip the password.
3. You are now in the Main Menu. Go to System Settings Menu.
4. Go to System Parameters.
5. Set the System Date and Time. Assign the unit some ID. Don't change the password.
6. Return to System Settings Menu.
7. Go to HDSL Parameters Menu. Set the HDSL operating mode to be Standard. Set transceiver mode to Auto and HDSL Rate to E1.
8. Return to main menu.
9. Go to Data Port Settings Menu.
10. Go to Bridge/Router configuration.
11. Set Bridge/Router mode to Bridge, Encapsulation to HDLC, and Timing source to Internal.
12. Return to Data Port Settings Menu. Perform Write NVRAM operation and Reset the interface.
13. Configure the other unit also with the same settings.
14. Connect the units to each other on Line Port. Connect unit1 to the Hub1 and unit2 to the Hub2 on 10BaseT ports.

15. Connect the two terminals 1 and 2 on hubs 1 and 2, respectively.

16. Check the connectivity of the two terminals by Pinging each other.

B. LAN connectivity over a WAN by routers using HDSL link

1. Repeat steps 1 to 10 from part A.
2. Set Bridge/Router mode to Router and Encapsulation to HDLC.
3. Assign LAN and Line IP addresses and subnet masks. Enter the default gateway address. (Note: All IP addresses will be specified by the instructors in the lab).
4. Return to Data Port Settings Menu. Perform Write NVRAM operation and Reset the interface.
5. Configure the other unit also with the same settings except the IP addresses for this unit that will be specified by the instructors in the lab.
6. Repeat steps 14 to 16 from part A.

Experiment # 10
Design of Core Networks with Internet Connectivity using CISCO ConfigMaker

Objective:

In this experiment students will learn to design a core network with internet connectivity using CISCO ConfigMaker.

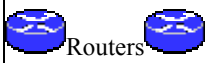
Introduction:

Cisco ConfigMaker is an easy-to-use Windows 98/Me/NT/2000 application that configures Cisco routers, switches, hubs, and other devices. Using a graphical user interface (GUI), you draw your network, and then Cisco ConfigMaker creates the Cisco IOS configuration files for the devices on your network without requiring you to know the Cisco IOS command-line interface (CLI). You can also use Cisco ConfigMaker as an off-line tool. Without having the devices on-hand, you can draw and configure your entire network until you are ready to deliver the configuration to them.

To start Cisco ConfigMaker, select ***Start>Programs>Cisco ConfigMaker V2.5.1*** from the Windows Start menu.

Supported Devices and Modules:

Cisco ConfigMaker supports the following Cisco devices, network modules, WICs, and VICs:


Routers

Cisco 800 series:	801, 802, 803, 804, 805, 811, 813
Cisco 1000 series:	1003, 1004, 1005
Cisco 1600 series:	1601, 1602, 1603, 1604, 1605
Cisco 1700 series:	1710, 1720, 1750, 1751
Cisco 2500 series:	2501, 2503, 2505, 2507, 2509, 2509-RJ, 2511, 2511-RJ, 2514, 2516, 2520, 2522, 2524
Cisco 2600 series:	2610, 2611, 2620, 2621
Cisco 3600 series:	3620, 3640
Cisco 4000 series:	4500, 4500-M, 4700, 4700-M

1600 Network Interface Cards

WICs

1 serial	1 T1 CSU/DSU
1 56/64K CSU/DSU	
1 ISDN BRI (U, S/T) {Cisco 1601, 1602, and 1605 only}	
1 ISDN BRI (S/T) LL {Cisco 1603 and 1604 only}	

1700 Network Interface Cards

WICs

1 serial	1 56/64K CSU/DSU
2 serial	1 T1 CSU/DSU
1 ISDN BRI (U, S/T)	2 async/sync
1 Ethernet	ADSL WIC (hardware detection only)

VICs {Cisco 1750 and Cisco 1751 only}

2 voice FXS	2 voice FXO	2 voice E/M
2 voice BRI-NT/TE	2 voice FXO-M1	2 voice FXO-M2
2 voice FXO-M3	2 voice DID/FXS	

2524 Network Interface Cards

WICs

5-in-1 serial	1 T1 CSU/DSU
1 ISDN BRI (U, S/T)	2-wire 56/64 Kbps CSU/DSU

	4-wire 56/64 Kbps CSU/DSU

2600 Network Interface Cards

Network Modules:

1 Ethernet	2 E1/ISDN PRI
4 Ethernet	4 async/sync
4 ISDN BRI (U, S/T)	8 async/sync
8 ISDN BRI (U, S/T)	16 async
1 T1/ISDN PRI	32 async
2 T1/ISDN PRI	1 slot VIC
1 E1/ISDN PRI	2 slot VIC

WICs

1 serial	1 56/64K CSU/DSU
2 serial	1 T1 CSU/DSU
1 ISDN BRI (U, S/T)	2 async/sync

VICs

2 voice FXS	2 voice FXO	2 voice E/M

3600 Network Interface Cards

Network Modules:

1 Ethernet	1 10/100 Ethernet, 1 T1/ISDN PRI	4 serial
4 Ethernet	1 10/100 Ethernet, 2 T1/ISDN PRI	4 async/sync
1 Ethernet, 2 WAN Slot	1 10/100 Ethernet, 1 E1/ISDN PRI	8 async/sync
2 Ethernet, 2 WAN Slot	1 10/100 Ethernet, 2 E1/ISDN PRI	16 async
1 Fast Ethernet	1 T1/ISDN PRI	32 async
Compression Module	2 T1/ISDN PRI	1 slot VIC
4 ISDN BRI (U, S/T)	1 E1/ISDN PRI	2 slot VIC
8 ISDN BRI (U, S/T)	2 E1/ISDN PRI	

WICs

1 serial	1 56/64K CSU/DSU
1 ISDN BRI (U, S/T) {WIC-1B}	1 T1 CSU/DSU
1 ISDN BRI (U, S/T) {WIC36-1B}	

VICs

2 voice FXS	2 voice FXO	2 voice E/M

4000 Network Interface Cards

Network Modules:

2 Ethernet	4 ISDN BRI (U, S/T)	2 serial
6 Ethernet	8 ISDN BRI (U, S/T)	4 serial
1 Fast Ethernet	1 T1/ISDN PRI	2 serial, 16 async/sync
	1 E1/ISDN PRI	

Hubs

Cisco 1500 series	Cisco 1538, 1538M Micro Hub 10/100
Cisco Micro Hub Stack	Cisco Micro Hub 10/100 Stack
Cisco FastHub 400 series	Cisco FastHub 412, 412M, 424, 424M

Switches

Cisco 1548, 1548M Micro Switch 10/100

Practice:

- Design a primitive network of a university with internet connectivity.

Note: Network details including device type and IP address ranges will be specified in the lab by the instructors.

Experiment # 11

A Visit to KFUPM Data Network