INTRODUCTION TO INTERNET & COMPUTER NETWORKS

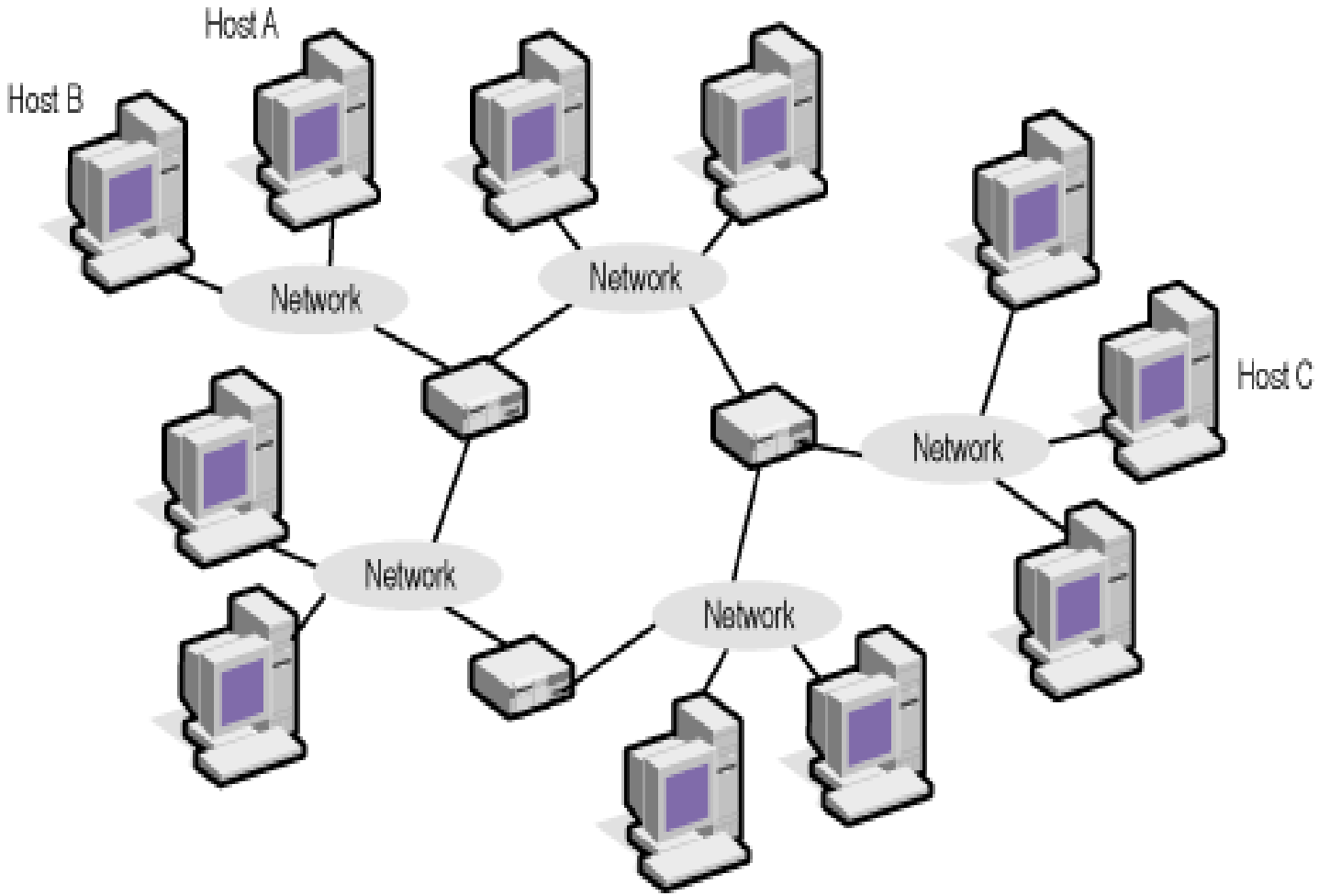
UNIVERSITY
OF PETROLEUM
& ENERGY STUDIES

| Aug 2014|

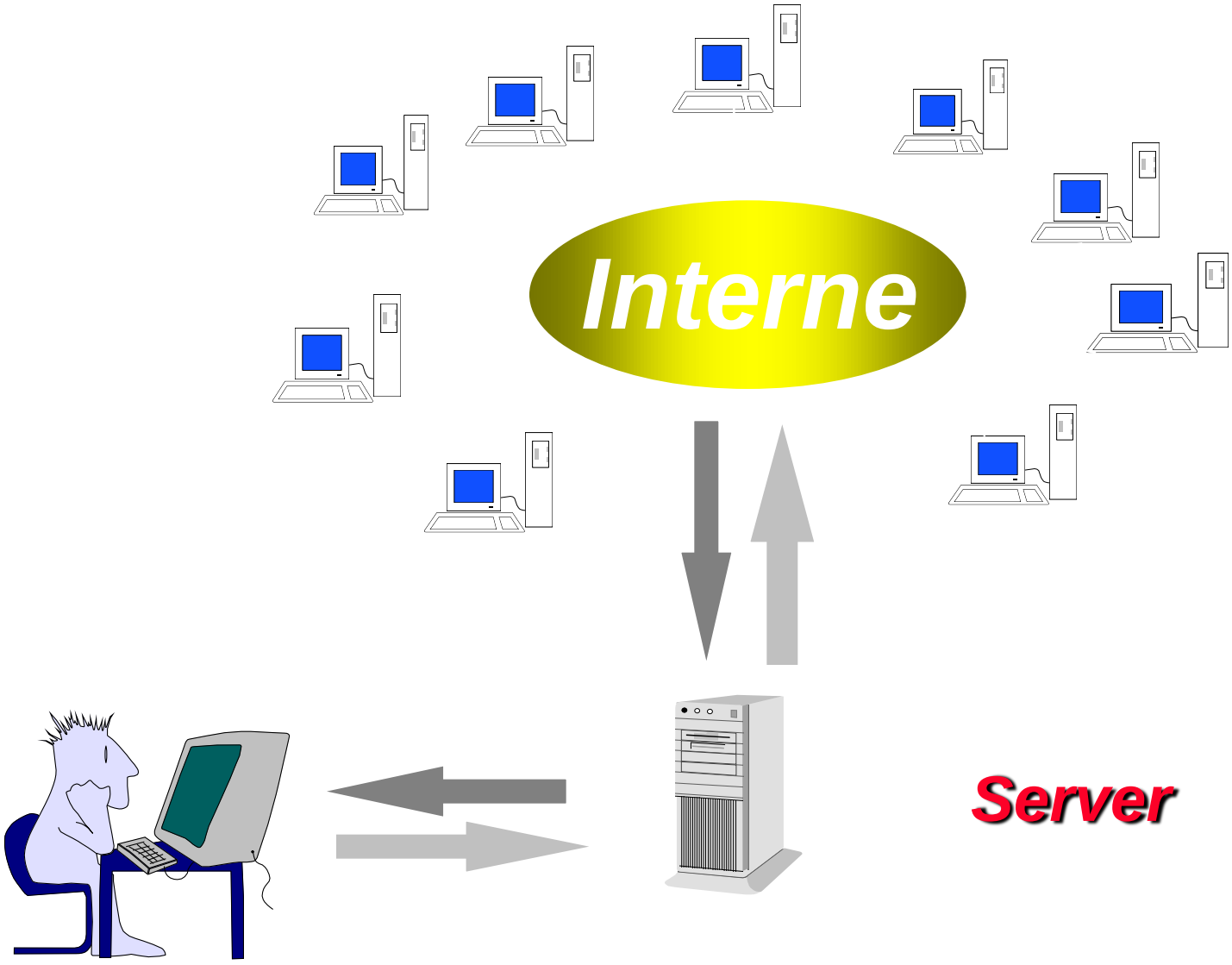
What is Internet?

- The Internet is “The Network of Networks”
- Internet is like a phone system which
  - -connects(almost anywhere in the world)
  - -Exchanges information
  - -Acts as Global link between regional networks
  - -Allows unrestricted access
- Used for
  - - Communication through email , Chatting
  - - News groups
  - - Files transfer
  - - Documents,data(multimedia)sharing etc

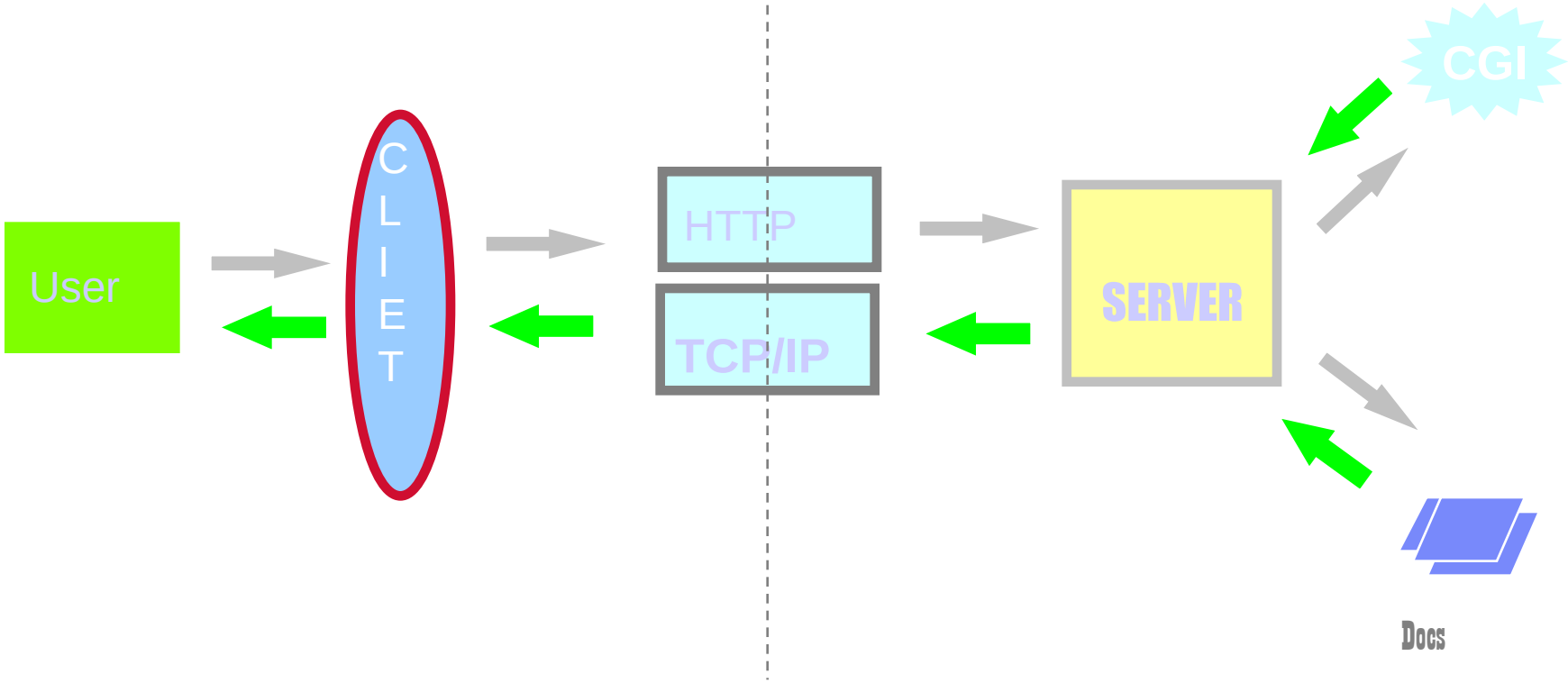
Internet: An Illustration



Model of Internet Setup



How it all works ?



Who Uses The Internet ?

- Institutions like : academic, government and commercial
  - -to allow their staff to collaborate with peers
  - -to rapidly coordinate complex, dispersed worldwide activities for information gathering and sharing
  - -by interconnecting their enterprise networks via Internet backbone providers
- Business enterprises which specialize in providing or for global trading
- General public via local access providers and gateways to commercial public e-mail carriers and other kinds of networks

What is the World Wide Web?

The World Wide Web (WWW) is a global interactive, dynamic, cross platform, graphical hypertext information system that runs on the Internet.

Internet Standard Domain Names

- edu educational organizations
- com commercial organizations
- gov government institutions
- mil military groups
- net major network support centres
- org organizations other than the above
- int international organizations
- country code two character identifier for a country in the geographical scheme

What is a Web Browser?

A Web Browser is special software such as Netscape, Mosaic or Internet Explorer. These browsers allow a user to view Web pages delivered from a client server (Web Site) situated at a particular URL on the World Wide Web

Netscape

Internet Explorer

Basic Terminology used in Internet Technology

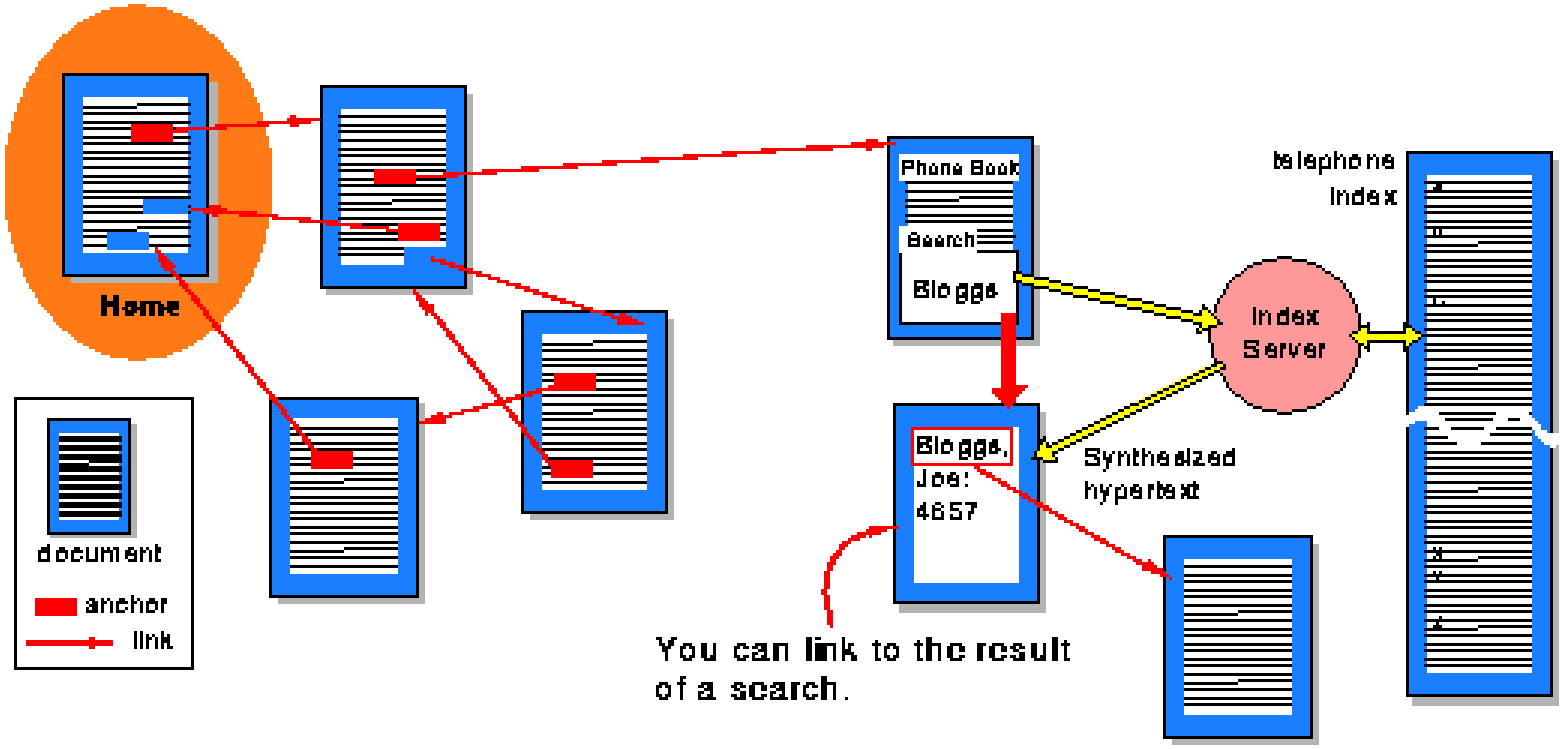
* World Wide Web (www)
* Web site
* Portal
* Uniform Resource Locater
* Home page
* Hyperlink
* Server s/w
* Browser s/w
* Protocols like TCP/IP, HTTP,FTP
* ISP (Internet Service Provider)

A web Page is a single document written in HTML (Hypertext Markup Language) that includes the text of the document,its structure, any links to other documents and graphic images and other media.

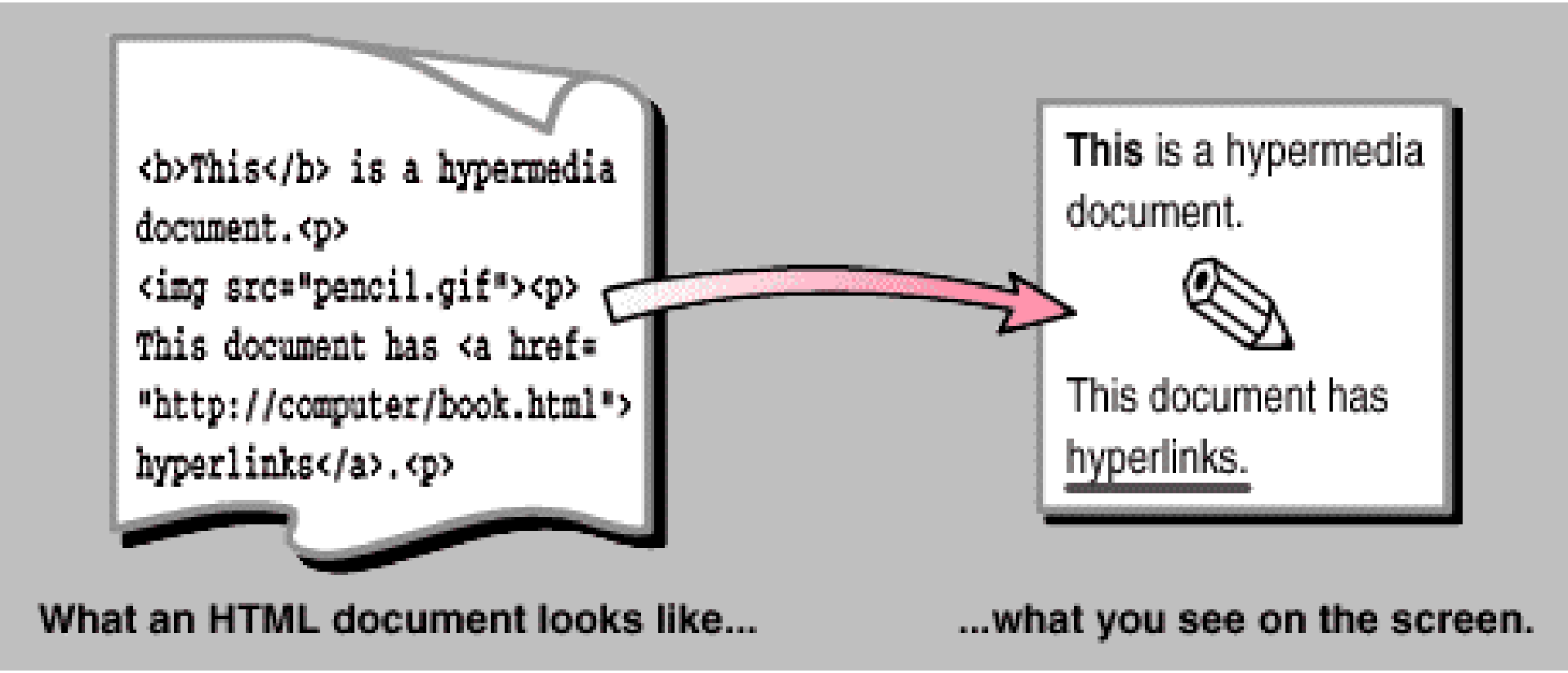
HTML- WWW documents are authored using the Hypertext Markup Language.

Homepage is a Hypertext document a server will serve as default.

HYPERTEXT



HTML



Uniform Resource Locator

- Method of accessing Internet Resources
- URLs are used by web browsers to connect you directly to a specific document or homepage on WWW, without having to know where that resource is physically located.

Jargon for the Internet ...

- **URL** , Uniform Resource Locator.

http://www.nic.in:80/nicnet.html

Retrieval Method

Host Address

Port

Path/Document

What is a protocol?

In networking and Communications, the formal specification that defines the procedures to be followed when transmitting and receiving data. Protocols define the format, timing, sequence and error checking used on the network.

HTTP- Hypertext Transfer Protocol is the stateless protocol used for data transfer within WWW.

Search Engines on the WWW

- Tools on the WWW used to search and find web sites related to a particular topic
- provide for searching using keywords and boolean operators
- Popular ones are Alta Vista, Infoseek, HotBot,Web Crawler, Lycos and Yahoo
- Over 600 + at present

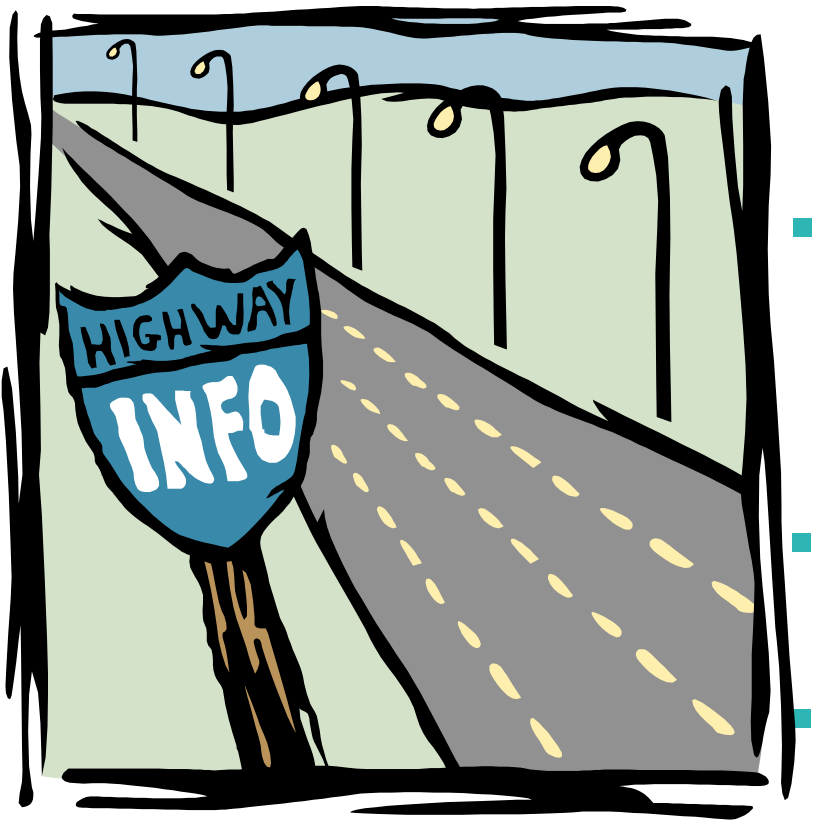
Web surfing

- Start the Web browser, for eg. Internet Explorer
- In the Address box type web site address of some search engine (for eg. http://www.google.com).
- In the Search box which appears, type in the topic on which You want information, then click to start search.
- A number of websites on the topic you have selected will appear with brief description.
- Select and double click the site which seems to be more relevant to your requirement.

What is a search engine?

- A search engine is an Internet tool that locates web pages and sorts them according to specified keywords.

Types of search engines

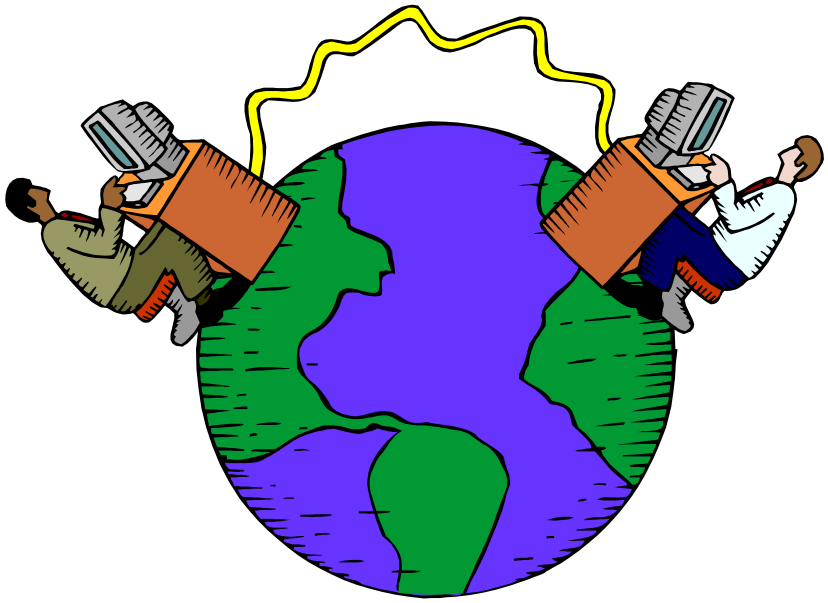


- Yahoo and Alta Vista are the most useful search engines for beginning searches.
- Google, Northern Light, and Snap access the greatest percentage of the World Wide Web--only around 15-16%.
- Dogpile will search through several search engines at once.
- A collection of search engine links is available at the OWL web site: owl.english.purdue.edu

Limit your keyword search

- It is a good idea to read the directions fo each search engine to get the most out of your search.
- Use words like AND and OR to limit your search and get more specified information.

Identify the web site



- Assess the authorship, content, and purpose of the web site.
- This is important because
  - many web sources are not checked for accuracy.
  - some personal sites are used to express individual opinions about issues, but not necessarily the facts.

List of some Search Engines

- www.yahoo.com
- www.indiaconnect.com
- www.lycos.com
- www.excite.com
- www.economictimes.com
- www.nic.in
- www.indianexpress.com
- www.askjeeves.com

Creating Bookmarks

1.Adding Current website to the desired "favourites " folder

- Click **Favourites>>Add to favourites**

If you want to keep the desired site address in a new folder then create it following the steps give below:

- Select **New Folder**
- Type the Folder Name
- Click **OK>>OK.**

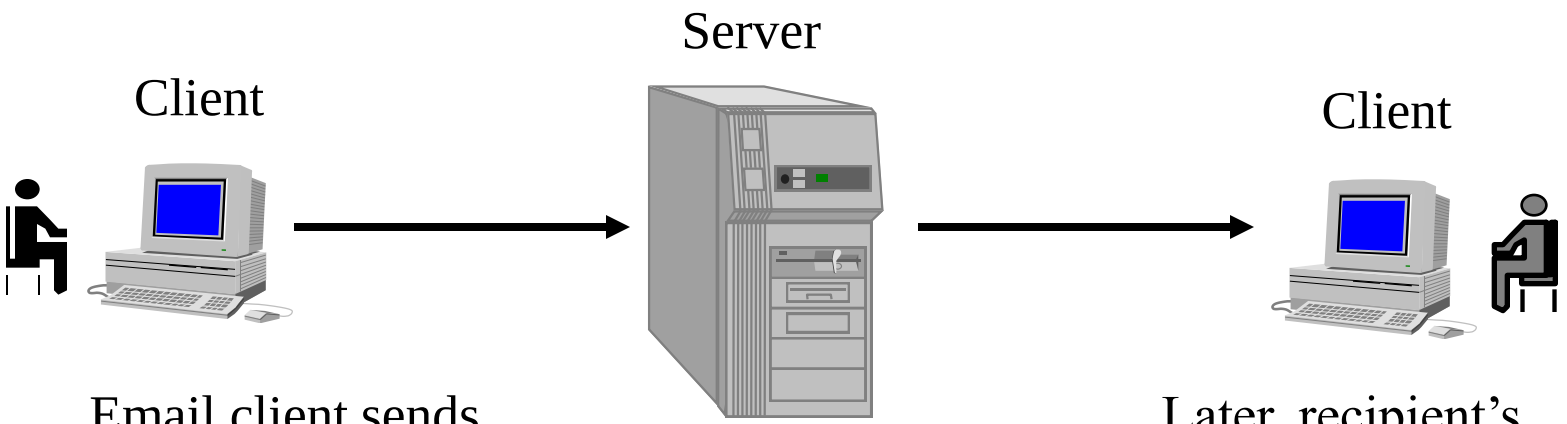
2.Visiting your favourites sites

- **Click Favourites**
- **Click on desired folder**
- **Select the desired site address, which you had earlier book marked.**

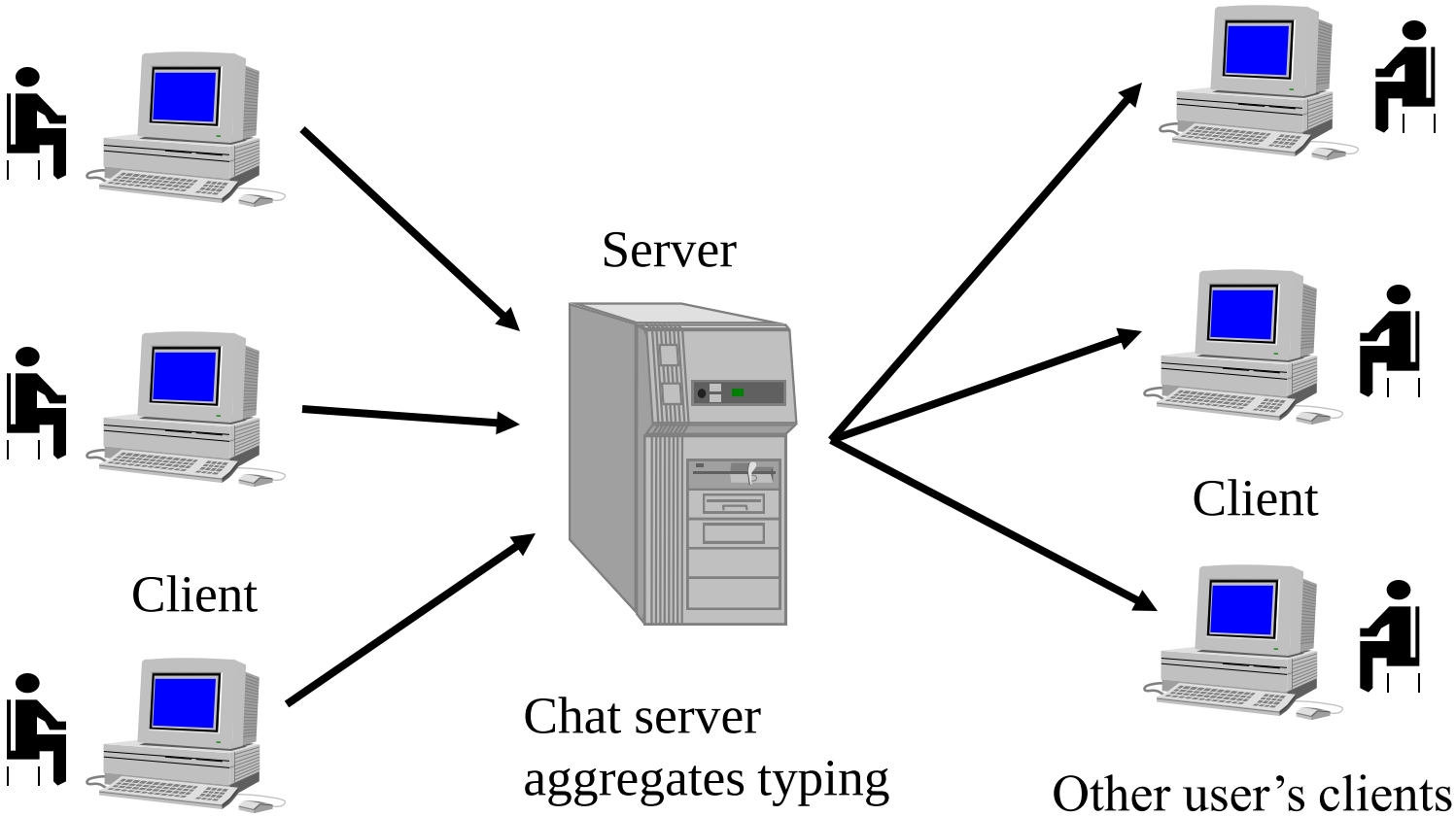
Web Based Email

- Pros
  - Graphical user interface
  - Greater functionality than host based
  - Complementary to client based mail
  - Need only browser
- Cons
  - Less functionality than client based
  - Live connection

Email application



Chat application



Chat clients send user's typing to server

Chat server aggregates typing from all users and sends to all clients

Other user's clients display aggregated typing from chat server

Visit the World Wide Web via the Internet

UNIVERSITY
OF PETROLEUM
& ENERGY STUDIES

Come and take your first trip into Cyber Space...

It won't be your last !

CYBER-SAFETY BASICS

INTRODUCTION

These slides provides some basic information and practical suggestions for protecting your personal information and computer from cyber-attacks. Cyber-safety topics covered include:

What is Cyber-safety?	Cyber-safety Threats	Consequences of Inaction
Cyber-safety Actions	Cyber-safety at Home &Work	Campus Cyber-safety Services

What is…

WHAT IS CYBER-SAFETY?

- Cyber-safety is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks.
- As part of this policy, all campus units provide annual reports demonstrating their level of compliance.
- Further, there are services in place to help all students, faculty and staff meet the cyber-safety standards.

UC Davis Mrak Hall

CYBER-SAFETY THREATS

First, let's talk about some common cyber-safety threats and the problems they can cause . . .

Viruses

Viruses infect computers through email attachments and file sharing. They delete files, attack other computers, and make your computer run slowly. One infected computer can cause problems for all computers on a network.

Hackers

Hackers are people who "trespass" into your computer from a remote location. They may use your computer to send spam or viruses, host a Web site, or do other activities that cause computer malfunctions.

Identity Thieves

People who obtain unauthorized access to your personal information, such as Social Security and financial account numbers. They then use this information to commit crimes such as fraud or theft.

Spyware

Spyware is software that "piggybacks" on programs you download, gathers information about your online habits, and transmits personal information without your knowledge. It may also cause a wide range of other computer malfunctions.

CONSEQUENCES OF INACTION

In addition to the risks identified on the previous slide, you may face a number of other consequences if you fail to take actions to protect personal information and your computer. Consequences include:

Loss of access to the campus computing network

Loss of confidentiality, integrity and/or availability of valuable university information, research and/or personal electronic data

Lawsuits, loss of public trust and/or grant opportunities, prosecution, internal disciplinary action or termination of employment

CYBER-SAFETY ACTIONS

- The following slides describe the top seven actions you can take to protect personal information and your computer. These actions will help you meet the Cyber-safety Program policy standards.
- By implementing all seven of these security measures, you will protect yourself, others, and your computer from many common threats.
- In most cases, implementing each of these security measures will only take a few minutes.

Top Seven Cyber-safety Actions

Faculty and staff should work with their technical support coordinator before implementing these measures.

1. Install OS/Software Updates

2. Run Anti-virus Software

3. Prevent Identity Theft

4. Turn on Personal Firewalls

5. Avoid Spyware/Adware

6. Protect Passwords

7. Back up Important Files

Install OS/Software Updates

- Updates-sometimes called *patches*-fix problems with your operating system (OS) (e.g., Windows XP, Windows Vista, Mac OS X) and software programs (e.g., Microsoft Office applications).
- Most new operating systems are set to download updates by default. After updates are downloaded, you will be asked to install them. Click yes!
- To download patches for your system and software, visit:
  - Windows Update: http://windowsupdate.microsoft.com to get or ensure you have all the latest operating system updates only. Newer Windows systems are set to download these updates by default.
  - Microsoft Update: http://www.update.microsoft.com/microsoftupdate/ to get or ensure you have all the latest OS **and** Microsoft Office software updates. You must sign up for this service.
  - Apple: http://www.apple.com/support
  - Unix: Consult documentation or online help for system update information and instructions.
- Be sure to restart your computer after updates are installed so that the patches can be applied immediately.

RUN ANTI-VIRUS SOFTWARE

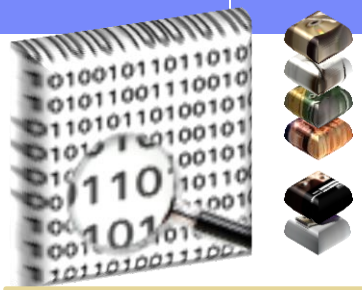
- To avoid computer problems caused by viruses, install and run an anti-virus program like Sophos.
- Periodically, check to see if your anti-virus is up to date by opening your anti-virus program and checking the *Last updated:* date.
- Anti-virus software removes viruses, quarantines and repairs infected files, and can help prevent future viruses.

PREVENT IDENTITY THEFT

- Don't give out financial account numbers, Social Security numbers, driver's license numbers or other personal identity information unless you know exactly who's receiving it. Protect others people's information as you would your own.
- Never send personal or confidential information via email or instant messages as these can be easily intercepted.
- Beware of phishing scams - a form of fraud that uses email messages that appear to be from a reputable business (often a financial institution) in an attempt to gain personal or account information. These often do not include a personal salutation. Never enter personal information into an online form you accessed via a link in an email you were not expecting. Legitimate businesses will not ask for personal information online.
- Order a copy of your credit report from each of the three major credit bureaus-Equifax, Experian, and Trans Union. Reports can be ordered online at each of the bureaus' Web sites. Make sure reports are accurate and include only those activities you have authorized.

Turn on Personal Firewalls

- Check your computer's security settings for a built-in personal firewall. If you have one, turn it on. Microsoft Vista and Mac OSX have built-in firewalls. For more information, see:
  - Mac Firewall (docs.info.apple.com/article.html?path=Mac/10.4/en/mh1042.html)
  - Microsoft Firewall (www.microsoft.com/windowsxp/using/networking/security/winfirewall.mspx)
  - Unix users should consult system documentation or online help for personal firewall instructions and/or recommendations.
- Once your firewall is turned on, test your firewall for open ports that could allow in viruses and hackers. Firewall scanners like the one on http://www.auditmypc.com/firewall-test.asp simplify this process.
- Firewalls act as protective barriers between computers and the internet.
- Hackers search the Internet by sending out pings (calls) to random computers and wait for responses. Firewalls prevent your computer from responding to these calls.



AVOID SPYWARE/ADWARE

- Spyware is a type of malware that is installed on computers and that collects information about users without their knowledge.
- Adware or advertising-supported software is any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used.
- Spyware and adware take up memory and can slow down your computer or cause other problems.
- Use Spybot and Ad-Aware to remove spyware/adware from your computer.
- Be wary of invitations to download software from unknown internet sources.

PROTECT PASSWORDS

- Do not share your passwords, and always make new passwords difficult to guess by avoiding dictionary words, and mixing letters, numbers and punctuation.
- Do not use one of these common passwords or any variation of them: qwerty1, abc123, letmein, password1, iloveyou1, (yourname1), baseball1.
- Change your passwords periodically.
- When choosing a password:
  - Mix upper and lower case letters
  - Use a minimum of 8 characters
  - Use mnemonics to help you remember a difficult password
- Store passwords in a safe place.

Back Up Important Files

- Reduce your risk of losing important files to a virus, computer crash, theft or disaster by creating back-up copies.
- Keep your critical files in one place on your computer's hard drive so you can easily create a back up copy.
- Save copies of your important documents and files to a CD, online back up service, flash or USB drive, or a server.
- Store your back-up media in a secure place away from your computer, in case of fire or theft.
- Test your back up media periodically to make sure the files are accessible and readable.

Home

CYBER-SAFETY AT HOME

- Physically secure your computer by using security cables and locking doors and windows in the dorms and off-campus housing.
- Avoid leaving your laptop unsupervised and in plain view in the library or coffee house, or in your car, dorm room or home.
- Set up a user account and password to prevent unauthorized access to your computer files.
- Do not install unnecessary programs on your computer.
- Microsoft users can download the free Secunia Personal Software Inspector (https://psi.secunia.com/), which lets you scan your computer for any missing operating system or software patches and provides instructions for getting all the latest updates.

CYBER-SAFETY AT WORK

- Be sure to work with your technical support coordinator before implementing new cyber-safety measures.
- Talk with your technical support coordinator about what cyber-safety measures are in place in your department.
- Report to your supervisor any cyber-safety policy violations, security flaws/weaknesses you discover or any suspicious activity by unauthorized individuals in your work area.
- Physically secure your computer by using security cables and locking building/office doors and windows.
- Do not install unnecessary programs on your work computer.

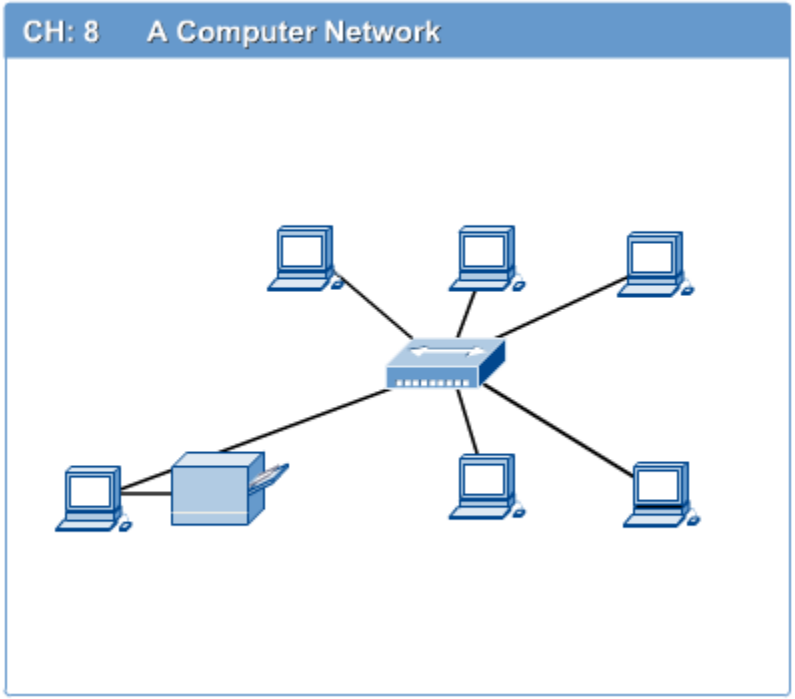
CAMPUS CYBER-SAFETY SERVICES

Offers services and software to protect the campus network against cyber-safety attacks. These include:

Services	Software
▪ Campus email virus filtering ▪ Campus firewall services ▪ Email attachment filtering ▪ Vulnerability scanning ▪ Intrusion prevention system	▪ Free anti-virus software: Sophos Anti-virus ▪ Free encryption software: Pointsec for PC ▪ Free change management software: Tripwire

Computer Networks

- Computer network connects two or more autonomous computers.
- The computers can be geographically located anywhere.



LAN, MAN & WAN

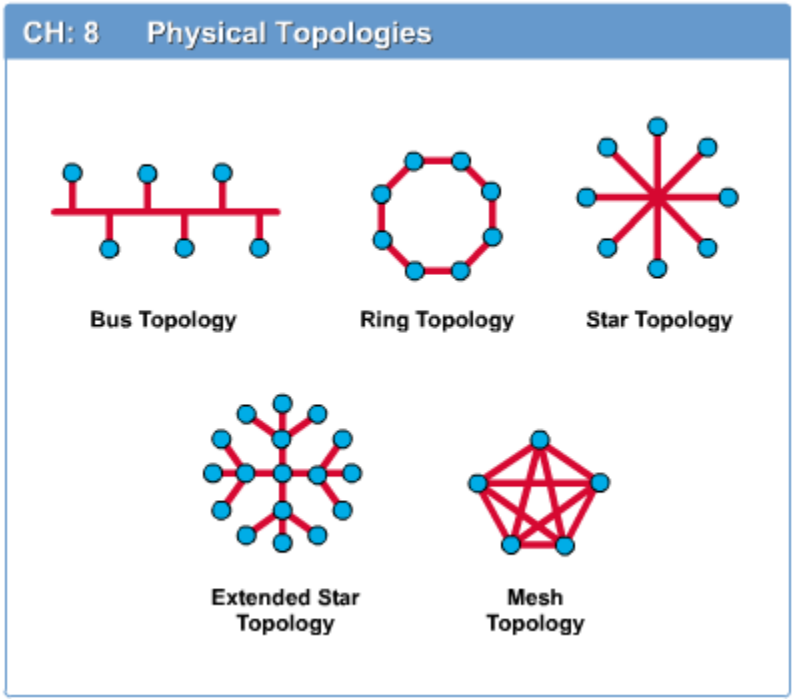
- Network in small geographical Area (Room, Building or a Campus) is called LAN (Local Area Network)
- Network in a City is call MAN (Metropolitan Area Network)
- Network spread geographically (Country or across Globe) is called WAN (Wide Area Network)

Applications of Networks

- **Resource Sharing**
  - Hardware (computing resources, disks, printers)
  - Software (application software)
- **Information Sharing**
  - Easy accessibility from anywhere (files, databases)
  - Search Capability (WWW)
- **Communication**
  - Email
  - Message broadcast
- **Remote computing**
- **Distributed processing (GRID Computing)**

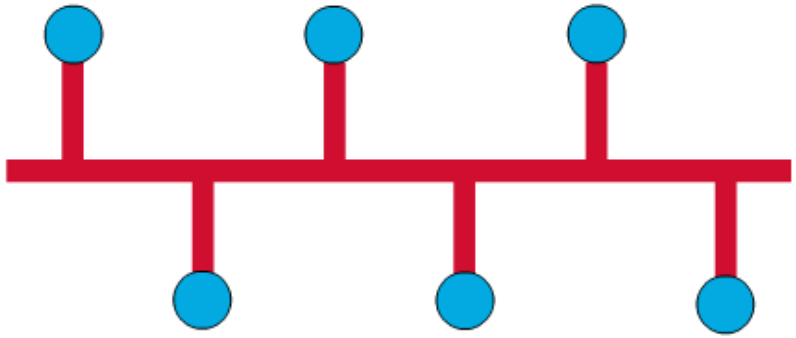
Network Topology

- The network topology defines the way in which computers, printers, and other devices are connected. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.



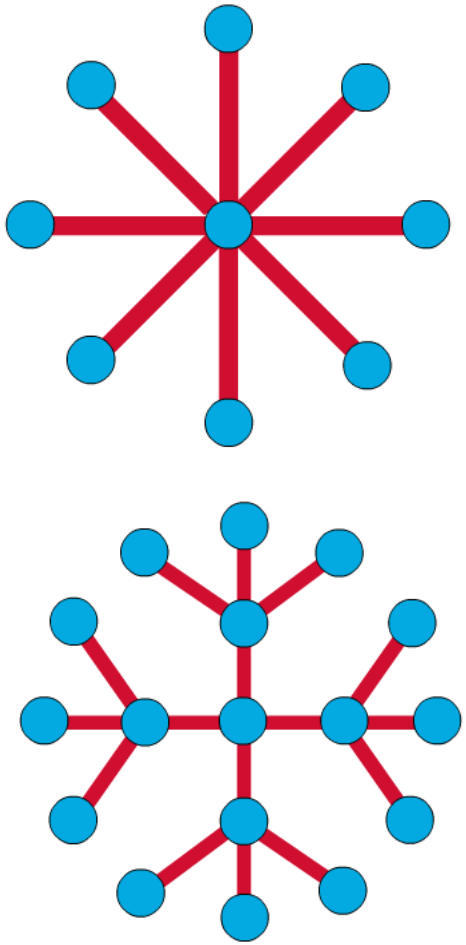
Bus Topology

- Commonly referred to as a linear bus, all the devices on a bus topology are connected by one single cable.



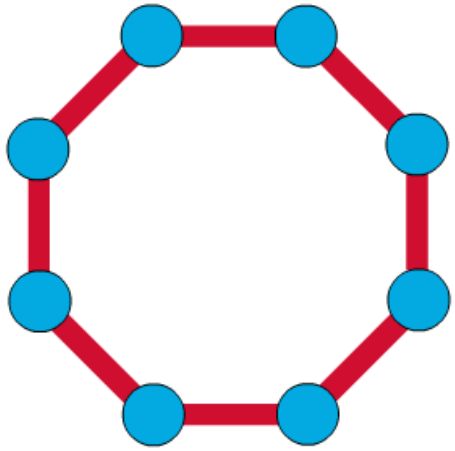
Star & Tree Topology

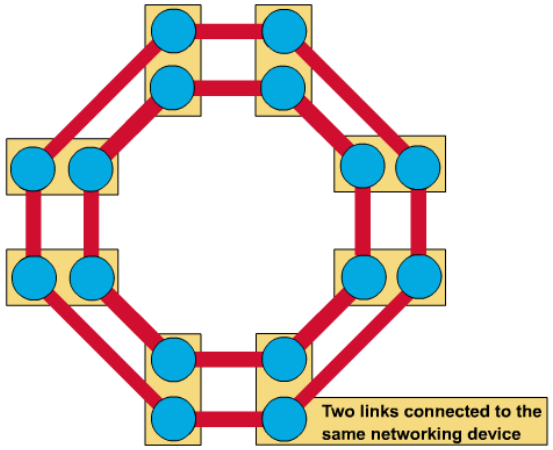
- The star topology is the most commonly used architecture in Ethernet LANs.
- When installed, the star topology resembles spokes in a bicycle wheel.
- Larger networks use the extended star topology also called tree topology. When used with network devices that filter frames or packets, like bridges, switches, and routers, this topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.



Ring Topology

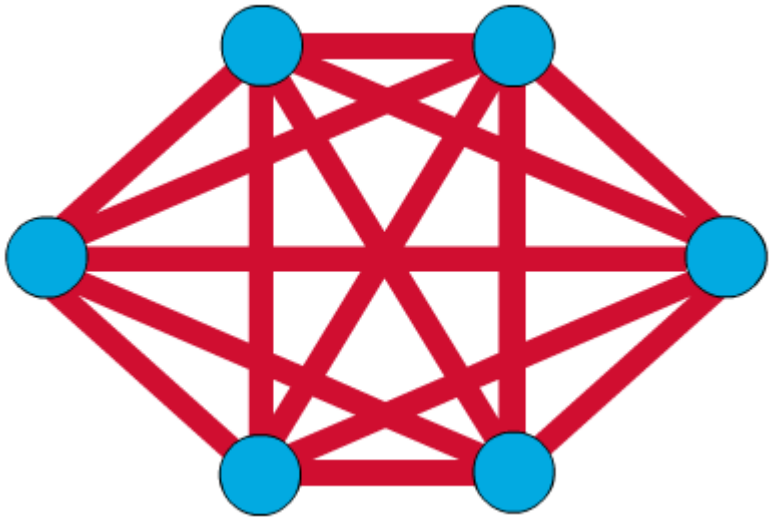
- **A frame travels around the ring, stopping at each node. If a node wants to transmit data, it adds the data as well as the destination address to the frame.**
- **The frame then continues around the ring until it finds the destination node, which takes the data out of the frame.**
  - Single ring – All the devices on the network share a single cable
  - Dual ring – The dual ring topology allows data to be sent in both directions.





Mesh Topology

- The mesh topology connects all devices (nodes) to each other for redundancy and fault tolerance.
- It is used in WANs t interconnect LANs and f mission critical networl like those used by banl and financial institutions.
- Implementing the mes topology is expensive ar difficult.



Network Components

- Physical Media
- Interconnecting Devices
- Computers
- Networking Software
- Applications

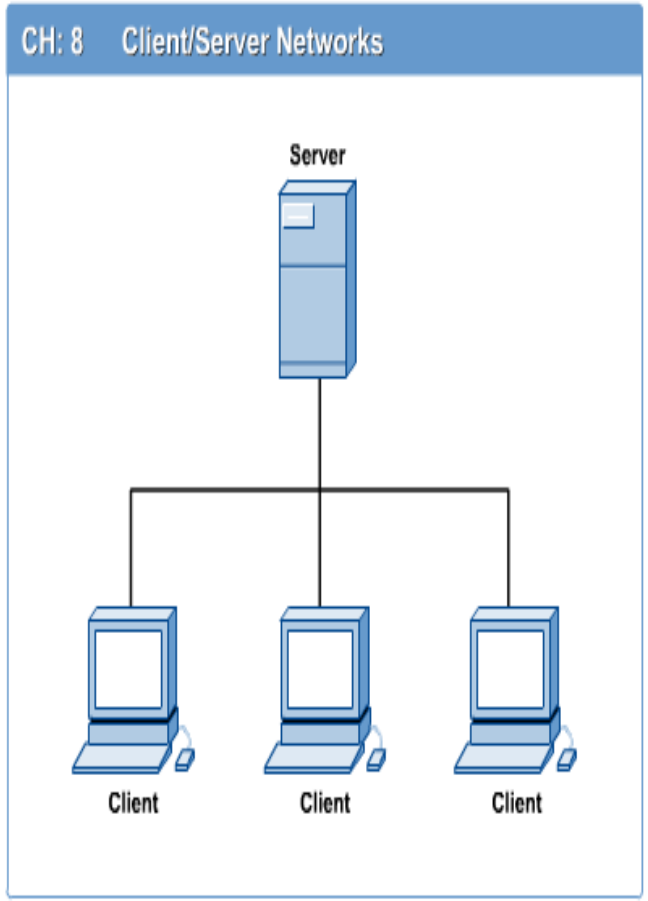
Networking Devices

- **HUB, Switches, Routers, Wireless Access Points, Modems etc.**

Computers: Clients and Servers

- In a client/server network arrangement, network services are located in a dedicated computer whose only function is to respond to the requests of clients.

- The server contains the file, print, application, security, and other services in a central computer that is continuously available to respond to client requests.



Transmission Media

UNIVERSITY OF PETROLEUM & ENERGY STUDIES
Harnessing Energy through Knowledge
UNIVERSITY
OF PETROLEUM
& ENERGY STUDIES

- Guided
  - Twisted Pair
  - Cable
  - Fiber
  - Medium more important than the signal
- Unguided
  - Atmosphere
  - Outer Space
  - Signal more important than the medium

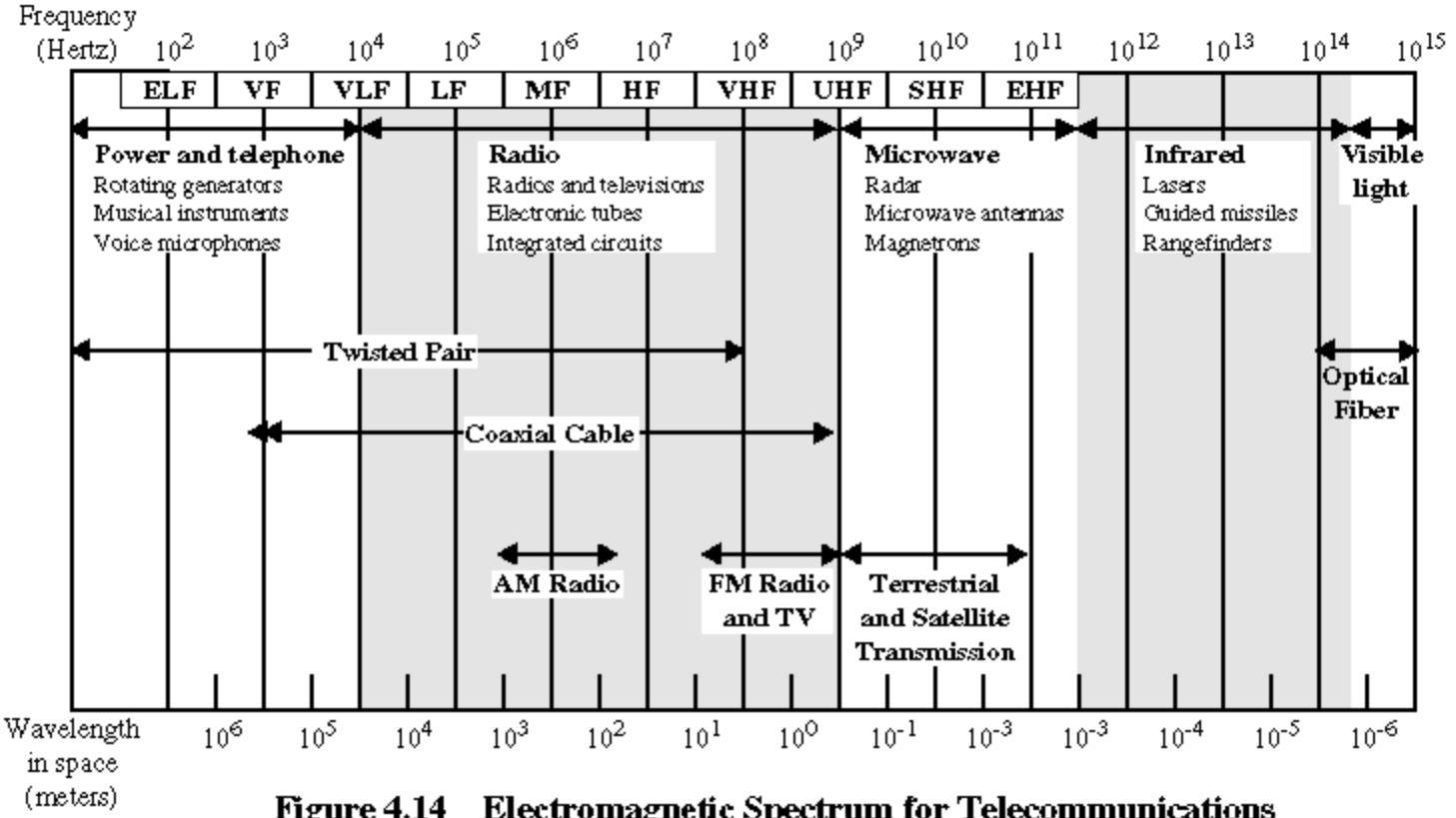


Figure 4.14 Electromagnetic Spectrum for Telecommunications

Twisted Pair

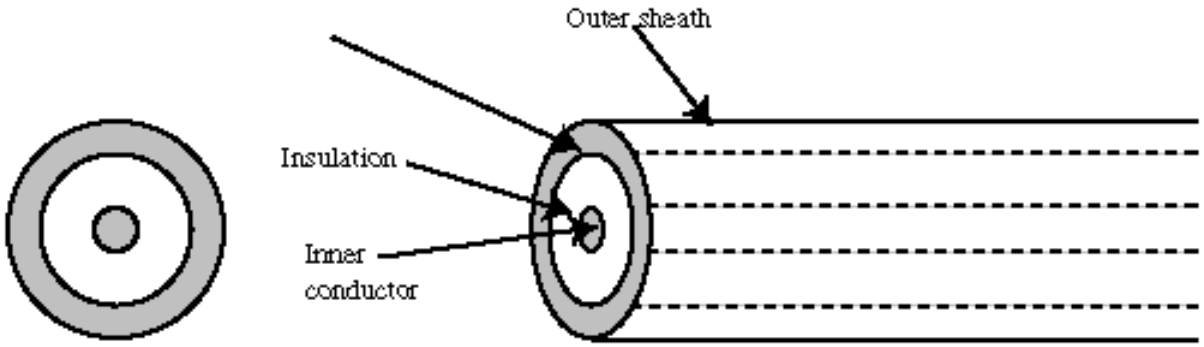
- Two insulated copper wires in a spiral
- Number of pairs are bundled together
- Twisting decreases crosstalk
- Most common form for analog and digital
- Used in telephone system
- Subscriber loops
  - From a person's home to the local office of the phone company
- LANS
  - 10Mbps with newer at 100Mbps

Twisted pair

- Long Distance
  - 4 Mbps
  - ISDN – Integrated Services Digital Network
- Digital
  - Repeaters required every 2 –3 kilometers
- Analog
  - Amplifiers required every 5-6 kilometers
  - Bandwidth of 250KHz, carry a few voice channels
- Susceptible to noise, shielded and unshielded
- Compared to optical and coax twisted pair is limited in bandwidth, distance, and data rate

Coaxial Cable

- Hollow outer cylindrical conductor surrounding a single view
- Most versatile of mediums, used for TV, long distance telephone,and LAN'S



—Outer conductor is braided shield
—Inner conductor is solid metal
—Separated by insulating material
—Covered by padding

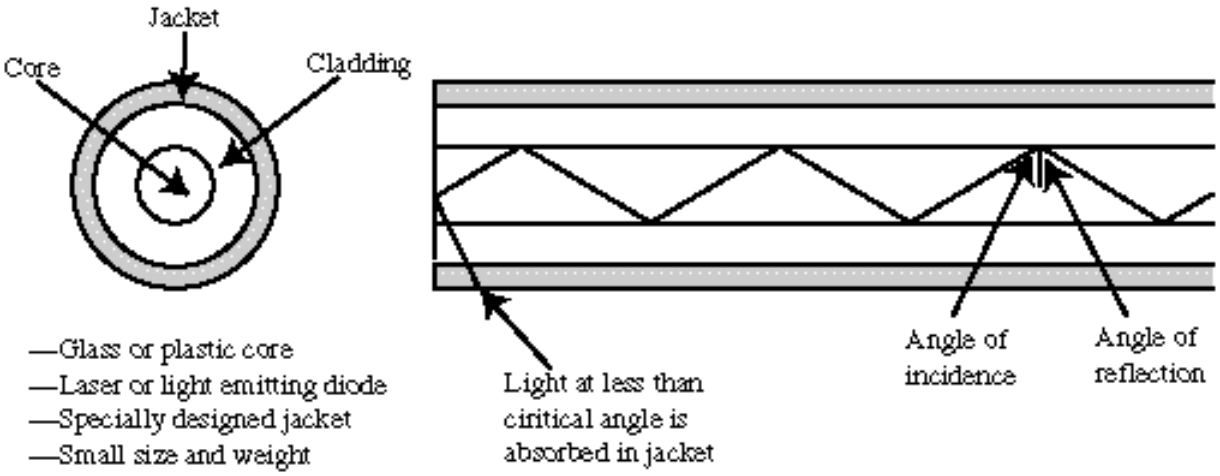
(b) Coaxial cable

Coaxial Cable

- Part of long distance telephone network
- With FDM can carry over 10,000 voice channels
- Transmits both analog and digital signals
- Frequency characteristics superior to twisted pair
  - Less susceptible to noise
- For long distance
  - Amplifiers needed every few kilometers
  - Repeaters needed every kilometer or so

Optical fiber

- Thin, flexible light passing material made from glass or plastic
- Grouped into cables



(c) Optical Fiber

Optical fiber

- Better than coaxial cable or twisted pair
- Data rates of 2Gbps over 10's of Km
- Light weight – good for buildings
- Lower attenuation than coax or twisted
- Not effected by extreme electromagnetic fields
  - Crosstalk and impulse
- Very difficult to tap – good security
- Applications
  - Long Haul trunks, metro trunks, rural exchange trunks, more recently beginning to displace twisted pair in subscriber loops and in LANS

Optical Fiber

- Operates in range 10**14 to 10**15 Hz
  - Infrared and visible spectrum
- Multimode
  - Variety of angles of light will reflect and propogate
- Single Mode
  - Radius of the core = order of a wavelength
  - Only single angle passes
  - Superior performance
- Two different light sources – both emit light when voltage applied
  - LED – Light Emitting Diode – less costly, longer life
  - ILD - Injection Laser Diode – greater data rate

Wireless

- Antennae
  - Directional
    - Focused EM beam
    - The higher frequency the more focused
  - Omnidirectional
    - Lower frequency
    - Spreads out to multiple receivers
- Three ranges of frequencies
  - 26GHz – 40GHz --- microwave
  - 30 MHz – 1GHz --- broadcast radio
  - 3x10**11 to 2x10**14 Hz --- infrared

Terrestrial Microwave

- Parabolic dish
- Narrow beam – line of sight on towers to avoid obstacles
- Series of towers for long distance
- Applications:
  - Long haul telephone
  - Voice and TV
  - Short point to point between buildings
- Main Source of loss
  - Attentuation – especially with rainful
  - Repeaters or amplifiers 10 to 100km
  - Interference with overlapping bands

Satellite Microwave

- It is essentially a microwave relay station
- Uplink
  - Receives transmission on one frequency
- Downlink
  - Transmits on a second frequency
- Operates on a number of frequency bands known as transponders
- Point to Point
  - Ground station to satellite to ground station
- Multipoint
  - Ground station to satellite to multiple receiving stations

Satellite Microwave

- Satellite orbit
  - 35,784 Km, to match earth rotation
  - Stays fixed above the transmitter/receiver station as earth rotates
- Satellites need to be separated by distance
  - Avoid interference
- Applications
  - TV, long distance telephone, private business networks
- Optimum frequency range
  - 1 – 10 GHz
  - Below 1GHz results in noise, above 10GHz results in severe attenuation

Broadcast Radio

- Omnidirectional unlike satellite
- Does not require dish like antennae
- Frequency range
  - Radio - 3kHz to 300Ghz
  - Broadcast radio – 30MHz to 1GHz
- Broadcast radio
  - Transmission limited to line of sight
  - Less sensitive to attenuation from rainfall than microwave
  - Prime source of interference is multipath

Infrared

- Tranceivers must be within line of sight of each other or via reflection
- Does not penetrate walls like microwave
- No frequency allocation or licensing

Satellite Communication

UNIVERSITY OF PETROLEUM & ENERGY STUDIES
Harnessing Energy through Knowledge
UNIVERSITY
OF PETROLEUM
& ENERGY STUDIES

Overview

- Satellite is a microwave repeater in the space.
- There are about 750 satellite in the space, most of them are used for communication.
- They are:
  - Wide area coverage of the earth's surface.
  - Transmission delay is about 0.3 sec.
  - Transmission cost is independent of distance.

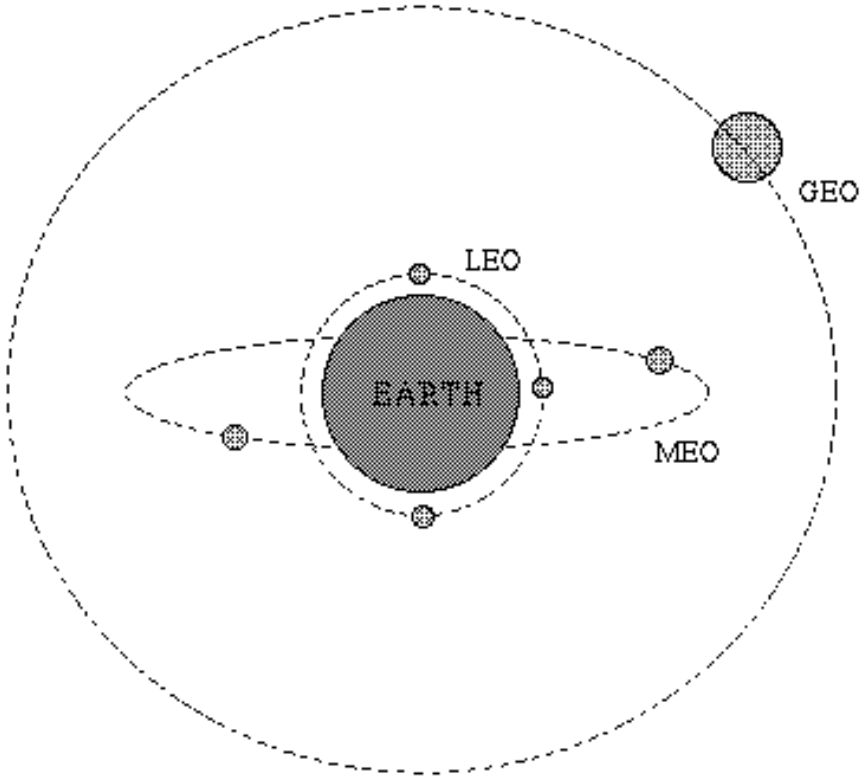
- Satellite up links and down links can operate in different frequency bands:

Band	Up-Link (Ghz)	Down-link (Ghz)	ISSUES

- The up-link is a highly directional, point to point link
- The down-link can have a footprint providing coverage for a substantial area "spot beam“.

Orbits:

- LEO: Low Earth Orbit.
- MEO: Medium Earth Orbit
- GEO: Geostationary Earth Orbit



- At the Geostationary orbit the satellite covers 42.2% of the earth’s surface.
- Theoretically 3 geostaionary satellites provides 100% earth coverage

MAC(Media Access Control) protocols for satellite links

- ALOHA:
  - Every station can transmit any time
  - Very low efficiency 18- 36 %.
- FDMA (Frequency Division Multiple Access)
  - It is the oldest and most common.
  - the available satellite channel bandwidth is broken into frequency bands for different earth stations.

- TDMA (Time Division Multiple Access)
  - channels are time multiplexed sequentially
  - Each earth station gets to transmit in a fixed time slot only.
  - More than one time slot can be assigned to stations with more bandwidth requirements.
  - Requires time synchronization between the Earth Stations.
- CDMA : (Code Division Multiple Access)
  - Combination of time/frequency multiplexing (a form of spread spectrum modulation).
  - It provides a decentralized way of providing separate channels without timing synchronization. It is a relatively new scheme but is expected to be more common in future satellites.

VSAT Network

- At the Very Small Aperture Terminal a lower performance microwave transceiver and lower gain dish antenna (smaller size) is used.
- VSAT networks are arranged in a star based topology.
- Ideal for centralized networks with a central host (Banking institutions with branches all over the country).
- Use the S-ALOHA and TDMA

DirecPC services:

- One of the most useful applications of VSAT networks
- Comes with an ISA computer card, a RF dish antenna (2 ft dia) equipped with an LNA, and supporting software.

Supporting two kinds of services

1. Digital Package Delivery
2. Turbo Internet

1. Digital Package Delivery

- downloading files at a speed 100 times faster than that supported by public telephone network.
- Large files can be received by multiple DirecPC end points.
- The download requests are made using the standard analog modem over telephone lines.

2. Turbo Internet

- The end user overcomes the telephone line barrier and is capable of receiving data
- A connection is setup with the local ISP (internet server provider) using the analog telephone line modem.
- All mouse and keyboard actions in the web browser are communicated to the web server on the other end using this link.

Applications

- E-mail
- Searchable Data (Web Sites)
- E-Commerce
- News Groups
- Internet Telephony (VoIP)
- Video Conferencing
- Chat Groups
- Instant Messengers
- Internet Radio


The Data
secure

Threats Today Include

- A belief on the part of senior management that there are no serious *threats* directed at their company.
- Terrorist acts
- Natural disasters
- Criminal Acts
- Network Attacks
  - Inside attacks
  - Outside attacks
  - Viruses/Malicious

The World We Live In Today

- General Internet attack trends are showing a 64% annual rate of growth.
- The average company experienced 32 attacks per week over the past 6 months.
- Two out of five companies that are hit by a disaster go out of business within 5 years.
- Gartner report indicates that average cost for network downtime is $42,000 per hour.

What Has Been Our Approach?

Building Bigger and More Complex Walls

Where Do You Begin?

what

what

how

over-protecting under-protecting

“good thing”

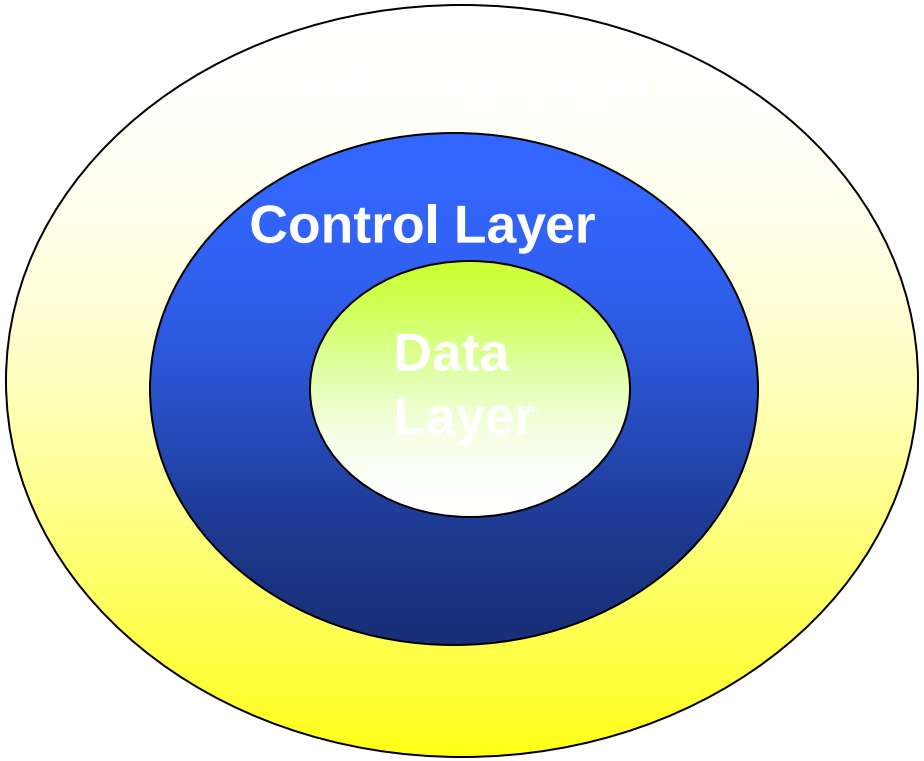
Network Protection Strategy

A well-conceived network protection strategy should take a layered approach. At a minimum it should include three layers of protection:

- The Gateway Layer - Answers the question," Can I come in?"
- The Control Layer - Answers the question "Where can I go?"
- The Data Layer - Answers the question "What can I do?"

Data Protection Strategy

Layered Approach



The Gateway Layer

Answers the question **“Can I come in?”**

Allows you to address how access is gained to your networks:

- Firewalls
- Intrusion Detection Systems
- Modems
- Remote Access such as VPN and ExtraNets
- User authentication methods

Benefits of Completing The Gateway Layer

- Eliminates reliance on **“passwords”** as the only means of protection thus eliminating risk and liabilities.
- Sets the architectural foundation for future e-business.
- Provides foundation for secure remote access.
- Provides your company with the ability to identify and react to all attacks directed at our networks from outside the company.

The Control Layer

Answers the question, **“Where can I go?”**

- Is your security access control program implement a role based security model?
- Do these roles identify exactly what each employee has and can have access to?

Bottom Line: Do you really know who has access to what, and can you control it?

Benefits of The Control Layer

- Provides you with the ability to manage access administration across heterogeneous environments.
- Allows you to quickly turn-on and turn-off access.
- Replaces your current traditional **“paper trail”** of access requests with fast and accurate electronic workflow approach.
- Provides an audit trail and strong security by consolidating all access information into a single database.
- Provides you with the means to quickly set up access for new applications implemented by the company.

The Data Layer

Answers the question, **“What can I do?”**

Do you have the methodology to identify and restrict the abilities of each user:

1. Can all users read all data?
2. Can all users modify all data?
3. Can all users delete all data?
4. Can you restrict access based on a users role what each can do?

Components of the Data Layer

- Use of strong Passwords to protect data
- Use of Encryption to protect sensitive data
- Use of Digital Rights Management
- PKI as a solution to access control
- Smart Cards and Tokens to access data

All Data is Subject to Compromise and Loss!

The ability to identify that you are being attacked, containment of the attacker and having the ability to terminate the attackers access can limit the amount of damage that can be caused. These are key elements and are essential in surviving an attack.

Remember

More Security Doesn't Always Make You More Secure…

Better Planning and Management Does

Managing the Risks

The world has changed dramatically based on the events of the past few years. We have learned that building more and higher walls by themselves do little in ensuring that critical and sensitive data receives adequate protection. We now must look not only at how we protect our networks but how we protect the actual data.

Remember – **Its All About The Data**

Closing Thought

When it comes to addressing our business risks, we never plan to fail.

We just fail to plan!

Thank You