EAST WEST UNIVERSITY

excellence in education

DEPARTMET OF

ELECTRONICS AND COMMUNICATIONS ENGINEERING

INTERNSHIP REPORT ON

Network Structure of Mutual Trust Bank Ltd.

মিউচুয়াল ট্রাস্ট ব্যাংক লিমিটেড

Mutual Trust Bank Ltd.

you can bank on us

Prepared By:

ABDUL WAKIL KHAN

2011-2-55-044

Dept. of ECE

Supervised by:

Md. Asif Hossain

DECLARATION

.

We declare that this proposal is our original work and has not been presented in any other university/institution for consideration of any certification. This interns paper proposal has been complemented by referenced sources duly acknowledged. Where text, data (including spoken words), graphics, pictures or tables have been borrowed from other sources, including the internet, these are specifically accredited and references cited using current APA system and in accordance with anti-plagiarism regulations.

ABDUL WAKIL KHAN

2011-2-55-044

Department of ECE

East West University

ACCEPTANCE

This report presented of the department of Electronics and Communication Engineering East West University is submitted in partial fulfillment of the requirement for degree of BSC in Electronics and Telecommunication Engineering, under complete supervision of the undersigned.

Md. Asif Hossain

Senior Lecturer

Department of Electronics and Communication Engineering

ACKNOWLEDGEMENT

Foremost, we would like to express our sincere gratitude to my advisor **MD ASIF HOSSAIN** for the continuous support of my ‘Intern Study’, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped us in all the time writing of this ‘Intern’. We could not have imagined having a better advisor and mentor for my ‘Intern’ study.

About Mutual Trust Bank Ltd.

The Company was incorporated as a Public Limited Company in 1999, under the Companies Act 1994, with an Authorized Share Capital of BDT 1,000,000,000 divided into 10,000,000 ordinary shares of BDT 100 each. At present, the Authorized Share Capital of the company is BDT 10,000,000,000 divided into 1,000,000,000 ordinary shares of BDT 10 each.

The Company was also issued Certificate for Commencement of Business on the same day and was granted license on October 05, 1999 by Bangladesh Bank under the Banking Companies Act 1991 and started its banking operation on October 24, 1999. As envisaged in the Memorandum of Association and as licensed by Bangladesh Bank under the provisions of the Banking Companies Act 1991, the Company started its banking operation and entitled to carry out the following types of banking business:

- Wholesale Banking
- Retail Banking
- International Trade Financing
- Small and Medium Enterprises (SME) Banking
- NRB Banking
- Privilege Banking
- Card Services
- Treasury Operations

The Company (Bank) operates through its Head Office at Dhaka and 95 branches. The Company/ Bank carries out international business through a Global Network of Foreign Correspondent Banks.

Registered Name of the Company

Mutual Trust Bank Limited

Company Registration No.

c38707(665)/99 on September 29, 1999

Bangladesh Bank Permission No.

BRPD (P)744(78)/99-3081 on October 5, 1999

Registered Office:

MTB Centre, 26 Gulshan Avenue
Plot 5, Block SE(D), Gulshan 1, Dhaka 1212

SWIFT CODE

MTBL BD DH

Corporate Website

www.mutualtrustbank.com

Memberships

- Metropolitan Chamber of Commerce and Industry, Dhaka (MCCI, D)
- The Institute of Banker's Bangladesh (IBB)
- Bangladesh Foreign Exchange Dealer's Association (BAFEDA)
- Bangladesh Institute of Bank Management (BIBM)
- International Chamber of Commerce Bangladesh Limited (ICCB)
- Bangladesh Association of Banks (BAB)
- Association of Bankers Bangladesh Limited (ABB)
- Bangladesh Association of Publicly Listed Companies (BAPLC)
- American Chamber of Commerce in Bangladesh (AMCHAM)
- Primary Dealers Bangladesh Limited (PDBL)

## Content

Introduction

In my Internship at Mutual Trust Bank Limited, I have learnt how to assign each interface on the router an IP address with a unique subnet. This intern report will give the basic information needed in order to configure routers for routing IP, such as how addresses are broken down and how subnetting works.

Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets). An IP address includes a network segment and a host segment. Subnets are designed by accepting bits from the IP address's host part and using these bits to assign a number of smaller sub-networks inside the original network. Subnetting allows an organization to add sub-networks without the need to acquire a new network number via the Internet service provider (ISP). Subnetting helps to reduce the network traffic and conceals network complexity. Subnetting is essential when a single network number has to be allocated over numerous segments of a local area network(LAN).Subnets were initially designed for solving the shortage of IP addresses over the Internet.

IP addresses are 32 bit numbers, most commonly represented in dotted decimal notation. Each decimal number represents eight bits of binary data, and therefore can have a decimal value between 0 and 255. IP addresses most commonly come as class A, B, or C. It's the value of the first number of the IP address that determines the class to which a given IP address belongs. Class D addresses are used for multi-cast applications.

I got an opportunity to work with most leading banking service provider that is Mutual Trust Bank Limited. The employer’s of this company look after to their methods, networking models and network behavior. And I was intending to look into the Networking division and how it looks like practically, how they interact with their other branch’s , how they design a system and what are their rules in their environmental work. I also got the chance to work in IT Division in Mutual Trust Bank Limited. We know computer networking is the principal part of our modern life. I decided to know about computer networking and how does it work, how to make subnet in a network and addressing network.

CHAPTER 1

Computer Network

A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other along network links (data connections). The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Computer networks differ in the transmission media used to carry their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent. In most cases, communications protocols are layered on (i.e. work using) other more specific or more general communications protocols, except for the physical layer that directly deals with the trans-mission media.

Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications.

1.1 History

The chronology of significant computer-network developments includes:

In the late 1950s early networks of computers included the military radar system Semi-Automatic Ground Environment (SAGE).

In 1959 Anatolii Ivanovich Kitov proposed to the Central Committee of the Communist Party of the Soviet Union a detailed plan for the re-organization of the control of the Soviet armed forces and of the Soviet economy on the basis of a network of computing centre.

In 1960 the commercial airline reservation system semi-automatic business research environment (SABRE) went online with two connected main-frames.

In 1962 J.C.R. Licklider developed a working group he called the "Intergalactic Computer Network", a precursor to the ARPANET, at the Advanced Re-search Projects Agency (ARPA).

In 1964 researchers at Dartmouth College developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at Massachusetts Institute of Technology, a re-search group supported by General Electric and Bell Labs use the computer to route and manage telephone connections. Throughout the 1960s, Leonard Kleinrock, Paul Baran, and Donald Davies independently developed network systems that used packets to transfer information between computers over a network.

In 1965, Thomas Marill and Lawrence G. Roberts created the first wide area network (WAN). This was an immediate precursor to the ARPANET, of which Roberts became program manager.
Also in 1965, Western Electric introduced the first widely used telephone switch that implemented true computer control.

In 1969 the University of California at Los Angeles, the Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah became connected as the beginning of the ARPANET networking 50 kbit/s circuits.

In 1972 commercial services using X.25 were deployed, and later used as an underlying infrastructure for expanding TCP/IP networks.

In 1973, Robert Metcalfe wrote a formal memo at Xerox PARC describing Ethernet, a networking sys-tem that was based on the Aloha network, developed in the 1960s by Norman Abramson and colleagues at the University of Hawaii. In July 1976, Robert Metcalfe and David Boggs published their paper "Ethernet: Distributed Packet Switching for Local Computer Networks"[4] and collaborated on several patents received in 1977 and 1978. In 1979 Robert Metcalfe pursued making Ethernet an open standard.

In 1976 John Murphy of Data point Corporation created ARCNET, a token-passing network first used to share storage devices.

In 1995 the transmission speed capacity for Ether-net increased from 10 Mbit/s to 100 Mbit/s. By 1998, Ethernet supported transmission speeds of a Gigabit. The ability of Ethernet to scale easily (such as quickly adapting to support new fiber optic cable speeds) is a contributing factor to its continued use as of 2015.

CHAPTER 2

Network packet

2.1 Main article: Network packet

Computer communication links that do not support packets, such as traditional point-to-point telecommunication links, simply transmit data as a bit stream. However, most information in computer networks is carried in packets. A network packet is a formatted unit of data carried by a packet-switched network.

In packet networks, the data is formatted into packets that are sent through the network to their destination. Once the packets arrive they are reassembled into their original message. With packets, the bandwidth of the transmission medium can be better shared among users than if the network were circuit switched. When one user is not sending packets, the link can be filled with packets from others users, and so the cost can be shared, with relatively little interference, provided the link isn't overused.

Packets consist of two kinds of data: control information, and user data(payload). The control information provides data the network needs to deliver the user data, for example: source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers, with payload data in between. Often the route a packet needs to take through a network is not immediately available. In that case the packet is queued and waits until a link is free.

CHAPTER 3

Network Topology

3.1.1 Main article: Network topology

The physical layout of a network is usually less important than the topology that connects network nodes. Most diagrams that describe a physical network are therefore topological, rather than geographic. The symbols on these diagrams usually denote network links and network nodes.

3.1.2 Network links

The transmission media (often referred to in the literature as the physical media) used to link devices to form a computer network include electrical cable(Ethernet, Home PNA, power line communication, G.hn), optical fiber (fiber-optic communication), and radio waves (wireless networking). In the OSI model, these are defined at layers 1 and 2 — the physical layer and the data link layer.

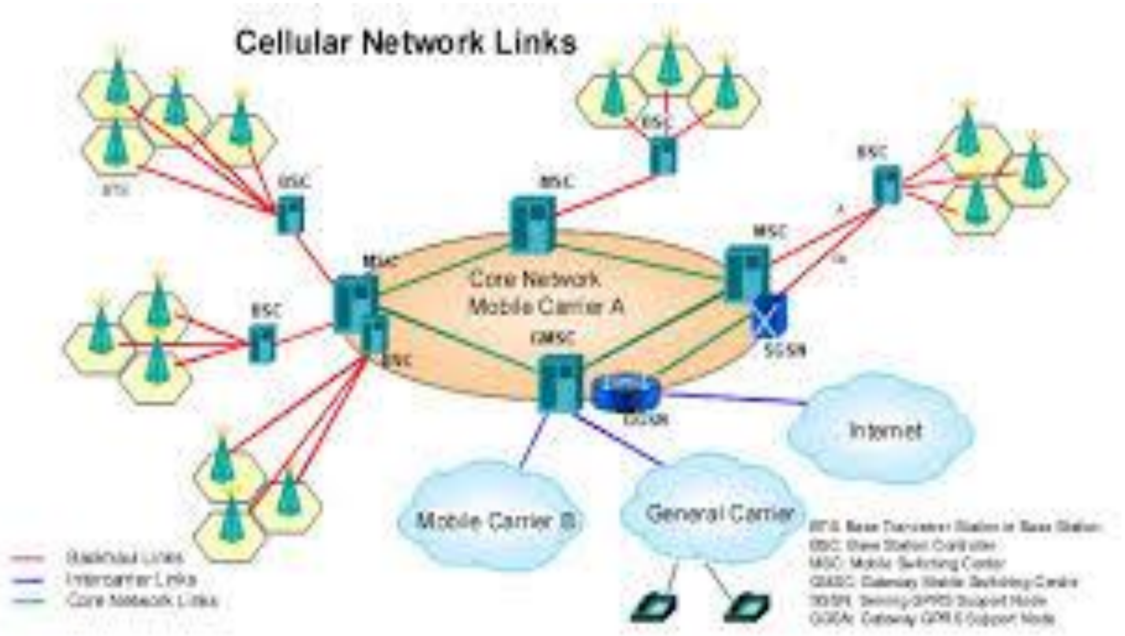

Cellular Network Links
BTS
BSC
BSC
MSC
BSC
MSC
BSC
MSC
Core Network
Mobile Carrier A
GMSC
BSC
SGSN
GGSN
BSC
Internet
Mobile Carrier B
General Carrier
BTS: Base Transceiver Station or Base Station
BSC: Base Station Controller
MSC: Mobile Switching Center
GMSC: Gateway Mobile Switching Centre
SGSN: Serving GPRS Support Node
GGSN: Gateway GPRS Support Node
Backhaul Links
Intercarrier Links
Core Network Links

Fig: Network links

3.1.3 Wired technologies

The orders of the following wired technologies are roughly from slowest to fastest transmission speed.

Fig: Wired technology

3.1.4 Wireless technologies

Terrestrial microwave–Terrestrial microwave communication uses Earth-based transmitters and receivers resembling satellite dishes. Terrestrial microwaves are in the low-gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48 km (30 mi) apart.

Communications satellites–Satellites communicate via microwave radio waves, which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically in geosynchronous orbit 35,400 km (22,000 mi) above the equator.

These computers are very often connected to networks using wireless links Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.

Figure 3.3: Computer connected with network

Cellular and PCS system use several radio communications technologies. The systems divide the region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.

Radio and spread spectrum technologies – Wireless local area networks use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. IEEE 802.11 de-fines a common flavor of open-standards wireless radio-wave technology known as wifi.

Free-space optical communication uses visible or in-visible light for communications. In most cases, line-of-sight propagation is used, which limits the physical positioning of communicating devices.

3.1.5 Exotic technologies

There have been various attempts at transporting data over exotic media:

IP over Avian Carriers was a humorous April fool’s Request for Comments, issued as RFC 1149. It was implemented in real life in 2001.

Extending the Internet to interplanetary dimensions via radio waves.

Both cases have a large round-trip delay time, which gives slow two-way communication, but doesn't prevent sending large amounts of information.

3.2.1 Network nodes

Apart from any physical transmission medium there may be, networks comprise additional basic system building blocks, such as network interface controller (NICs), repeaters, hubs, bridges, switches, routers, modems and firewalls.

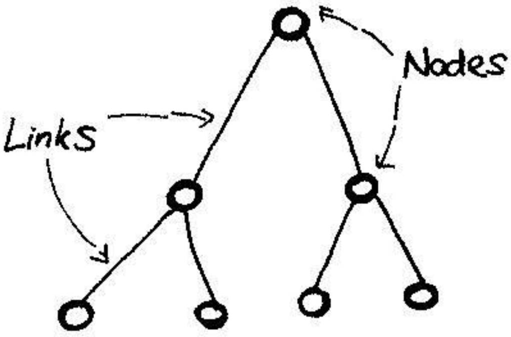


Fig: Network nodes

3.2.2 Network interfaces

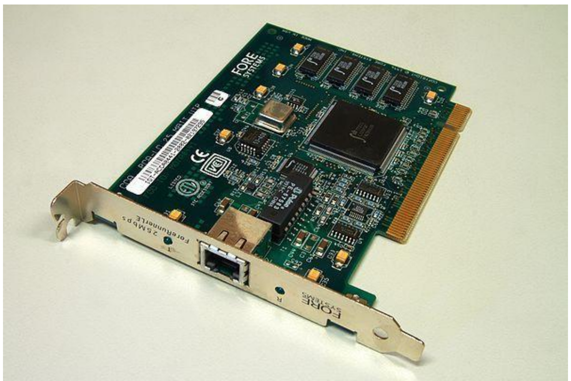


Figure 4.4:Network interface

An ATM network interface in the form of an accessory card. A lot of network interfaces are built-in.

A network interface controller (NIC) is computer hard ware that provides a computer with the ability to access the transmission media, and has the ability to process low-level network information. For example, the NIC may have a connector for accepting a cable, or an aerial for wireless transmission and reception, and the associated circuitry.

The NIC responds to traffic addressed to a network address for either the NIC or the computer as a whole.

In Ethernet networks, each network interface controller has a unique Media Access Control (MAC) address— usually stored in the controller's permanent memory. To avoid address conflicts between network devices, the Institute of Electrical and Electronics Engineers (IEEE)maintains and administers MAC address uniqueness. The size of an Ethernet MAC address is six octets. The three most significant octets are reserved to identify NIC manufacturers. These manufacturers, using only their as-signed prefixes, uniquely assign the three least-significant octets of every Ethernet interface they produce

3.2.3 Repeaters and hubs

A repeater is an electronic device that receives a net-work signal, cleans it of unnecessary noise and regenerates it. The signal is retransmitted at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. Most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. With fiber optics, repeaters can be tens or even hundreds of kilometers apart.

Fig: Repeaters and hubs

Hubs have been mostly deleted by modern switches; but repeaters are used for long distance links, notably undersea cabling.

3.2.4 Bridges

A network bridge connects and filters traffic between two network segments at the data link layer (layer 2) of the OSI model to form a single network. This breaks the network’s collision domain but maintains a unified broad-cast domain. Network segmentation breaks down a large, congested network into an aggregation of smaller, more efficient networks.

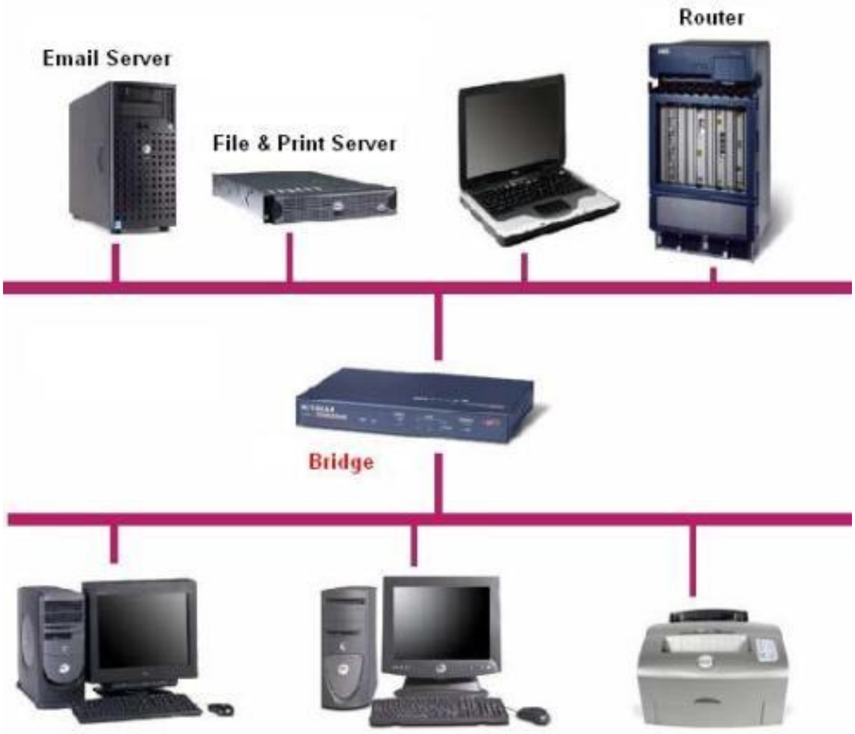


Fig: Network Bridges

Bridges come in three basic types:

Local bridges: Directly connect LANs

Remote bridges: Can be used to create a wide area network (WAN) link between

LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.

Wireless bridges: Can be used to join LANs or connect remote devices to LANs.

3.2.5 Switches

A network switch is a device that forwards and filters OSI layer 2 data grams(frames)between ports based on the MAC addresses in the frames A switch is distinct from a hub in that it only forwards the frames to the physical ports involved in the communication rather than all ports connected. It can be thought of as a multi-port bridge. It learns to associate physical ports to MAC addresses by examining the source addresses of received frames. If an unknown destination is targeted, the switch broadcasts to all ports but the source. Switches normally have numerous ports, facilitating a star topology for devices, and cascading additional switches.

Fig: Switches

Multi-layer switches are capable of routing based on layer3 addressing or additional logical levels. The term switch is often used loosely to include devices such as routers and bridges, as well as devices that may distribute traffic based on load or based on application content (e.g., a Web URL identifier).

3.2.6 Routers

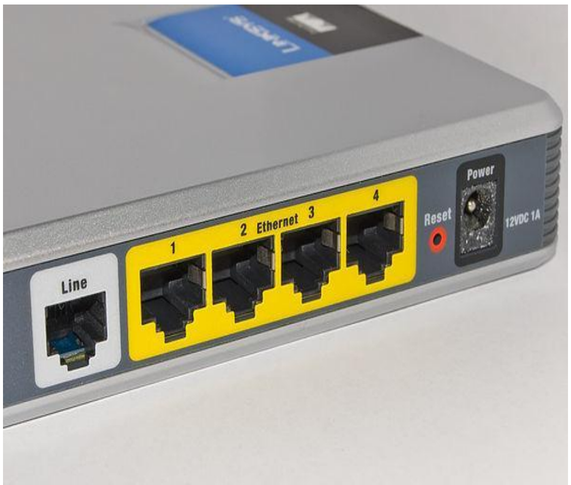


Figure 4.5:Routers

A typical home or small office router showing the ADSL telephone line and Ethernet network cable connections

A router is an internetworking device that forwards packets between networks by processing the routing in-formation included in the packet or datagram (Internet protocol information from layer 3). The routing information is often processed in conjunction with the routing table (or forwarding table). A router uses its routing table to determine where to forward packets. (A destination in a routing table can include a “null” interface, also known as the “black hole” interface because data can go into it, however, no further processing is done for said data.)

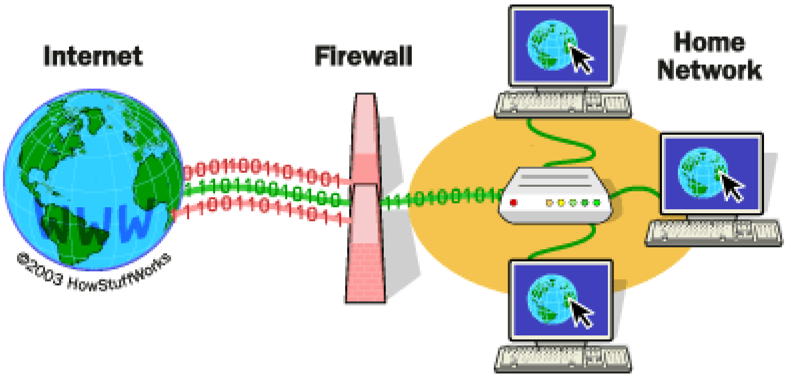
3.2.7 Modems

Modems(Modulator Demodulator) are used to connect network nodes via wire not originally designed for dig-ital network traffic, or for wireless. To do this one or more carrier signals are modulated by the digital signal to produce an analog signal that can be tailored to give the required properties for transmission. Modems are commonly used for telephone lines, using a Digital Subscriber Line technology.

Fig: Modems

3.2.8 Firewalls

A firewall is a network device for controlling network security and access rules. Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones. The vital role fire-walls play in network security grows in parallel with the constant increase in cyber attacks.



3.3.1 Network structure

Network topology is the layout or organizational hierarchy of interconnected nodes of a computer network. Different network topologies can affect throughput, but reliability is often more critical. With many technologies, such as bus networks, a single failure can cause the net-work to fail entirely. In general the more interconnections there are, the more robust the network is; but the more expensive it is to install.

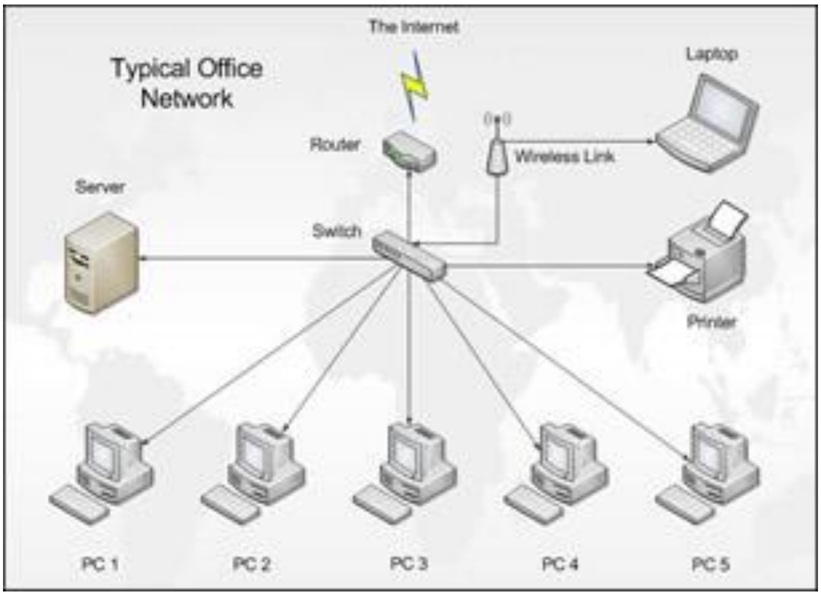


Fig: Network structure

3.3.2 Overlay network

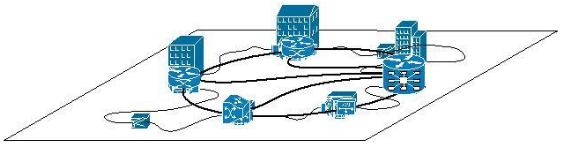


Figure: A sample overlay network

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay network are connected by virtual or logical links. Each link corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may (and often does) differ from that of the underlying one. For example, many peer-to-peer networks are overlay networks. They are organized as nodes of a virtual system of links that run on top of the Internet.

Overlay networks have been around since the invention of networking when computer systems were connected over telephone lines using modems, before any data network existed.

The most striking example of an overlay network is the Internet itself. The Internet itself was initially built as an overlay on the telephone network. Even today, each Internet node can communicate with virtually any other through an underlying mesh of sub-networks of wildly different topologies and technologies. Address resolution and routing are the means that allow mapping of a fully connected IP overlay network to its underlying network.

Another example of an overlay network is a distributed hash table, which maps keys to nodes in the network. In this case, the underlying network is an IP network, and the overlay network is a table (actually a map) indexed by keys.

Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees to achieve higher-quality streaming media. Previous proposal. On the other hand, an overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. The overlay network has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes that a message traverses before it reaches its destination.

For example, Akamai Technologies manages an overlay network that provides reliable, efficient content delivery (a kind of multicast). Academic research includes end system multicast, resilient routing and quality of ser-vice studies, among others.

CHAPTER 4

Communications protocols

4.1 TCP/IP – model

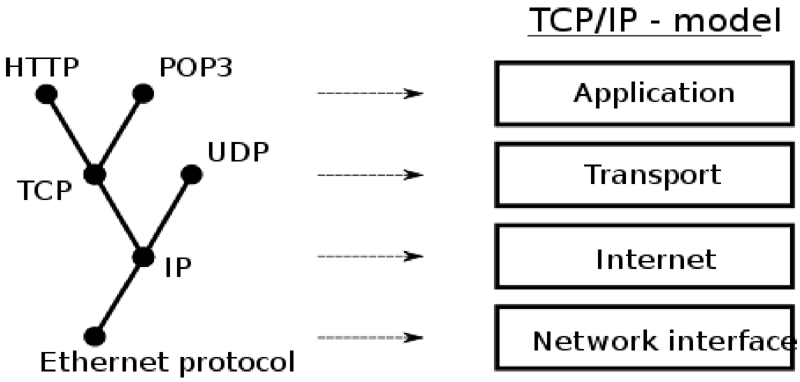


Figure : TCP/IP model

The TCP/IP model or Internet layering scheme and its relation to common protocols often layered on top of it an indication of congestion; IP is a network layer protocol whereas TCP is a transport layer protocol.

Communication protocols have various characteristics. They may be connection-oriented or connectionless, they may use circuit mode or packet switching, and they may use hierarchical addressing or flat addressing. There are many communication protocols, a few of which are described below.

4.2 IEEE 802

The TCP/IP model or Internet layering scheme and its relation to common protocols often layered on top of it.

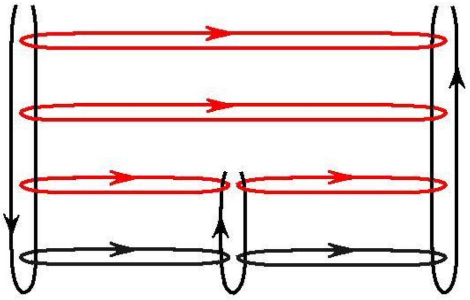


Figure: TCP/IP model

The complete IEEE 802 protocol suite provides a diverse set of networking capabilities. The protocols have a flat addressing scheme. They operate mostly at levels 1 and 2 of the OSI model.

4.2.1 Ethernet

A communications protocol is a set of rules for exchanging information over network links. In a protocol stack (also see the OSI model), each protocol leverages the ser-vices of the protocol below it. An important example of a protocol stack is HTTP (the World Wide Web protocol) running over TCP over IP (the Internet protocols) over IEEE 802.11 (the Wi-Fi protocol). This stack is used between the wireless router and the home user's personal computer when the user is surfing the web.

Fig: Ethernet

4.2.2 Wireless LAN

Wireless LAN, also widely known as WLAN or WiFi, is probably the most well-known member of the IEEE 802 protocol family for home users today.

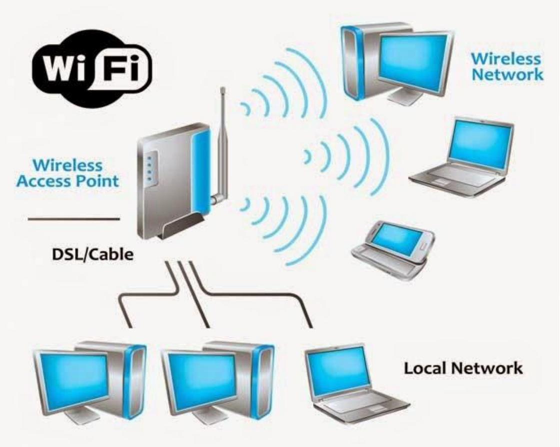


Fig: Wireless LAN

4.3 Internet Protocol Suite

The Internet Protocol Suite, also called TCP/IP, is the foundation of all modern networking. It offers connection-less as well as connection-oriented services over an inherently unreliable network traversed by data-gram transmission at the Internet protocol (IP) level. At its core, the protocol suite defines the addressing, identification, and routing specifications for Internet Protocol version 4 (IPv4) and for IPv6, the next generation of the protocol with a much enlarged addressing capability.

4.4 SONET/SDH

Synchronous optical networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers. They were originally designed to transport circuit mode communications from a variety of different sources, primarily to support real-time, uncompressed, circuit-switched voice encoded in PCM (Pulse-Code Modulation) format. However, due to its protocol neutrality and transport-oriented features, SONET/SDH also was the obvious choice for transporting Asynchronous Transfer Mode (ATM) frames.

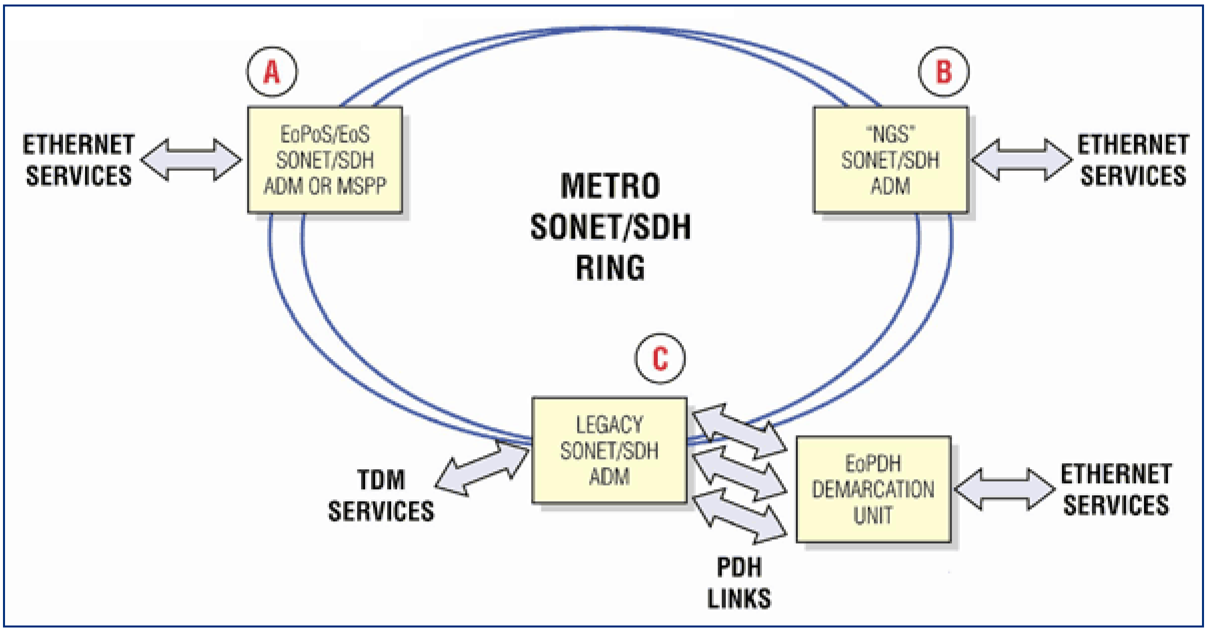


Fig: Metro SONET/SDH Ring

4.5 Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is a switching technique for telecommunication networks. It uses asynchronous time-division multiplexing and encodes data into small, fixed-sized cells. This differs from other protocols such as the Internet Protocol Suite or Ethernet that use variable sized packets or frames. ATM has similarity with both circuit and packet switched networking. This makes it a good choice for a network that must handle both traditional high-throughput data traffic, and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.

While the role of ATM is diminishing in favor of next-generation networks, it still plays a role in the last mile, which is the connection between an Internet service provider and the home user.

CHAPTER 5

Geographic scale

A network can be characterized by its physical capacity or its organizational purpose.

5.1 Nano-scale Network

A nanoscale communication network has key components implemented at the nanoscale including message carriers and leverages physical principles that differ from macroscale communication mechanisms. Nanoscale communication extends communication to very small sensors and actuators such as those found in biological systems and also tends to operate in environments that would be too harsh for classical communication.

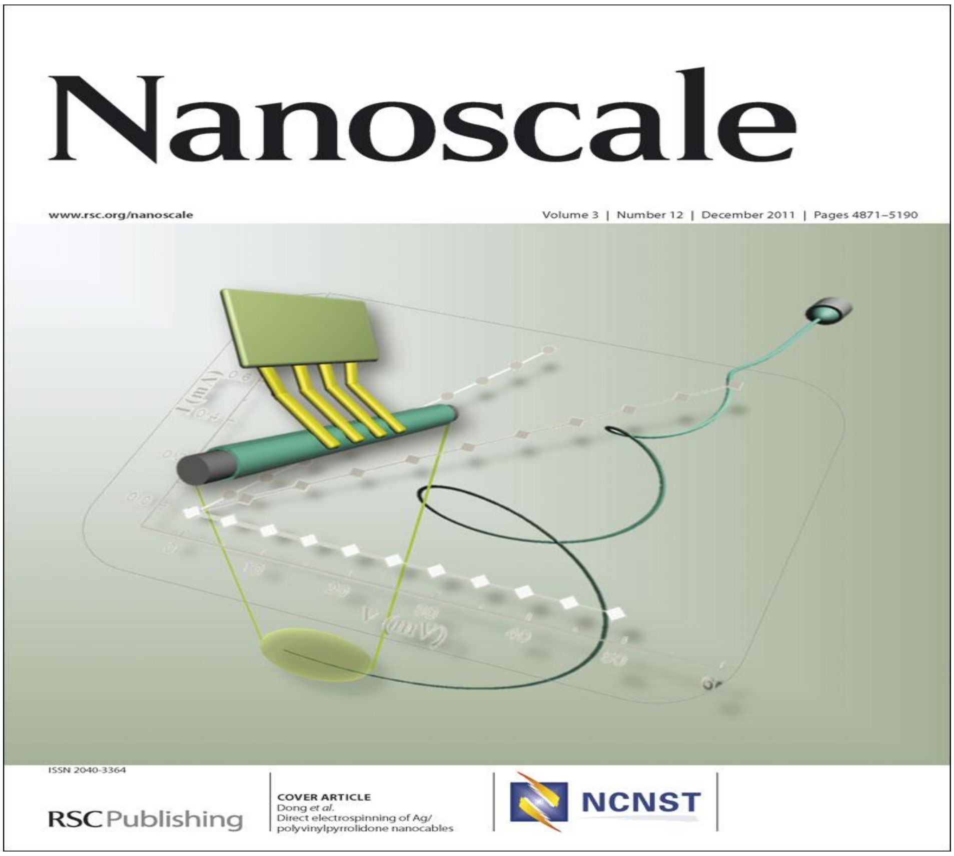

Nanoscale
www.rsc.org/nanoscale
Volume 3 | Number 12 | December 2011 | Pages 4871–5190
I (mA)
V (mV)
ISSN 2040-3364
RSC Publishing
COVER ARTICLE
Dong et al.
Direct electrospinning of Ag/polyvinylpyrrolidone nanocables
NCNST

Fig : Nanoscale

5.2 Personal area network

A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters. A wired PAN is usually constructed with USB and FireWire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

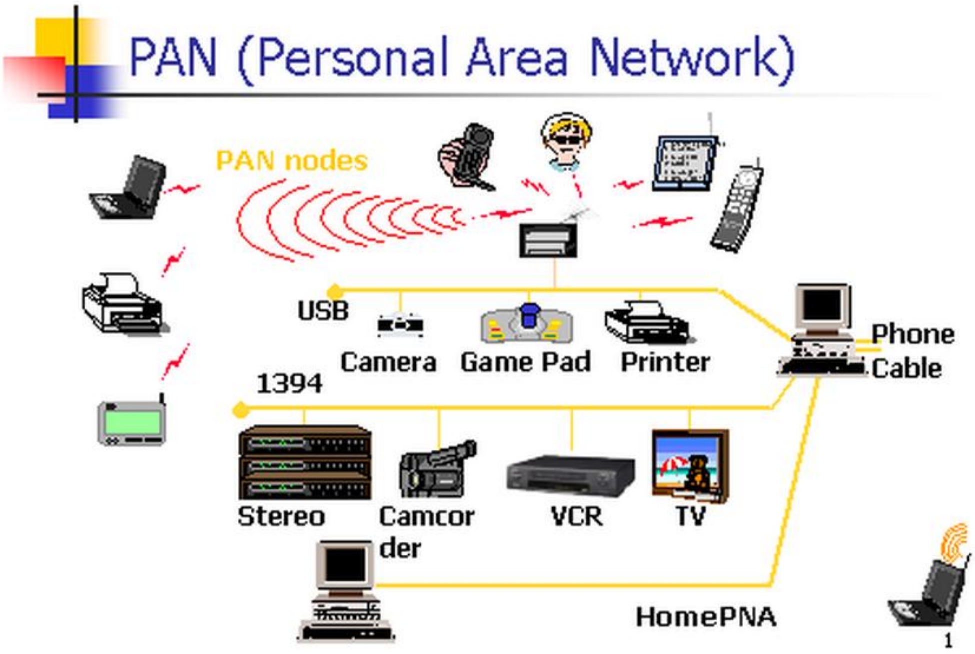


Fig: Personal area network

5.3 Local area network

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as a home, school, office building, or closely positioned group of buildings. Each computer or device on the net-work is a node. Wired LANs are most likely based on Ethernet technology. Newer standards such as ITU-Tso provide a way to create a wired LAN using existing wiring, such as coaxial cables, telephone lines, and power lines.

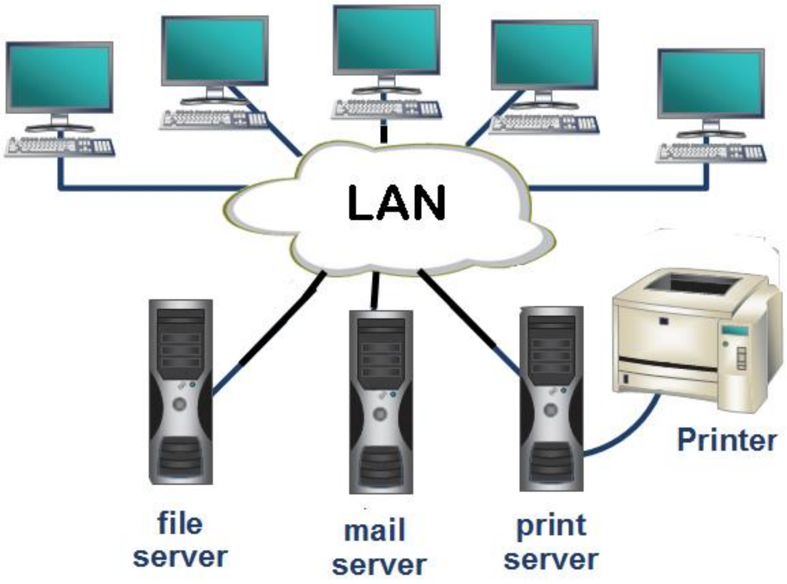


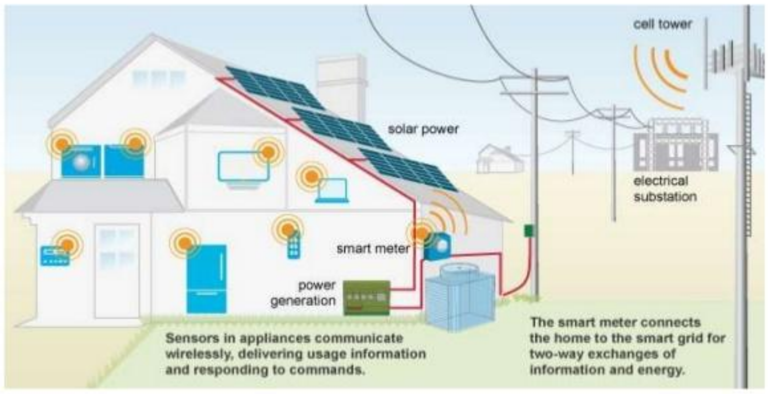
Fig: Local Area Network

5.4 Home area network

A home area network (HAN) is a residential LAN used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a cable TV or digital subscriber line (DSL) provider.

Home Area Network

Home Area Network (HAN) connects thermostats, refrigerators and other electrical devices in a Smart Home to an energy management system.



Sensors in appliances communicate wirelessly, delivering usage information and responding to commands.

The smart meter connects the home to the smart grid for two-way exchanges of information and energy.

Source: www.smartgrid portal.org

Fig: Home Area Network

5.5 Storage area network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices. The cost and complexity of SANs dropped in the early 2000s to levels allowing wider adoption across both enterprise and small to medium-sized business environments.

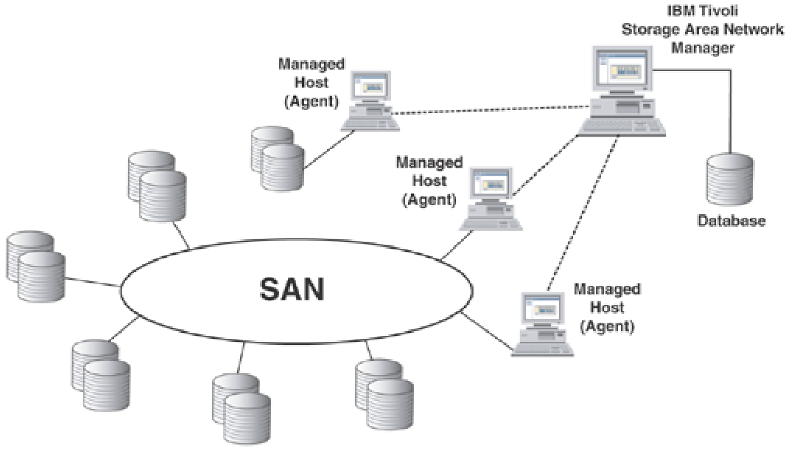


Fig : Storage Area Network

5.6 Campus area network

A campus area network (CAN) is made up of an inter-connection of LANs within a limited geographical area. The networking equipment (switches, routers) and trans-mission media (optical fiber, copper plant, Cat5 cabling, etc.) are almost entirely owned by the campus tenant / owner (an enterprise, university, government, etc.).

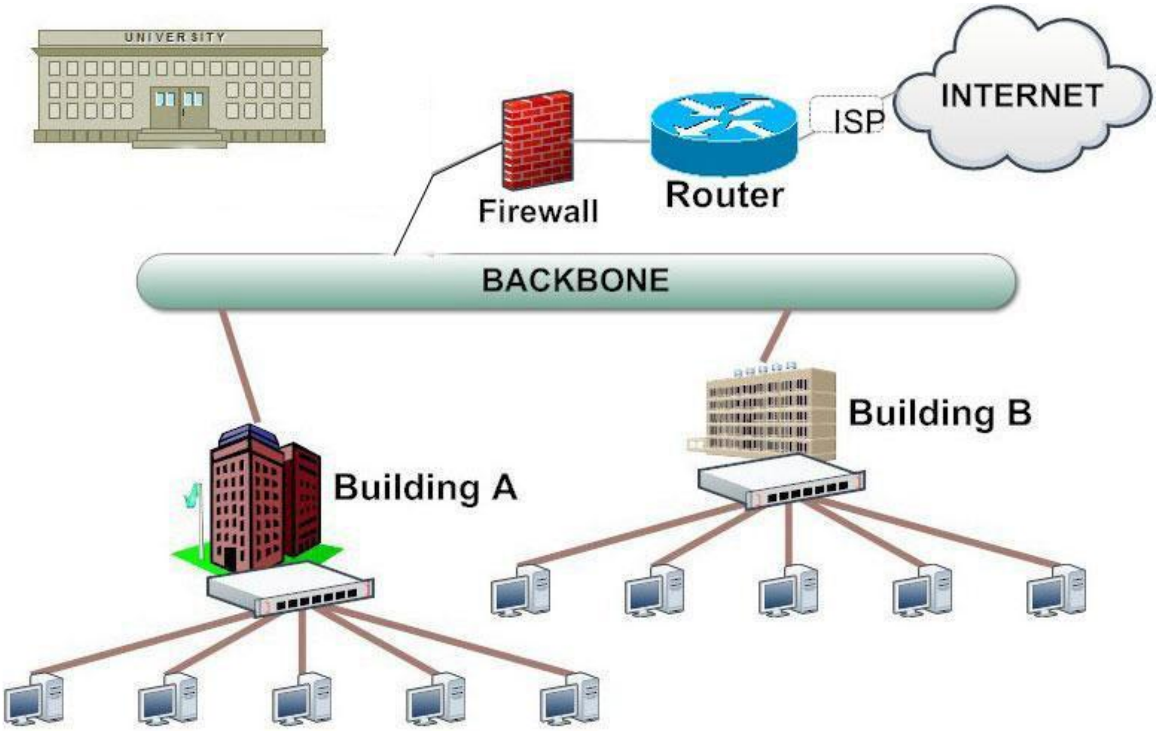


Fig: Campus Area Network

5.7 Backbone network

A backbone network is part of a computer network infrastructure that provides a path for the exchange of information between different LANs or sub-networks. A back-bone can tie together diverse networks within the same building, across different buildings, or over a wide area.

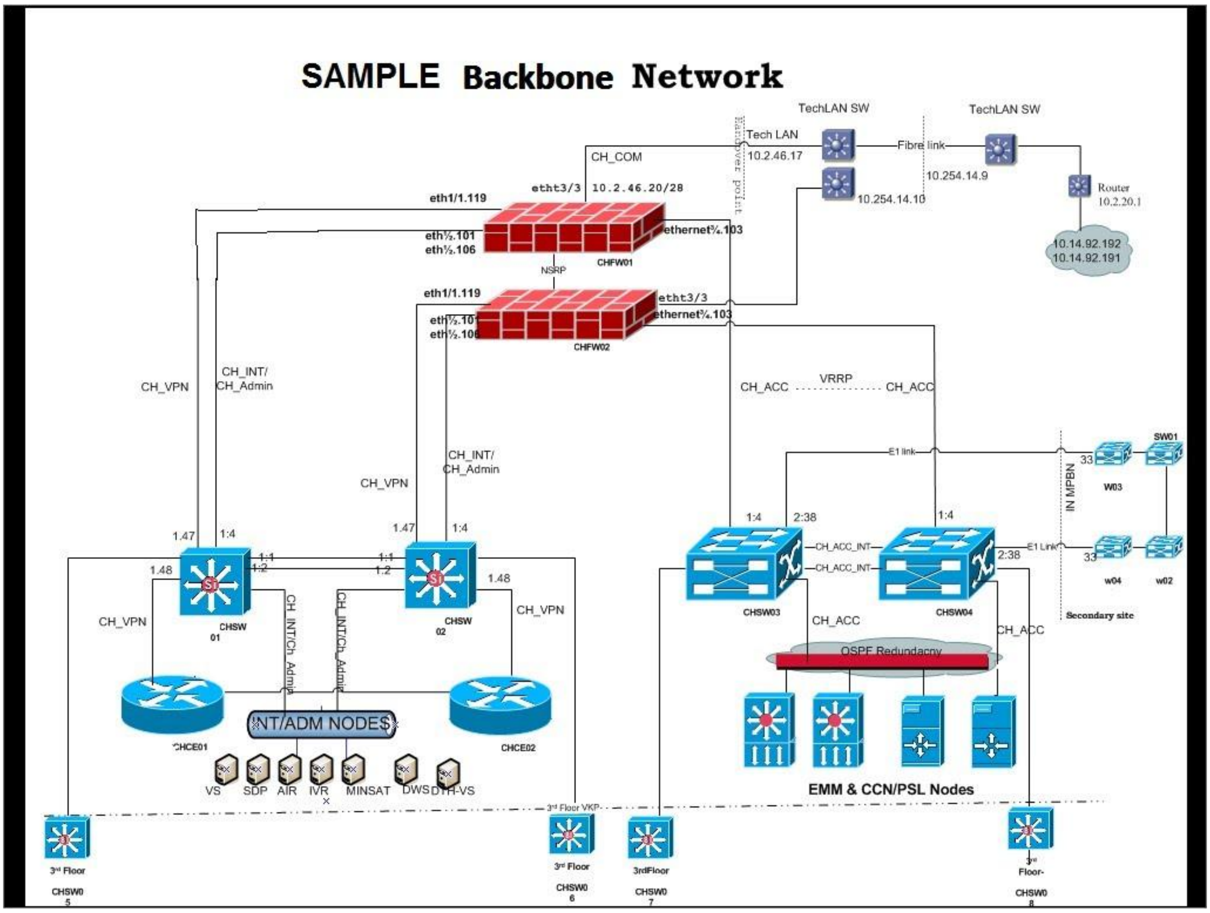


Fig: Backbone of a Network

5.8 Enterprise private network

An enterprise private network is a network that a single organization builds to interconnect its office locations (e.g., production sites, head offices, remote offices, shops) so they can share computer resources.

5.9 Virtual private network

A virtual private network (VPN) is an overlay network in which some of the links between nodes are carried by open connections or virtual circuits in some larger net-work (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

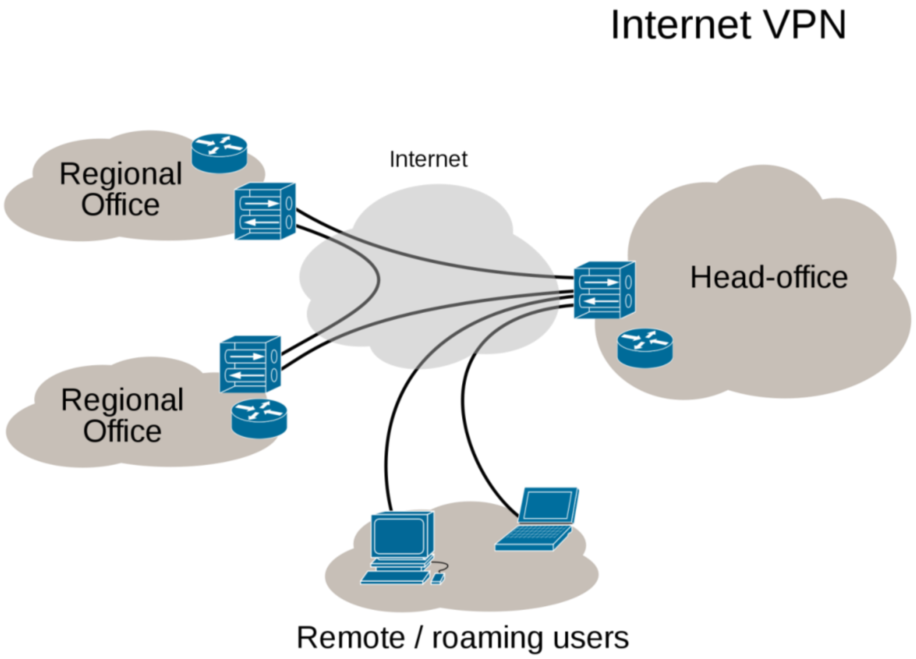


Fig: Virtual private network

5.10 Global area network

A global area network (GAN) is a network used for sup-porting mobile across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial wireless LANs.

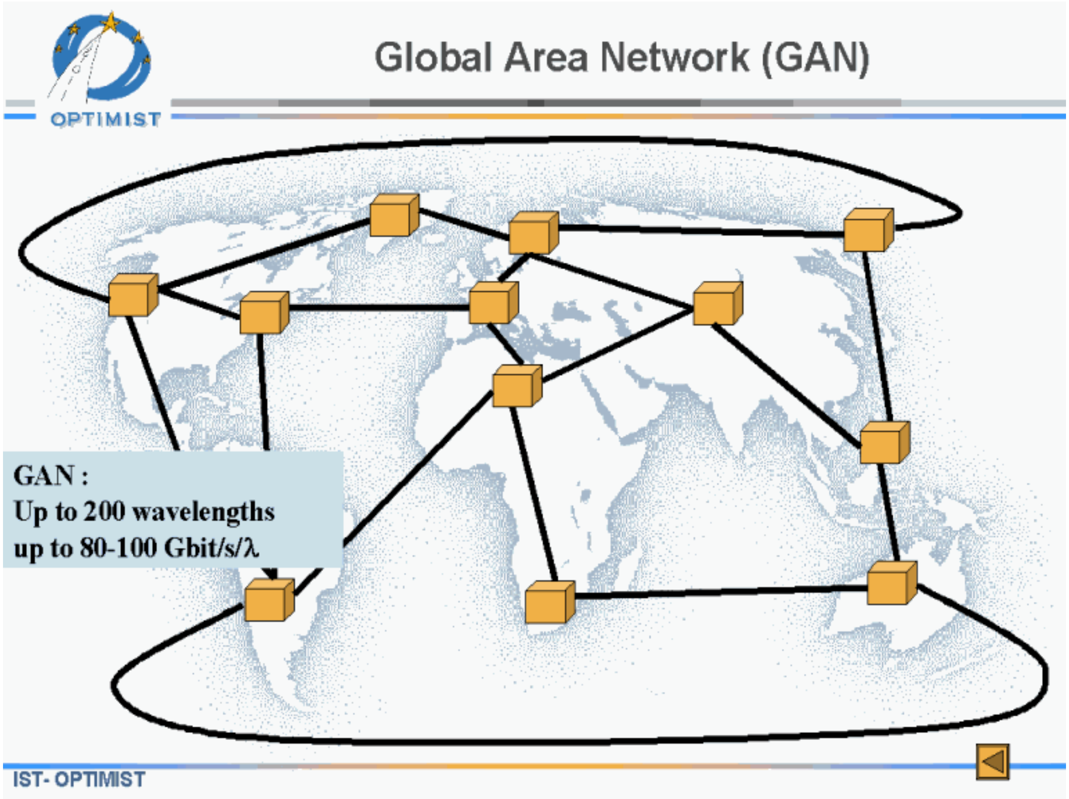
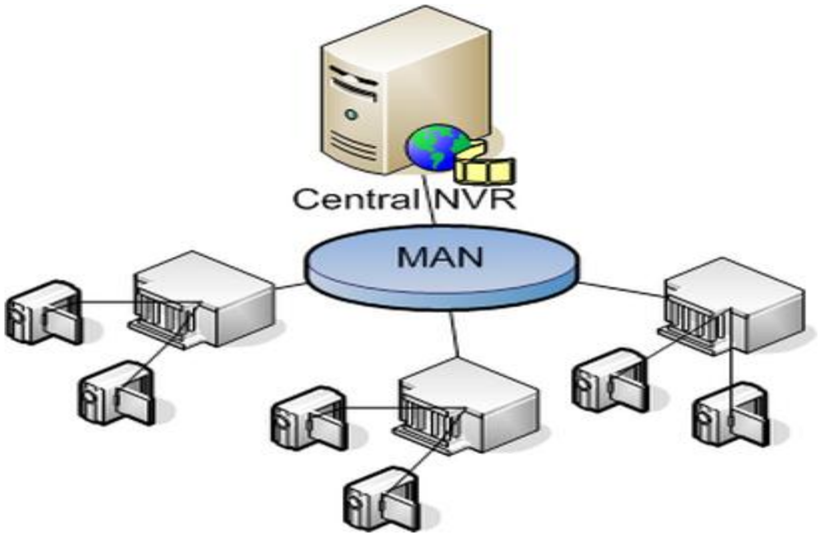


Fig: Global Area Network

5.11 Metropolitan area network

A Metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.



5.12 Wide area network

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances. A WAN uses a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often makes use of transmission facilities provided by common carriers, such as telephone companies.

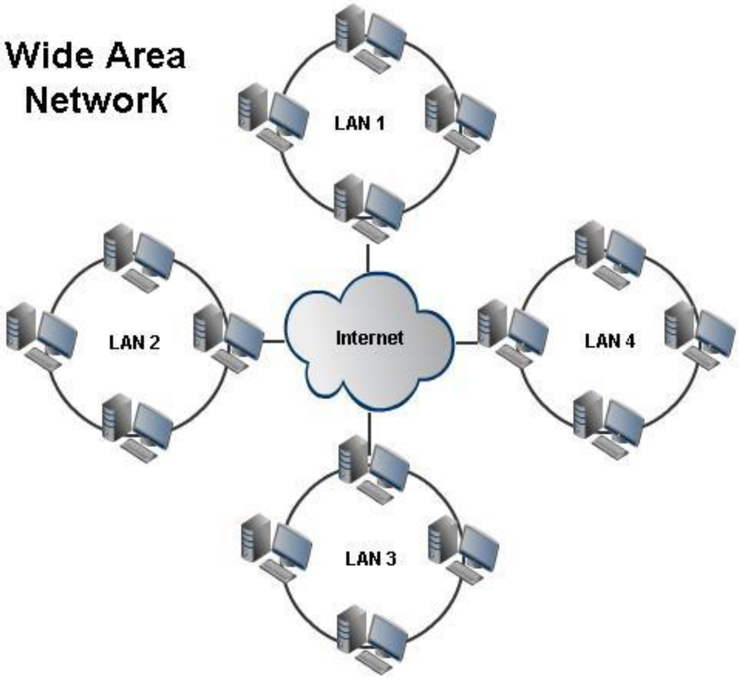


Fig: Wide area network

CHAPTER 6

Organizational scope

Networks are typically managed by the organizations that own them. Private enterprise networks may use a combination of intranets and extranets. They may also provide network access to the Internet, which has no single owner and permits virtually unlimited global connectivity.

6.1 Intranets

An intranet is a set of networks that are under the control of a single administrative entity. The intranet uses the IP protocol and IP-based tools such as web browsers and file transfer applications. The administrative entity limits use of the intranet to its authorized users. Most commonly, an intranet is the internal LAN of an organization. A large intranet typically has at least one web server to provide users with organizational information. An intranet is also anything behind the router on a local area network.

6.2 Extranet

An extranet is a network that is also under the administrative control of a single organization, but supports a limited connection to a specific external network. For example, an organization may provide access to some aspects of its intranet to share data with its business partners or customers. These other entities are not necessarily trusted from a security standpoint. Network connection to an extranet is often, but not always, implemented via WAN technology.

6.3 Internetwork

An internetwork is the connection of multiple computer networks via a common routing technology using routers.

6.4 Internet

Partial map of the Internet based on the January 15, 2005 data found on opte.org. Each line is drawn between two nodes, rep-resenting two IP addresses. The length of the lines are indicative of the delay between those two nodes. This graph represents less than 30% of the Class C networks reachable.

The Internet is the largest example of an internetwork. It is a global system of interconnected governmental, academic, corporate, public, and private computer networks. It is based on the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Re-search Projects Agency Network (ARPANET) developed by DARPA of the United States Department of Defense. The Internet is also the communications backbone under-lying the World Wide Web (WWW).

6.5 Darknet

A Darknet is an overlay network, typically running on the internet, that is only accessible through specialized soft-ware. A darknet is an anonymizing network where connections are made only between trusted peers — some-times called “friends” (F2F)— using non-standard protocols and ports.

Darknets are distinct from other distributed peer-to-peer networks as sharing is anonymous (that is, IP addresses are not publicly shared), and therefore users can communicate with little fear of governmental or corporate interference.

CHAPTER 7

Routing

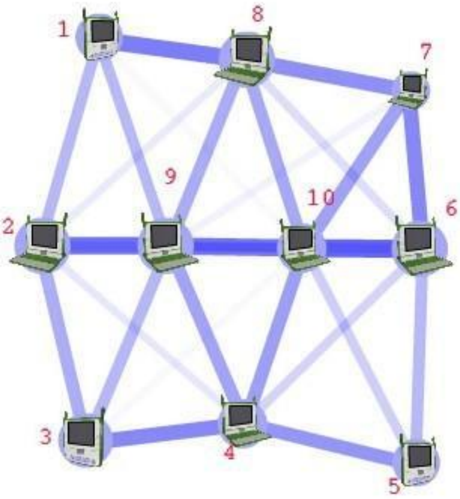


Figure 8.1: Routing

Routing calculates good paths through a network for information to take. For example, from node 1 to node 6 the best routes are likely to be 1-8-7-6 or 1-8-10-6, as this has the thickest routes.

Routing is the process of selecting network paths to carry network traffic. Routing is performed for many kinds of networks, including circuit switching networks and packet switched networks.

In packet switched networks, routing directs packet for- warding(the transit of logically addressed network packets from their source toward their ultimate destination) through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and per-form routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing.

There are usually multiple routes that can be taken, and to choose between them, different elements can be considered to decide which routes get installed into the routing table, such as (sorted by priority):

1. Prefix-Length: where longer subnet masks are preferred (independent if it is within a routing protocol or over different routing protocol)

2. Metric: where a lower metric/cost is preferred (only valid within one and the same routing protocol)

3. Administrative distance: where a lower distance is preferred (only valid between different routing protocols)

Most routing algorithms use only one network path at a time. Multipath routing techniques enable the use of multiple alternative paths.

Routing, in a more narrow sense of the term, is often contrasted with bridging in its assumption that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured ad-dressing (routing, in the narrow sense) outperforms un-structured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within localized environments.

7.1 Network service

Network services are applications hosted by servers on a computer network, to provide some functionality for members or users of the network, or to help the network itself to operate.

The World Wide Web, E-mail, printing and network file sharing are examples of well-known network ser-vices. Network services such as DNS (Domain Name System)give names for IP and MAC addresses and DHCP to ensure that the equipment on the network has a valid IP address.
Services are usually based on a service protocol that de-fines the format and sequencing of messages between clients and servers of that network service.

CHAPTER 8

Network performance

8.1 Quality of service

Depending on the installation requirements, network performance is usually measured by the quality of service of a telecommunications product. The parameters that affect this typically can include throughput, jitter, bit error rate and latency.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network, viz. ATM:

Circuit-switched networks: In circuit switched net-works, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include the level of noise and echo.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

8.2 Network congestion

Network congestion occurs when a link or node is carrying so much data that its quality of service deteriorates. Typical effects include queuing delay, packet loss or the blocking of new connections. A consequence of these latter two is that incremental increases in offered load lead either only to small increase in network throughput, or to an actual reduction in network throughput.

Network protocols that use aggressive retransmissions to compensate for packet loss tend to keep systems in a state of network congestion—even after the initial load is reduced to a level that would not normally induce network congestion. Thus, networks using these protocols can exhibit two stable states under the same level of load. The stable state with low throughput is known as congestive collapse.

8.3 Network resilience

Network resilience is “the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.”

CHAPTER 9

Security

9.1 Network security

Network security consists of provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and its network-accessible resources. Network security is the authorization of access to data in a network, which is con-trolled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. Network security is used on a variety of computer networks, both public and private, to secure daily transactions and communications among businesses, government agencies and individuals.

9.2 Network surveillance

Network surveillance is the monitoring of data being transferred over computer networks such as the Internet. The monitoring is often done surreptitiously and may be done by or at the behest of governments, by corporations, criminal organizations, or individuals. It may or may not be legal and may or may not require authorization from a court or other independent agency.

Computer and network surveillance programs are widespread today, and almost all Internet traffic is or could potentially be monitored for clues to illegal activity.

Surveillance is very useful to governments and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. With the advent of programs such as the Total Information Awareness program, technologies such as high speed surveillance computers and biometrics software, and laws such as the Communications Assistance For Law Enforcement Act, governments now possess an unprecedented ability to monitor the activities of citizens.

However, many civil rights and privacy groups—such as Reporters Without Borders, the Electronic Frontier Foundation and the American Civil Liberties Union—have expressed concern that increasing surveillance of citizens may lead to a mass surveillance society, with limited political and personal freedoms. Fears such as this have led to numerous lawsuits.

9.3 End to end encryption

End-to-end encryption (E2EE) is a digital communications paradigm of uninterrupted protection of data traveling between two communicating parties. It involves the originating party encrypting data so only the in-tended recipient can decrypt it, with no dependency on third parties. End-to-end encryption prevents intermediaries, such as Internet providers or application service providers from discovering or tampering with communications. End-to-end encryption generally protects both confidentiality and integrity.

Examples of end-to-end encryption include PGP for email, OTR for instant messaging, ZRTP for telephony and TETRA for radio.

Typical server-based communications systems do not include end-to-end encryption. These systems can only guarantee protection of communications between clients and servers, not between the communicating parties themselves. Examples of non-E2EE systems are Google Talk, Yahoo Messenger, Facebook and Dropbox. Some such systems, for example Lava Bit and Secret Ink, have even described themselves as offering "end-to-end" encryption when they do not. Some systems that normally offer end-to-end encryption have turned out to contain a back door that subverts negotiation of the encryption key between the communicating parties, for example Skype or Hush mail.

The end-to-end encryption paradigm does not directly ad-dress risks at the communications endpoints themselves, such as the technical exploitation of clients, poor quality random number generators, or key escrow. E2EE also does not address traffic analysis, which relates to things such as the identities of the end points and the times and quantities of messages that are sent.

CHAPTER 10

Views of networks

Users and network administrators typically have different views of their networks. Users can share printers and some servers from a workgroup, which usually means they are in the same geographic location and are on the same LAN, whereas a Network Administrator is responsible to keep that network up and running. A community of interest has less of a connection of being in a local area, and should be thought of as a set of arbitrarily located users who share a set of servers, and possibly also communicate via peer-to-peer technologies.

Network administrators can see networks from both physical and logical perspectives. The physical perspective involves geographic locations, physical cabling, and the network elements (e.g., routers, bridges and application layer gateways) that interconnect via the transmission media. Logical networks, called, in the TCP/IP architecture, subnets, map onto one or more transmission media. For example, a common practice in a campus of buildings is to make a set of LAN cables in each building appear to be a common subnet, using virtual LAN (VLAN) technology.

Both users and administrators are aware, to varying ex-tents, of the trust and scope characteristics of a net-work. Again using TCP/IP architectural terminology, an intranet is a community of interest under private administration usually by an enterprise, and is only accessible by authorized users (e.g. employees). Intranets do not have to be connected to the Internet, but generally have a limited connection. An extranet is an extension of an intranet that allows secure communications to users outside of the intranet (e.g. business partners, customers).

Unoffcially, the Internet is the set of users, enterprises, and content providers that are interconnected by Internet Service Providers (ISP). From an engineering view point, the Internet is the set of subnets, and aggregates of sub-nets, which share the registered IP address space and ex-change information about the reach ability of those IP ad-dresses using the Border Gateway Protocol. Typically, the human-readable names of servers are translated to IP addresses, transparently to users, via the directory function of the Domain Name System (DNS).

Over the Internet, there can be business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) communications. When money or sensitive information is exchanged, the communications are apt to be protected by some form of communications security mechanism. Intranets and extranets can be securely superimposed onto the Internet, without any access by general Internet users and administrators, using secure Virtual Private Network (VPN) technology.

Conclusion

Internship is a period from where we can get some knowledge that can be helpful in our professional life. From there I have learned how to behave with others and deal with the networks. I worked as an intern in the IT division at Mutual Trust Bank Ltd. I served there with dedicative mind and got the respect from them. I have gathered a lot of experience throughout the entire internship period. I got a scope in the field of card captured from card division very 1st time. Then got the opportunity in network operation, design & implementation. It is a great opportunity to use the knowledge and skills that I had acquired. Now I am able to serve any other company on this specific field.

References

[1] Computer network definition, retrieved 2011-11-12

[2] [The story of how a cybernetics pioneer became unnecessary to the USSR].ria. ru(in Russian). 2010-08-09. Retrieved 2015-03-04 [One can regard the magnum opus of Kitov’s career as his elaboration of the plan - unfortunately never brought into practical form - for the establishment of a computer network (the Unified State Network of Computer Centres - EGSVTs) for the control of the national economy and simultaneously for the resolution of military tasks. Anatolii Ivanovich presented this plan directly to the highest levels, sending a letter in January 1959 to the General Secretary of the Communist Party of the Soviet Union Nikita Khrushchev. Not receiving a reply (although supported in various circles), in the autumn of the same year he again sent a letter to the very top, appending a 200-page detailed project plan, called the 'Red Book.

[3] Chris Sutton. “Internet Began 35 Years Ago at UCLA with First Message Ever Sent Between Two Computers”. UCLA. Archived from the original on March 8, 2008.

[4] Ethernet: Distributed Packet Switching for Local Computer Networks, Robert M. Metcalfe and David R. Boggs, Communications of the ACM (pp 395–404, Vol. 19, No. 5), July 1976.

[5] Spurgeon, Charles E. (2000). Ethernet The Definitive Guide. O'Reilly & Associates.ISBN1-56592-660-9.

[6] , The Disadvantages of Wired Technology, Laura Acevedo, Demand Media.

[7] “Bergen Linux User Group’s CPIP Implementation”. Blug.linux.no. Retrieved 2014-03-01.

[8] A. Hooke (September 2000), Interplanetary Internet (PDF), Third Annual International Symposium on Advanced Radio Technologies, retrieved 2011-11-12

[9] “Define switch.”. WWW.Wikipedia.com. Retrieved April 8, 2008.

[10] http://compnetworking.about.com/cs/internetworking/g/ bldef_bridge.htm

[11] D. Andersen; H. Balakrishnan; M. Kaashoek; R. Morris (October 2001), Resilient Overlay Networks, Association for Computing Machinery, retrieved 2011-11-12

[12] “End System Multicast”. project web site. Carnegie Mel-lon University. Retrieved May 25, 2013.

[13] Wakeman, I (Jan 1992). “Layering considered harmful”.

IEEE Network: pp. 20–24.

[14]Kurose, James; Ross, Kieth (2005). Computer Networking: A Top-Down Approach. Pearson.

[15]For an interesting write-up of the technologies involved, including the deep stacking of communications protocols used, see. Martin, Thomas. “Design Principles for DSL-Based Access Solutions” (PDF). Retrieved 18 June 2011.

[16]Nanoscale Communication Networks, Bush, S. F., ISBN978-1-60807-003-9, Artech House, 2010.

[17]“personal area network (PAN)". Retrieved January 29,2011.

[18]New global standard for fully networked home,ITU-T,2008-12-12, retrieved 2011-11-12

[19]IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force, retrieved 2011-11-12

[20]“Mobile Broadband Wireless connections (MBWA)".Retrieved 2011-11-12.

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 10