Networking Architecture of National Institute of Hydrology Roorkee

Minor Project Thesis

Submitted By:

Akshay Singh Dhami

For the partial fulfilment of the

Degree of B-Tech in Computer Science and Technology

Submitted to
Quantum School of Technology
Roorkee (Uttrakhand)

August 2016

Akshay Singh Dhami
130430101090
akshaysinghdhami@gmail.com

Certificate

We hereby certify that the project work entitled "NIH Networking Architecture" carried out by Mr. Akshay Singh Dhami, B-tech (Computer Science and Technology), Quantum Global Campus, Roorkee is authentic record of work carried out by him during June 11,2016 to July 26,2016 under our guidance.

We appreciate the sincerity and hard work put by Mr. Akshay Singh Dhami for completing the task in 45 days period. We wish him Success in his future endeavour.

(Prabhash K. Mishra)

Scientist 'B' & OIC
Computer Centre,
NIH Roorkee

(Dr. A.K Lohani)

Scientist 'G' & Head
Computer Centre,
NIH Roorkee

ACKNOWLEDGEMENT

I would like to express my gratitude to the Director, National Institute of Hydrology (NIH) Roorkee and Head, Research Management and Outreach Division (RMOD) for giving permission to work under the Summer Internship Program in the institute. I would like to express the deepest appreciation to Dr. A.K. Lohani, Sc G & Head, Computer Centre and Shri P.K. Mishra, Sc B & OIC, Computer Centre who have shown keen interest in guiding us continuously and persuasively through the entire internship program. Without their supervision and constant help this dissertation would not have been possible. I am also thankful to Quantum School of Technology for their help rendered during this study period.

I would also like to express my gratitude to Mr. Navdeep Sirohi, Sr.Manager – Training and Placement, Quantum Global Campus for their cooperation and assistance during the study period.

I also take this opportunity to thank Mr. Abhishek Agarwal & Mr. Amardeep for their valuable information provided by them in their respective field during the study.

Lastly, I would like to thank my loved ones, who have supported me throughout the entire process, both by keeping harmonious and helping me putting pieces together. I will be grateful forever for their love.

Akshay

Akshay Singh Dhami

Abstract

As we all know that networking is very essential part in any Organization as it provides the facility to communicate from one end to other. With the help of networking we can easily send any information (data) without travelling to the destination. We can find essence of networking in almost everything around us, from our mobile phones to the internet in our laptops. In the present work, networking model existing at National Institute of Hydrology (NIH) Roorkee has been visited and discussed. In the study discussion has been made how the connection (networking) is being made at NIH and how the configuration is done of various devices like PC's, Switches, Hubs, Routers, Server, etc. In this project several passwords like enable, secret, telnet password, etc. have been explored. However, due to paucity of time, more substantial study could have been done with the data available at the Computer Centre of NIH Roorkee. This study is just an attempt to understand the concept of Networking Architecture in a real organisation.

Table of Contents

LIST OF FIGURES

About NIH

THE ROLE AND FUNCTIONS OF NATIONAL INSTITUTE OF HYDROLOGY

- To undertake, aid, promote and coordinate systematic and scientific work on all aspects of hydrology.

- To cooperate and collaborate with other national, foreign and international organizations in the field of hydrology.

- To establish and maintain a research reference library in pursuance of the objectives of the Society and equip the same with books, reviews, magazines and other relevant publications.

- To do all other such things as the Society may consider necessary, incidental or conducive for the attainment of the objectives for which the Institute has been established.

AREAS OF SPECIALIZATION:-

- ENVIRONMENTAL GROUND
- WATER
- HYDROLOGY
- HYDROLOGY
- SURFACE WATER
- WATER
- RESOURCES
- HYDROLOGY
- SYSTEMS
- HYDROLOGICAL
- INVESTIGATIONS
- ACTIVITIES

BASIC, APPLIED AND STRATEGIES

- RESEARCH
- SOFTWARE DEVELOPMENT
- USER DEFINED, DEMAND DRIVEN RESEARCH PROJECTS
- CONSULTANCY
- TECHNOLOGY TRANSFER
- INCOH SECRETARIAT
- WATER AVAILABILITY

Computer Centre in NIH ROORKEE:-

The Computer Centre is responsible for providing computing, networking, internet and email facilities to Scientists and Staff at the Institute. Computing has become an essential tool for almost all scientific research. Computers of latest configuration are available in the Institute for conducting complex hydrological analyses and modelling studies. Internet and email facilities are routinely utilized for accessing scientific literature as well as for correspondence. The Institute also uses computers for processing of administrative and accounting data. The centre procures and provides maintenance to computers and related peripherals available with the Scientists and Staff.

The local area network (LAN) provides interconnectivity between the computers in different building blocks of the campus. The network comprises of switches in various blocks and UTP connections to individual machines. The LAN is connected to Internet by a 50 Mbps leased line link from BSNL.VSAT connectivity from ERNET India also exists for email communication. A centralized server receives and

Stores/forwards emails to respective users. A dedicated web server (www.nih.ernet.in) provides a platform for hosting institute information, research publications, important announcements, tender notices etc. and some useful hydrology related information. To maintain the integrity and security of Institute's network, a firewall restricts access from outside to machines within the LAN. All the facilities existing at the Computer Centre are upgraded from time to time to meet the evolving standards of Information Technology.

History of Networking

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

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

- In 1962, J.C.R. Licklider developed a working group he called the Intergalactic Computer Network and a precursor to the ARPANET, at the Advanced Research Projects.

- In 1964, researchers at Dartmouth developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at Massachusetts Institute of Technology, a research group supported by General Electric and Bell Labs used a computer to route and manage telephone connections.

- Throughout the 1960s, Leonard Klein rock, Paul Baron, and Donald Davies independently developed network systems that used packets to transfer information between computers

- In 1965, Thomas Merrill and Lawrence G. Roberts created the first wide area network (WAN). This was an immediate precursor to the ARPANET, of which are Roberts became program manager.

- Also in 1965, the first widely used telephone switch that implemented true computer control was introduced by Western Electric.

- 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 were connected as the beginning of the ARPANET network using 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, networking system that was based on the Aloha network, developed in the 1960s by Norman Abramson and colleagues at the University of Hawaii.

- 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 Ethernet was increased from 10 Mbit/s to 100Mbit/s. By 1998, Ethernet supported transmission speeds of a Gigabit. The ability of Ethernet to scale easily (such as quickly adapting to support new fibre optic cable speeds) is a contributing factor to its continued use today.

- Today, computer networks are the core of modern communication. All modern aspects of the public switched telephone network (PSTN) are computer-controlled. Telephony increasingly runs over the Internet Protocol, although not necessarily the public Internet.

- Computer network. Computer networks, and the technologies that make communication between networked computers possible, continue to drive computer hardware, software, and peripherals industries. The expansion of related industries is mirrored by growth in the numbers and types of people using networks, from the researcher to the home user.

- 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 are Roberts became program manager.

The communication media used to link devices to form a computer network include electrical cable (Home PNA, power line Communication, G.hn), optical fibre (fibre-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.

A widely adopted family of communication media used in local area network (LAN) technology is collectively known as Ethernet. The media and protocol standards that enable communication between networked devices over Ethernet are defined by IEEE 802.3.Ethernet transmit data over both copper and fibre cables. Wireless LAN standards (e.g. those defined by IEEE 802.11) use radio waves, or others use infrared signals as a transmission medium. Power line communication uses a building& power cabling to transmit data.

Wired technologies

Fibre optic cables are used to transmit light from one computer/network node to another. The orders of the following wired technologies are, roughly, from slowest to fastest

- Twisted pair wire is the most widely used medium for all telecommunication. Twisted-pair cabling consist of copper wires that are twisted into pairs. Ordinary telephone wires consist of two insulated copper wires twisted into pairs. Computer network cabling(wired Ethernet as defined by IEEE 802.3) consists of 4 pairs of copper cabling that can be utilized for both voice and data transmission. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed ranges from 2million bits per second to 10 billion bits per second. Twisted pair cabling comes in two forms: unshielded twisted pair (UTP) and shielded twisted-pair (STP). Each form comes in several category ratings, designed for use in various scenarios.

- Coaxial cable is widely used for cable television systems, office buildings, and other work-sites for local area networks. The cables consist of copper or aluminium wire surrounded by an insulating layer (typically a flexible material with a high dielectric constant), which itself is surrounded by a conductive layer. The insulation helps minimize interference and distortion. Transmission speed ranges from 200 million bits per second to more than 500million bits per second.

- ITU-T G.hn technology uses existing home wiring (coaxial cable, phone lines and power lines) to create a high-speed (up to 1 Gigabit/s) local area network.

- An optical fibre is a glass fibre. It carries pulses of light that represent data. Some advantages of optical fibre over metal wires are very low transmission loss and immunity from electrical interference. Optical fibres can simultaneously carry multiple wavelengths of light, which greatly increases the rate that data can be sent, and helps enable data rates of up to trillions of bits per second. Optic fibres can be used for long runs of cable carrying very high data rates, and are used for undersea cables to interconnect continents.

Wireless technologies

Computers are very often connected to networks using wireless links.

- 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 & atmosphere. The satellites are stationed in space, typically in geosynchronous orbit 35,400 km (22,000 mi) above the equator. These Earth-

orbiting systems are capable of receiving and relaying voice, data, and TV signals.

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

Routers

A router is a networking device that forwards data packets between computer networks. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.[1]

A router is connected to two or more data lines from different networks (as opposed to a network switch, which connects data lines from one single network). When a data packet comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. This creates an overlay internetwork.

The most familiar type of routers are home and small office routers that simply pass data, such as web pages, email, IM, and videos between the home computers and the Internet. An example of a router would be the owner's cable or DSL router, which connects to the Internet through an ISP. More sophisticated routers, such as enterprise routers, connect large business or ISP networks up to the powerful core routers that forward data at high speed along the optical fiber lines of the Internet backbone. Though routers are typically dedicated hardware devices, use of software-based routers has grown increasingly common.

NIH Router

Applications of Router

When multiple routers are used in interconnected networks, the routers exchange information about destination addresses using a dynamic routing protocol. Each router builds up a table listing the preferred routes between any two systems on the interconnected networks. A router has interfaces for different physical types of network connections, such as copper cables, fibre optic, or wireless transmission. It also contains firmware for different networking communications protocol standards.

Each network interface uses this specialized computer software to enable data packets to be forwarded from one protocol transmission system to another.

Routers may also be used to connect two or more logical groups of computer devices known as subnets, each with a different sub-network address. The subnet addresses recorded in the router do not necessarily map directly to the physical interface connections.

A router has two stages of operation called planes:

- Control plane: A router maintains a routing table that lists which route should be used to forward a data packet, and through which physical interface connection. It does this using internal pre-configured directive, called static routes, or by learning routes using a dynamic routing protocol. Static and dynamic routes are stored in the Routing Information Base (RIB). The control-plane logic then strips the RIB from non essential directives and builds a Forwarding Information Base (FIB) to be used by the forwarding-plane.

- **Forwarding plane**: The router forwards data packets between incoming and outgoing interface connections. It routes them to the correct network type using information that the packet header contains. It uses data recorded in the routing table control plane.

Routers may provide connectivity within enterprises, between enterprises and the Internet, or between 'internet service providers' (ISPs) networks. The largest routers (such as the Cisco CRS-1 or JuniperT1600) interconnect the various ISPs, or may be used in large enterprise networks.[Smaller routers usually provide connectivity for typical home and office networks. Other networking solutions may be provided by a backbone Wireless Distribution System (WDS), which avoids the costs of introducing networking cables into buildings.

- Access

Access routers, including 'small office/home office' (SOHO) models, are located at customer sites such as branch offices that do not need hierarchical routing of their own. Typically, they are optimized for low cost. Some SOHO routers are capable of running alternative free Linux-based firm wares like Tomato, Open Wart or DD-WRT.

- Distribution

Distribution routers aggregate traffic from multiple access routers, either at the same site, or to collect the data streams from multiple sites to a major enterprise location. Distribution routers are often responsible for enforcing quality of service across a wide area network (WAN), so they may have considerable memory installed, multiple WAN interface connections, and substantial onboard data processing routines. They may also provide connectivity to groups of file servers or other external networks.

- Security

External networks must be carefully considered as part of the overall security strategy. A router may include a firewall, VPN handling, and other security functions, or these may be handled by separate devices.

Many companies produced security-oriented routers, including Cisco PIXseries, Juniper Net Screen and Watch Guard. Routers also commonly perform network address translation, (which allows multiple devices on a network to share a single public IP address) and stateful packet inspection. Some experts argue that open source routers are more secure and reliable than closed source routers because open source routers allow mistakes to be quickly found and corrected.

- Core

In enterprises, a core router may provide a "collapsed backbone" interconnecting the distribution tier routers from multiple buildings of a campus, or large enterprise locations. They tend to be optimized for high bandwidth, but lack some of the features of Edge Routers.

Internet connectivity and internal use

Routers intended for ISP and major enterprise connectivity usually exchange routing information using the Border Gateway Protocol (BGP). RFC 4098standard defines the types of BGP routers according to their functions:

- *Edge router*: Also called a Provider Edge router, is placed at the edge of an ISP network. The router uses External BGP to EBGP routers in other ISPs, or a large enterprise Autonomous System.
- *Subscriber edge router*: Also called a Customer Edge router, is located at the edge of the subscriber's network, it also uses EBGP to its provider's Autonomous System. It is typically used in an (enterprise) organization.
- *Inter-provider border router*: Interconnecting ISPs is a BGP router that maintains BGP sessions with other BGP routers in ISP Autonomous Systems.
- Core router: A *core router* resides within an Autonomous System as a back bone to carry traffic between edge routers.[
- Within an ISP: In the ISP's Autonomous System, a router uses internal BGP to communicate with other ISP edge routers, other intranet core routers, or the ISP's intranet provider border routers.

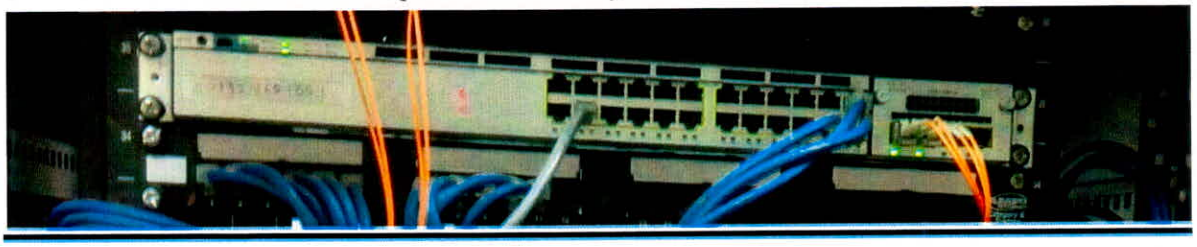
- "Internet backbone:" The Internet no longer has a clearly identifiable backbone, unlike its predecessor networks. See default-free zone (DFZ). The major ISPs' system routers make up what could be considered to be the current Internet backbone core. ISPs operate all four types of the BGP routers described here. An ISP "core" router is used to interconnect its edge and border routers. Core routers may also have specialized functions in virtual private networks based on a combination of BGP and Multi-Protocol Label Switching protocols.
- Voice/Data/Fax/Video Processing Routers: Commonly referred to as access servers or gateways, these devices are used to route and process voice, data, video and fax traffic on the Internet. Since 2005, most long-distance phone calls have been processed as IP traffic (VOIP) through a voice gateway. Use of access server type routers expanded with the advent of the Internet, first with dial-up access and another resurgence with voice phone service..

Switch

A network switch (also called switching hub, bridging hub, officially MAC bridge) is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device. Unlike less advanced network hubs, a nctwork switch forwards data only to one or multiple devices that need to receive it, rather than broadcasting the same data out of each of its ports.

A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality that most commonly uses IP addresses to perform packet forwarding; such switches are commonly known as layer-3 switches or multilayer switches. Beside most commonly used Ethernet switches, they exist for various types of networks, including Fibre Channel, Asynchronous Transfer Mode, and Infinity Band. The first Ethernet switch was introduced by Kalpana in 1990.

- Switch used in NIH(L3 Switch)



- Applications of Switch

The network switch plays an integral role in most modern Ethernet local area networks (LANs). Mid-to-large sized LANs contain a number of linked managed switches. Small office/home office (SOHO) applications typically use a single switch, or an all-purpose converged device such as a residential gateway to access small office/home broadband services such as DSL or cable Internet. In most of these cases, the end-user device contains a router and components that interface to the particular physical broadband technology. User devices may also include a telephone interface for Voice over IP (VoIP) protocol.

- Micro segmentation

Segmentation involves the use of a bridge or a switch (or a router) to split a larger collision domain into smaller ones in order to reduce collision probability, and to improve overall network throughput. In the extreme case (i.e. micro segmentation), each device is located on a dedicated switch port. In contrast to an Ethernet hub, there is a separate collision domain on each of the switch ports. This allows computers to have

dedicated bandwidth on point-to-point connections to the network and also to run in full-duplex without collisions. Full-duplex mode has only one transmitter and one receiver per "collision domain", making collisions impossible.

- Role of switches in a network

Switches may operate at one or more layers of the OSI model, including the data link and network layers. A device that operates simultaneously at more than one of these layers is known as a *multilayer switch.*

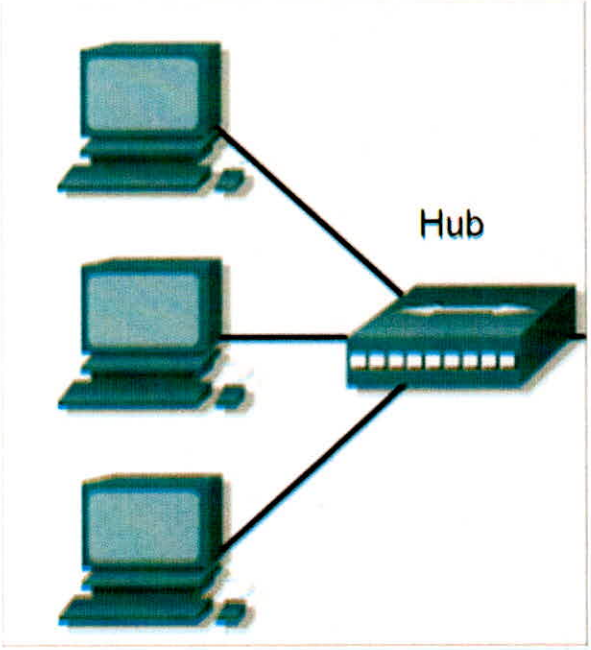
In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, including Ethernet, Fibre Channel, Rapid IO, ATM, ITU-TG.hn and 802.11. This connectivity can be at any of the layers mentioned. While the layer-2 functionality is adequate for bandwidth-shifting within one technology, interconnecting technologies such as Ethernet and token ring is performed easier at layer 3 or via routing. Devices that interconnect at the layer 3 are traditionally called routers, so layer 3 switches can also be regarded as relatively primitive and specialized routers.

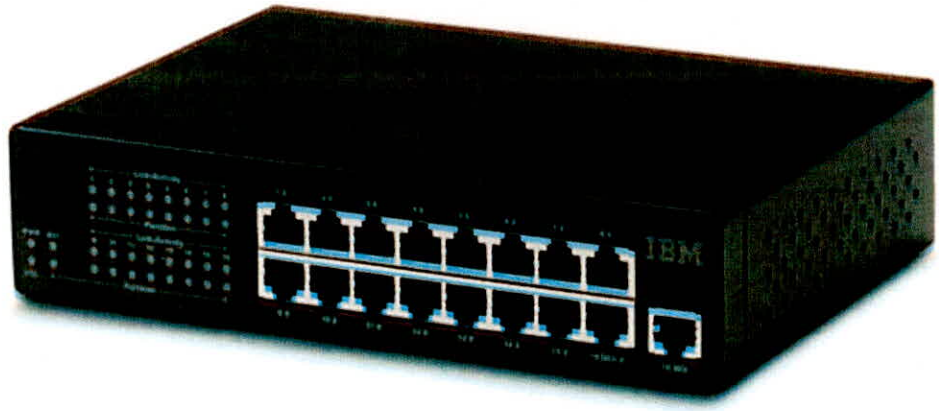
Where there is a need for a great deal of analysis of network performance and security, switches may be connected between WAN routers as places for analytic modules. Some vendors provide firewall, network intrusion detection, and performance analysis modules that can plug into switch ports. Some of these functions may be on combined modules.

In other cases, the switch is used to create a mirror image of data that can go to an external device. Since most switch port mirroring provides only one mirrored stream, network hubs can be useful for fanning out data to several read-only analyzers, such as intrusion detection systems and packet sniffers.

HUB

A Hub is a networking device which receives signal from the source, amplifies it and send it to multiple destinations or computers. If you ever some across subject 'Computer Networking' then you must heard this word. Sometimes, hubs are also called Ethernet Hub, Repeater Hub, Active Hub and Network Hub. Basically it is a networking device which is used multiple devices like Computers, Servers etc to each other and make them work as a single network segment. Hubs are used in 'Physical Layer' of OSI Model.





Construction of Hub

Practically Hubs is a small box in rectangular shape which have multiple ports for connecting various devices to it. It receives its power supply from auxiliary power sources. The main work of Hub is to receive incoming data signals, amplify them in the form of electrical signals and then send them to each connected device. A Hub may contain a number of ports. Minimum amount of ports that a hub can have is 4 and it can have up to 24 ports for connecting various devices and peripherals to it.

Types of Hub: On the basis of its working methods, the Hubs can be divided into three types, given as:

- Active Hub
- Passive Hub
- Intelligent Hub

Active Hub: As its name suggests, Active Hub is a hub which can amplify or regenerate the information signal. This type of bus has an advantage as it also amplifies the incoming signal as well as forwards it to multiple devices. This Bus is also known as Multiport Repeater. It can upgrade the properties if incoming signal before sending them to destination.

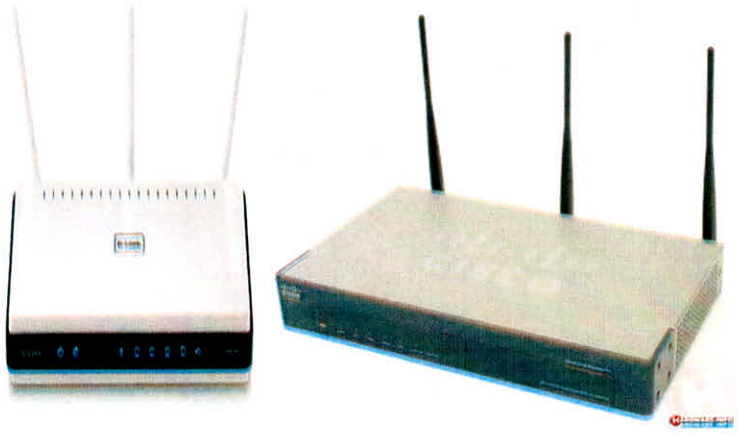
Passive Hub: Passive Hub works like a simple Bridge. It is used for just creating a connection between various devices. It does not have the ability to amplify or regenerate any incoming signal. It receives signal and then forward it to multiple devices.

Intelligent Hub: This is the third and last type of Bus. It can perform tasks of both Active and Passive buses. Also, it can perform some other tasks like Bridging and routing. It increases the speed and effectiveness of total network thus makes the performance of whole network fast and efficient.

Applications Of Hub: Networking Hub is widely used networking connectivity device. It has many advantages over other connectivity devices. Some Application of Networking Hub is given below:

- Hubs are used to create small Home Networks.
- Hubs are used for monitoring the networks.
- Hubs are used in Organizations and Computer Labs for connectivity.
- It makes one device or peripheral available throughout the whole network.

Access point



In computer networking, a wireless access point (WAP) is a networking hardware device that allows a Wi-Fi compliant device to connect to a wired network. The WAP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself. A WAP is differentiated from a hotspot, which is the physical location where Wi-Fi access to a WLAN is available.

Contents of Access Point

- ## Introduction

Linksys "WAP54G" 802.11g wireless access point Embedded Router Board 112 with U.FL-RSMA pigtail and R52 mini PCI Wi-Fi card widely used by wireless Internet service providers (WISPs) across the world Prior to wireless networks, setting up a computer network in a business, home or school often required running many cables through walls and ceilings in order to deliver network access to all of the network-enabled devices in the building. With the creation of the wireless access point, network users are now able to add devices that access the network with few or no cables. A WAP normally connects directly to a wired Ethernet connection and the WAP then provides wireless connections using radio frequency links for other devices to utilize that wired connection.

Most WAPs support the connection of multiple wireless devices to one wired connection.

Modern WAPs are built to support a standard for sending and receiving data using these radio frequencies. Those standards and the frequencies they use are defined by the IEEE. Most APs use IEEE 802.11 standards.

- Common AP applications

Typical corporate use involves attaching several WAPs to a wired network and then providing wireless access to the office LAN. The wireless access points are managed by a WLAN Controller which handles automatic adjustments to RF power, channels, authentication, and security. Furthermore, controllers can be combined to form a wireless mobility group to allow inter-controller roaming. The controllers can be part of a mobility domain to allow clients access throughout large or regional office locations. This saves the clients time and administrators overhead because it can automatically re-associate or re-authenticate.

A hotspot is a common public application of WAPs, where wireless clients can connect to the Internet without regard for the particular networks to which they have attached for the moment. The concept has become common in large cities, where a combination of coffeehouses, libraries, as well as privately owned open access points, allow clients to stay more or less continuously connected to the Internet, while moving around. A collection of connected hotspots can be referred to as a lily pad network.

WAPs are commonly used in home wireless networks. Home networks generally have only one AP to connect all the computers in a home. Most are wireless routers, meaning converged devices that include the WAP, arouter, and, often, an Ethernet switch. Many also include a broadbandmodem. In places where most homes have their own WAP within range of the neighbours' AP, it's possible for technically savvy people to turn off their encryption and set up a wireless community network, creating an intra-city communication network although this does not negate the requirement for a wired network.

A WAP may also act as the network's arbitrator, negotiating when each nearby client device can transmit. However, the vast majority of currently installed IEEE 802.11 networks do not implement this, using a distributed pseudo-random algorithm called CSMA/CA instead.

- Wireless access point vs. ad hoc network

Some people confuse wireless access points with wireless ad hoc networks. An ad hoc network uses a connection between two or more devices without using a wireless access point: the devices communicate directly when in range. An ad hoc network is used in situations such as a quick data exchange or a multiplayer LAN game because setup is easy and does not require an access point. Due to its peer-to-peer layout, ad hoc connections are similar to Bluetooth ones.

But ad hoc connections are generally not recommended for a permanent installation.[citation needed] The reason is that Internet access via ad hoc networks, using features like Windows' Internet Connection Sharing, may work well with a small number of devices that are close to each other, but ad hoc networks don't scale well. Internet traffic will converge to the nodes with direct internet connection, potentially congesting these nodes. For internet-enabled nodes, access points have a clear advantage, with the possibility of having multiple access points connected by a wired LAN.

- Limitations

One IEEE 802.11 AP can typically communicate with 30 client systems located within a radius of 103 metres.[citation needed] However, the actual range of communication can vary significantly, depending on such variables as indoor or outdoor placement, height above ground, nearby obstructions, other electronic devices that might actively interfere with the signal by broadcasting on the same frequency, type of antenna, the current weather, operating radio frequency, and the power output of devices. Network designers can extend the range of APs through the use of repeaters and reflectors, which can bounce or amplify radio signals that ordinarily would go un-received. In experimental conditions, wireless networking has operated over distances of several hundred kilometres.

Most jurisdictions have only a limited number of frequencies legally available for use by wireless networks. Usually, adjacent WAPs will use different frequencies (Channels) to communicate with their clients in order to avoid interference between the two nearby systems. Wireless devices can "listen" for data traffic on other frequencies, and can rapidly switch from one frequency to another to achieve better reception. However, the limited number of frequencies becomes problematic in crowded downtown areas with tall buildings using multiple WAPs. In such an environment, signal overlap becomes an issue causing interference, which results in signal drop page and data errors.

Wireless networking lags wired networking in terms of increasing bandwidth and throughput. While (as of 2013) high-density 256-QAM (TurboQAM) modulation, 3-antenna wireless devices for the consumer market can reach sustained real-world speeds of some 240 Mbit/s at 13 m behind two standing walls (NLOS) depending on their nature or 360 Mbit/s at 10 m line of sight or 380 Mbit/s at 2 m line of sight (IEEE 802.11ac) or 20 to 25 Mbit/s at 2 m line of sight (IEEE 802.11g), wired hardware of similar cost reaches somewhat less than 1000 Mbit/s up to specified distance of 100 m with twisted-pair cabling (Cat-5, Cat-5e, Cat-6, or Cat-7) (Gigabit Ethernet). One impediment to increasing the speed of wireless communications comes from Wi-Fi's use of a shared communications medium: Thus, two stations in infrastructure mode that are communicating with each other even over the same AP must have each and every frame transmitted twice: from the sender to the AP, then from the AP to the receiver. This approximately halves the effective bandwidth, so an AP is only able to use somewhat less than half the actual over-the-air rate for data throughput. Thus a typical 54 Mbit/s wireless connection actually carries TCP/IP data at 20 to 25 Mbit/s. Users of legacy wired networks expect faster speeds, and people using wireless connections keenly want to see the wireless networks catch up.

By 2012, 802.11n based access points and client devices have already taken a fair share of the marketplace and with the finalization of the 802.11n standard in 2009 inherent problems integrating products from different vendors are less prevalent.

- Security

Wireless access has special security considerations. Many wired networks base the security on physical access control, trusting all the users on the local network, but if wireless access points are connected to the network, anybody within range of the AP (which typically extends farther than the intended area) can attach to the network.

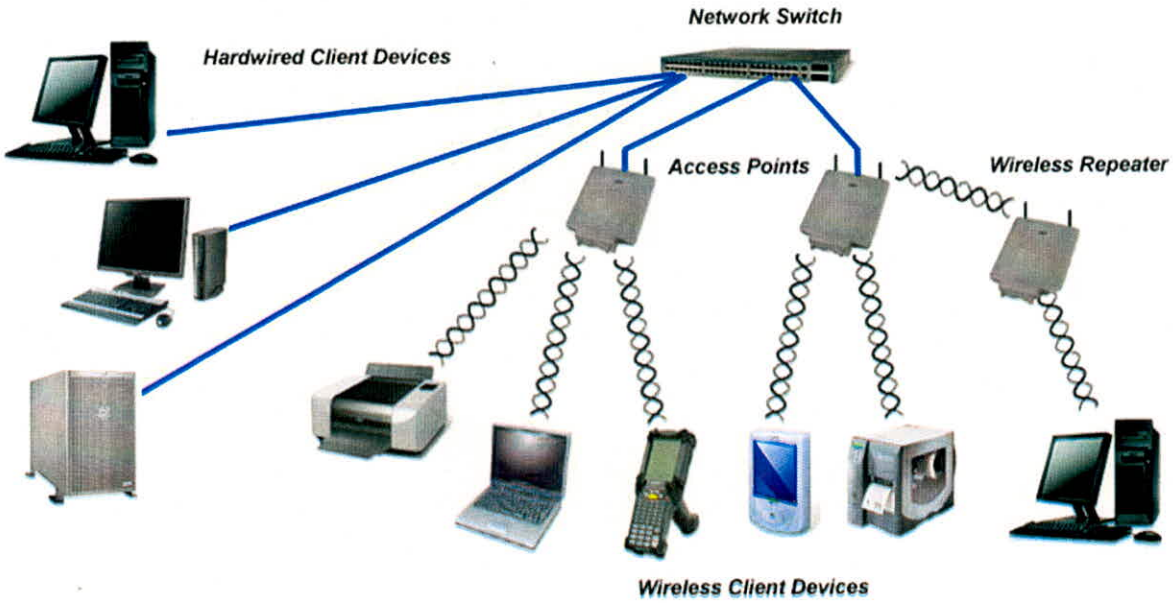
The most common solution is wireless traffic encryption. Modern access points come with built-in encryption. The first generation encryption scheme 'WEP' proved easy to crack; the second and third generation schemes, WPA and WPA2, are considered secure if a strong enough password or passphrase is used.

Some APs support hotspot style authentication using RADIUS and other authentication servers.

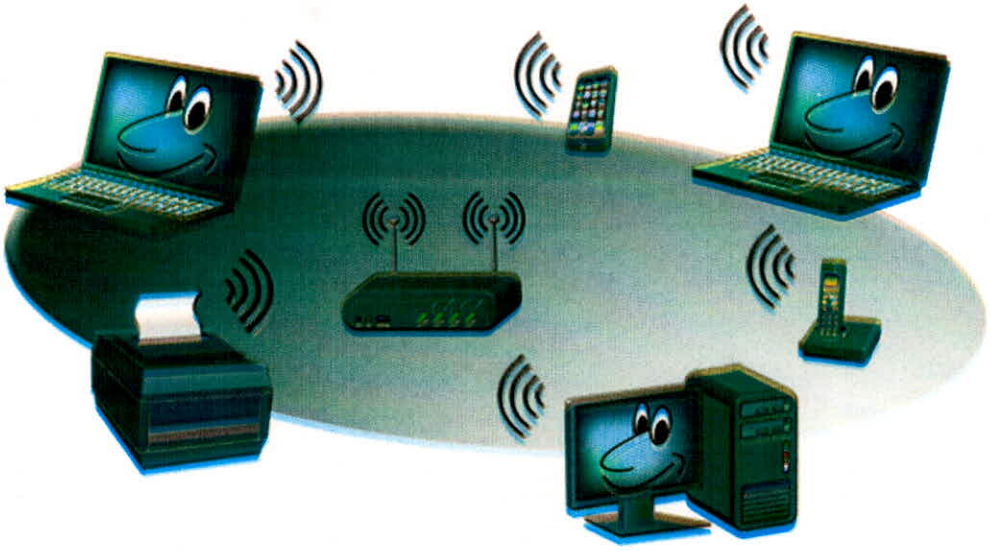
Opinions about wireless network security vary widely. For example, in a 2008 article for wired magazine, Bruce Schneider asserted the net benefits of open Wi-Fi without passwords outweigh the risks, a position supported in 2014 by Peter Eckersley of the Electronic Frontier Foundation.

The opposite position was taken by Nick Mediate in an article for PC World, in which he takes the position that every wireless access point should be locked down with a password.

Wireless devices



In-Building Wireless LAN Diagram



The first wireless transmitters went on the air in the early 20th century using radiotelegraphy (Morse code). Later, as modulation made it possible to transmit voices and music via wireless, the medium came to be called "radio." With the advent of television, fax, data communication, and the effective use of a larger portion of the spectrum, the term "wireless" has been resurrected.

Common examples of wireless equipment in use today include:

- Cellular phones and pagers -- provide connectivity for portable and mobile applications, both personal and business
- Global Positioning System (GPS) -- allows drivers of cars and trucks, captains of boats and ships, and pilots of aircraft to ascertain their location anywhere on earth
- Cordless computer peripherals -- the cordless mouse is a common example; keyboards and printers can also be linked to a computer via wireless
- Cordless telephone sets -- these are limited-range devices, not to be confused with cell phones
- Home-entertainment-system control boxes -- the VCR control and the TV channel control are the most common examples; some hi-fi sound systems and FM broadcast receivers also use this technology.

- Remote garage-door openers -- one of the oldest wireless devices in common use by consumers; usually operates at radio frequencies. Two-way radios -- this includes Amateur and Citizens Radio Service, as well as business, marine, and military communications

- Baby monitors -- these devices are simplified radio transmitter/receiver units with limited range
- Satellite television -- allows viewers in almost any location to select from hundreds of channels
- Wireless LANs or local area networks -- provide flexibility and reliability for business computer users

Firewall

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

- ## How are Firewalls Used?

Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

- ## Hardware and Software Firewalls

Firewalls can be either hardware or software but the ideal firewall configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins.

Hardware firewalls can be purchased as a stand-alone product but are also typically found in broadband routers, and should be considered an important part of your system and network set-up.

Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

Software firewalls are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer.

- ## Common Firewall Filtering Techniques

Firewalls are used to protect both home and corporate networks. A typical firewall program or hardware device filters all information coming through the Internet to your network or computer system. There are several types of firewall techniques that will prevent potentially harmful information from getting through:

- Packet Filter

Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

- Application Gateway

Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.

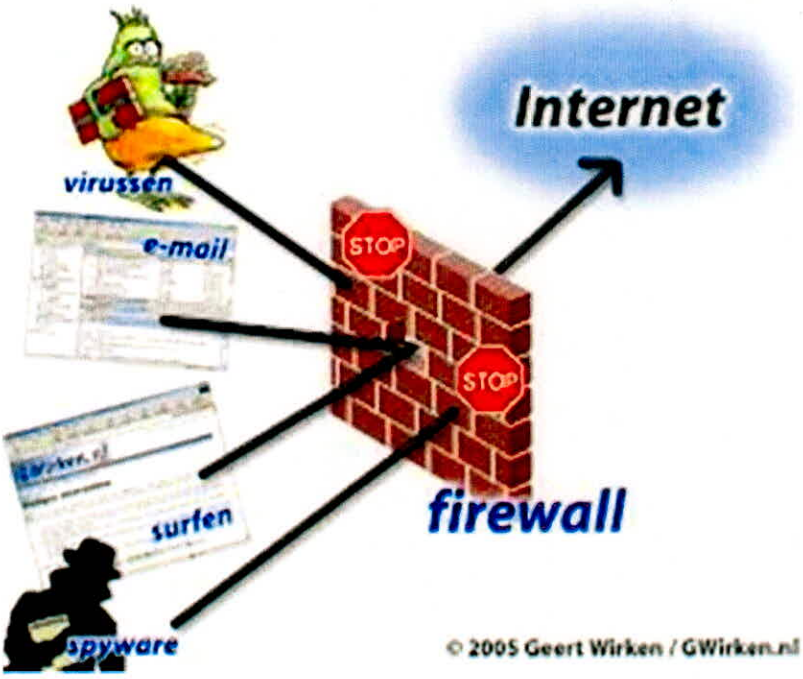
- Circuit-level Gateway

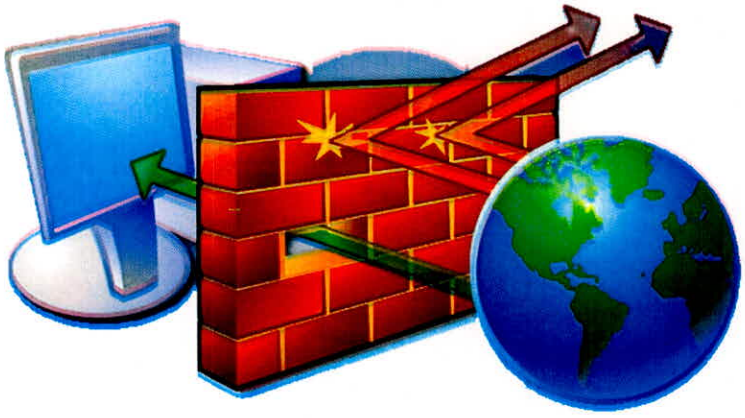
Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

- Proxy Server

Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

- Diagram of Firewall :-





OSI MODEL

The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the

interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. The original version of the model defined seven layers.

A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that comprise the contents of that path. Two instances at the same layer are visualized as connected by a *horizontal* connection in that layer.

❖ Layer 1: Physical Layer

The physical layer has the following major functions:

- It defines the electrical and physical specifications of the data connection. It defines the relationship between a device and a physical transmission medium (e.g., a copper or fiber optical cable, radio frequency). This includes the layout of pins, voltages, line impedance, cable specifications, signal timing and similar characteristics for connected devices and frequency (5 GHz or 2.4 GHz etc.) for wireless devices.

  - It is responsible for transmission and reception of unstructured raw data in a physical medium.
  - It defines transmission mode i.e. simplex, half duplex, full duplex.
  - It defines the network topology as bus, mesh, or ring being some of the most common.
  - It mostly deals with raw data.

The physical layer of Parallel SCSI operates in this layer, as do the physical layers of Ethernet and other local-area networks, such as

Token Ring, FDDI, ITU-T G.hn, and IEEE 802.11 (Wi-Fi), as well as personal area networks such as Bluetooth and IEEE 802.15.4.

❖ Layer 2: Data Link Layer

The data link layer provides node-to-node data transfer—a link between two directly connected nodes. It detects and possibly corrects errors that may occur in the physical layer. It, among other things, defines the protocol to establish and terminate a connection between two physically connected devices. It also defines the protocol for flow control between them.

IEEE 802 divides the data link layer into two sub layers:-

- Media Access Control (MAC) layer - responsible for controlling how devices in a network gain access to medium and permission to transmit it.
- Logical Link Control (LLC) layer - responsible for identifying Network layer protocols and then encapsulating them and controls error checking and frame synchronization.

The MAC and LLC layers of IEEE 802 networks such as 802.3Ethernet, 802.11Wi-Fi, and 802.15.4ZigBee, operate at the data link layer.

The Point-to-Point Protocol (PPP) is a data link layer that can operate over several different physical layers, such as synchronous and asynchronous serial lines.

The ITU-TG.hn standard, which provides high-speed local area networking over existing wires (power lines, phone lines and coaxial cables), includes a complete data link layer that provides both error correction and flow control by means of a repeat sliding.

❖ Layer 3: Network Layer:-

The network layer provides the functional and procedural means of transferring variable length data sequences (called datagram) from one node to another connected to the same *network.*

It translates logical network address into physical machine address. A network is a medium to which many nodes can be connected, on which every node has an *address* and which permits nodes connected to it to

transfer messages to other nodes connected to it by merely providing the content of a message and the address of the destination node and letting the network find the way to deliver the message to the destination node, possibly routing it through intermediate nodes. If the message is too large to be transmitted from one node to another on the data link layer between those nodes, the network may implement message delivery by splitting the message into several fragments at one node, sending the fragments independently, and reassembling the fragments at another node. It may, but need not, report delivery errors.

Message delivery at the network layer is not necessarily guaranteed to be reliable; a network layer protocol may provide reliable message delivery, but it need not do so.

A number of layer-management protocols, a function defined in the *management annex*, ISO 7498/4, belong to the network layer. These include routing protocols, multicast group management, network-layer information and error, and network-layer address assignment. It is the function of the payload that makes these belong to the network layer, not the protocol that carries them.

❖ Layer 4: Transport Layer

The transport layer provides the functional and procedural means of transferring variable-length data sequences from a source to a destination host via one or more networks, while maintaining the quality of service functions.

An example of a transport-layer protocol in the standard Internet stack is Transmission Control Protocol (TCP), usually built on top of the Internet Protocol (IP).

The transport layer controls the reliability of a given link through flow control, segmentation/de-segmentation, and error control.

This means that the transport layer can keep track of the segments and retransmit those that fail. The transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred. The transport layer creates packets out of the

message received from the application layer. Packetizing is a process of dividing the long message into smaller messages.

OSI defines five classes of connection-mode transport protocols ranging from class 0 (which is also known as TP0 and provides the fewest features) to class 4 (TP4, designed for less reliable networks, similar to the Internet). Class 0 contains no error recovery, and was designed for use on network layers that provide error-free connections. Class 4 is closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the session layer. Also, all OSI TP connection-mode protocol classes provide expedited data and preservation of record boundaries

❖ Layer 5: Session Layer:-

The session layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes check pointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session check pointing and recovery, which is not usually used in the Internet Protocol Suite. The session layer is commonly implemented explicitly in application environments that use remote procedure calls.

❖ Layer 6: Presentation Layer:-

The presentation layer establishes context between application-layer entities, in which the application-layer entities may use different syntax and semantics if the presentation service provides a mapping between them. If a mapping is available, presentation service data units are encapsulated into session protocol data units, and passed down the protocol stack.

This layer provides independence from data representation (e.g., encryption) by translating between application and network formats. The presentation layer transforms data into the form that the application

accepts. This layer formats and encrypts data to be sent across a network. It is sometimes called the syntax layer.

The original presentation structure used the Basic Encoding Rules of Abstract Syntax Notation One (ASN.1), with capabilities such as converting an EBCDIC-coded text file to an ASCII-coded file, or serialization of objects and other data structures from and to XML.

❖ Layer 7: Application Layer

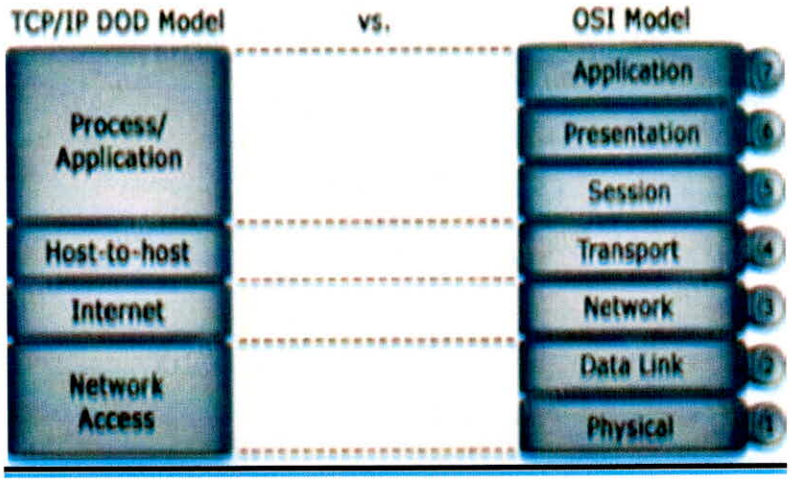
The application layer is the OSI layer closest to the end user, which means both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application-layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific.

TCP/IP and The DOD Model

The Transmission Control Protocol / Internet Protocol (TCP/IP) was created by the Department of Defence (DoD) to make sure and protect data integrity, and also maintained communications in the time of disastrous war. However, if designed and deployed properly according to standard, a TCP/IP network can be a truly reliable and flexible one.

Essentially, the Department of Defence (DOD) Model is a reduced version of the OSI Reference Model. The DOD model based on four layers:

1. Process/Application layer
2. Host-to-Host layer
3. Internet layer
4. Network Access layer



In the DOD model and OSI reference model, the two are same in theory but each has a dissimilar number of layers with different names. But, when the different protocols in the IP stack are discussed, the Internet layer and the Network layer provides the same functions, as do the Host-to-Host layer and the Transport layer.

❖ The Process/Application Layer

The Process/Application layer of the DOD model merges a huge collection of protocols to combine numerous processes focusing on both sides of the OSI's equivalent top three layers (Application, Presentation and Session). The Process/Application layer classifies protocols for node to node application communication and also controls user interface specifications.

❖ The Host-to-Host Layer

This layer works similar to the Transport layer of the OSI reference model. The host to host layer specifying protocols for setting up the level of transmission service for applications. It creates the end to end reliable communication and handles the whole process's troubles, even though, ensuring the error-free delivery of data. The host-to-host layer also tackles packet sequencing and preserves data reliability.

❖ The Internet Layer

The Internet layer communicates with the third layer of the OSI reference model, the Network layer, assigning the protocols involving in the logical transmission of packets of the whole network. The Internet layer handles the issues of the addressing of hosts by providing them an IP (Internet Protocol) address, and also responsible for the routing of packets among many networks.

❖ The Network Access Layer

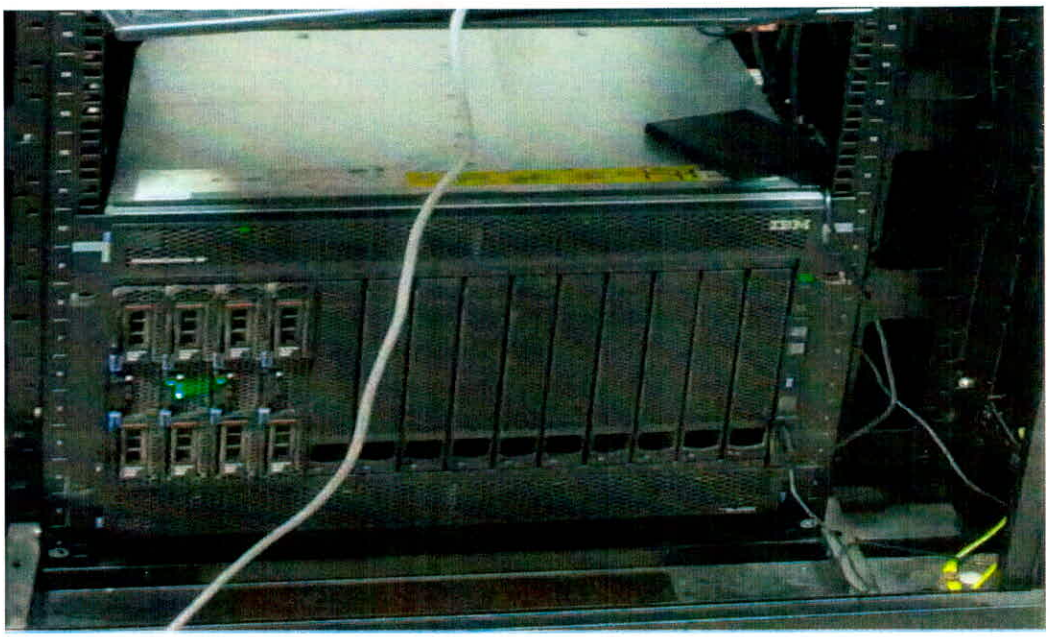
The Network Access layer is equivalent to the Data Link layer and the Physical layer of the OSI reference model. This is the last layer at the bottom of the DOD model. It supervises the data transmission between the host and the network. The Network Access layer manages the hardware addresses or MAC addressing and defines the protocols for physical media for the transmission of data.

Bellow you'll find an exemplary snapshot that will illustrate you the TCP/IP protocol suite and how TCP/IP's protocols has an interconnection with the DOD model layers. I'll talk in more detail about different protocols in my next coming articles.

Server (computing)

- In computing, a server is a computer program or a device that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model, and a single overall computation is distributed across multiple processes or devices. Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers. A client process may run on the same device or may connect over a network to a server on a different device. Typical servers are database servers, file servers, mail servers, print servers, web servers, game servers, and application servers.
- Client–server systems are today most frequently implemented by (and often identified with) the request–response model: a client sends a request to the server, which performs some action and sends a response back to the client, typically with a result or acknowledgement. Designating a computer as "server-class hardware" implies that it is specialized for running servers on it. This often implies that it is more powerful and reliable than standard personal computers, but alternatively, large computing clusters may be composed of many relatively simple, replaceable server components.

❖ Server in NIH



Networking cables

Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers to share printer, scanner etc. Different types of network cables like Coaxial cable, Optical fiber cable, Twisted Pair cables are used depending on the network's topology, protocol and size. The devices can be separated by a few meters (e.g. via Ethernet) or nearly unlimited distances (e.g. via the interconnections of the Internet).

While wireless networks are much easier deployed when total throughput is not an issue, most permanent larger computer networks use cables to transfer signals from one point to another.

❖ Twisted pair

Twisted pair cabling is a form of wiring in which pairs of wires (the forward and return conductors of a single circuit) are twisted together for the purposes of cancelling out electromagnetic interference (EMI) from other wire pairs and from external sources. This type of cable is used for home and corporate Ethernet networks.

There are two major types of twisted pair cables: shielded, unshielded.

❖ Ethernet crossover cable

An *Ethernet crossover cable* is a type of twisted pair Ethernet cable used to connect computing devices together directly that would normally be connected via a network switch, hub or router, such as directly connecting two personal computers via their network adapters. Most current Ethernet devices support Auto MDI-X, so it doesn't matter whether you use crossover or straight cables.

❖ Fiber optic cable

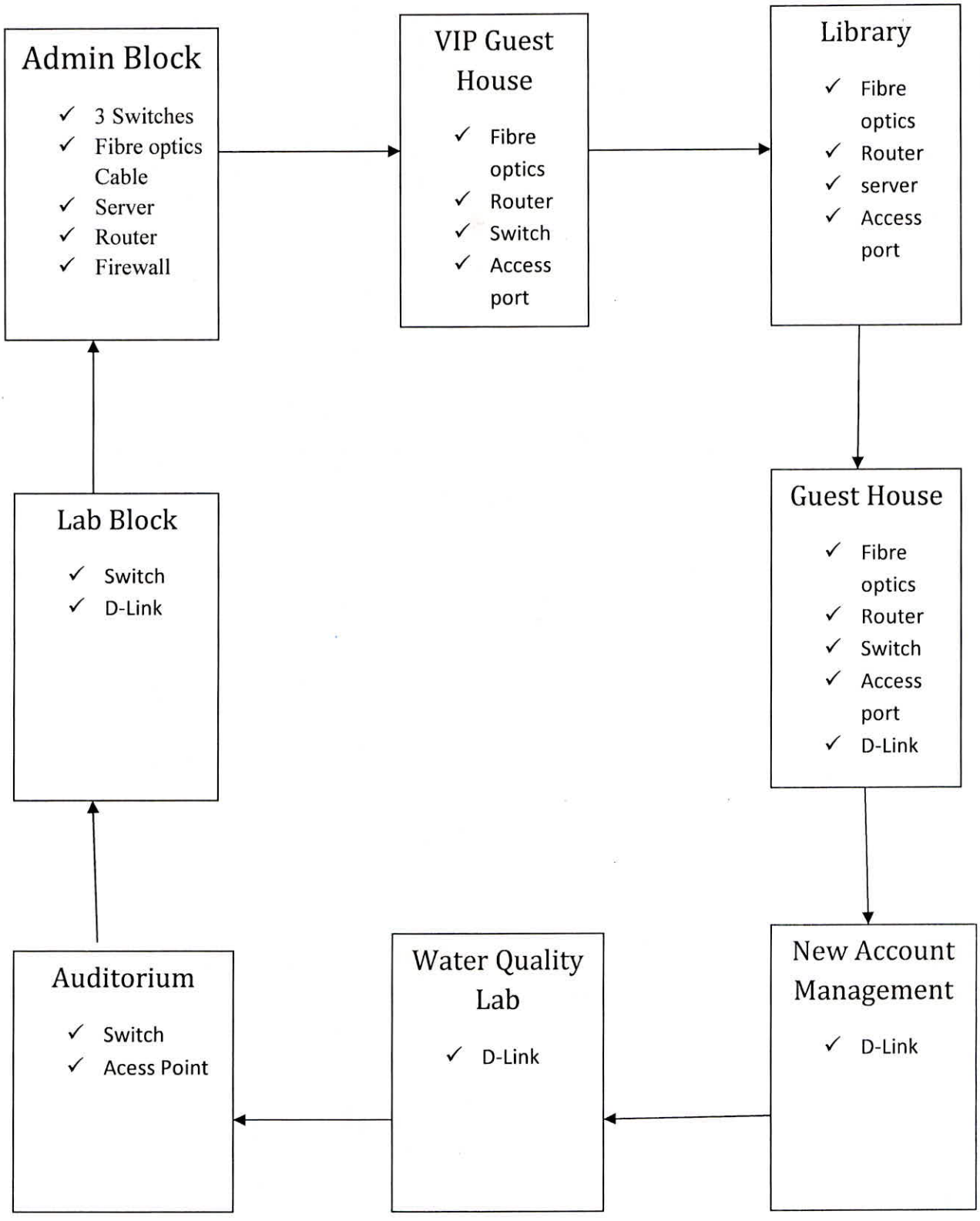
An optical fiber cable consists of a centre glass core surrounded by several layers of protective material. The outer insulating jacket is made of Teflon or PVC to prevent interference. Optical fiber deployment is more expensive than copper but offers higher bandwidth and can cover longer distances. There are two major types of optical fiber cables: short-range multi-mode fiber and long-range single-mode fiber.

❖ Coaxial cable

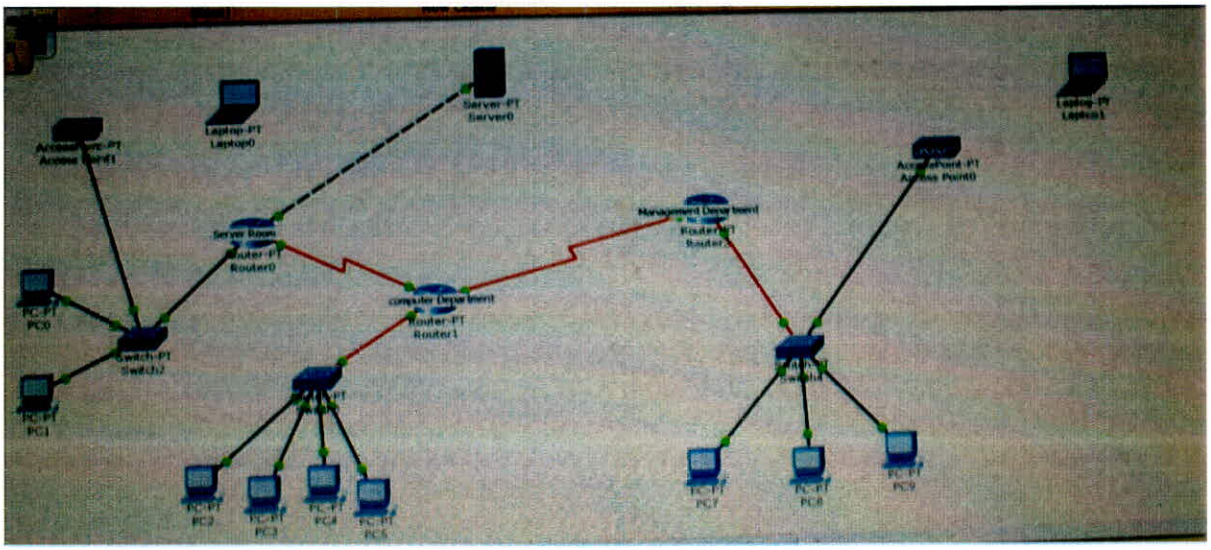
Coaxial lines confine the electromagnetic wave inside the cable, between the centre conductor and the shield. The transmission of energy in the line occurs totally through the dielectric inside the cable between the conductors. Coaxial lines can therefore be bent and twisted (subject to limits) without negative effects, and they can be strapped to conductive supports without inducing unwanted currents in them.

The most common use for coaxial cables is for television and other signals with a bandwidth of several hundred megahertz to gigahertz. Although in most homes coaxial cables have been installed for transmission of TV signals, new technologies (such as the ITU-TG.hn standard) open the possibility of using home coaxial cable for high-speed home networking applications (Ethernet over coax).

BLOCK DIAGRAM OF NIH (NATIONAL INSTITUTE OF HYDROLOGY) ROORKEE



❖ Architecture of NIH:-



Command Line Interface used in above networking Model

Configure Router R0:-

```
R0>enable
R0#configure terminal
R0(config)#interface fastethernet 0/0
R0(config-if)#ip address 10.0.0.1 255.0.0.0
R0(config-if)#no shutdown
R0(config-if)#exit
R0>enable
R0#configure terminal
R0(config)#interface serial 2/0
R0(config-if)#ip address 13.0.0.1 255.0.0.0
R0(config-if)#no shutdown
R0(config-if)#exit
```

Enable DHCP in R0:-

```
R0>enable
R0#configure terminal
R0(config)# ip dhcp pool 1
R0(dhcp-config)#network 10.0.0.0 255.0.0.0
R0(dhcp-config)#default-router 10.0.0.1
R0(dhcp-config)#exit
R0(config)#ip dhcp exclude-address 10.0.0.1 10.0.0.1
R0(config)#exit
```

Configure Router R1:-

```
R1>enable
R1#configure terminal
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 11.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1>enable
R1#configure terminal
R1(config)#interface serial 2/0
R1(config-if)#ip address 13.0.0.2 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1>enable
R1#configure terminal
R1(config)#interface serial 2/0
R1(config-if)#ip address 14.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

Enable DHCP in R1

```
R1>enable
R1#configure terminal
R1(config)# ip dhcp pool 1
```

R1(dhcp-config)#network 11.0.0.0 255.0.0.0
R1(dhcp-config)#default-router 11.0.0.1
R1(dhcp-config)#exit
R1(config)#ip dhcp exclude-address 11.0.0.1 11.0.0.1

Configure Router R2

R2>enable
R2#configure terminal
R2(config)#interface fastethernet 0/0
R2(config-if)#ip address 12.0.0.1 255.0.0.0

R2(config-if)#no shutdown
R2(config-if)#exit
R2>enable
R2#configure terminal
R2(config)#interface serial 2/0
R2(config-if)#ip address 14.0.0.2 255.0.0.0

Enable DHCP in R2

R2>enableR2#configure terminal
R2(config)# ip dhcp pool 1
R2(dhcp-config)#network 12.0.0.0 255.0.0.0
R2(dhcp-config)#default-router 12.0.0.1
R2(dhcp-config)#exit
R2(config)#ip dhcp exclude-address 12.0.0.1 12.0.0.1
R2(config)#exit

Static Routing used

On Router R0

R0> enable
R0#configure terminal
R0 (config)# ip route 14.0.0.0 255.0.0.0 13.0.0.2

R0 (config)#exit

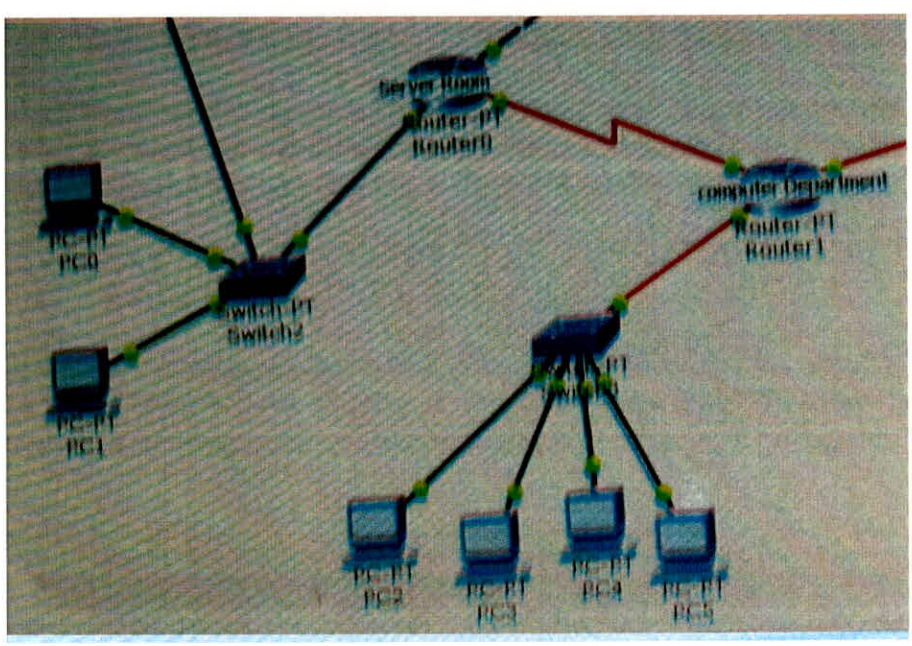
On Router R1

R1> enable
R1#configure terminal
R1 (config)# ip route 10.0.0.0 255.0.0.0 13.0.0.1
R1 (config)#exit
R1> enable
R1#configure terminal
R1(config)# ip route 12.0.0.0 255.0.0.0 14.0.0.2
R1(config)#exit

ON Router R2:-

R2> enable
R2#configure terminal
R2(config)# ip route 13.0.0.0 255.0.0.0 14.0.0.1
R2(config)#exit

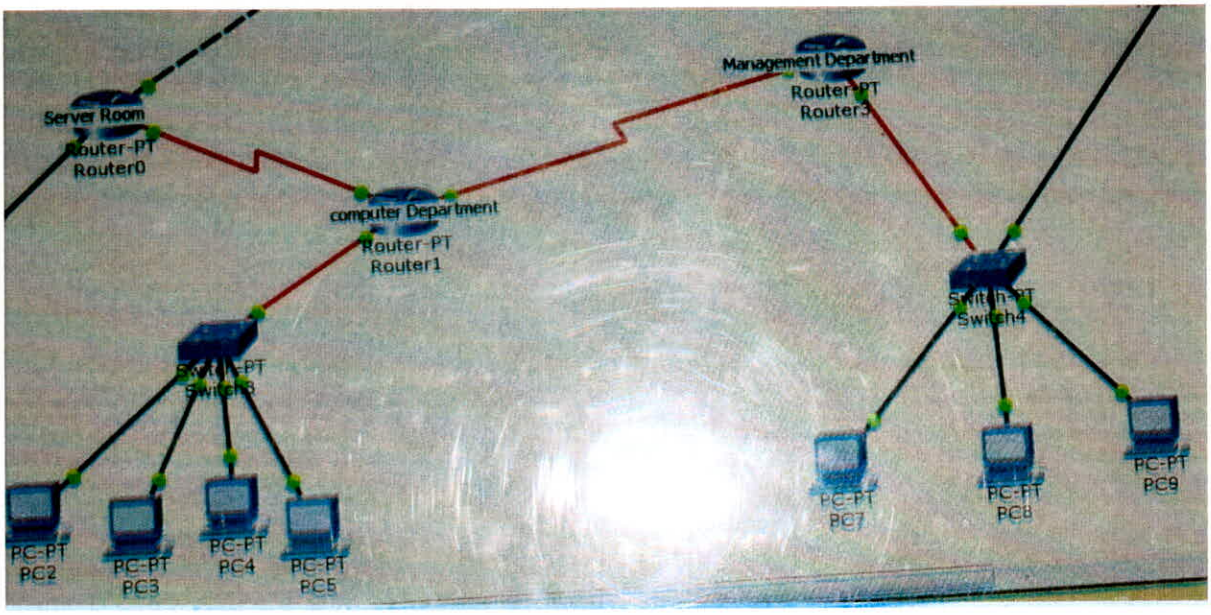
Configure standard access list on router



On Router R0 enabling ACL

R1>enable
R1>config terminal
R1(config)# access list 1 deny 192.168.2.3 0.0.0.0
R1(config)# access list 1 deny 192.168.2.4 0.0.0.0
R1(config)# access list 1 deny 192.168.2.5 0.0.0.0
R1(config)# access list 1 permit any
R1(config)#exit
R1(config)#wr

On Router 2 enabling ACL



R2>enable
R2>config terminal
R2(config)# access list 2 deny 192.168.3.3 0.0.0.0
R2(config)# access-list 2 deny 192.168.3.4 0.0.0.0
R2(config)# access-list 2 deny 192.168.3.5 0.0.0.0
R2(config)# access list 2 permit any
R2(config)#exit

Routing protocol used- RIP Routing

On Router 0

R0>enable
R0#config terminal
R0(config)#router rip
R0(config)#network 10.0.0.0
R0(config#network 13.0.0.0
R0(config)#exit

On Router 1

R1>enable
R1#config terminal
R1(config)#router rip
R1(config)#network 11.0.0.0
R1(config#network 13.0.0.0
R1(config)#exit
R1#config terminal
R1(config)#router rip
R1(config)#network 12.0.0.0
R1(config#network 14.0.0.0
R1(config)#exit

On Router 2

R2>enable
R2#config terminal
R2(config)#router rip
R2(config)#network 10.0.0.0
R2(config#network 13.0.0.0
R2(config)#exit

Configuring Vlan(Virtual Lan)

On Switch 0

Switch>enable
Switch #config terminal
Switch (config)#vlan 50
Switch (config)#name serverroom
Switch (config)#exit
Switch #config terminal
Switch (config)#interface fastethernet 0/1
Switch (config)#switchport mode access
Switch (config)#switchport access vlan 50
Switch (config)#exit

Switch #config terminal
Switch (config)#interface fastethernet 1/1
Switch(config)#switchport mode access
Switch(config)#switchport access vlan 50
Switch(config)#exit

On Switch 1

Switch>enable
Switch #config terminal
Switch (config)#vlan 60
Switch (config)#name compdept
Switch (config)#exit
Switch #config terminal
Switch (config)#interface fastethernet 0/1
Switch (config)#switchport mode access
Switch (config)#switchport access vlan 60
Switch (config)#exit

Switch #config terminal
Switch (config)#interface fastethernet 1/1
Switch (config)#switchport mode access
Switch (config)#switchport access vlan 60
Switch (config)#exit
Switch #config terminal
Switch (config)#interface fastethernet 2/1
Switch (config)#switchport mode access
Switch (config)#switchport access vlan 60
Switch (config)#exit
Switch #config terminal
Switch (config)#interface fastethernet 3/1
Switch (config)#switchport mode access
Switch (config)#switchport access vlan 60
Switch (config)#exit

On Switch 2

Switch>enable
Switch #config terminal
Switch (config)#vlan 70
Switch (config)#name mangdept
Switch (config)#exit
Switch #config terminal
Switch (config)#interface fastethernet 0/1
Switch (config)#switchport mode access
Switch (config)#switchport access vlan 70
Switch (config)#exit

Switch #config terminal
Switch (config)#interface fastethernet 1/1
Switch (config)#switchport mode access
Switch (config)#switchport access vlan 70
Switch (config)#exit

```
Switch #config terminal
Switch (config)#interface fastethernet 2/1
Switch (config)#switchport mode access
Switch (config)#switchport access vlan 70
Switch (config)#exit
Switch #config terminal
Switch (config)#interface fastethernet 3/1
Switch (config)#switchport mode access
Switch (config)#switchport access vlan 70
Switch (config)#exit
```

Configuring password in Router R0

```
R0>enable
R0#config terminal
R0(config)# line console 0
R0(config)#password cisco
R0(config)#login
R0(config)#exit

R0(config)#line vty 0 4
R0(config)#password cisco
R0(config)#login
R0(config)#exit

R0(config)#enable secret serverroom
R0(config)#exit
```

Configuring password in Router R1

```
R1>enable
R1#config terminal
```

R1(config)# line console 0
R1(config)#password cisco
R1(config)#login
R1(config)#exit

R1(config)#line vty 0 4
R1(config)#password cisco
R1(config)#login
R1(config)#exit

R1(config)#enable secret compdept
R1(config)#exit

Configuring password in Router R2

R2>enable
R2#config terminal
R2(config)# line console 0
R2(config)#password cisco
R2(config)#login
R2(config)#exit

R2(config)#line vty 0 4
R2(config)#password cisco
R2(config)#login
R2(config)#exit

R2(config)#enable secret mangdept
R2(config)#exit

Configuring password in Switch 0

Switch>enable
Switch#config terminal

Switch(config)#hostname serverroom
serverroom (config)# line console 0
serverroom (config)#password cisco
serverroom (config)#login
serverroom (config)#exit

serverroom (config)#line vty 0 4
serverroom (config)#password cisco
serverroom (config)#login
serverroom (config)#exit

serverroom (config)#enable secret serverroom
serverroom (config)#exit

Configuring password in Switch 1

Switch>enable
Switch#config terminal
Switch(config)#hostname compdept
compdept (config)# line console 0
compdept (config)#password cisco
compdept (config)#login
compdept (config)#exit

compdept (config)#line vty 0 4
compdept (config)#password cisco
compdept (config)#login
compdept (config)#exit

compdept (config)#enable secret compdept
compdept (config)#exit

Configuring password in Switch 0

Switch>enable
Switch#config terminal
Switch(config)#hostname serverroom

serverroom (config)# line console 0
serverroom (config)#password cisco
serverroom (config)#login
serverroom (config)#exit

serverroom (config)#line vty 0 4
serverroom (config)#password cisco
serverroom (config)#login
serverroom (config)#exit

serverroom (config)#enable secret serverroom
serverroom (config)#exit

Configuring password in Switch 2

Switch>enable
Switch#config terminal
Switch(config)#hostname mangdept
mangdept (config)# line console 0
mangdept (config)#password cisco
mangdept (config)#login
mangdept (config)#exit

mangdept (config)#line vty 0 4
mangdept (config)#password cisco
mangdept (config)#login
mangdept (config)#exit
mangdept (config)#enable secret compdept
mangdept (config)#exit

CONCLUSIONS

In the present study, the architecture of NIH networking system has been discussed. The networking systems are managed in the Institute by the Computer Centre. . The Centre is equipped with Servers, routers such as R2, R3. Networking has been done in such a manner that only one terminal from each department is used and rest are blocked from accessing server room computers. Here each switch and router is enabled and protected by passwords. The computers are assigned automatic IP addresses by using DHCP command. The Routers interacts with each other with the help of RIP (Routing Information Protocol). However, since the study was of short span and restrictions in data sharing due to security reasons, there were certain limitations as discussed below:-

LIMITATIONS:-

- Since the study was short in span, hence resources are not used at real time and work was done in software, forming a similar network as that of the NIH Institute Roorkee.
- Lack of real time devices in our simulated model will somehow differ with the real networking with minor difference.

REFERENCES

1. CCNA Book - Todd Lammle (6th Edition)
2. Routing-Protocols-and-Concepts-CCNA- Exploration-Labs-and-Study-Guide.
3. www.w3schools.com
4. https://m.youtube.com>Networkinginc
5. https://en.m.wikipedia.org/wiki/computer_network
6. www.cisco.com
7. www.webopidia.com

GLOSSARY

- Access Layer:- One of the layers in Cisco's three-Layers hierarchical model. The access layer provides user with access to the interwork.
- Access List:- A set of test conditions kept by routers that determines "interesting traffic" to and from the router for various services on the network.
- Acknowledgement:- Verification sent from one network device to another signifying that event has occurred.
- Bit:- one binary digit; either 0 or 1. Eight bits make one byte.
- Bootstrap protocol:- A protocol used to dynamically assign ip address and gateway to requesting clients.
- Bridge:-A device used to connect two segments of network and translating packets between them.
- Buffer:- A storage area dedicated to handling data while in transit. Buffers are used to store deliveries of data bursts, usually receives from faster devices.
- CLI:- Command line interface. Allows you to configure Cisco routers and switches with maximum Flexibility.
- Datagram:-A logical collection of information transmitted as a network layer unit over a medium without a previously established virtual circuit.
- Excess burst size:- The amount of traffic by which the user may exceed the committed burst size.
- Firewall:- A barrier created between a connected public networks and a private network that uses access security and other methods for security of private networks.
- RIP Routing Information Protocol:- The most commonly used protocol in the internet.

- Subnet mask:-a 32 bit address mask used in IP to identify the bits of an IP address that are used for the subnet address.
- TCP Transmission Control Protocol:- a connection oriented protocol that is defined at the transport layer of OSI Model. Provides reliable delivery of data.
- VTP Vlan Truncking Protocol:- used to update switches in switch fabric about vlan configured in VTP server.VTP devices can be VTP server, clients, or transport devices.
- Wildcard: - used with the access lists and OSPF configuration. They are designations used to identify a range of subnets.