***INDUSTRIAL TRAINING REPORT***

***Computer Networking***

*Submitted in partial fulfilment of the requirements*

*for the award of the degree of*

**Bachelor of Technology**

**Computer Science and Engineering**

Guide: Submitted by:

Rajesh Chaudhary Ojassvi Pradhan

04113302716



**HMR INSTITUTE OF TECHNOLOGY & MANGEMENT**

**HAMIDPUR, DELHI 110 036**

**Affiliated to**

**GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY**

**Sector - 16C Dwarka, Delhi - 110075, India**

**2016-2020**



**DECLARATION**

I, student of B.Tech (CSE 7th semester) hereby declare that the summer training entitled “COMPUTER NETWORKING” which is submitted to Department of CSE, HMR Institute of Technology & Management, Hamidpur Delhi, affiliated to Guru Gobind Singh Indraprastha University, Dwarka (New Delhi) in partial fulfillment of requirement for the award of the degree of Bachelor of Technology in CSE, has not been previously formed the basis for the award of any degree, diploma or other similar title or recognition.

Date: Name of Student: Ojassvi Pradhan

Enrollment No.: 04113302716

**ACKNOWLEDGEMENT**

I would like to take this opportunity to thank and acknowledge several individuals without whom this project could not have been carried through. **I am thankful to the management of National Thermal Power Corporation (NTPC) for giving me this wonderful opportunity of working with them for these 6 weeks. It has been the most enriching experience.** I would also like to express my sincere gratitude to all my guides and mentors who made it possible for me to complete this submission. I would like to thanks Shri Rajni Kanth, AGM IT Communication and my guide Shri Rajesh Choudhary, Manager (IT) Communication, without whose guidance this submission would not have been possible.

I would also like to acknowledge the teachers, staff and my fellow friends of HMRITM who encouraged me during the course of the project and helped me make it a success.

Lastly, I take this opportunity to thank my co-trainees who have been kind supports throughout.

(OJASSVI PRADHAN)

**ojassvi.pradhan@gmail.com**

**ABSTRACT**

The primary purpose of a computer network is to share resources. A computer network is referred to as client/server if (at least) one of the computers is used to "serve" other computers referred to as "clients". Besides the computers, other types of devices can be part of the network. In the early days of networking, there will be once central server that contains the data and all the clients can access this data through a Network Interface Card. Later on Client server architecture came into existence, where still burden is there on the server machine. To avoid the disadvantages in distributed computing was introduced which reduces the burden on the server by providing work sharing capabilities1 . This paper describes how the concept of distributed computing came into existence based on the advantages and disadvantages that raised in earlier networking concepts. The concept of distributed computing speaks that once data is available within the server(s), it should be able to be accessed and processed from any kind of client device like computer, mobile phone, PDA, etc.

**CONTENTS**

**COMMUNICATION**

* **ARCHITECTURE ……………………………………...……………………. I**
* **HISTORY ………………………………………………...…………………… ii**
* **COMMUNICATION MEDIA ……………………………………………….. iii**
* **COMMUNICATION PROTOCOLS ...………………...…………………… iv**
* **NEED OF COMMUNICATION IN NETWORKING……………………….. v**

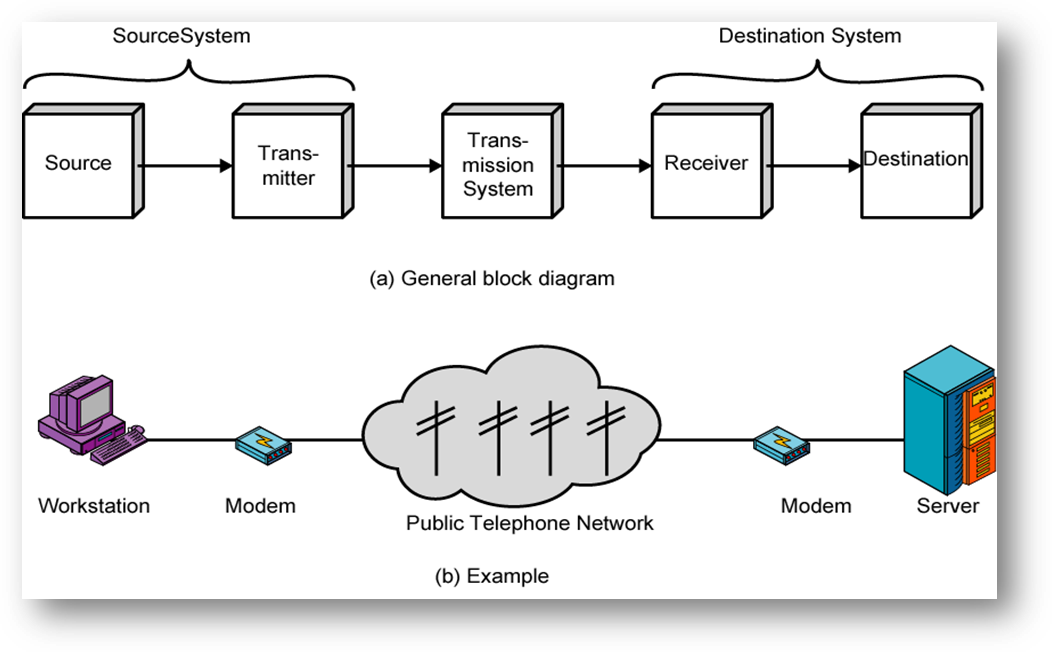
**NETWOKING**

* **BRIEF INTRODUCTION …...……………………………………………… vi**
* **TYPES OF NETWORK ……………………………………………………… vii**
* **NETWORK DEVICES ….………………………………………………….. viii**
* **NETWORK TOPOLOGIES ………………………………………………….. ix**
* **OSI MODEL …………………………………………………………………… x**
* **TCP/IP REFRENCE MODEL ….…..……………………………………… xi**
* **IP ADDRESS ……………………………………………………………… xii**
* **SUBNETTING ……………………………………………………………… xiii**
* **VLSM ………………………………………………………………………... xiv**

**FIREWALL & CISCO DEVICES**

**COMMUNICATION**

* **ARCHITECTURE**



* **History**

Before the advent of computer networks that were based upon some type of telecommunications system, communication between calculation machines and early computers was performed by human users by carrying instructions between them. Many of the social behaviors seen in today's Internet were demonstrably present in the nineteenth century and arguably in even earlier networks using visual signals.

In September 1940 George Stibitz used a Teletype machine to send instructions for a problem set from his Model at Dartmouth College to his Complex Number Calculator in New York and received results back by the same means. Linking output systems like teletypewriters to computers was an interest at the Advanced Research Projects Agency (ARPA) when, in 1962, J.C.R. Licklider was hired and developed a working group he called the "Intergalactic Network", a precursor to the ARPANET.

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

The commercial airline reservation system Semi-Automatic Business Research Environment (SABRE) which went online with two connected mainframes in 1960.

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 Kleinrock, Paul Baran and Donald Davies independently conceptualized and developed network systems which used packets that could be used in a network between computer systems.

* **Communication media**

Computer networks can be classified according to the hardware and associated software technology that is used to interconnect the individual devices in the network, such as electrical cable (HomePNA, power line communication, (G.hn), optical fiber, and radio waves (wireless LAN). In the OSI model, these are located at levels 1 and 2.

A well-known *family* of communication media is collectively known as Ethernet. It is defined by IEEE 802 and utilizes various standards and media that enable communication between devices. Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium.

**Wired technologies**

Twisted pair ***wire*** is the most widely used medium for 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 networking 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.

* Coaxial cableis widely used for cable television systems, office buildings, and other work-sites for local area networks. The cables consist of copper or aluminum wire wrapped with insulating layer typically of a flexible material with a high dielectric constant, all of which are surrounded by a conductive layer.
* Optical fiber ***cable*** consists of one or more filaments of glass fiber wrapped in protective layers that carries data by means of pulses of light. It transmits light which can travel over extended distances. Fiber-optic cables are not affected by electromagnetic radiation.

**Wireless technologies**

* ***Terrestrial*** microwave– Terrestrial microwaves use Earth-based transmitter and receiver. The equipment looks similar to satellite dishes. Terrestrial microwaves use low-gigahertz range, which limits all communications to line-of-sight. Path between relay stations spaced approx, 48 km (30 miles) apart. Microwave antennas are usually placed on top of buildings, towers, hills, and mountain peaks.

* ***Communications*** satellites– The satellites use microwave radio as their telecommunications medium which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically 35,400 km (22,200 miles) (for geosynchronous satellites) above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.
* ***Cellular and PCS systems*** – Use several radio communications technologies. The systems are divided to different geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.
* ***Wireless LANs*** – Wireless local area network 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. An example of open-standards wireless radio-wave technology is IEEE 802.11.
* Infrared communicationcan transmit signals between devices within small distances of typically no more than 10 meters. In most cases, line-of-sight propagation is used, which limits the physical positioning of communicating devices.

**Exotic technologies**

There have been various attempts at transporting data over more or less 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.

A practical limit in both cases is the round-trip delay time which constrains useful communication.

* **COMMUNICATION PROTOCOLS**

A communications protocol defines the formats and rules for exchanging information via a network and typically comprises a complete protocol suite which describes the protocols used at various usage levels. An interesting feature of communications protocols is that they may be - and in fact very often are - stacked above each other, which means that one is used to carry the other. *The* example for this is HTTP running over TCP over IP over IEEE 802.11, where the second and third are members of the Internet Protocol Suite, while the last is a member of the Ethernet protocol suite. This is the stacking which exists between the wireless router and the home user's personal computer when surfing the World Wide Web.

### **Ethernet**

Ethernet is a family of connectionless protocols used in LANs, described by a set of standards together called IEEE 802 published by the Institute of Electrical and Electronics Engineers. It has a flat addressing scheme and is mostly situated at levels 1 and 2 of the OSI model. For home users today, the most well-known member of this protocol family is IEEE 802.11, otherwise known as Wireless LAN(WLAN).

### **Internet Protocol Suite**

The Internet Protocol Suite is used not only in the eponymous Internet, but today nearly ubiquitously in any computer network. While at the Internet Protocol (IP) level it operates connectionless, it also offers a connection-oriented service layered on top of IP, the Transmission Control Protocol (TCP). Together, TCP/IP offers a semi-hierarchical addressing scheme (IP address plus port number).

### **SONET/SDH**

Synchronous Optical NET working (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers.

### **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.

* **Need of communication in networking**

Today computer is available in many offices and homes and therefore there is a need to share data and programs among various computers with the advancement of data communication facilities. The communication between computers has increased and it thus it has extended the power of computer beyond the computer room.

**NETWORKING**

* **INTRODUCTION**

In the world of computers, **networking** is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.



* **TYPES OF NETWORK**

**LAN - Local Area Network**

LAN connects networking devices with in short spam of area, i.e. small offices, home, internet cafes etc. LAN uses TCP/IP network protocol for communication between computers. It is often but not always implemented as a single IP subnet. Since LAN is operated in short area so It can be control and administrate by single person or organization.

**WAN - Wide Area Network**

As “word” Wide implies, WAN, wide area network cover large distance for communication between computers. The Internet it self is the biggest example of Wide area network, WAN, which is covering the entire earth. WAN is distributed collection of geographically LANs.

**Wireless - Local Area Network**

A LAN, local area network based on wireless network technology mostly referred as Wi-Fi. Unlike LAN, in   WLAN no wires are used, but radio signals are the medium for communication.

**MAN - Metropolitan Area Network**

This kind of network is not mostly used but it has its own importance for some government bodies and organizations on larger scale. MAN, metropolitan area network falls in middle of LAN and WAN, It covers large span of physical area than LAN but smaller than WAN, such as a city.

**CAN - Campus Area Network**

Networking spanning with multiple LANs but smaller than a Metropolitan area network, MAN. This kind of network mostly used in relatively large universities or local business offices and buildings.

**SAN - Storage Area Network**

SAN technology is used for data storage and it has no use for most of the organization but data oriented organizations. Storage area network connects servers to data storage devices by using Fiber channel technology.

**SAN - System Area Network**

* **NETWORK DEVICES**

**ROUTER**

A **router** is a device that forwards data packets between telecommunications networks, creating an overlay internet work. A router is connected to two or more data lines from different networks. When data comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination.

**APPLICATION**

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.

The subnets 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 records a routing table listing what route should be used to forward a data packet, and through which physical interface connection. It does this using internal pre-configured addresses, called static routes
* Forwarding plane**:** The router forwards data packets between incoming and outgoing interface connections. It routes it 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, and between internet service providers (ISPs) networks. The largest routers (such as the Cisco CRS-1or Juniper T1600) .

**ETHERNET HUB**

An **Ethernet hub**, **active hub**, **network hub**, **repeater hub** or **hub** is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

**APPLICATIONS**

Historically, the main reason for purchasing hubs rather than switches was their price. This motivator has largely been eliminated by reductions in the price of switches, but hubs can still be useful in special circumstances:

* For inserting a protocol analyzer into a network connection, a hub is an alternative to a network tap or port mirroring.
* When a switch is accessible for end users to make connections, for example, in a conference room, an inexperienced or careless user (or saboteur) can bring down the network by connecting two ports together, causing a loop.

* A hub with a 10BASE2 port can be used to connect devices that only support 10BASE2 to a modern network.

**NETWORK SWITCH**

A **network switch** or **switching hub** is a computer networking device that connects network segments.

The term commonly refers to a multi-port network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (Layer 3) and above are often referred to as Layer 3 switches or multilayer switches.

The first Ethernet switch was introduced by Kalpana in 1990

**APPLICATION**

Switches may operate at one or more layers of the OSI model, including data link, network, or transport (i.e., end-to-end). 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, ATM, ITU-T G.hn and 802.11. This connectivity can be at any of the layers mentioned. While Layer 2 functionality is adequate for bandwidth-shifting within one technology, interconnecting technologies such as Ethernet and token ring are easier at Layer 3.

**NETWORK BRIDGE**

**Bridging** is a forwarding technique used in packet-switched computer networks. Unlike routing, bridging makes no assumptions about where in a network a particular address is located. Instead, it depends on flooding and examination of source addresses in received packet headers to locate unknown devices. Once a device has been located, its location is recorded in a table where the MAC address is stored so as to preclude the need for further broadcasting. The utility of bridging is limited by its dependence on flooding, and is thus only used in local area networks.

**REPEATER**

A **repeater** is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances.

The term "repeater" originated with telegraphy and referred to an electromechanical device used by the army to regenerate telegraph signals. Use of the term has continued in telephony and data communications.

In telecommunication, the term **repeater** has the following standardized meanings:

1. An analog device that amplifies an input signal regardless of its nature (analog or digital).
2. A digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission..

**NETWORK TOPOLOGIES**

**Network topology** is the layout pattern of interconnections of the various elements (links, nodes, etc.) of a computer or biological network. Network topologies may be physical or logical. Physical topology refers to the physical design of a network including the devices, location and cable installation. Logical topology refers to how data is actually transferred in a network as opposed to its physical design. In general, physical topology relates to a core network whereas logical topology relates to basic network.

Topology can be understood as the shape or structure of a network. This shape does not necessarily correspond to the actual physical design of the devices on the computer network. The computers on a home network can be arranged in a circle but it does not necessarily mean that it represents a ring topology.

There are two basic categories of network topologies:

* Physical topologies
* Logical topologies

The logical topology, in contrast, is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices. A network's logical topology is not necessarily the same as its physical topology. For example, the original twisted pair Ethernet using repeater hubs was a logical bus topology with a physical star topology layout. Token Ring is a logical ring topology, but is wired a physical star from the Media Access Unit.

The study of network topology recognizes seven basic topologies:

* Point-to-point
* Bus
* Star
* Ring
* Mesh
* Tree
* Hybrid
* Daisy chain

### **Point-to-point**

The simplest topology is a permanent link between two endpoints. Switched point-to-point topologies are the basic model of conventional telephony. The value of a permanent point-to-point network is unimpeded communications between the two endpoints. The value of an on-demand on is proportional to the number of potential pairs of subscribers, and has been expressed as Metcalfe's Law.

**Switched:**

Using circuit-switching or packet-switching technologies, a point-to-point circuit can be set up dynamically, and dropped when no longer needed. This is the basic mode of conventional telephony.

**BUS:**

In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient.

**Linear bus**

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk.

**Distributed bus**

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium.

**STAR**

In local area networks with a star topology, each network host is connected to a central hub with a point-to-point connection. All traffic that traverses the network passes through the central hub. The hub acts as a signal repeater. The star topology is considered the easiest topology to design and A point-to-point link (described above) is sometimes categorized as a special instance of the physical star topology – therefore, the simplest type of network that is based upon the physical star topology would consist of one node with a single point-to-point link to a second node, the choice of which node is the 'hub' and which node is the 'spoke' being arbitrary.

A type of network topology in which a network that is based upon the physical star topology has one or more repeaters between the central node (the 'hub' of the star) and the peripheral or 'spoke' nodes, the repeater.

**Distributed Star**

A type of network topology that is composed of individual networks that are based upon the physical star topology connected together in a linear fashion – i.e., 'daisy-chained' – with no central or top level connection point (e.g., two or more 'stacked' hubs, along with their associated star connected nodes or 'spokes').

**RING**

A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the right acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring. The network is dependent on the ability of the signal to travel around the ring.

**MESH**

The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

**TREE**

The type of network topology in which a central 'root' node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy (i.e., the second level) with a point-to-point link between each of the second level nodes and the top level central 'root' node.

1. A network that is based upon the physical hierarchical topology and with a branching factor of 1 would be classified as a physical linear topology.
2. are lower in the hierarchy. Such a type of network topology is very useful and highly recommended.

**HYBRID**

Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). For example, a tree network connected to a tree network is still a tree network topology. A hybrid topology is always produced when two different basic network topologies are connected. Two common examples for Hybrid network are: *star ring network* and *star bus network*

* A Star ring network consists of two or more star topologies connected using a multistation access unit (MAU) as a centralized hub.
* A Star Bus network consists of two or more star topologies connected using a bus trunk (the bus

trunk serves as the network's backbone).

* **OSI REFRENCE MODEL**

The **Open Systems Interconnection model** (**OSI model**) was a product of the Open Systems Interconnection effort at the International Organization for Standardization. It is a way of sub-dividing a communications system into smaller parts called layers. Similar communication functions are grouped into logical layers. A layer provides services to its upper layer while receiving services from the layer below. On each layer, an instance provides service to the instances at the layer above and requests service from the layer below.

**HISTORY**

Work on a layered model of network architecture was started and the International Organization for Standardization (ISO) began to develop its OSI framework architecture. OSI had two major components: an *abstract model* of networking, called the Basic Reference Model or seven-layer model, and a set of specific protocols.

### **Layer 1: Physical Layer**

The Physical Layer defines electrical and physical specifications for devices. In particular, it defines the relationship between a device and a transmission, such as a copper or optical cable. This includes the layout of pins, voltages, cable specifications, hubs, repeaters, network, host bus adapters (HBA used in storage area networks) and more.

### **Layer 2: Data Link Layer**

The Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer. Originally, this layer was intended for point-to-point and point-to-multipoint media, characteristic of wide area media in the telephone system.

#### ***WAN Protocol architecture***

Connection-oriented WAN data link protocols, in addition to framing, detect and may correct errors. They are also capable of controlling the rate of transmission. A WAN Data Link Layer might implement a sliding window flow control and acknowledgment mechanism to provide reliable delivery of frames; that is the case for SDLC and HDLC, and derivatives of HDLC such as LAPB and LAPD.

#### ***IEEE 802 LAN architecture***

Practical, connectionless LANs began with the pre-IEEE Ethernet specification, which is the ancestor of IEEE 802.3. This layer manages the interaction of devices wit

### **Layer 3: Network Layer**

The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network, while maintaining the quality of service requested by the Transport Layer.

### **Layer 4: Transport Layer**

The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The Transport Layer controls the reliability of a given link through flow control. segmentation/desegmentation, and error control. Some protocols are state- and connection-oriented. 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.

### **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 checkpointing, adjournment, termination, and restart procedures.

### **Layer 6: Presentation Layer**

The Presentation Layer establishes context between Application Layer entities, in which the higher-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 stack.

### **Layer 7: Application Layer**

The Application Layer is the OSI layer closest to the end user, which means that 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 layer.

**TCP/IP REFRENCE MODEL**

**TCP/IP LAYERS**

The layers near the top are logically closer to the user application, while those near the bottom are logically closer to the physical transmission of the data. Viewing layers as providing or consuming a service is a method of abstraction to isolate upper layer protocols from the nitty-gritty detail of transmitting bits over, for example, Ethernet and collision detection, while the lower layers avoid having to know the details of each and every application and its protocol.

1. For multiaccess links with their own addressing systems (e.g. Ethernet) an address mapping protocol is needed. Such protocols can be considered to be below IP but above the existing link system. While the IETF does not use the terminology, this is a subnetwork dependent convergence facility according to an extension to the OSI model, the Internal Organization of the Network Layer (IONL).
2. ICMP & IGMP operate on top of IP but do not transport data like UDP or TCP. Again, this functionality exists as layer management extensions to the OSI model, in its *Management Framework*(OSIRM MF)

*The following is a description of each layer in the TCP/IP networking model starting from the lowest level.*

### **Link Layer**

The Link Layer (or Network Access Layer) is the networking scope of the local network connection to which a host is attached. This regime is called the *link* in Internet literature. This is the lowest component layer of the Internet protocols, as TCP/IP is designed to be hardware independent. As a result TCP/IP is able to be implemented on top of virtually any hardware networking technology.

The Link Layer is used to move packets between the Internet Layer interfaces of two different hosts on the same link.

### **Internet Layer**

The Internet Layer solves the problem of sending packets across one or more networks. Internetworking requires sending data from the source network to the destination network. This process is called routing.

In the Internet Protocol Suite, the Internet Protocol performs two basic functions:

* *Host addressing and identification*: This is accomplished with a hierarchical addressing system (see IP address).
* *Packet routing*: This is the basic task of getting packets of data (datagrams) from source to destination by sending them to the next network node (router) closer to the final destination.

### **Transport Layer**

The Transport Layer's responsibilities include end-to-end message transfer capabilities independent of the underlying network, along with error control, segmentation, flow control, congestion control, and application addressing (port numbers). End to end message transmission or connecting applications at the transport layer can be categorized as either connection-oriented, implemented in Transmission Control Protocol (TCP), or connectionless, implemented in User Datagram Protocol (UDP).

* data arrives in-order
* data has minimal error (i.e. correctness)
* duplicate data is discarded
* lost/discarded packets are resent
* includes traffic congestion control

TCP and UDP are used to carry an assortment of higher-level applications. The appropriate transport protocol is chosen based on the higher-layer protocol application

The applications at any given network address are distinguished by their TCP or UDP port. By convention certain *well known ports* are associated with specific applications. (*See*List of TCP and UDP port numbers*.*)

### **Application Layer**

The Application Layer refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP).

switches do not typically "look inside" the encapsulated traffic to see what kind of application protocol it represents, rather they just provide a conduit for it.

**DIFFERENCE BETWEEN OSI AND TCP/IP MODEL**

The three top layers in the OSI model—the Application Layer, the Presentation Layer and the Session Layer—are not distinguished separately in the TCP/IP model where it is just the Application Layer. While some pure OSI protocol applications, such as X.400, also combined them, there is no *requirement* that a TCP/IP protocol stack needs to impose monolithic architecture above the Transport Layer. For example, the Network File System (NFS) application protocol runs over the eXternal Data Representation (XDR) presentation protocol, which, in turn, runs over a protocol with Session Layer functionality, Remote Procedure Call (RPC). RPC provides reliable record transmission, so it can run safely over the best-effort User Datagram Protocol (UDP) transport.

for the network layer. In like manner, the IONL provides a structure for "subnetwork dependent convergence facilities" such as ARP and RARP.

* **IP ADDRESS**

An IP Address is a 32 bit unique number used to identify a host on a TCP/IP network. IP address is represented as 4 octets, each consisting of 8 bits. each octate is converted to a decimal format and a period(.) separates the decimal no. to make them readable for humans.

From bits:00000000=0

11111111=255

So, the decimal in IP ranges in 0 to 255.

IP address are expressed in dotted-decimal format, with four numbers separated by periods, such as 192.168.1.9(IP address).

An IP address has following 2 parts:

1: 1st part of an IP address is used as a network address.

2: 2nd part of an IP address is used as a host address.

An IP address is a 32 bit add, has 4 octates division.

8bit.8bit.8bit.8bit

Sub divided into classes: A, B, C, D, E (class D and class E are in higher observation under laboratory)

**SUBNET MASK:**

Class A:255.0.0.0

Class B:255.255.0.0

Class C:255.255.255.0

If we convert these no. into binary formats they will be:

11111111.00000000.00000000.00000000 (contains max. host bits)

11111111.11111111.00000000.00000000

The Internet Routing Scheme was first developed in 1970’s.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CLASS | 1st bits | Network bits | Host bits | Initial bytes | No. of host per network | No. of network |
| CLASS A | 0 | 7 | 24 | 0-126 | 16,777,214 | 126 |
| CLASS B | 10 | 14 | 16 | 128-191 | 65,532 | 16,384 |
| CLASS C | 110 | 21 | 8 | 192-223 | 254 | 2,092,152 |
| CLASS D | 1110 | 28 multicast add. Bit |  | 224-247 |  |  |
| CLASS E | 1111 | 28 reserved add. Bit |  | 248-256 |  |  |

The 0.0.0.0 isn’t permitted as network or host address.

127.0.0.0 network is reserved for testing.

255 is also not permitted as the network or host address. For finding Subnet mask we have a formula 2n-2.

IP versions: IPv3, IPv4, IPv5, IPv6.

|  |  |  |
| --- | --- | --- |
| (Different in points) | (IPv4) | (IPv6) |
| Address in bits | 32 | 128 |
| Address representation | Binary no. | Hexadecimal no. |
| Separator | (.) | (:) |
| Example | 192.168.1.1 | 1080:0:0:8:800:200C:417A |

Different classes have their starting and ending bits.

|  |  |  |
| --- | --- | --- |
| CLASS | STARTING BITS | ENDING BITS |
| A | 1.0.0.0 | 126.255.255.255 |
| B | 128.0.0.1 | 191.255.255.255 |
| C | 192.0.0.1 | 223.255.255.255 |
| D | 224.0.0.1 | 239.255.255.255 |
| E | 240.0.0.1 | 247.255.255.255 |

CLASS A

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | 0 | N | | 8 | 8 | 8 |

0 is reserved bit. N is from 1-126.

No. of network bits=8

No. of network bits=28-`1=27=128 networks

* + 1. not valid

127.0.0.0 for testing.

So, for Class A there are 126 networks

CLASS B

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | 10 | N | |  |  |  |

N is from 128-191.

Similarly, No. of bits=16

No. of bits=216-2=214=16,384

And these steps are similar for CLASS C and so on.

255 bits is reserved for broadcasting

**SUBNETTING**

The process of breaking down a single network address into(our)separate network addresses is called subnetting. We increase network bits and dec. the host bits.

Subnets-The resulting individual network segment are called subnets.

SUBNET MASK

Subnet mask is a value which tells us about network bits and host bits in an IP If the value of bits are equal to 1 then it is a network octed and if it is equal to 0,then it will be a host octed .In subnetting we break down the network address into multiple subnet addresse s.Here the IP is divided and can according our need.

USES: 1.Division of network

2.Security

3.Reduces the wastage of IP addresses.

CLASSES AND SUBNET MASKS:

CLASS A 255.0.0.0

CLASS B 255.255.0.0

CLASS C 255.255.255.0

The smaller groups are known as subnets.

|  |
| --- |
| **Variable Length Subnet Mask (VLSM)** Variable Length Subnet Masking - VLSM - is a technique that allows network administrators to divide an IP address space into subnets of different sizes, unlike simple same-size Subnetting.  Variable Length Subnet Mask (VLSM) in a way, means subnetting a subnet. To simplify further, VLSM is the breaking down of IP addresses into subnets (multiple levels) and allocating it according to the individual need on a network. It can also be called a classless IP addressing. A classful addressing follows the general rule that has been proven to amount to IP address wastage. |

Reduction in the overall network traffic which increases the network performance.

Easy to manage and troubleshoot small network.

Increased control an address space in a network.

Looking at the diagram, we have three LANs connected to each other with two WAN links.

The first thing to look out for is the number of subnets and number of hosts. In this case, an ISP allocated 192.168.1.0/24. Class C

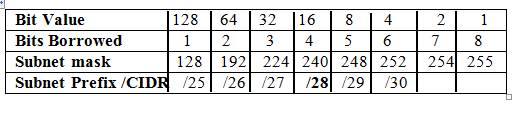
HQ = 50 host

RO1 = 30 hosts

RO2 = 10 hosts

2 WAN links

We will try and subnet 192.168.1.0 /24 to sooth this network which allows a total number of 254 hosts I recommend you get familiar with this table below. I never leave home without it!



**WAN Link 2**= 112+4=116

WAN Link from HQ to RO2 Network address = 192.168.1.116 /30

HQ = 192.168.1.117   subnet mask 255.255.255.252

RO2 = 192.168.1.118 Subnet mask 255.255.255.252

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Prefix / CIDR | Subnet mask | Usable IP address/hosts | Usable IP addresses + Network and Broadcast address |
| /26 | 255.255.255.192 | 62 | 64 |
| /27 | 255.255.255.224 | 30 | 32 |
| /28 | 255.255.255.240 | 14 | 16 |
| /29 | 255.255.255.248 | 6 | 8 |
| /30 | 255.255.255.252 | 2 | 4 |

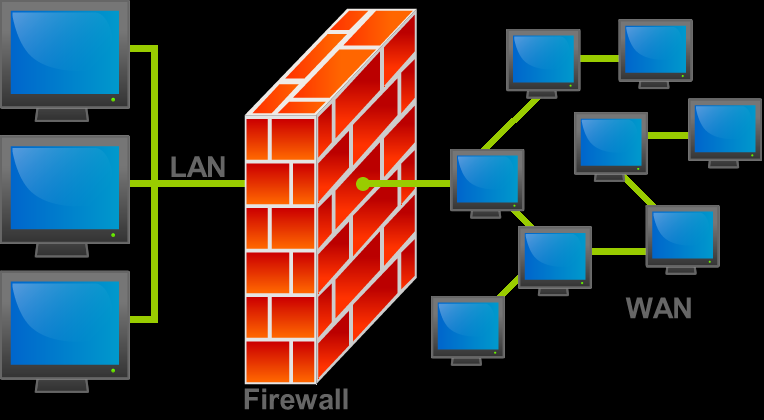
**FIREWALL**

**INTRODUCTION:**

The Project "firewall" can be used as a server or a client-side application which is in this context used by the systems administrator for surveying the systems on the network that are presently connected and vulnerable to attack

client machines about packets and thereby getting a detail report about the port to which the packet was send across the Network. When one machine sends its request, the request is encapsulated in an **'IP packet'.** The **'IP packet'** consists of two parts, i.e. **header** and **data part.** The header part consists of all information of data i.e. the **'Source IP Address'** and **'Destination IP Addresses',** the send time and checksums. This can be used for analyzing data integrity.

A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules



**First generation: packet filters**

The first paper published on firewall technology was in 1988, when engineers from **Digital Equipment Corporation** (DEC) developed filter systems known as packet filter firewalls.

This type of packet filtering pays no attention to whether a packet is part of an existing stream of traffic **(**i.e. it stores no information on connection "state"**)**. Instead, it filters each packet based only on information contained in the packet

**Second generation: application layer**

The key benefit of **application layer filtering** is that it can "understand" certain applications and protocols **(**such as **File Transfer Protocol, DNS, or web browsing)**, and it can detect if an unwanted protocol is sneaking through on a **non-standard port** or if a protocol is being abused in any harmful way.

An **application firewall** is much more secure and reliable compared to packet filter firewalls because it works on all seven layers of the **OSI model**, from the application

Third-generation firewalls, in addition to what first- and second-generation look Though there is still a set of static rules in such a firewall, the

**Subsequent developments**

In **1992**, **Bob Braden** and **Annette DeSchon** at the **University of Southern California** (USC) were refining the concept of a firewall. The product known as "**Visas**" was the first system to have a visual integration interface with colors and icons, which could be easily implemented and accessed on a computer operating system such as Microsoft's

**FIREWALL CONFIGURATION**

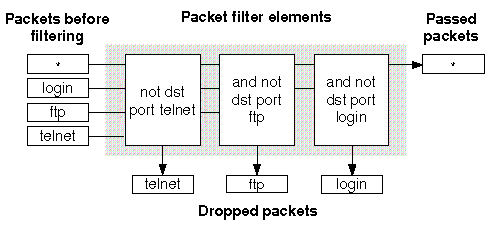
A basic firewall configuration consists of two components

* Two routers that do packet filtering
* An application gateway

**PACKET FILTER**

Each **packet filter** is a standard router equipped with some extra functionality. The extra functionality allows every incoming or outgoing packet packet to be inspected. Packets meeting some criterion are forwarded normally. Those that fail

the test are dropped.



Most likely the packet filters on the inside LAN checks the incoming packets. Packets crossing the first hurdle go to the application gateway for further examination.

Packet filters are typically driven by tables configured by the system administrator.

**APPLICATION GATEWAY:**

Also known as application proxy or application-level proxy, an application gateway is an application program that runson a firewall system between two networks. When a client program establishes a connection to a destination service, it connects to an application gateway, or proxy.

NAT traversal filters to be plugged into the gateway to support address and port

An ALG may offer the following functions:

* network layer address information found inside an application payload between the addresses acceptable by the hosts on either side of the firewall/NAT. This aspect introduces the term 'gateway' for an ALG.
* Recognizing application-specific commands and offering granular security controls over them

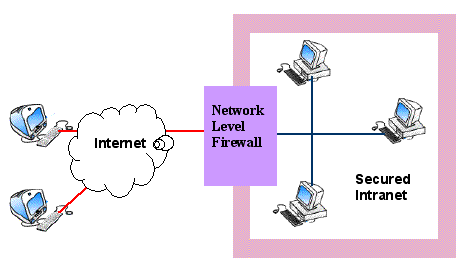
**Deep packet-inspection** of all the packets handled by ALGs over a given network makes this functionality possible. An ALG understands the protocol used by the specific applications that it supports.

**TYPES OF FIREWALL**

Some of the most powerful firewall software on the market is designed to run on an ordinary computer — probably a dedicated server if you're securing a large network.

**Network-Level Firewalls:**

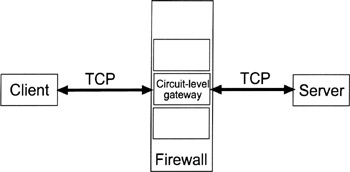
The first generation of firewalls (c. 1988) worked at the network level by inspecting packet headers and filtering traffic based on the IP address of the source and the destination, the port and the service. Some of these primeval security applications could also filter packets based on protocols, the domain name of the source and a few other attributes**.**



Network-level firewalls are fast, and today you'll find them built into most network appliances, particularly routers. These firewalls, however, don't support sophisticated rule-based models. They don’t understand languages like HTML.

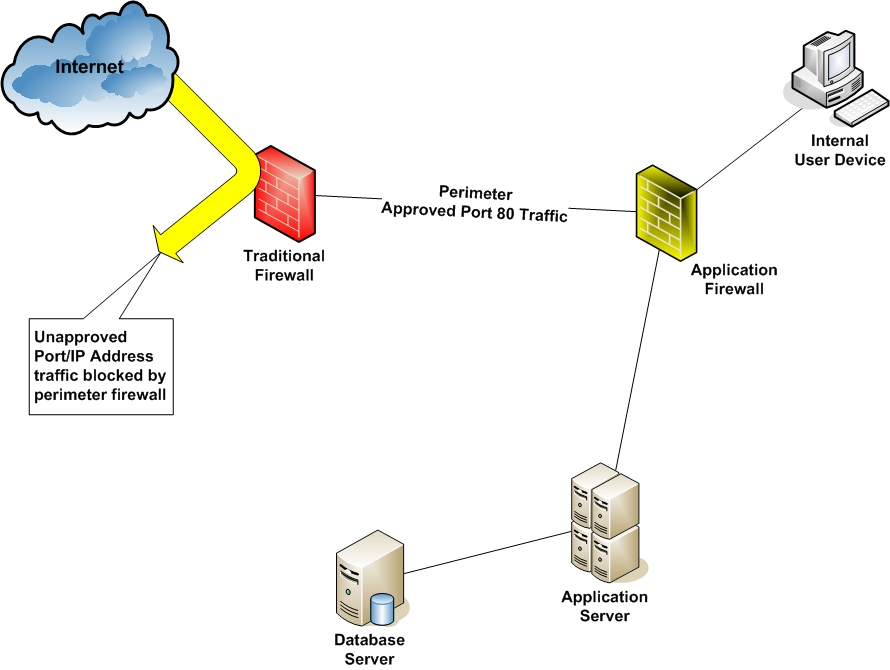
**Circuit-Level Firewalls:**

These applications, which represent the second-generation of firewall technology, monitor TCP handshaking between packets to make sure a session is legitimate.



**Application-Level Firewalls:**

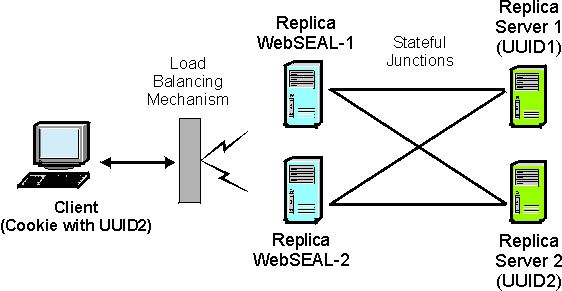
Recently, application-level firewalls (sometimes called proxies) have been looking more deeply into the application data going through their filters. By consideringaddress.



If that sounds too good to be true, it is. The downside to deep packet inspection is that the more closely a firewall examines network data flow, the longer it takes, and the heavier hit your network performance will sustain.

**Stateful Multi-level Firewalls:**

SML vendors claim that their products deploy the best features of the other three firewall types. They filter packets at the network level.



**PROXIES:**

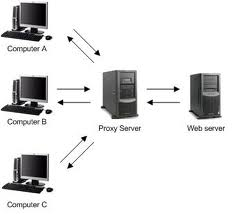
In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, for the same content directly.

Most proxies are a web proxy, allowing access to content on the World Wide Web.

A proxy server has a large variety of potential purposes, including:

* To keep machines behind it anonymous (mainly for security).
* To circumvent regional restrictions.

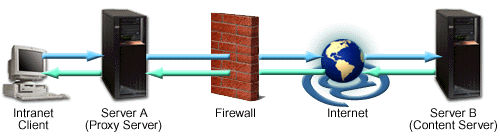
To allow a web site to make web requests to externally hosted resources (e.g. images, music files, etc.) when cross-domain restrictions prohibit the web site from linking directly to the outside domains.



A proxy server that passes requests and replies unmodified is usually called a gateway or sometimes tunneling proxy.

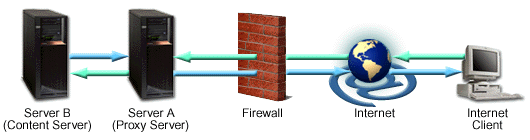
A proxy server can be placed in the user's local computer or at various points

* **FORWARD PROXY-**



Forward proxies are proxies where the client server names the target server to connect to. Forward proxies are able to retrieve from a wide range of sources (in most cases anywhere on the Internet).

**REVERSE PROXY**



A reverse proxy is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more origin servers which handle the request. The response is returned as if it came directly from the proxy server.[3]



**Modes of operation**

There are two very distinct and different modes for network firewalls to operate in.

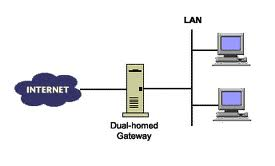
* **Default allow firewalls** allow all traffic in and out of a site.Some specified services may be blocked on the firewall, but all others can freely pass through.
* **Default deny firewalls** block all traffic in or out of a site (though commonly they only block inbound, rather than outbound, traffic).Only named services

This is a secure firewall design comprising an application gateway and a packet

filtering router. It is called “dual homed” because the gateway has two network

interfaces, one attached to the Internet, the other to the organisation's network.

**The Dual Homed Gateway**

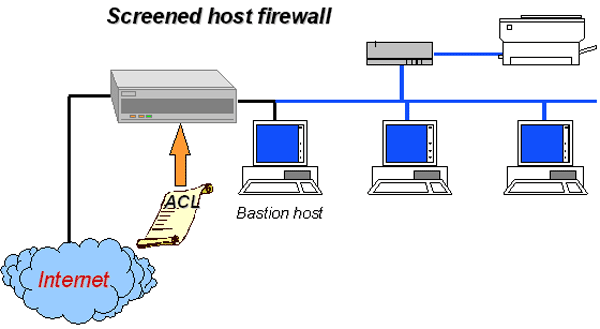


This is a secure firewall design comprising an application gateway and a packet

filtering router. It is called “dual homed” because the gateway has two network

interfaces, one attached to the Internet, the other to the organisation's network.

**The Screened Host Gateway**



The screened host gateway is similar to the above, but more flexible and less secure, since trusted traffic may pass directly from the Internet into the private network, thereby bypassing the application gateway.