NETWORKING

&

APPLICATION

Submitted by:

**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 (your college name) 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

ABOUT OUR GUIDE

**Rajesh Choudhary, Manager (IT)**

**BE Comp Science and Engineering, MBM Engineering College Jodhpur**

**Joined NTPC as Executive Trainee in 2006**

**IBM** Certified Associate Developer **WSAD 5.0**

**IBM**Certified Database Associate**DB2 UDB V8.1**Family

https://ssl.gstatic.com/ui/v1/icons/mail/images/cleardot.gif

INDEX

**COMMUNICATION**

* **ARCHITECTURE**
* **HISTORY**
* **COMMUNICATION MEDIA**
* **COMMUNICATION PROTOCOLS**
* **NEED OF COMMUNICATION IN NETWORKING**

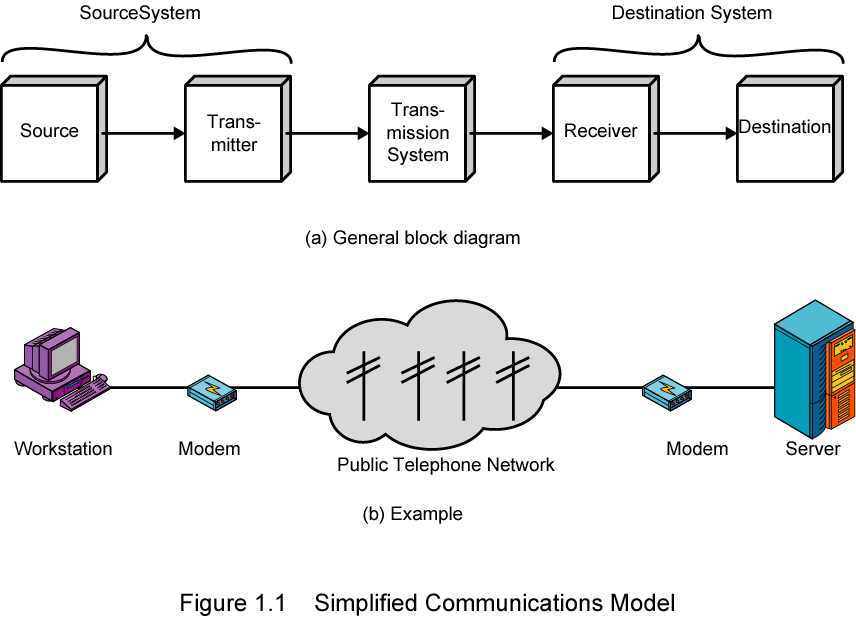
**NETWOKING**

* **BRIEF INTRODUCTION**
* **TYPES OF NETWORK**
* **NETWORK DEVICES**
* **NETWORK TOPOLOGIES**
* **OSI MODEL**
* **TCP/IP REFRENCE MODEL**
* **IP ADDRESS**
* **SUBNETTING**
* **VLSM**

**FIREWALL & CISCO DEVICES**

**COMMUNICATION**

* ARCHITECTURE



* History

Before the advent of computer networks that were based upon some type of [telecommunications](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/George_Stibitz) used a Teletype machine to send instructions for a problem set from his Model at [Dartmouth College](http://en.wikipedia.org/wiki/Dartmouth_College) to his [Complex Number Calculator](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/ARPANET).
* Early networks of communicating computers included the military radar system [Semi-Automatic Ground Environment](http://en.wikipedia.org/wiki/Semi-Automatic_Ground_Environment) (SAGE), started in the late 1950s
* The commercial airline reservation system [Semi-Automatic Business Research Environment](http://en.wikipedia.org/wiki/Semi-Automatic_Business_Research_Environment) (SABRE) which went online with two connected mainframes in 1960.[[2]](http://en.wikipedia.org/wiki/Computer_network" \l "cite_note-1)[[3]](http://en.wikipedia.org/wiki/Computer_network" \l "cite_note-2)
* In 1964, researchers at Dartmouth developed the [Dartmouth Time Sharing System](http://en.wikipedia.org/wiki/Dartmouth_Time_Sharing_System) for distributed users of large computer systems. The same year, at [Massachusetts Institute of Technology](http://en.wikipedia.org/wiki/Massachusetts_Institute_of_Technology), a research group supported by [General Electric](http://en.wikipedia.org/wiki/General_Electric) and [Bell Labs](http://en.wikipedia.org/wiki/Bell_Labs) used a computer to route and manage telephone connections.
* Throughout the 1960s [Leonard Kleinrock](http://en.wikipedia.org/wiki/Leonard_Kleinrock), [Paul Baran](http://en.wikipedia.org/wiki/Paul_Baran) and [Donald Davies](http://en.wikipedia.org/wiki/Donald_Davies) independently conceptualized and developed network systems which used [packets](http://en.wikipedia.org/wiki/Packet_(information_technology)) that could be used in a network between computer systems.
* 1965 [Thomas Merrill](http://en.wikipedia.org/w/index.php?title=Thomas_Merrill_(scientist)&action=edit&redlink=1) and [Lawrence G. Roberts](http://en.wikipedia.org/wiki/Lawrence_G._Roberts) created the first [wide area network](http://en.wikipedia.org/wiki/Wide_area_network) (WAN).
* The first widely used [telephone switch](http://en.wikipedia.org/wiki/Telephone_switch) that used true computer control was introduced by [Western Electric](http://en.wikipedia.org/wiki/Western_Electric) in 1965.
* In 1969 the [University of California at Los Angeles](http://en.wikipedia.org/wiki/University_of_California_at_Los_Angeles), the [Stanford Research Institute](http://en.wikipedia.org/wiki/Stanford_Research_Institute), [University of California at Santa Barbara](http://en.wikipedia.org/wiki/University_of_California_at_Santa_Barbara), and the [University of Utah](http://en.wikipedia.org/wiki/University_of_Utah) were connected as the beginning of the[ARPANET](http://en.wikipedia.org/wiki/ARPANET) network using 50 kbit/s circuits.[[4]](http://en.wikipedia.org/wiki/Computer_network" \l "cite_note-3)
* Commercial services using [X.25](http://en.wikipedia.org/wiki/X.25) were deployed in 1972, and later used as an underlying infrastructure for expanding [TCP/IP](http://en.wikipedia.org/wiki/TCP/IP) networks.

Today, computer networks are the core of modern communication. All modern aspects of the [Public Switched Telephone Network](http://en.wikipedia.org/wiki/Public_Switched_Telephone_Network) (PSTN) are computer-controlled, and telephony increasingly runs over the Internet Protocol, although not necessarily the public Internet. The scope of communication has increased significantly in the past decade, and this boom in communications would not have been possible without the progressively advancing computer network. Computer networks, and the technologies needed to connect and communicate through and between them, continue to drive computer hardware, software, and peripherals industries. This expansion is mirrored by growth in the numbers and types of users of networks from the researcher to the home user.

* 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](http://en.wikipedia.org/wiki/Cable)([HomePNA](http://en.wikipedia.org/wiki/HomePNA), [power line communication](http://en.wikipedia.org/wiki/Power_line_communication), [G.hn](http://en.wikipedia.org/wiki/G.hn)), [optical fiber](http://en.wikipedia.org/wiki/Optical_fiber), and [radio waves](http://en.wikipedia.org/wiki/Radio_waves) ([wireless LAN](http://en.wikipedia.org/wiki/Wireless_LAN)). In the [OSI model](http://en.wikipedia.org/wiki/OSI_model), these are located at levels 1 and 2.

A well-known *family* of communication media is collectively known as [Ethernet](http://en.wikipedia.org/wiki/Ethernet). It is defined by [IEEE 802](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Radio_waves) or [infrared](http://en.wikipedia.org/wiki/IrDA) signals as a transmission medium.

**Wired technologies**

* [***Twisted pair***](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Ethernet) as defined by [IEEE 802.3](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Crosstalk_(electronics)) and [electromagnetic induction](http://en.wikipedia.org/wiki/Electromagnetic_induction). The transmission speed ranges from 2 million bits per second to 10 billion bits per second. Twisted pair cabling comes in two forms which are Unshielded Twisted Pair (UTP) and Shielded twisted-pair (STP) which are rated in categories which are manufactured in different increments for various scenarios.
* [***Coaxial cable***](http://en.wikipedia.org/wiki/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 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. The layers of insulation help minimize interference and distortion. Transmission speed range from 200 million to more than 500 million bits per second.
* [ITU-T](http://en.wikipedia.org/wiki/ITU-T) [G.hn](http://en.wikipedia.org/wiki/G.hn) technology uses existing [home wiring](http://en.wikipedia.org/wiki/Home_wiring) ([coaxial cable](http://en.wikipedia.org/wiki/Ethernet_over_coax), phone lines and [power lines](http://en.wikipedia.org/wiki/Power_line_communication)) to create a high-speed (up to 1 Gigabit/s) local area network.
* [***Optical fiber***](http://en.wikipedia.org/wiki/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. Transmission speed may reach trillions of bits per second. The transmission speed of fiber optics is hundreds of times faster than for coaxial cables and thousands of times faster than a twisted-pair wire. This *capacity* may be further increased by the use of colored light, i.e., light of multiple wavelengths. Instead of carrying one message in a stream of monochromatic light impulses, this technology can carry multiple signals in a single fiber.

**Wireless technologies**

* ***Terrestrial***[***microwave***](http://en.wikipedia.org/wiki/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***](http://en.wikipedia.org/wiki/Satellite) – 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](http://en.wikipedia.org/wiki/IEEE_802.11).
* [***Infrared communication***](http://en.wikipedia.org/wiki/Infrared_communication) can transmit signals between devices within small distances of typically no more than 10 meters. In most cases, [line-of-sight propagation](http://en.wikipedia.org/wiki/Line-of-sight_propagation) is used, which limits the physical positioning of communicating devices.
* A [global area network](http://en.wikipedia.org/wiki/Global_area_network) (GAN) is a network used for supporting mobile communications across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off the user communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial [wireless LANs](http://en.wikipedia.org/wiki/Wireless_LAN).[[7]](http://en.wikipedia.org/wiki/Computer_network" \l "cite_note-6)

**Exotic technologies**

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

* [IP over Avian Carriers](http://en.wikipedia.org/wiki/IP_over_Avian_Carriers) was a humorous April fool's [Request for Comments](http://en.wikipedia.org/wiki/Request_for_Comments), issued as [**RFC 1149**](http://tools.ietf.org/html/rfc1149). It was implemented in real life in 2001.[[8]](http://en.wikipedia.org/wiki/Computer_network" \l "cite_note-7)
* Extending the Internet to interplanetary dimensions via radio waves.[[9]](http://en.wikipedia.org/wiki/Computer_network" \l "cite_note-8)

A practical limit in both cases is the [round-trip delay time](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Protocol_suite) which describes the protocols used at various [usage levels](http://en.wikipedia.org/wiki/OSI_model). 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](http://en.wikipedia.org/wiki/HTTP) running over [TCP](http://en.wikipedia.org/wiki/Transmission_Control_Protocol) over [IP](http://en.wikipedia.org/wiki/Internet_Protocol) over [IEEE 802.11](http://en.wikipedia.org/wiki/IEEE_802.11), where the second and third are members of the [Internet Protocol Suite](http://en.wikipedia.org/wiki/Internet_Protocol_Suite), while the last is a member of the [Ethernet](http://en.wikipedia.org/wiki/Ethernet) protocol suite. This is the stacking which exists between the [wireless router](http://en.wikipedia.org/wiki/Wireless_router) and the home user's[personal computer](http://en.wikipedia.org/wiki/Personal_computer) when surfing the [World Wide Web](http://en.wikipedia.org/wiki/World_Wide_Web).

Communication protocols have themselves various properties, such as whether they are [connection-oriented](http://en.wikipedia.org/wiki/Connection-oriented_communication) versus [connectionless](http://en.wikipedia.org/wiki/Connectionless_communication), whether they use [circuit mode](http://en.wikipedia.org/wiki/Circuit_mode) or [packet switching](http://en.wikipedia.org/wiki/Packet_switching), or whether they use hierarchical or flat addressing.

There exist a multitude of communication protocols, a few of which are described below.

### Ethernet

Ethernet is a family of connectionless protocols used in LANs, described by a set of standards together called [IEEE 802](http://en.wikipedia.org/wiki/IEEE_802) published by the [Institute of Electrical and Electronics Engineers](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/OSI_model). For home users today, the most well-known member of this protocol family is [IEEE 802.11](http://en.wikipedia.org/wiki/IEEE_802.11), otherwise known as [Wireless LAN](http://en.wikipedia.org/wiki/Wireless_LAN)(WLAN). However, the complete protocol suite deals with a multitude of networking aspects not only for home use, but especially when the technology is deployed to support a diverse range of business needs. [MAC](http://en.wikipedia.org/wiki/Media_access_control) [bridging](http://en.wikipedia.org/wiki/Bridging_(networking)) ([IEEE 802.1D](http://en.wikipedia.org/wiki/IEEE_802.1D)) deals with the routing of Ethernet packets using a [Spanning Tree Protocol](http://en.wikipedia.org/wiki/Spanning_Tree_Protocol), [IEEE 802.1Q](http://en.wikipedia.org/wiki/IEEE_802.1Q) describes [VLANs](http://en.wikipedia.org/wiki/Virtual_LAN), and [IEEE 802.1X](http://en.wikipedia.org/wiki/IEEE_802.1X) defines a port-based [Network Access Control](http://en.wikipedia.org/wiki/Network_Access_Control) protocol which forms the basis for the authentication mechanisms used in VLANs, but also found in WLANs - it is what the home user sees when they have to enter a "wireless access key".

### Internet Protocol Suite

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

### SONET/SDH

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

### Asynchronous Transfer Mode

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

While the role of ATM is diminishing in favor of [next-generation networks](http://en.wikipedia.org/wiki/Next_generation_network), it still plays a role in the [last mile](http://en.wikipedia.org/wiki/Last_mile), which is the connection between an [Internet service provider](http://en.wikipedia.org/wiki/Internet_service_provider) and the home user

* Need of coomunication 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. Now a user sitting at one place can communicate computers of any remote sites through communication channel. The aim of this chapter is to introduce you the various aspects of computer network

**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. A network connecting device router connects LANs to WANs. WAN used network protocols like ATM, X.25, and Frame Relay for long distance connectivity.

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. Wireless network cards are required to be installed in the systems for accessing any wireless network around. Mostly wireless cards connect to wireless routers for communication among computers or accessing WAN, internet.

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

SAM 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

SAN, system area networks are also known as cluster area network and it connects high performance computers with high speed connections in cluster configuration.

* **NETWORK DEVICES**

**ROUTER**

A **router** is a device that forwards [data packets](http://en.wikipedia.org/wiki/Data_packet) between [telecommunications networks](http://en.wikipedia.org/wiki/Telecommunications_network), creating an overlay [internetwork](http://en.wikipedia.org/wiki/Internetwork). 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. Then, using information in its [routing table](http://en.wikipedia.org/wiki/Routing_table) or [routing policy](http://en.wikipedia.org/wiki/Routing_policy), it directs the packet to the next network on its journey or drops the packet. A data packet is typically forwarded from one router to another through networks that constitute the internetwork until it gets to its destination node.[[1]](http://en.wikipedia.org/wiki/Router_(computing)" \l "cite_note-0)

The most familiar type of routers are [home and small office routers](http://en.wikipedia.org/wiki/Home_router) that simply pass data, such as web pages and email, between the home computers and the owner's [cable](http://en.wikipedia.org/wiki/Cable_modem) or [DSL modem](http://en.wikipedia.org/wiki/DSL_modem), which connects to the Internet ([ISP](http://en.wikipedia.org/wiki/Internet_service_provider)). However more sophisticated routers range from enterprise routers, which connect large business or ISP networks up to the powerful [core routers](http://en.wikipedia.org/wiki/Core_router) that forward data at high speed along the [optical fiber](http://en.wikipedia.org/wiki/Optical_fiber) lines of the [Internet backbone](http://en.wikipedia.org/wiki/Internet_backbone).

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. A router has interfaces for different physical types of network connections, (such as copper cables, fiber optic, or wireless transmission). It also contains [firmware](http://en.wikipedia.org/wiki/Firmware) for different networking [protocol](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Subnetwork), each with a different sub-[network address](http://en.wikipedia.org/wiki/IP_address). The subnets addresses recorded in the router do not necessarily map directly to the physical interface connections.[[2]](http://en.wikipedia.org/wiki/Router_(computing)" \l "cite_note-1) A router has two stages of operation called planes:[[3]](http://en.wikipedia.org/wiki/Router_(computing)" \l "cite_note-2)

* [Control plane](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Header_(information_technology))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](http://en.wikipedia.org/wiki/Internet_service_provider) (ISPs) networks. The largest routers (such as the [Cisco](http://en.wikipedia.org/wiki/Cisco_Systems) [CRS-1](http://en.wikipedia.org/wiki/CRS-1)or Juniper T1600) interconnect the various ISPs, or may be used in large enterprise networks.[[4]](http://en.wikipedia.org/wiki/Router_(computing)" \l "cite_note-3)Smaller routers usually provide connectivity for typical home and office networks. Other networking solutions may be provided by a backbone [Wireless Distribution System](http://en.wikipedia.org/wiki/Wireless_Distribution_System) (WDS), which avoids the costs of introducing networking cables into buildings.

**ETHERNET HUB**

An **Ethernet hub**, **active hub**, **network hub**, **repeater hub** or **hub** is a device for connecting multiple [twisted pair](http://en.wikipedia.org/wiki/Ethernet_over_twisted_pair) or [fiber optic](http://en.wikipedia.org/wiki/Optical_fiber) [Ethernet](http://en.wikipedia.org/wiki/Ethernet) devices together and making them act as a single [network segment](http://en.wikipedia.org/wiki/Network_segment). Hubs work at the [physical layer](http://en.wikipedia.org/wiki/Physical_layer) (layer 1) of the [OSI model](http://en.wikipedia.org/wiki/OSI_model).[[1]](http://en.wikipedia.org/wiki/Ethernet_hub" \l "cite_note-networkingtext-0) The device is a form of [multiport repeater](http://en.wikipedia.org/wiki/Multiport_repeater). Repeater hubs also participate in collision detection, forwarding a [jam signal](http://en.wikipedia.org/wiki/Jam_signal) to all ports if it detects a[collision](http://en.wikipedia.org/wiki/Collision_(telecommunications)).

Hubs also often come with a [BNC](http://en.wikipedia.org/wiki/BNC_connector) and/or [Attachment Unit Interface](http://en.wikipedia.org/wiki/Attachment_Unit_Interface) (AUI) connector to allow connection to legacy [10BASE2](http://en.wikipedia.org/wiki/10BASE2) or [10BASE5](http://en.wikipedia.org/wiki/10BASE5) network segments. The availability of low-priced [network switches](http://en.wikipedia.org/wiki/Network_switch) has largely rendered hubs obsolete but they are still seen in older installations and more specialized applications.

APPLICATIONS

Historically, the main reason for purchasing hubs rather than [switches](http://en.wikipedia.org/wiki/Network_switch) 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](http://en.wikipedia.org/wiki/Protocol_analyzer) into a network connection, a hub is an alternative to a [network tap](http://en.wikipedia.org/wiki/Network_tap) or [port mirroring](http://en.wikipedia.org/wiki/Port_mirroring).[[4]](http://en.wikipedia.org/wiki/Ethernet_hub" \l "cite_note-3)
* When a switch is accessible for end users to make connections, for example, in a conference room, an inexperienced or careless user (or [saboteur](http://en.wikipedia.org/wiki/Sabotage)) can bring down the network by connecting two ports together, causing a loop. This can be prevented by using a hub, where a loop will break other users on the hub, but not the rest of the network. This hazard can also be avoided by using switches that can detect and deal with loops, for example by implementing the [spanning tree protocol](http://en.wikipedia.org/wiki/Spanning_tree_protocol).
* A hub with a 10BASE2 port can be used to connect devices that only support 10BASE2 to a modern network. The same goes for linking in an old 10BASE5 network segment using an AUI port on a hub (individual devices that were intended for thicknet can be linked to modern Ethernet by using an AUI-10BASE-T [transceiver](http://en.wikipedia.org/wiki/Transceiver)).

**NETWORK SWITCH**

A **network switch** or **switching hub** is a [computer networking device](http://en.wikipedia.org/wiki/Computer_networking_device) that connects [network segments](http://en.wikipedia.org/wiki/Network_segment).

The term commonly refers to a multi-port [network bridge](http://en.wikipedia.org/wiki/Network_bridge) that processes and routes data at the [data link layer](http://en.wikipedia.org/wiki/Data_link_layer) (layer 2) of the [OSI model](http://en.wikipedia.org/wiki/OSI_model). Switches that additionally process data at the[network layer](http://en.wikipedia.org/wiki/Network_layer) (Layer 3) and above are often referred to as Layer 3 switches or [multilayer switches](http://en.wikipedia.org/wiki/Multilayer_switch).

The first [Ethernet](http://en.wikipedia.org/wiki/Ethernet) switch was introduced by [Kalpana](http://en.wikipedia.org/wiki/Kalpana_(company)) in 1990

APPLICATION

Switches may operate at one or more layers of the OSI model, including [data link](http://en.wikipedia.org/wiki/Data_link_layer), [network](http://en.wikipedia.org/wiki/Network_layer), or [transport (i.e., end-to-end)](http://en.wikipedia.org/wiki/Transport_layer). A device that operates simultaneously at more than one of these layers is known as a [multilayer switch](http://en.wikipedia.org/wiki/Multilayer_switch).

In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, including [Ethernet](http://en.wikipedia.org/wiki/Ethernet), [Fibre Channel](http://en.wikipedia.org/wiki/Fibre_Channel), [ATM](http://en.wikipedia.org/wiki/Asynchronous_Transfer_Mode), [ITU-T](http://en.wikipedia.org/wiki/ITU-T) [G.hn](http://en.wikipedia.org/wiki/G.hn) and [802.11](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Ethernet) and [token ring](http://en.wikipedia.org/wiki/Token_ring) are easier at Layer 3.

Interconnection of different Layer 3 networks is done by [routers](http://en.wikipedia.org/wiki/Router_(computing)). If there are any features that characterize "Layer-3 switches" as opposed to general-purpose routers, it tends to be that they are optimized, in larger switches, for high-density Ethernet connectivity.

In some service provider and other environments 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](http://en.wikipedia.org/wiki/Firewall_(computing)),[[2]](http://en.wikipedia.org/wiki/Network_switch" \l "cite_note-1)[[3]](http://en.wikipedia.org/wiki/Network_switch" \l "cite_note-2) network [intrusion detection](http://en.wikipedia.org/wiki/Intrusion_detection),[[4]](http://en.wikipedia.org/wiki/Network_switch" \l "cite_note-3) and performance analysis modules that can plug into switch ports. Some of these functions may be on combined modules.[[5]](http://en.wikipedia.org/wiki/Network_switch" \l "cite_note-4)

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](http://en.wikipedia.org/wiki/Network_hub) can be useful for fanning out data to several read-only analyzers, such as [intrusion detection systems](http://en.wikipedia.org/wiki/Intrusion_detection_system) and [packet sniffers](http://en.wikipedia.org/wiki/Packet_sniffer).

**NETWORK BRIDGE**

**Bridging** is a [forwarding](http://en.wikipedia.org/wiki/Packet_forwarding) technique used in [packet-switched](http://en.wikipedia.org/wiki/Packet_switching) [computer networks](http://en.wikipedia.org/wiki/Computer_network). Unlike [routing](http://en.wikipedia.org/wiki/Routing), bridging makes no assumptions about where in a network a particular address is located. Instead, it depends on [flooding](http://en.wikipedia.org/wiki/Flooding_(computer_networking)) 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](http://en.wikipedia.org/wiki/MAC_address) is stored so as to preclude the need for further [broadcasting](http://en.wikipedia.org/wiki/Broadcasting_(computing)). The utility of bridging is limited by its dependence on flooding, and is thus only used in [local area networks](http://en.wikipedia.org/wiki/Local_area_network).

Bridging generally refers to *transparent bridging* or *Learning bridge* operation which predominates in [Ethernet](http://en.wikipedia.org/wiki/Ethernet). Another form of bridging, Source, was developed for [token ring](http://en.wikipedia.org/wiki/Token_ring) networks.

A **network bridge** connects multiple [network segments](http://en.wikipedia.org/wiki/Network_segment) at the [data link layer](http://en.wikipedia.org/wiki/Data_link_layer) (Layer 2) of the [OSI model](http://en.wikipedia.org/wiki/OSI_model). In Ethernet networks, the term *bridge* formally means a device that behaves according to the [IEEE 802.1D](http://en.wikipedia.org/wiki/IEEE_802.1D) standard. A [bridge and a switch](http://en.wikipedia.org/wiki/Ethernet" \l "Bridging_and_switching) are very much alike; a switch being a bridge with numerous ports. *Switch* or *Layer 2 switch* is often used interchangeably with *bridge*.

Bridges are similar to [repeaters](http://en.wikipedia.org/wiki/Repeater) or [network hubs](http://en.wikipedia.org/wiki/Network_hub), devices that connect network segments at the [physical layer](http://en.wikipedia.org/wiki/Physical_layer) (Layer 1) of the [OSI model](http://en.wikipedia.org/wiki/OSI_model); however, with bridging, traffic from one network is managed rather than simply rebroadcast to adjacent network segments. Bridges are more complex than hubs or repeaters. Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.

**REPEATER**

A **repeater** is an [electronic](http://en.wikipedia.org/wiki/Electronics) device that receives a [signal](http://en.wikipedia.org/wiki/Signal_(information_theory)) and [retransmits](http://en.wikipedia.org/wiki/Retransmit) 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](http://en.wikipedia.org/wiki/Telegraphy) and referred to an [electromechanical](http://en.wikipedia.org/wiki/Electromechanical) device used by the army to regenerate telegraph signals. Use of the term has continued in [telephony](http://en.wikipedia.org/wiki/Telephony) and [data](http://en.wikipedia.org/wiki/Data) [communications](http://en.wikipedia.org/wiki/Telecommunication).

In [telecommunication](http://en.wikipedia.org/wiki/Telecommunication), the term **repeater** has the following standardized meanings:

1. An [analog](http://en.wikipedia.org/wiki/Analog_(signal)) [device](http://en.wikipedia.org/wiki/Information_appliance) that [amplifies](http://en.wikipedia.org/wiki/Amplifier) an input [signal](http://en.wikipedia.org/wiki/Signal_(information_theory)) regardless of its nature (analog or [digital](http://en.wikipedia.org/wiki/Digital)).
2. A [digital](http://en.wikipedia.org/wiki/Digital) device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for[retransmission](http://en.wikipedia.org/wiki/Transmission_(telecommunications))..

* NETWORK TOPOLOGIES

**Network topology** is the layout pattern of interconnections of the various elements ([links](http://en.wikipedia.org/wiki/Data_link), [nodes](http://en.wikipedia.org/wiki/Node_(networking)), etc.) of a [computer](http://en.wikipedia.org/wiki/Computer_network)[[1]](http://en.wikipedia.org/wiki/Network_topologies" \l "cite_note-Groth-0)[[2]](http://en.wikipedia.org/wiki/Network_topologies" \l "cite_note-atis-1) or [biological network](http://en.wikipedia.org/wiki/Biological_network).[[3]](http://en.wikipedia.org/wiki/Network_topologies" \l "cite_note-Proulx05-2) Network topologies may be physical or logical. [Physical topology](http://en.wikipedia.org/wiki/Topology) refers to the physical design of a network including the devices, location and cable installation. [Logical topology](http://en.wikipedia.org/wiki/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.

Any particular network topology is determined only by the graphical mapping of the configuration of physical and/or logical connections between nodes. The study of network topology uses [graph theory](http://en.wikipedia.org/wiki/Graph_theory). Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ in two networks and yet their topologies may be identical.

A [local area network](http://en.wikipedia.org/wiki/Local_area_network) (LAN) is one example of a network that exhibits both a physical topology and a logical topology. Any given node in the LAN has one or more links to one or more nodes in the network and the mapping of these links and nodes in a graph results in a geometric shape that may be used to describe the physical topology of the network. Likewise, the mapping of the data flow between the nodes in the network determines the logical topology of the network. The physical and logical topologies may or may not be identical in any particular

There are two basic categories of network topologies:

* Physical topologies
* Logical topologies

The shape of the cabling layout used to link devices is called the physical topology of the network. This refers to the layout of [cabling](http://en.wikipedia.org/wiki/Structured_cabling), the locations of nodes, and the interconnections between the nodes and the cabling.[[1]](http://en.wikipedia.org/wiki/Network_topologies" \l "cite_note-Groth-0) The physical topology of a network is determined by the capabilities of the network access devices and media, the level of control or fault tolerance desired, and the cost associated with cabling or telecommunications circuits.

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](http://en.wikipedia.org/wiki/Twisted_pair_Ethernet) using [repeater hubs](http://en.wikipedia.org/wiki/Repeater_hub) was a logical bus topology with a physical star topology layout. [Token Ring](http://en.wikipedia.org/wiki/Token_Ring) is a logical ring topology, but is wired a physical star from the [Media Access Unit](http://en.wikipedia.org/wiki/Media_Access_Unit).

The logical classification of network topologies generally follows the same classifications as those in the physical classifications of network topologies but describes the path that the *data* takes between nodes being used as opposed to the actual *physical* connections between nodes. The logical topologies are generally determined by network protocols as opposed to being determined by the physical layout of cables, wires, and network devices or by the flow of the electrical signals, although in many cases the paths that the electrical signals take between nodes may closely match the logical flow of data, hence the convention of using the terms *logical topology* and *signal topology*interchangeably.

Logical topologies are often closely associated with [Media Access Control](http://en.wikipedia.org/wiki/Media_Access_Control) methods and protocols. Logical topologies are able to be dynamically reconfigured by special types of equipment such as [routers](http://en.wikipedia.org/wiki/Router_(computing)) and switches.

The study of network topology recognizes seven basic topologies:[[5]](http://en.wikipedia.org/wiki/Network_topologies" \l "cite_note-Bicsi.2C_B._2002-4)

* 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](http://en.wikipedia.org/wiki/Point-to-point_(telecommunications)) 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](http://en.wikipedia.org/wiki/Metcalfe's_Law).

**Permanent (dedicated)**

Easiest to understand, of the variations of point-to-point topology, is a point-to-point [communications channel](http://en.wikipedia.org/wiki/Channel_(communications)) that appears, to the user, to be permanently associated with the two endpoints. A children's [tin can telephone](http://en.wikipedia.org/wiki/Tin_can_telephone) is one example of a *physical dedicated* channel.

Within many [switched telecommunications systems](http://en.wikipedia.org/w/index.php?title=Switched_telecommunications_systems&action=edit&redlink=1), it is possible to establish a permanent circuit. One example might be a telephone in the lobby of a public building, which is programmed to ring only the number of a telephone dispatcher. "Nailing down" a switched connection saves the cost of running a physical circuit between the two points. The resources in such a connection can be released when no longer needed, for example, a television circuit from a parade route back to the studio.

**Switched:**

Using [circuit-switching](http://en.wikipedia.org/wiki/Circuit-switching) or [packet-switching](http://en.wikipedia.org/wiki/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. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data does match the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the [single point of failure](http://en.wikipedia.org/wiki/Single_point_of_failure). If the network cable breaks, the entire network will be down.

**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](http://en.wikipedia.org/wiki/Backbone_network), or [trunk](http://en.wikipedia.org/wiki/Trunk_(telecommunications))) – all [data](http://en.wikipedia.org/wiki/Data) that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be [received](http://en.wikipedia.org/wiki/Receiver_(Information_Theory)) by all nodes in the network simultaneously.[[1]](http://en.wikipedia.org/wiki/Network_topologies" \l "cite_note-Groth-0)

.

**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 – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common 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](http://en.wikipedia.org/wiki/Repeater). The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the hub represents a single point of failure.

**Notes**

1. 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.[[1]](http://en.wikipedia.org/wiki/Network_topologies" \l "cite_note-Groth-0)
2. After the special case of the point-to-point link, as in note (1) above, the next simplest type of network that is based upon the physical star topology would consist of one central node – the 'hub' – with two separate point-to-point links to two peripheral nodes – the 'spokes'.
3. Although most networks that are based upon the physical star topology are commonly implemented using a special device such as a [hub](http://en.wikipedia.org/wiki/Network_hub) or [switch](http://en.wikipedia.org/wiki/Network_switch) as the central node (i.e., the 'hub' of the star), it is also possible to implement a network that is based upon the physical star topology using a computer or even a simple common connection point as the 'hub' or central node.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]
4. Star networks may also be described as either [broadcast multi-access](http://en.wikipedia.org/w/index.php?title=Broadcast_multi-access&action=edit&redlink=1) or [no broadcast multi-access](http://en.wikipedia.org/w/index.php?title=Nonbroadcast_multi-access&action=edit&redlink=1) (NBMA), depending on whether the technology of the network either automatically propagates a signal at the hub to all spokes, or only addresses individual spokes with each communication.

**Extended star**

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 repeaters being used to extend the maximum transmission distance of the point-to-point links between the central node and the peripheral nodes beyond that which is supported by the transmitter power of the central node or beyond that which is supported by the standard upon which the physical layer of the physical star network is based.

If the repeaters in a network that is based upon the physical extended star topology are replaced with hubs or switches, then a hybrid network topology is created that is referred to as a physical hierarchical star topology, although some texts make no distinction between the two topologies.

**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.[[4](http://en.wikipedia.org/wiki/Network_topologies" \l "cite_note-Inc.2C_S._2002-3)

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](http://en.wikipedia.org/wiki/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, while each of the second level nodes that are connected to the top level central 'root' node will also have one or more other nodes that are one level lower in the hierarchy (i.e., the third level) connected to it, also with a point-to-point link, the top level central 'root' node being the only node that has no other node above it in the hierarchy (The hierarchy of the tree is symmetrical.) Each node in the network having a specific fixed number, of nodes connected to it at the next lower level in the hierarchy, the number, being referred to as the 'branching factor' of the hierarchical tree. This tree has individual peripheral nodes.

1. A network that is based upon the physical hierarchical topology must have at least three levels in the hierarchy of the tree, since a network with a central 'root' node and only one hierarchical level below it would exhibit the physical topology of a star.
2. 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.
3. The branching factor, f, is independent of the total number of nodes in the network and, therefore, if the nodes in the network require ports for connection to other nodes the total number of ports per node may be kept low even though the total number of nodes is large – this makes the effect of the cost of adding ports to each node totally dependent upon the branching factor and may therefore be kept as low as required without any effect upon the total number of nodes that are possible.
4. The total number of point-to-point links in a network that is based upon the physical hierarchical topology will be one less than the total number of nodes in the network.
5. If the nodes in a network that is based upon the physical hierarchical topology are required to perform any processing upon the data that is transmitted between nodes in the network, the nodes that are at higher levels in the hierarchy will be required to perform more processing operations on behalf of other nodes than the nodes that 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](http://en.wikipedia.org/wiki/Media_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).

While grid networks have found popularity in [high-performance computing](http://en.wikipedia.org/wiki/High-performance_computing) applications, some systems have used [genetic algorithms](http://en.wikipedia.org/wiki/Genetic_algorithm) to design custom networks that have the fewest possible hops in between different nodes. Some of the resulting layouts are nearly incomprehensible, although they function quite well.

A Snowflake topology is really a "Star of Stars" network, so it exhibits characteristics of a hybrid network topology but is not composed of two different basic network topologies being connected together.

* OSI REFRENCE MODEL

The **Open Systems Interconnection model** (**OSI model**) was a product of the [Open Systems Interconnection](http://en.wikipedia.org/wiki/Open_Systems_Interconnection) effort at the [International Organization for Standardization](http://en.wikipedia.org/wiki/International_Organization_for_Standardization). It is a way of sub-dividing a [communications system](http://en.wikipedia.org/wiki/Communications_system) into smaller parts called [layers](http://en.wikipedia.org/wiki/Abstraction_layer). 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*](http://en.wikipedia.org/wiki/Instance_(computer_science)) provides service to the instances at the layer above and requests service from the layer below.

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 make up the contents of that path. Two instances at one layer are connected by a horizontal connection on that layer

HISTORY

Work on a layered model of network architecture was started and the [International Organization for Standardization](http://en.wikipedia.org/wiki/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.

Note: The standard documents that described the OSI model could be freely downloaded from the ITU-T as the **X.200**-series of recommendations.[[1]](http://en.wikipedia.org/wiki/OSI_model" \l "cite_note-0) A number of the protocol specifications were also available as part of the ITU-T X series. The equivalent ISO and ISO/IEC standards for the OSI model were available from ISO, but only some of them at no charge.[[2]](http://en.wikipedia.org/wiki/OSI_model" \l "cite_note-1)

The concept of a 7 layer model was provided by the work of Charles, Honeywell Information Services. Various aspects of OSI design evolved from experiences with the ARPANET, the fledgling Internet, NPLNET, EIN, CYCLADES network and the work in IFIP WG6.1. The new design was documented in ISO 7498 and its various addenda. In this model, a networking system was divided into layers. Within each layer, one or more entities implement its functionality. Each entity interacted directly only with the layer immediately beneath it, and provided facilities for use by the layer above it.

Protocols enabled an entity in one host to interact with a corresponding entity at the same layer in another host. Service definitions abstractly described the functionality provided to an (N)-layer by an (N-1) layer, where N was one of the seven layers of protocols operating in the local host.

### Layer 1: Physical Layer

The [Physical Layer](http://en.wikipedia.org/wiki/Physical_Layer) defines [electrical](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Lead_(electronics)), [voltages](http://en.wikipedia.org/wiki/Voltage), [cable](http://en.wikipedia.org/wiki/Cable) [specifications](http://en.wikipedia.org/wiki/Specification), [hubs](http://en.wikipedia.org/wiki/Network_hub), repeaters, network, [host bus adapters](http://en.wikipedia.org/wiki/Host_adapter) (HBA used in [storage area networks](http://en.wikipedia.org/wiki/Storage_area_network)) and more.

To understand the function of the Physical Layer, contrast it with the functions of the Data Link Layer. Think of the Physical Layer as concerned primarily with the interaction of a single device with a medium, whereas the Data Link Layer is concerned more with the interactions of multiple devices (i.e., at least two) with a shared medium [[*clarification needed*](http://en.wikipedia.org/wiki/Wikipedia:Please_clarify)]. Standards such as [RS-232](http://en.wikipedia.org/wiki/RS-232) do use physical wires to control access to the medium.

The major functions and services performed by the Physical Layer are:

* Establishment and termination of a [connection](http://en.wikipedia.org/wiki/Electrical_connector) to a [communications](http://en.wikipedia.org/wiki/Communication) [medium](http://en.wikipedia.org/wiki/Transmission_medium).
* Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and [flow control](http://en.wikipedia.org/wiki/Flow_control).
* [Modulation](http://en.wikipedia.org/wiki/Modulation), or conversion between the representation of [digital data](http://en.wikipedia.org/wiki/Digital_data) in user equipment and the corresponding signals transmitted over a communications [channel](http://en.wikipedia.org/wiki/Channel_(communications)). These are signals operating over the physical cabling (such as copper and [optical fiber](http://en.wikipedia.org/wiki/Optical_fiber)) or over a [radio link](http://en.wikipedia.org/wiki/Electromagnetic_wave" \l "Radio_waves).

[Parallel SCSI](http://en.wikipedia.org/wiki/Parallel_SCSI) buses operate in this layer, although it must be remembered that the logical [SCSI](http://en.wikipedia.org/wiki/SCSI) protocol is a Transport Layer protocol that runs over this bus. Various Physical Layer Ethernet standards are also in this layer; Ethernet incorporates both this layer and the Data Link Layer. The same applies to other local-area networks, such as [token ring](http://en.wikipedia.org/wiki/IBM_token_ring), [FDDI](http://en.wikipedia.org/wiki/Fiber_distributed_data_interface), [ITU-T](http://en.wikipedia.org/wiki/ITU-T) [G.hn](http://en.wikipedia.org/wiki/G.hn) and [IEEE 802.11](http://en.wikipedia.org/wiki/IEEE_802.11), as well as personal area networks such as [Bluetooth](http://en.wikipedia.org/wiki/Bluetooth) and [IEEE 802.15.4](http://en.wikipedia.org/wiki/IEEE_802.15" \l "Task_group_4_.28Low_Rate_WPAN.29).

### Layer 2: Data Link Layer

The [Data Link Layer](http://en.wikipedia.org/wiki/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. Local area network architecture, which included broadcast-capable multi-access media, was developed independently of the ISO work in [IEEE Project 802](http://en.wikipedia.org/wiki/IEEE_802). IEEE work assumed [sub layering](http://en.wikipedia.org/wiki/Sublayer) and management functions not required for WAN use. In modern practice, only error detection, not flow control using sliding window, is present in data link protocols such as Point (PPP), and, on local area networks, the IEEE 802.2 [LLC](http://en.wikipedia.org/wiki/Logical_Link_Control) layer is not used for most protocols on the Ethernet, and on other local area networks, its flow control and acknowledgment mechanisms are rarely used. Sliding window flow control and acknowledgment is used at the Transport Layer by protocols such as [TCP](http://en.wikipedia.org/wiki/Transmission_Control_Protocol), but is still used in niches where [X.25](http://en.wikipedia.org/wiki/X.25) offers performance advantages.

The [ITU-T](http://en.wikipedia.org/wiki/ITU-T) [G.hn](http://en.wikipedia.org/wiki/G.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](http://en.wikipedia.org/wiki/Data_Link_Layer) which provides both error correction and flow control by means of a [selective repeat](http://en.wikipedia.org/wiki/Selective_repeat) [Sliding Window Protocol](http://en.wikipedia.org/wiki/Sliding_Window_Protocol).

Both WAN and LAN service arrange bits, from the Physical Layer, into logical sequences called frames. Not all Physical Layer bits necessarily go into frames, as some of these bits are purely intended for Physical Layer functions. For example, every fifth bit of the [FDDI](http://en.wikipedia.org/wiki/FDDI) bit stream is not used by the Layer.

#### WAN Protocol architecture

[Connection-oriented](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Sliding_window) flow control and acknowledgment mechanism to provide reliable delivery of frames; that is the case for [SDLC](http://en.wikipedia.org/wiki/Synchronous_Data_Link_Control) and [HDLC](http://en.wikipedia.org/wiki/HDLC), and derivatives of HDLC such as [LAPB](http://en.wikipedia.org/wiki/LAPB) and [LAPD](http://en.wikipedia.org/wiki/Link_Access_Procedures,_D_channel).

#### IEEE 802 LAN architecture

Practical, [connectionless](http://en.wikipedia.org/wiki/Connectionless) LANs began with the pre-IEEE [Ethernet](http://en.wikipedia.org/wiki/Ethernet) specification, which is the ancestor of [IEEE 802.3](http://en.wikipedia.org/wiki/IEEE_802.3). This layer manages the interaction of devices with a shared medium, which is the function of a [Media Access Control](http://en.wikipedia.org/wiki/Media_Access_Control) (MAC) sub layer. Above this MAC sub layer is the media-independent [IEEE 802.2](http://en.wikipedia.org/wiki/IEEE_802.2) [Logical Link Control](http://en.wikipedia.org/wiki/Logical_Link_Control) (LLC) sub layer, which deals with addressing and multiplexing on multi-access media.

While IEEE 802.3 is the dominant wired LAN protocol and [IEEE 802.11](http://en.wikipedia.org/wiki/IEEE_802.11) the wireless LAN protocol, obsolescent MAC layers include [Token Ring](http://en.wikipedia.org/wiki/Token_Ring) and [FDDI](http://en.wikipedia.org/wiki/FDDI). The MAC sub layer detects but does not correct errors.

### Layer 3: Network Layer

The [Network Layer](http://en.wikipedia.org/wiki/Network_Layer) provides the functional and procedural means of transferring variable length [data](http://en.wikipedia.org/wiki/Data) sequences from a source host on one network to a destination host on a different network, while maintaining the [quality of service](http://en.wikipedia.org/wiki/Quality_of_service) requested by the Transport Layer (in contrast to the data link layer which connects hosts within the same network). The Network Layer performs network [routing](http://en.wikipedia.org/wiki/Routing) functions, and might also perform fragmentation and reassembly, and report delivery errors. [Routers](http://en.wikipedia.org/wiki/Router_(computing)) operate at this layer—sending data throughout the extended network and making the Internet possible. This is a logical addressing scheme – values are chosen by the network engineer. The addressing scheme is not hierarchical.

Careful analysis of the Network Layer indicated that the Network Layer could have at least three sub layers:

1. Sub network Access – that considers protocols that deal with the interface to networks, such as X.25;
2. Sub network Dependent Convergence – when it is necessary to bring the level of a transit network up to the level of networks on either side;
3. Sub network Independent Convergence – which handles transfer across multiple networks.

The best example of this latter case is CLNP, or IPv7 ISO 8473. It manages the [connectionless](http://en.wikipedia.org/wiki/Connectionless_protocol) transfer of data one hop at a time, from end system to [ingress router](http://en.wikipedia.org/wiki/Ingress_router), router to router, and from [egress router](http://en.wikipedia.org/wiki/Egress_router) to destination end system. It is not responsible for reliable delivery to a next hop, but only for the detection of erroneous packets so they may be discarded. In this scheme, IPv4 and IPv6 would have to be classed with X.25 as subnet access protocols because they carry interface addresses rather than node addresses.

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](http://en.wikipedia.org/wiki/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.

Although not developed under the OSI Reference Model and not strictly conforming to the OSI definition of the Transport Layer, typical examples of Layer 4 are the [Transmission Control Protocol](http://en.wikipedia.org/wiki/Transmission_Control_Protocol) (TCP) and [User Datagram Protocol](http://en.wikipedia.org/wiki/User_Datagram_Protocol) (UDP).

Of the actual OSI protocols, there are five classes of connection-mode transport protocols ranging from class 0 (which is also known as TP0 and provides the least 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, both of which TCP is incapable. Detailed characteristics of TP0-4 classes are shown in the following table:[[4]](http://en.wikipedia.org/wiki/OSI_model" \l "cite_note-3)

Perhaps an easy way to visualize the Transport Layer is to compare it with a Post Office, which deals with the dispatch and classification of mail and parcels sent. Do remember, however, that a post office manages the outer envelope of mail. Higher layers may have the equivalent of double envelopes, such as cryptographic presentation services that can be read by the addressee only. Roughly speaking, [tunneling protocols](http://en.wikipedia.org/wiki/Tunneling_protocol) operate at the Transport Layer, such as carrying non-IP protocols such as [IBM](http://en.wikipedia.org/wiki/IBM)'s [SNA](http://en.wikipedia.org/wiki/IBM_Systems_Network_Architecture) or [Novell](http://en.wikipedia.org/wiki/Novell)'s [IPX](http://en.wikipedia.org/wiki/Internetwork_Packet_Exchange) over an IP network, or end-to-end encryption with [IPsec](http://en.wikipedia.org/wiki/IPsec). While [Generic Routing Encapsulation](http://en.wikipedia.org/wiki/Generic_Routing_Encapsulation) (GRE) might seem to be a Network Layer protocol, if the encapsulation of the payload takes place only at endpoint, GRE becomes closer to a transport protocol that uses IP headers but contains complete frames or packets to deliver to an endpoint. [L2TP](http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol) carries [PPP](http://en.wikipedia.org/wiki/Point-to-Point_Protocol) frames inside transport packet.

### Layer 5: Session Layer

The [Session Layer](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Duplex_(telecommunications)), [half-duplex](http://en.wikipedia.org/wiki/Half-duplex), or [simplex](http://en.wikipedia.org/wiki/Simplex_communication) operation, and establishes checkpointing, 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](http://en.wikipedia.org/wiki/Transmission_Control_Protocol), and also for session checkpointing 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](http://en.wikipedia.org/wiki/Remote_procedure_call).

### Layer 6: Presentation Layer

The [Presentation Layer](http://en.wikipedia.org/wiki/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.

This layer provides independence from data representation (e.g., [encryption](http://en.wikipedia.org/wiki/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.[[5]](http://en.wikipedia.org/wiki/OSI_model" \l "cite_note-4)

The original presentation structure used the basic encoding rules of [Abstract Syntax Notation One](http://en.wikipedia.org/wiki/Abstract_Syntax_Notation_One) (ASN.1), with capabilities such as converting an [EBCDIC](http://en.wikipedia.org/wiki/EBCDIC)-coded text [file](http://en.wikipedia.org/wiki/Computer_file) to an [ASCII](http://en.wikipedia.org/wiki/ASCII)-coded file, or [serialization](http://en.wikipedia.org/wiki/Serialization) of [objects](http://en.wikipedia.org/wiki/Object_(computer_science)) and other [data structures](http://en.wikipedia.org/wiki/Data_structure) from and to [XML](http://en.wikipedia.org/wiki/XML).

### Layer 7: Application Layer

The [Application Layer](http://en.wikipedia.org/wiki/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. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network or the requested communication exist. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer.

* TCP/IP REFRENCE MODEL

The **TCP/IP model** is a description framework for [computer network protocols](http://en.wikipedia.org/wiki/Protocol_(computing)) created in the 1970s by [DARPA](http://en.wikipedia.org/wiki/DARPA), an agency of the [United States Department of Defense](http://en.wikipedia.org/wiki/United_States_Department_of_Defense). It evolved from [ARPANET](http://en.wikipedia.org/wiki/ARPANET), which was the world's first [wide area network](http://en.wikipedia.org/wiki/Wide_area_network) and a predecessor of the [Internet](http://en.wikipedia.org/wiki/Internet). The [TCP/IP](http://en.wikipedia.org/wiki/TCP/IP) Model is sometimes called the *Internet Model* or the [*DoD*](http://en.wikipedia.org/wiki/United_States_Department_of_Defense)*Model.*

The TCP/IP model, or [Internet Protocol Suite](http://en.wikipedia.org/wiki/Internet_Protocol_Suite), describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a [network](http://en.wikipedia.org/wiki/Computer_network). TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, [routed](http://en.wikipedia.org/wiki/Routing) and received at the destination. Protocols exist for a variety of different types of communication services between computers.

TCP/IP has four [abstraction layers](http://en.wikipedia.org/wiki/Abstraction_layer) as defined in [RFC 1122](http://tools.ietf.org/html/rfc1122). This layer architecture is often compared with the seven-layer [OSI Reference Model](http://en.wikipedia.org/wiki/OSI_Reference_Model); using terms such as *Internet reference model*, incorrectly, however, because it is descriptive while the OSI Reference Model was intended to be prescriptive, hence being a reference model.

The TCP/IP model and related protocols are maintained by the [Internet Engineering Task Force](http://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) (IETF

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](http://en.wikipedia.org/wiki/Abstraction_(computer_science)) to isolate upper layer protocols from the nitty-gritty detail of transmitting bits over, for example, [Ethernet](http://en.wikipedia.org/wiki/Ethernet) and [collision detection](http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_detection), while the lower layers avoid having to know the details of each and every application and its protocol.

This abstraction also allows upper layers to provide services that the lower layers cannot, or choose not to, provide. Again, the original [OSI Reference Model](http://en.wikipedia.org/wiki/OSI_Reference_Model) was extended to include connectionless services (OSIRM CL).[[5]](http://en.wikipedia.org/wiki/TCP/IP_model" \l "cite_note-4)For example, IP is not designed to be reliable and is a [best effort delivery](http://en.wikipedia.org/wiki/Best_effort_delivery)protocol. This means that all transport layer implementations must choose whether or not to provide reliability and to what degree. UDP provides data integrity (via a [checksum](http://en.wikipedia.org/wiki/Checksum)) but does not guarantee delivery; TCP provides both data integrity and delivery guarantee (by retransmitting until the receiver acknowledges the reception of the packet).

This model lacks the formalism of the OSI reference model and associated documents, but the IETF does not use a formal model and does not consider this a limitation, as in the comment by [David D. Clark](http://en.wikipedia.org/wiki/David_D._Clark), "We reject: kings, presidents and voting. We believe in: rough consensus and running code." Criticisms of this model, which have been made with respect to the OSI Reference Model, often do not consider ISO's later extensions to that model.

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).[[6]](http://en.wikipedia.org/wiki/TCP/IP_model" \l "cite_note-5)
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) [[7]](http://en.wikipedia.org/wiki/TCP/IP_model" \l "cite_note-6)
3. The SSL/TLS library operates above the transport layer (uses TCP) but below application protocols. Again, there was no intention, on the part of the designers of these protocols, to comply with OSI architecture.
4. The link is treated like a black box here. This is fine for discussing IP (since the whole point of IP is it will run over virtually anything). The IETF explicitly does not intend to discuss transmission systems, which is a less academic but practical alternative to the OSI Reference Model.

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

### Link Layer

The [Link Layer](http://en.wikipedia.org/wiki/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. The processes of transmitting and receiving packets on a given link can be controlled both in the [software](http://en.wikipedia.org/wiki/Software) [device driver](http://en.wikipedia.org/wiki/Device_driver) for the [network card](http://en.wikipedia.org/wiki/Network_card), as well as on[firmware](http://en.wikipedia.org/wiki/Firmware) or specialized [chipsets](http://en.wikipedia.org/wiki/Chipsets). These will perform [data link](http://en.wikipedia.org/wiki/Data_Link_Layer) functions such as adding a [packet header](http://en.wikipedia.org/wiki/Packet_header) to prepare it for transmission, then actually transmit the frame over a [physical](http://en.wikipedia.org/wiki/Physical_Layer) [medium](http://en.wikipedia.org/wiki/Transmission_medium). The TCP/IP model includes specifications of translating the network addressing methods used in the Internet Protocol to data link addressing, such as [Media Access Control](http://en.wikipedia.org/wiki/Media_Access_Control) (MAC), however all other aspects below that level are implicitly assumed to exist in the Link Layer, but are not explicitly defined.

This is also the layer where packets may be selected to be sent over a [virtual private network](http://en.wikipedia.org/wiki/Virtual_private_network) or other [networking tunnel](http://en.wikipedia.org/wiki/Tunneling_protocol). In this scenario, the Link Layer data may be considered application data which traverses another instantiation of the IP stack for transmission or reception over another IP connection. Such a connection, or virtual link, may be established with a transport protocol or even an application scope protocol that serves as a [tunnel](http://en.wikipedia.org/wiki/Tunneling_protocol) in the Link Layer of the protocol stack. Thus, the TCP/IP model does not dictate a strict hierarchical encapsulation sequence.

### Internet Layer

The [Internet Layer](http://en.wikipedia.org/wiki/Internet_Layer) solves the problem of sending packets across one or more networks. [Internetworking](http://en.wikipedia.org/wiki/Internetworking) requires sending data from the source [network](http://en.wikipedia.org/wiki/Computer_network) to the destination network. This process is called [routing](http://en.wikipedia.org/wiki/Routing).[[8]](http://en.wikipedia.org/wiki/TCP/IP_model" \l "cite_note-7)

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](http://en.wikipedia.org/wiki/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.

IP can carry data for a number of different [upper layer protocols](http://en.wikipedia.org/wiki/Upper_layer_protocol). These protocols are each identified by a unique [protocol number](http://en.wikipedia.org/wiki/List_of_IP_protocol_numbers): for example, [Internet Control Message Protocol](http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol) (ICMP) and [Internet Group Management Protocol](http://en.wikipedia.org/wiki/Internet_Group_Management_Protocol) (IGMP) are protocols 1 and 2, respectively.

Some of the protocols carried by IP, such as ICMP (used to transmit diagnostic information about IP transmission) and IGMP (used to manage [IP Multicast](http://en.wikipedia.org/wiki/IP_Multicast) data) are layered on top of IP but perform internetworking functions. This illustrates the differences in the architecture of the TCP/IP stack of the Internet and the OSI model.

### Transport Layer

The [Transport Layer](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Connection-oriented), implemented in [Transmission Control Protocol](http://en.wikipedia.org/wiki/Transmission_Control_Protocol) (TCP), or [connectionless](http://en.wikipedia.org/wiki/Connectionless), implemented in [User Datagram Protocol](http://en.wikipedia.org/wiki/User_Datagram_Protocol) (UDP).

The Transport Layer can be thought of as a transport mechanism, e.g., a vehicle with the responsibility to make sure that its contents (passengers/goods) reach their destination safely and soundly, unless another protocol layer is responsible for safe delivery.

The Transport Layer provides this service of connecting applications through the use of [service ports](http://en.wikipedia.org/wiki/TCP_and_UDP_port). Since IP provides only a [best effort delivery](http://en.wikipedia.org/wiki/Best_effort_delivery), the Transport Layer is the first layer of the TCP/IP stack to offer reliability. IP can run over a reliable data link protocol such as the[High-Level Data Link Control](http://en.wikipedia.org/wiki/High-Level_Data_Link_Control) (HDLC). Protocols above transport, such as RPC, also can provide reliability.

For example, the Transmission Control Protocol (TCP) is a connection-oriented protocol that addresses numerous reliability issues to provide a [reliable byte stream](http://en.wikipedia.org/wiki/Reliable_byte_stream):

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

The newer [Stream Control Transmission Protocol](http://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol) (SCTP) is also a reliable, connection-oriented transport mechanism. It is [Message-stream-oriented](http://en.wikipedia.org/w/index.php?title=Message-stream-oriented&action=edit&redlink=1) — not [byte-stream-oriented](http://en.wikipedia.org/w/index.php?title=Byte-stream-oriented&action=edit&redlink=1) like TCP — and provides multiple streams multiplexed over a single connection. It also provides [multi-homing](http://en.wikipedia.org/wiki/Multi-homed) support, in which a connection end can be represented by multiple [IP addresses](http://en.wikipedia.org/wiki/IP_address) (representing multiple physical interfaces), such that if one fails, the connection is not interrupted. It was developed initially for telephony applications (to transport [SS7](http://en.wikipedia.org/wiki/Signaling_System_7) over [IP](http://en.wikipedia.org/wiki/Internet_Protocol)), but can also be used for other applications.

User Datagram Protocol is a connectionless [datagram](http://en.wikipedia.org/wiki/Datagram) protocol. Like IP, it is a best effort, "unreliable" protocol. Reliability is addressed through [error detection](http://en.wikipedia.org/wiki/Error_detection) using a weak [checksum](http://en.wikipedia.org/wiki/Checksum) algorithm. UDP is typically used for applications such as streaming media (audio, video,[Voice over IP](http://en.wikipedia.org/wiki/Voice_over_IP) etc) where on-time arrival is more important than reliability, or for simple query/response applications like [DNS](http://en.wikipedia.org/wiki/Domain_Name_System) lookups, where the overhead of setting up a reliable connection is disproportionately large. [Real-time Transport Protocol](http://en.wikipedia.org/wiki/Real-time_Transport_Protocol) (RTP) is a datagram protocol that is designed for real-time data such as [streaming audio and video](http://en.wikipedia.org/wiki/Streaming_media).

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. For example, the [File Transfer Protocol](http://en.wikipedia.org/wiki/File_Transfer_Protocol) expects a reliable connection, but the [Network File System](http://en.wikipedia.org/wiki/Network_File_System_(protocol)) (NFS) assumes that the subordinate [Remote Procedure Call](http://en.wikipedia.org/wiki/Remote_Procedure_Call) protocol, not transport, will guarantee reliable transfer. Other applications, such as VoIP, can tolerate some loss of packets, but not the reordering or delay that could be caused by retransmission.

The applications at any given network address are distinguished by their TCP or UDP [port](http://en.wikipedia.org/wiki/TCP_and_UDP_port). By convention certain *well known ports* are associated with specific applications. (*See*[*List of TCP and UDP port numbers*](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)*.*)

### Application Layer

The [Application Layer](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/File_Transfer_Protocol) (FTP) and the [Simple Mail Transfer Protocol](http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol) (SMTP).[[9]](http://en.wikipedia.org/wiki/TCP/IP_model" \l "cite_note-8) Data coded according to application layer protocols are then [encapsulated](http://en.wikipedia.org/wiki/Encapsulation_(networking)) into one or (occasionally) more transport layer protocols (such as the [Transmission Control Protocol](http://en.wikipedia.org/wiki/Transmission_Control_Protocol)(TCP) or [User Datagram Protocol](http://en.wikipedia.org/wiki/User_Datagram_Protocol) (UDP)), which in turn use [lower layer protocols](http://en.wikipedia.org/wiki/Lower_layer_protocol) to effect actual data transfer.

Since the IP stack defines no layers between the application and transport layers, the application layer must include any protocols that act like the OSI's presentation and session layer protocols. This is usually done through [libraries](http://en.wikipedia.org/wiki/Library_(computer_science)).

Application Layer protocols generally treat the transport layer (and lower) protocols as "[black boxes](http://en.wikipedia.org/wiki/Black_Box)" which provide a stable network connection across which to communicate, although the applications are usually aware of key qualities of the transport layer connection such as the [end point](http://en.wikipedia.org/wiki/Transport_Layer) [IP addresses](http://en.wikipedia.org/wiki/IP_Address) and [port numbers](http://en.wikipedia.org/wiki/Port_number). As noted above, layers are not necessarily clearly defined in the Internet protocol suite. Application layer protocols are most often associated with [client–server](http://en.wikipedia.org/wiki/Client–server) applications, and the commoner [servers](http://en.wikipedia.org/wiki/Server_(computing)) have specific [ports](http://en.wikipedia.org/wiki/TCP_and_UDP_port) assigned to them by the [IANA](http://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority): [HTTP](http://en.wikipedia.org/wiki/HyperText_Transfer_Protocol) has port 80; [Telnet](http://en.wikipedia.org/wiki/Telnet) has port 23; etc. [Clients](http://en.wikipedia.org/wiki/Client_(computing)), on the other hand, tend to use [ephemeral ports](http://en.wikipedia.org/wiki/Ephemeral_port), i.e. port numbers assigned at random from a range set aside for the purpose.

Transport and lower level layers are largely unconcerned with the specifics of application layer protocols. [Routers](http://en.wikipedia.org/wiki/Router_(computing)) and [switches](http://en.wikipedia.org/wiki/Network_switch) 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. However, some [firewall](http://en.wikipedia.org/wiki/Firewall_(computing)) and [bandwidth throttling](http://en.wikipedia.org/wiki/Bandwidth_throttling) applications do try to determine what's inside, as with the [Resource Reservation Protocol](http://en.wikipedia.org/wiki/Resource_Reservation_Protocol)(RSVP). It's also sometimes necessary for [Network Address Translation](http://en.wikipedia.org/wiki/Network_Address_Translation) (NAT) facilities to take account of the needs of particular application layer protocols. (NAT allows hosts on private networks to communicate with the outside world via a single visible IP address using [port forwarding](http://en.wikipedia.org/wiki/Port_forwarding), and is an almost ubiquitous feature of modern domestic [broadband routers](http://en.wikipedia.org/wiki/Broadband_router))

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

The three top layers in the OSI model—the [Application Layer](http://en.wikipedia.org/wiki/Application_Layer), the [Presentation Layer](http://en.wikipedia.org/wiki/Presentation_Layer) and the [Session Layer](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Network_File_System) (NFS) application protocol runs over the [eXternal Data Representation](http://en.wikipedia.org/wiki/External_Data_Representation) (XDR) presentation protocol, which, in turn, runs over a protocol with Session Layer functionality, [Remote Procedure Call](http://en.wikipedia.org/wiki/Remote_Procedure_Call) (RPC). RPC provides reliable record transmission, so it can run safely over the best-effort [User Datagram Protocol](http://en.wikipedia.org/wiki/User_Datagram_Protocol) (UDP) transport.

The Session Layer roughly corresponds to the Telnet [virtual terminal](http://en.wikipedia.org/wiki/Virtual_terminal) functionality[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)], which is part of text based protocols such as the [HTTP](http://en.wikipedia.org/wiki/HTTP) and [SMTP](http://en.wikipedia.org/wiki/SMTP) TCP/IP model Application Layer protocols. It also corresponds to TCP and UDP port numbering, which is considered as part of the transport layer in the TCP/IP model. Some functions that would have been performed by an OSI presentation layer are realized at the Internet application layer using the [MIME](http://en.wikipedia.org/wiki/MIME) standard, which is used in application layer protocols such as [HTTP](http://en.wikipedia.org/wiki/HTTP) and [SMTP](http://en.wikipedia.org/wiki/SMTP).

Since the IETF protocol development effort is not concerned with strict layering, some of its protocols may not appear to fit cleanly into the OSI model. These conflicts, however, are more frequent when one only looks at the original OSI model, ISO 7498, without looking at the annexes to this model (e.g., ISO 7498/4 Management Framework), or the ISO 8648 Internal Organization of the Network Layer (IONL). When the IONL and Management Framework documents are considered, the [ICMP](http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol) and [IGMP](http://en.wikipedia.org/wiki/Internet_Group_Management_Protocol) are neatly defined as layer management protocols for the network layer. In like manner, the IONL provides a structure for "subnetwork dependent convergence facilities" such as [ARP](http://en.wikipedia.org/wiki/Address_Resolution_Protocol) and [RARP](http://en.wikipedia.org/wiki/Reverse_Address_Resolution_Protocol).

IETF protocols can be encapsulated recursively, as demonstrated by tunneling protocols such as [Generic Routing Encapsulation](http://en.wikipedia.org/wiki/Generic_Routing_Encapsulation) (GRE). While basic OSI documents do not consider tunneling, there is some concept of tunneling in yet another extension to the OSI architecture, specifically the transport layer gateways within the International Standardized Profile framework.[[10]](http://en.wikipedia.org/wiki/TCP/IP_model" \l "cite_note-9) The associated OSI development effort, however, has been abandoned given the overwhelming adoption of TCP/IP protocols

* 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.Within the network,the IP address is interpreted in a binary format consisting of o and 1 .Any device which is connected to the network,such as a computer,router,or printer has an IP address for identification.

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

11111111.11111111.11111111.00000000(contains max. network bits)The 1s represents network bits and 0s represents host bits….

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CLASS | 1st bits | Network bits | Host bits | Intial 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 there 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 bit is reserved for broadcasting

* **SUBNETTING**

The process of breaking down a single network address into(our)separate network addresses is called subnetting.we increases 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 addresses.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.

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.

If company have 6 departments,each department wants to be 150 networks.Future plans will have a growth of company expanding in 4 regions having independent departments.(1 department have 5 Pc’s in it).IP range-196.11.12.0/24

SUBNETTING FOR THE COMPANY NEED:

Subnet=5

Host=30

Range of IP=192.11.12.0/24

Subnet mask=?Given subnet mask=255.255.255.0

Calculating subnet mask,no. of host<=2n-2 in each network.

n=host bit

30=2n-2

32=2n

n=25

n=5…..

Given host bit=8

Calculated host bit=5

Therefore, 8 bit will be moved to network bit=24+3=27

11111111.11111111.11111111.11100000

255.255.255.224

Decreasing host bits known as subnetting.

Private IP Address is provided by IETE:

CLASS A 10.0.0.1 - 10.255.255.255

CLASS B 172.16.0.1-172.31.255.255

CLASS C 192.168.0.1-192.168.255.255

|  |  |
| --- | --- |
| |  | | --- | | 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](http://www.orbit-computer-solutions.com/Subnetting-IP-addresses.php).   Variable Length Subnet Mask (VLSM) in a way, means subnetting a subnet. To simplify futher, 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.  Before you can understand VLSM, you have to be very familiar with [IP address](http://www.orbit-computer-solutions.com/IP-Addressing.php) structure.  The best way you can learn how to subnet a subnet (VLSM) is with examples. Lets work with the diagram below:    VLSM Explained | |

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](http://www.orbit-computer-solutions.com/The-Internet---A-Network-of-Networks.php) allocated 192.168.1.0/24. Class C

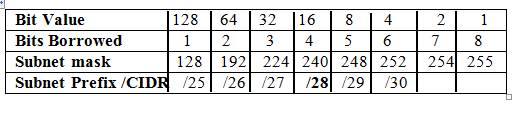
HQ = 50 host

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!



Lets begin with **HQ** with 50 hosts, using the table above:

We are borrowing 2 bits with value of 64. This is the closest we can get for 50 hosts.

HQ - 192.168.1.0 /26 Network address

HQ = **192.168.1.1** Gateway address

**192.168.1.2**, First usable address

**192.168.1.62**- Last usable address. Total address space -192.168.1.2 to 192.168.1.62

**192.168.1.63** will be the broadcast address (remember to reserve the first and last address for the Network and Broadcast)

HQ **Network Mask 255.255.255.192**  - we got the **192** by adding the bit value from the left to the value we borrowed = 128+64=192

HQ address will look like this 192.168.1.0 /26

**RO1** = 30 hosts

We are borrowing 3 bits with value of 32; this again is the closest we can get to the number of host needed.

RO1 address will start from **192.168.1.64** -  Network address

Now we add the 32 to the 64 we borrowed earlier = 32+64 = 96

RO1 = 192.168.1.65 Gateway address

192.168.1.66 - First usable IP address

192.168.1.94 - Last usable IP address

192.168.1.95 Broadcast address – total address space – 192.168.1.66 –192.168.1. 94

Network Mask 255.255.255.224 I.e. 128+64+32=224 or  192.168.1.64/27

**RO2** = 192.168.1.96 Network address

We borrow 4 bits with the value of 16. That’s the closest we can go.

**96+16= 112**

So, 192.168.1.97- Gateway address

192.168.1.98 - First usable address

192.168.1.110 - Last usable address

192.168.1.111 broadcast

Total host address space – 192.168.1.98 to 192.168.1.110

Network Mask 255.255.255.**240** or 192.168.1.96 /28

**WAN links** = we are borrowing 6 bit with value of 4

=**112 + 4 =116**

WAN links from HQ to RO1 Network address will be 192.168.1.112 /30 :

HQ se0/0 = 192.168.1.113

RO1 se0/0= 192.168.1.114

Mask for both links=  255.255.255.**252** ( we got 252 by adding the bits value we borrowed i.e

124 +64 +32 +16+ 8 +4=252

**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

Firewall is a software application that watches the traffic in between the server and host machine and examines against the patterns of suspicious activity. Typical port scanner software requires a separate installation and a highly specific and dedicated system to watch packets traveling across a single network segment. The system only monitors the network segment it is installed on.

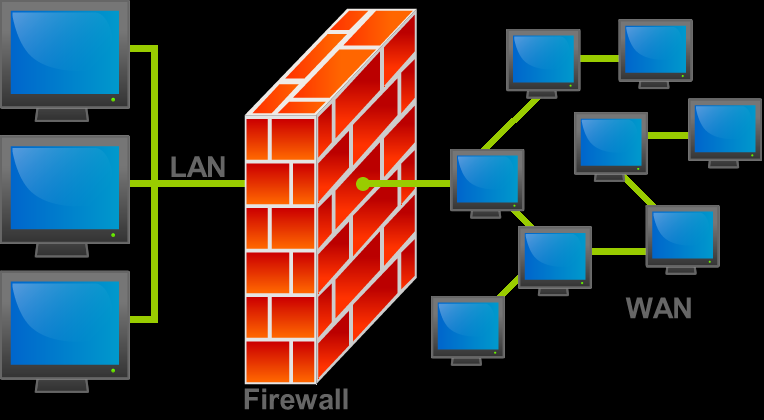
All firewall systems which were tested were found to be susceptible to packet spoofing which tricks the server into thinking packets have come from a trusted host, or into using its intrusion-detection counter measures to cut connectivity to legitimate sites.

Detection mainly via sending packets (requests) and collecting responses from 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 and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass.

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions

Firewalll are just a mordern adaptation of that old medieval security standby: digging moat around your castle.This designed forced everyone entering or leavingthe castle to pass over a single drawbridge, where they could be inspected by the I/o police . twith networks, the same trick is possible : a company can have many LANs connected in arbitary ways, but all traffic to or from the company is forced through an electronic drawbridge.



**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 fairly basic system was the first generation of what became a highly evolved and technical internet security feature. At **AT&T Bell Labs**, **Bill Cheswick** and **Steve Bellovin** were continuing their research in packet filtering and developed a working model for their own company based on their original first generation architecture.

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 itself (most commonly using a combination of the packet's source and destination address, its protocol, and, for TCP and UDP traffic, the port number).

TCP and UDP protocols constitute most communication over the Internet, and because TCP and UDP traffic by convention uses well known ports for particular types of traffic, a "stateless" packet filter can distinguish between, and thus control, those types of traffic (such as web browsing, remote printing, email transmission, file transfer), unless the machines on each side of the packet filter are both using the same non-standard ports.

Packet filtering firewalls work mainly on the first three layers of the OSI reference model, which means most of the work is done between the network and physical layers, with a little bit of peeking into the transport layer to figure out source and destination port numbers. When a packet originates from the sender and filters through a firewall, the device checks for matches to any of the packet filtering rules that are configured in the firewall and drops or rejects the packet accordingly. When the packet passes through the firewall, it filters the packet on a protocol/port number basis (GSS). For example, if a rule in the firewall exists to block telnet access, then the firewall will block the IP protocol for port number 23esearch in packet filtering and developed a working model for their own company based on their original first generation architecture.

**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 down to the physical Layer. This is similar to a packet filter firewall but here we can also filter information on the basis of content. Good examples of application firewalls are MS-ISA (Internet Security and Acceleration) server, McAfee Firewall Enterprise & Palo Alto PS Series firewalls. An application firewall can filter higher-layer protocols such as FTP, Telnet, DNS, DHCP, HTTP, TCP, UDP and TFTP (GSS). For example, if an organization wants to block all the information related to "foo" then content filtering can be enabled on the firewall to block that particular word. Software-based firewalls (MS-ISA) are much slower than hardware based stateful firewalls but dedicated appliances (McAfee & Palo Alto) provide much higher performance levels for Application Inspection.

In 2009/2010 the focus of the most comprehensive firewall security vendors turned to expanding the list of applications such firewalls are aware of now covering hundreds and in some cases thousands of applications which can be identified automatically. Many of these applications can not only be blocked or allowed but manipulated by the more advanced firewall products to allow only certain functionality enabling network security administrations to give users functionality without enabling unnecessary vulnerabilities. As a consequence these advanced version of the "Second Generation" firewalls are being referred to as "Next Generation" and surpass the "Third Generation" firewall. It is expected that due to the nature of malicious communications this trend will have to continue to enable organizations to be truly secure.

**Third generation: "stateful" filters**

From 1989-1990 three colleagues from **AT&T Bell Laboratories**, Dave Presetto, Janardan Sharma, and Kshitij Nigam, developed the third generation of firewalls, calling them **circuit level firewalls**.

Third-generation firewalls, in addition to what first- and second-generation look for, regard placement of each individual packet within the packet series. This technology is generally referred to as a **stateful packet inspection** as it maintains records of all connections passing through the firewall and is able to determine whether a packet is the start of a new connection, a part of an existing connection, or is an **invalid packet**. Though there is still a set of static rules in such a firewall, the state of a connection can itself be one of the criteria which trigger specific rules.

This type of firewall can actually be exploited by certain **Denial-of-service attacks** which can fill the connection tables with illegitimate connections

**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

Windows or Apple's MacOS. In **1994** an **Israeli company** called **Check Point Software Technologies** built this into readily available software known as FireWall-1.

The existing deep packet inspection functionality of modern firewalls can be shared by **Intrusion-prevention systems** (IPS).

Currently, the Middlebox Communication Working Group of **the Internet Engineering Task Force** (IETF) is working on standardizing protocols for managing firewalls and other middleboxes.

Another axis of development is about integrating identity of users into Firewall rules. Many firewalls provide such features by binding user identities to IP or MAC addresses, which is very approximate and can be easily turned around. The NuFW firewall provides real identity-based firewalling, by requesting the user's signature for each connection. authpf on BSD systems loads firewall rules dynamically per user, after authentication via SSH.

**FIREWALLL CONFIGURATION**

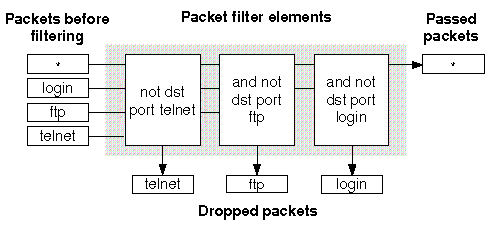
A basic firewalll configuration consist of two components

* Two routers that do packet filtering
* An appplication 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.

The point of putting the two packet filters on different LANs is to ensure that no packet gets in or out without having to pass through the application gateway: there is no path around it

Packet filters are typically driven by tables configured by the system administrator. these tables list sources and destination that are acceptable, sources and destination that are blocked, and default rules about what to do wit packets coming rom or goin to other machine.

**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.

The client then negotiates with the proxy server in order to communicate with the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall.

This creates two connections: one between the client and the proxy server and one between the proxy server and the destination. Once connected, the proxy makes all packet-forwarding decisions. Since all communication is conducted through the proxy server, computers behind the firewall are protected.

While this is considered a highly secure method of firewall protection, application gateways require great memory and processor resources compared to other firewall technologies, such as stateful inspection.

In the context of computer networking, an application-level gateway (also known as **ALG or application layer gateway**) consists of a security component that augments a firewall or **NAT** employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as **FTP**, **BitTorrent**, **SIP**, **RTSP**, file transfer in IM applications etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (**firewall pinhole**) dynamically as required.

Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

An ALG may offer the following functions:

* Allowing client applications to use dynamic ephemeral TCP/ UDP ports to communicate with the known ports used by the server applications, even though a firewall-configuration may allow only a limited number of known ports. In the absence of an ALG, either the ports would get blocked or the network administrator would need to explicitly open up a large number of ports in the firewall — rendering the network vulnerable to attacks on those ports.
* Converting the 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
* Synchronizing between multiple streams/sessions of data between two hosts exchanging data. For example, an FTP application may use separate connections for passing control commands and for exchanging data between the client and a remote server. During large file transfers, the control connection may remain idle. An ALG can prevent the control connection getting timed out by network devices before the lengthy file transfer completes.

**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.

For instance, for (SIP) Back-to-Back User agent (B2BUA), an ALG can allow firewall traversal with SIP. If the firewall has its SIP traffic terminated on an ALG then the responsibility for permitting SIP sessions passes to the ALG instead of the firewall. An ALG can solve another major SIP headache: NAT traversal. Basically a NAT with a builtin ALG can rewrite information within the SIP messages and can hold address-bindings[disambiguation needed] until the session terminates.

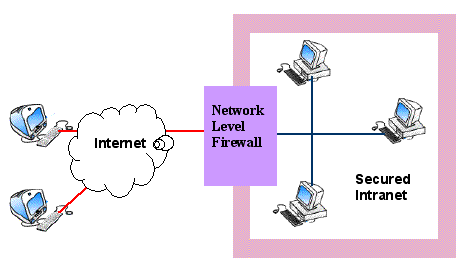
An ALG is very similar to a proxy server, as it sits between the client and real server, facilitating the exchange. There seems to be an industry convention that an ALG does its job without the application being configured to use it, by intercepting the messages. A proxy, on the other hand, usually needs to be configured in the client application. The client is then explicitly aware of the proxy and connects to it, rather than the real server.

**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. Other firewall software is designed to run on proprietary hardware that you have to buy along with the software, turning the bundle into a "security appliance." As a general rule, appliances are faster, easier to install and operate — and also more expensive. But there's no guarantee that an appliance will do a better job than a software-only firewall. Software firewalls tend to be more flexible, and it's easier to upgrade the hardware it's running on.

**Network-Level Firewalls:**

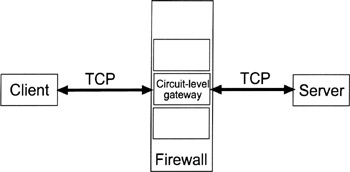
The first generation of firewalls (c. 1988) worked at the network level by inspecting packet headers and filtering traffic based on the IP address of the source and the destination, the port and the service. Some of these primeval security applications could also filter packets based on protocols, the 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 and XML, and they are capable of decoding SSL-encrypted packets to examine their content. As a result, they can’t validate user inputs or detect maliciously modified parameters in an URL request. This leaves your network vulnerable to a number of serious threats**.**

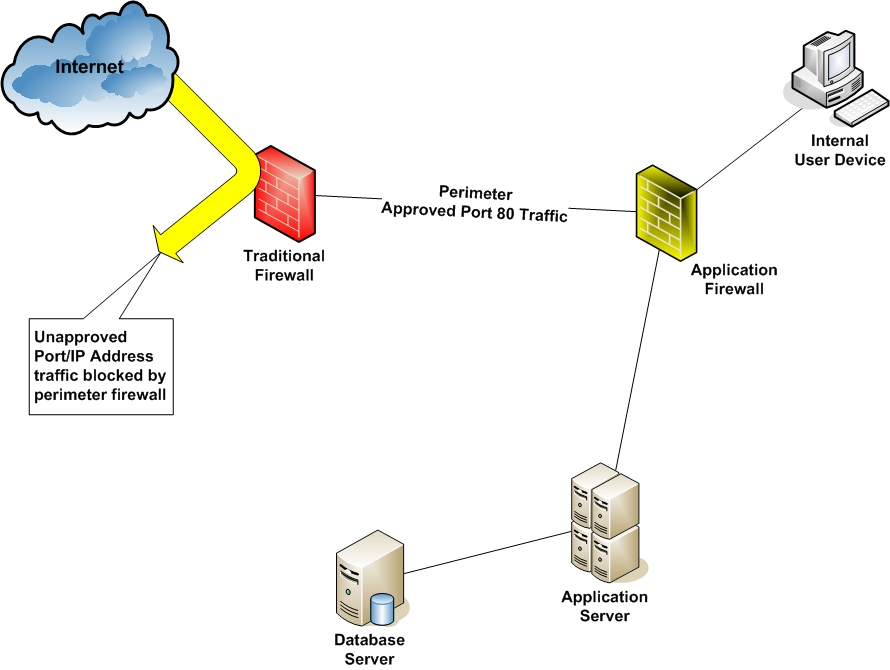
**Circuit-Level Firewalls:**

These applications, which represent the second-generation of firewall technology, monitor TCP handshaking between packets to make sure a session is legitimate. Traffic is filtered based on specified session rules and may be restricted to recognized computers only. Circuit-level firewalls hide the network itself from the outside, which is useful for denying access to intruders. But they don't filter individual packets.



**Application-Level Firewalls:**

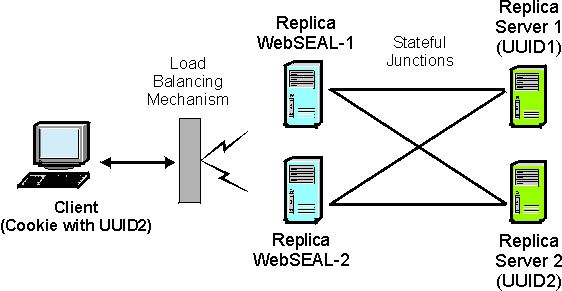
Recently, application-level firewalls (sometimes called proxies) have been looking more deeply into the application data going through their filters. By considering the context of client requests and application responses, these firewalls attempt to enforce correct application behavior, block malicious activity and help organizations ensure the safety of sensitive information and systems. They can log user activity too. Application-level filtering may include protection against spam and viruses as well, and be able to block undesirable Web sites based on content rather than just their IP

address.

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. This is why the highest-end security appliances include lots of RAM to speed packet processing. And of course you'll pay for the added chips.

**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 and they recognize and process application-level data, but since they don't employ proxies, they deliver reasonably good performance in spite of the deep packet analysis. On the downside, they are not cheap, and they can be difficult to configure and administer



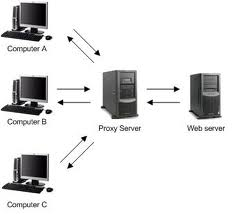
**PROXIES:**

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, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client. A proxy server may optionally alter the client's request or the server's response, and sometimes it may serve the request without contacting the specified server. In this case, it 'caches' responses from the remote server, and returns subsequent requests 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 speed up access to resources (using caching). Web proxies are commonly used to cache web pages from a web server.[2]
* To apply access policy to network services or content, e.g. to block undesired sites.
* To log / audit usage, i.e. to provide company employee Internet usage reporting.
* To bypass security / parental controls.
* To scan transmitted content for malware before delivery.
* To scan outbound content, e.g., for data leak protection.
* To circumvent regional restrictions.

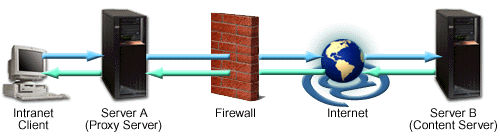
To allow a web site to make web requests to externally hosted resources (e.g. images, music files, etc.) when cross-domain restrictions prohibit the web site from linking directly to the outside domains.  
  
  


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 between the user and the destination servers on the Internet.

A reverse proxy is (usually) an Internet-facing proxy used as a front-end to control and protect access to a server on a private network, commonly also performing tasks such as load-balancing, authentication, decryption or caching**.**

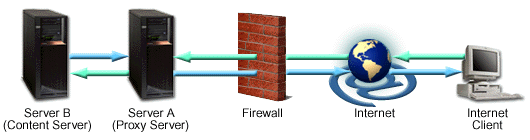
* **TYPES OF PROXY:**
* **FORWARD PROXY-**



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).

The terms "forward proxy" and "forwarding proxy" are a general description of behaviour (forwarding traffic) and thus ambiguous. Except for Reverse proxy, the types of proxies described on this article are more specialized sub-types of the general forward proxy concept

* **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]

Reverse proxies are installed in the neighborhood of one or more web servers. All traffic coming from the Internet and with a destination of one of the web servers goes through the proxy server. The use of "reverse" originates in its counterpart "forward proxy" since the reverse proxy sits closer to the web server and serves only a restricted set of websites.

* **OPEN PROXY**



An open proxy is a forwarding proxy server that is accessible by any Internet user. Gordon Lyon estimates there are "hundreds of thousands" of open proxies on the Internet. An anonymous open proxy allows users to conceal their IP address while browsing the Web or using other Internet services.

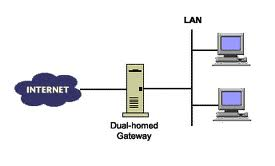
**Modes of operation**

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 are allowed to pass through the firewall. The“textbook” recommendation is to run default deny, but such a policy would intuitively be in stark contrast to the notion of“academic freedom”.As a result, the vast majority of UK

**Firewall Configurations-**

**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. Only

applications with proxy services on the application gateway are able to operate

through the firewall. Since IP forwarding is disabled in the host, IP packets must be

directed to one of the proxy servers on the host, or be rejected. Some manufacturers

build the packet filtering capability and the application proxies into one box, thereby

simplifying the design (but removing the possibility of having an optional info server

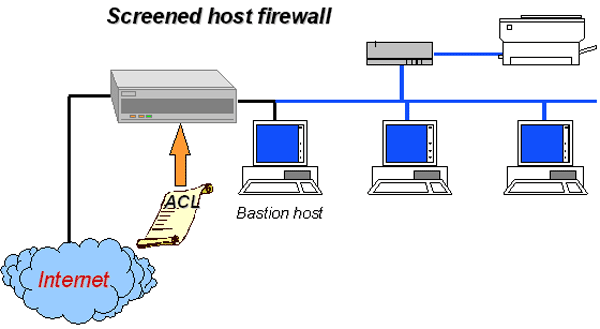
and modems attached to the screened subnet. The disadvantages of the

dual homed gateway are that it may be a bottleneck to performance, and it may be too

secure for some sites (!) since it is not possible to let trusted applications bypass the

firewall and communicate directly with peers on the Internet. They must have a proxy

**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. In this design the application gateway only

needs a single network connection

The IP router will normally be configured to pass Internet traffic to the application

gateway or to reject it. Traffic from the corporate network to the Internet will also be

rejected, unless it originates from the application gateway. The only exception to

these rules will be for trusted traffic that will be allowed straight through.