COMPUTER NETWORKS

DATA COMMUNICATIONS

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. Delivery. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. Accuracy. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. Timeliness. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
4. Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

डेटा संचार दो उपकरणों के बीच डेटा के आदान-प्रदान के माध्यम से होता है, जैसे कि ट्रांसमिशन केबल। डेटा संचार होने के लिए, संचार उपकरण हार्डवेयर (भौतिक उपकरण) और सॉफ्टवेयर (प्रोग्राम) के संयोजन से बने संचार प्रणाली का हिस्सा होना चाहिए। डेटा संचार प्रणाली की प्रभावशीलता चार मौलिक विशेषताओं पर निर्भर करती है: वितरण, सटीकता, समयबद्धता और घबराहट।

1. Delivery - सिस्टम को सही गंतव्य तक डेटा पहुंचाना होगा। डेटा केवल इच्छित डिवाइस या उपयोगकर्ता द्वारा प्राप्त किया जाना चाहिए और केवल उस डिवाइस या उपयोगकर्ता द्वारा प्राप्त किया जाना चाहिए।

2. Accuracy. सिस्टम को डेटा को सही तरीके से वितरित करना चाहिए। डेटा जो ट्रांसमिशन में बदल दिया गया है और बिना ठीक किए छोड़ दिया गया है वह अनुपयोगी है।

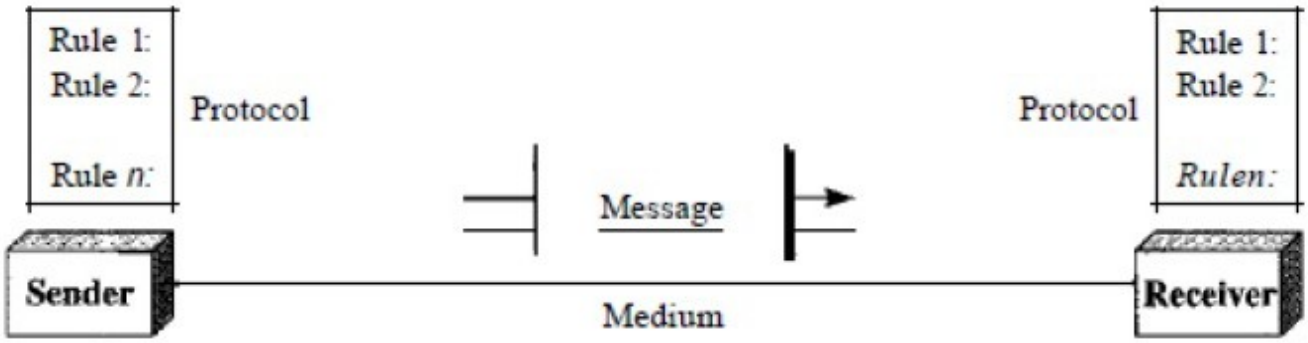
3. Timeliness- सिस्टम को समय पर डेटा देना होगा। देरी से दिया गया डेटा बेकार है। वीडियो और ऑडियो के मामले में, समय पर डिलीवरी का मतलब है कि वे उत्पादित किए गए डेटा को वितरित कर रहे हैं, उसी क्रम में जो वे उत्पादित किए जाते हैं, और महत्वपूर्ण देरी के बिना। इस तरह की डिलीवरी को रियल-टाइम ट्रांसमिशन कहा जाता है।

4. Jitter -जिटर पैकेट आगमन समय में भिन्नता को दर्शाता है। यह ऑडियो या वीडियो पैकेट के वितरण में असमान देरी है।

Components:

A data communications system has five components-

अवयव:- एक डेटा संचार प्रणाली में पाँच घटक होते हैं



1. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video. संदेश संचारित होने वाली सूचना (डेटा) है। सूचना के लोकप्रिय रूपों में पाठ, संख्याएं, चित्र, ऑडियो और वीडियो शामिल हैं।

2. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on. प्रेषक वह उपकरण है जो डेटा संदेश भेजता है। यह एक कंप्यूटर, वर्कस्टेशन, टेलीफोन हैंडसेट, वीडियो कैमरा, आदि हो सकता है।

3. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on. रिसीवर वह डिवाइस है जो संदेश प्राप्त करता है। यह एक कंप्यूटर, वर्कस्टेशन, टेलीफोन हैंडसेट, टेलीविज़न इत्यादि हो सकता है।

4. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves ट्रांसमिशन माध्यम वह भौतिक पथ है जिसके द्वारा एक संदेश प्रेषक से रिसीवर तक जाता है। ट्रांसमिशन मीडिया के कुछ उदाहरणों में मुड़-जोड़ी तार, समाक्षीय केबल, फाइबर-ऑप्टिक केबल और रेडियो तरंगें शामिल हैं

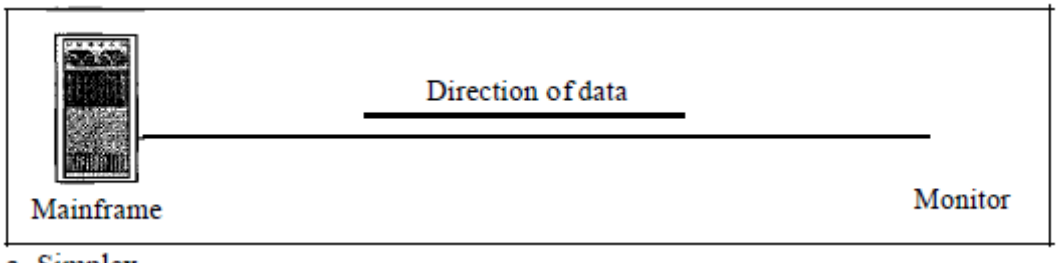
5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. एक प्रोटोकॉल नियमों का एक समूह है जो डेटा संचार को नियंत्रित करता है। यह संचार उपकरणों के बीच एक समझौते का प्रतिनिधित्व करता है।

DATA TRANSMISSION MODES

Communication between two devices can be simplex, half-duplex, or full-duplex. दो उपकरणों के बीच संचार सरल, आधा-द्वैध या पूर्ण-द्वैध हो सकता है।

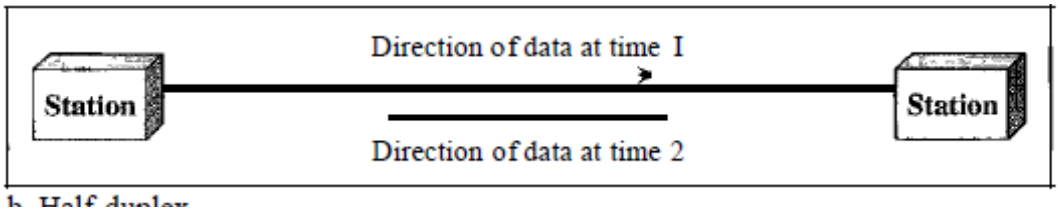
Simplex:

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction. सिम्प्लेक्स मोड में, संचार एक-तरफ़ा है, जैसा कि एक-तरफ़ा सड़क पर है। लिंक पर दो उपकरणों में से केवल एक ही संचारित हो सकता है; अन्य केवल प्राप्त कर सकते हैं। कीबोर्ड और पारंपरिक मॉनिटर सिंप्लेक्स उपकरणों के उदाहरण हैं। कीबोर्ड केवल इनपुट पेश कर सकता है; मॉनिटर केवल आउटपुट स्वीकार कर सकता है। सिम्प्लेक्स मोड एक दिशा में डेटा भेजने के लिए चैनल की संपूर्ण क्षमता का उपयोग कर सकता है।



Half-Duplex:

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction. आधे-द्वैध मोड में, प्रत्येक स्टेशन संचारित और प्राप्त कर सकता है, लेकिन एक ही समय में नहीं। जब एक उपकरण भेज रहा है, तो दूसरा केवल प्राप्त कर सकता है, और इसके विपरीत। आधे-द्वैध संचरण में, एक चैनल की पूरी क्षमता को दो उपकरणों में से जो भी उस समय संचारित होता है, द्वारा लिया जाता है। वाकी-टॉकी और सीबी (नागरिक बैंड) रेडियो दोनों अर्ध-द्वैध प्रणाली हैं। आधे-द्वैध मोड का उपयोग उन मामलों में किया जाता है जहां एक ही समय में दोनों दिशाओं में संचार की आवश्यकता नहीं होती है; चैनल की संपूर्ण क्षमता का उपयोग प्रत्येक दिशा के लिए किया जा सकता है।

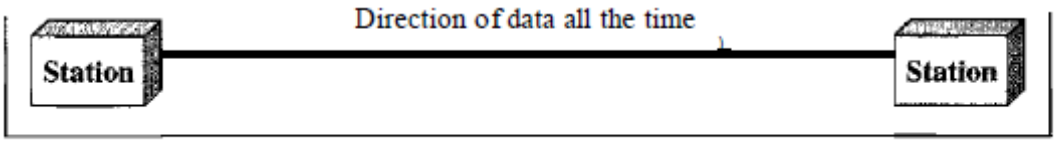


Full-Duplex:

In full-duplex both stations can transmit and receive simultaneously. The full-duplex mode is like a two way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when

communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

पूर्ण-द्वैध में दोनों स्टेशन एक साथ संचारित और प्राप्त कर सकते हैं। फुल-डुप्लेक्स मोड एक दो तरह की सड़क है, जिसमें एक ही समय में दोनों दिशाओं में ट्रैफ़िक बहता है। पूर्ण-द्वैध मोड में, एक दिशा में जाने वाले संकेत लिंक की क्षमता साझा करते हैं: संकेतों के साथ दूसरी दिशा में जा रहे हैं। पूर्ण-द्वैध संचार का एक सामान्य उदाहरण टेलीफोन नेटवर्क है। जब दो लोग एक टेलीफोन लाइन द्वारा संवाद कर रहे होते हैं, तो दोनों एक ही समय में बात कर सकते हैं और सुन सकते हैं। पूर्ण-द्वैध मोड का उपयोग तब किया जाता है जब हर समय दोनों दिशाओं में संचार की आवश्यकता होती है। हालांकि, चैनल की क्षमता को दो दिशाओं के बीच विभाजित किया जाना चाहिए।



c. Full·duplex

NETWORKS model

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. एक नेटवर्क संचार लिंक द्वारा जुड़े उपकरणों (अक्सर नोड्स के रूप में संदर्भित) का एक सेट है। एक नोड एक कंप्यूटर, प्रिंटर, या नेटवर्क पर अन्य नोड्स द्वारा उत्पन्न डेटा भेजने और / या प्राप्त करने में सक्षम कोई अन्य उपकरण हो सकता है।

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security. एक नेटवर्क को कुछ निश्चित मानदंडों को पूरा करने में सक्षम होना चाहिए। इनमें से सबसे महत्वपूर्ण प्रदर्शन, विश्वसनीयता और सुरक्षा हैं।

Performance:

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software. प्रदर्शन को कई तरीकों से मापा जा सकता है, जिसमें पारगमन समय और प्रतिक्रिया समय शामिल है। एक डिवाइस से दूसरे डिवाइस पर यात्रा करने के लिए संदेश के लिए ट्रांजिट टाइम आवश्यक राशि है। प्रतिक्रिया समय एक जांच और एक प्रतिक्रिया के बीच बीता हुआ समय है। एक नेटवर्क का प्रदर्शन कई कारकों पर निर्भर करता है, जिसमें उपयोगकर्ताओं की संख्या, ट्रांसमिशन माध्यम का प्रकार, कनेक्टेड हार्डवेयर की क्षमता और सॉफ्टवेयर की दक्षता शामिल है।

Reliability:

Network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe. नेटवर्क की विश्वसनीयता को विफलता की आवृत्ति से मापा जाता है, जिस समय यह एक विफलता से उबरने के लिए लिंक लेता है, और एक आपदा में नेटवर्क की मजबूती।

Security:

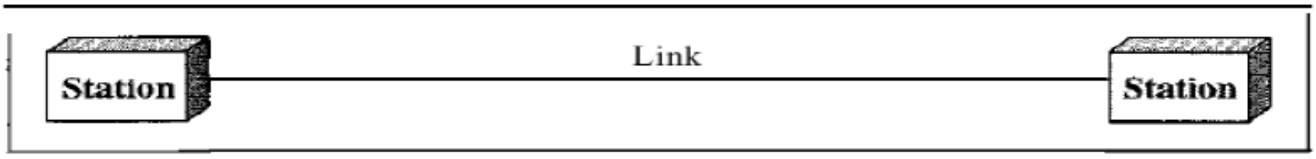
Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses. नेटवर्क सुरक्षा के मुद्दों में अनाधिकृत उपयोग से डेटा की रक्षा, क्षति और विकास से डेटा की सुरक्षा, और उल्लंघनों और डेटा हानि से पुनर्प्राप्ति के लिए नीतियों और प्रक्रियाओं को लागू करना शामिल है।

PHYSICAL STRUCTURES

TYPES OF CONNECTIONS: A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. There are two possible types of connections: point-to-point and multipoint. कनेक्शन के प्रकार: एक नेटवर्क लिंक के माध्यम से जुड़े दो या अधिक उपकरण हैं। एक लिंक एक संचार मार्ग है जो डेटा को एक डिवाइस से दूसरे में स्थानांतरित करता है। कनेक्शन के दो संभावित प्रकार हैं: पॉइंट-टू-पॉइंट और मल्टीपॉइंट।

Point-to-Point

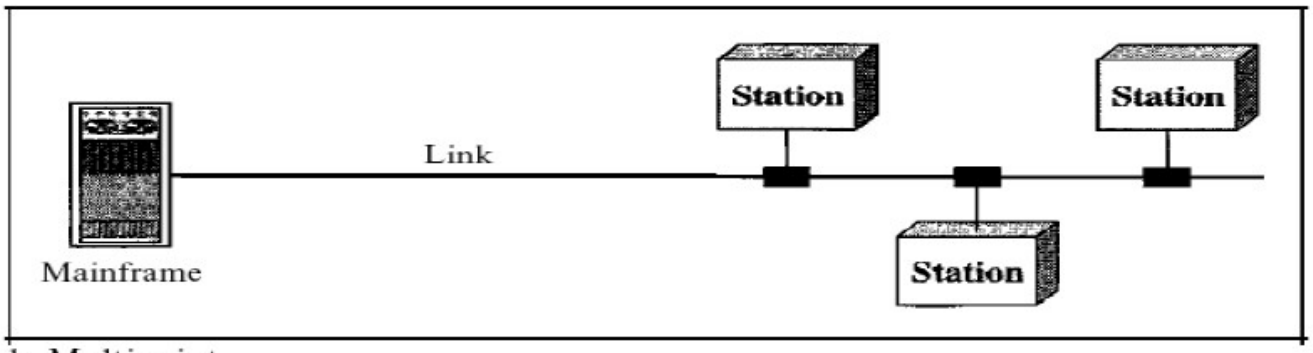
A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system. एक बिंदु से बिंदु कनेक्शन दो उपकरणों के बीच एक समर्पित लिंक प्रदान करता है। लिंक की पूरी क्षमता उन दो उपकरणों के बीच संचरण के लिए आरक्षित है। अधिकांश पॉइंट-टू-पॉइंट कनेक्शन दो छोरों को जोड़ने के लिए तार या केबल की वास्तविक लंबाई का उपयोग करते हैं, लेकिन अन्य विकल्प, जैसे कि माइक्रोवेव या सैटेलाइट लिंक भी संभव हैं। जब आप अवरक्त रिमोट कंट्रोल द्वारा टेलीविजन चैनल बदलते हैं, तो आप रिमोट कंट्रोल और टेलीविजन के नियंत्रण प्रणाली के बीच एक बिंदु से बिंदु कनेक्शन स्थापित कर रहे हैं।



a. Point-to-point

Multipoint

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection. एक मल्टीपॉइंट (जिसे मल्टीड्रॉप भी कहा जाता है) कनेक्शन वह है जिसमें दो से अधिक विशिष्ट डिवाइस एक ही लिंक साझा करते हैं। एक बहुपरत वातावरण में, चैनल की क्षमता साझा की जाती है, या तो स्थानिक रूप से या अस्थायी रूप से। यदि कई डिवाइस एक साथ लिंक का उपयोग कर सकते हैं, तो यह एक स्थानिक रूप से साझा किया गया कनेक्शन है। यदि उपयोगकर्ताओं को टर्न लेना है, तो यह एक टाइमशेड कनेक्शन है।

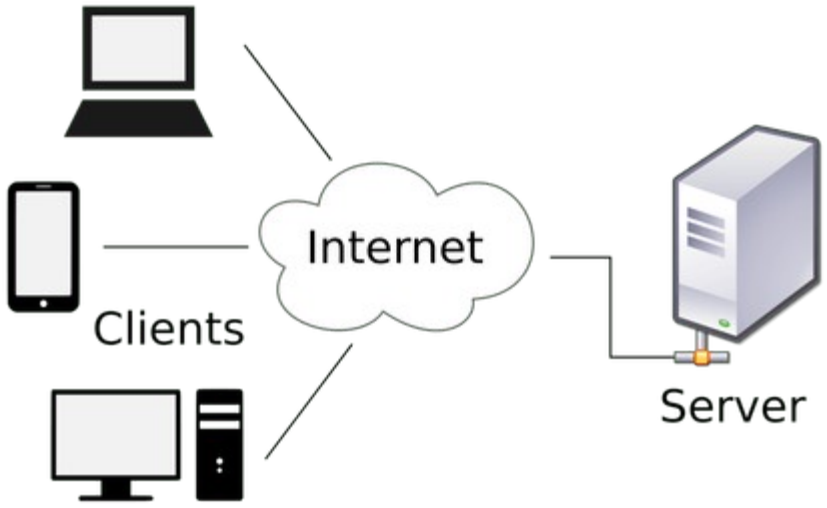


b. Multipoint

What is Client Server Architecture (क्लाइंट सर्वर आर्किटेक्चर क्या हैं)

क्लाइंट-सर्वर आर्किटेक्चर (क्लाइंट / सर्वर) एक नेटवर्क आर्किटेक्चर है जिसमें नेटवर्क पर प्रत्येक कंप्यूटर या तो क्लाइंट या सर्वर होता है। जिसमें सर्वर क्लाइंट द्वारा उपभोग किए जाने वाले अधिकांश संसाधनों और सेवाओं को होस्ट करता है, वितरित करता है और प्रबंधित करता है। इस प्रकार के आर्किटेक्चर में नेटवर्क या इंटरनेट कनेक्शन पर केंद्रीय सर्वर से जुड़े एक या अधिक क्लाइंट कंप्यूटर होते हैं। क्लाइंट / सर्वर आर्किटेक्चर को नेटवर्किंग कंप्यूटिंग मॉडल या क्लाइंट / सर्वर नेटवर्क के रूप में भी जाना जाता है क्योंकि सभी अनुरोध और सेवाएं नेटवर्क पर वितरित की जाती हैं। सर्वर कंप्यूटर या डिस्क ड्राइव (फ़ाइल सर्वर), प्रिंटर (प्रिंट सर्वर), या नेटवर्क यातायात (नेटवर्क सर्वर) के प्रबंधन के लिए समर्पित प्रक्रियाएं हैं। क्लाइंट पीसी या वर्कस्टेशन हैं जिन पर उपयोगकर्ता एप्लिकेशन चलाते हैं।

क्लाइंट संसाधनों के लिए सर्वर पर भरोसा करते हैं, जैसे फाइल, डिवाइस और यहां तक कि प्रोसेसिंग पावर।

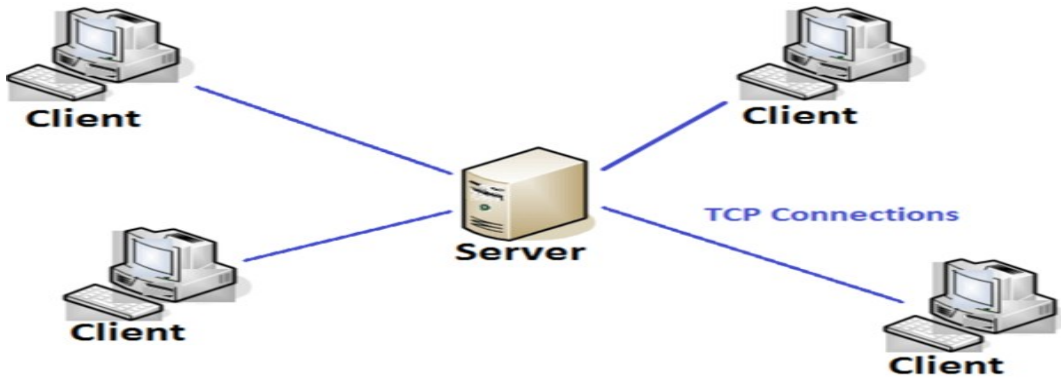


जहॉ पर कम्प्यूटरो की संख्या अधिक होती हैं इस प्रकार के वातावरण के लिये क्लाइंट सर्वर आर्किटेक्चर को तैयार किया गया था। उदाहणार्थ, बहुत सारे कम्प्यूटरो को आपस मे नेटवर्क तकनीक के द्वारा जोड दिये जाते है। इनमे किसी एक कम्प्यूटर को Workstation बना दिया जाता है। Server पर इन सभी कम्प्यूटरो की फाइले सेव होती है इस माडॅल को Client Server मॉडल कहते है। इस मॉडल मे एक या एक से अधिक कम्प्यूटर क्लाइंट होते है तथा Server एक होता है। इस मॉडल मे क्लाइंट अपनी रिक्वेस्ट नेटर्वक के द्वारा सर्वर पर भेजता है तथा Server उस रिक्वेस्ट को Response करता है। इस तरह का नेटर्वक संसाधनो का साझा उपयोग करने मे मदद करता है। इस तरह के मॉडल मे हम हार्डवेयर तथा सॉफ्टवेयर को Share कर सकते है। उदाहरणतः प्रिटंर को Server से Connect कर देते है तो फिर किसी भी वर्कस्टेशन से किसी भी फाइल का प्रिटंआउट निकाल सकते है।

क्लाइंट प्रक्रिया (Client Process)

क्लाइंट एक कंप्यूटर सिस्टम हैं जो किसी तरह के नेटवर्क के जरिय अन्य कंप्यूटरों पर सर्विस एक्सेज करता है क्लाइंट एक ऐसी प्रक्रिया है जो सर्वर को संदेश भेजता है और सर्वर उस कार्य को पूरा करता है। क्लाइंट प्रोग्राम आमतौर पर एप्लिकेशन के User interface हिस्से का प्रबंधन करते हैं, क्लाइंट-आधारित प्रक्रिया उस एप्लिकेशन का फ्रंट-एंड है जिसे उपयोगकर्ता देखता है और उससे संपर्क करता है। क्लाइंट प्रक्रिया स्थानीय संसाधनों का प्रबंधन भी

करती है जो उपयोगकर्ता मॉनीटर, कीबोर्ड, वर्कस्टेशन सीपीयू जैसे इंटरैक्ट करता है। क्लाइंट वर्कस्टेशन के प्रमुख तत्वों में से एक ग्राफिकल यूजर इंटरफेस (जीयूआई) है।



सर्वर प्रक्रिया (Server Process)

क्लाइंट सर्वर आर्किटेक्चर मे, सर्वर प्रोसेस एक ऐसा प्रोग्राम है, जो क्लाइंट द्वारा रिक्वेस्ट किये गये कार्य को पूरा करता है। आमतौर पर सर्वर प्रोग्राम क्लाइंट प्रोग्राम से रिक्वेस्ट प्राप्त करता है तथा क्लाइंट को Response करता है। सर्वर आधारित प्रोसेस नेटर्वक की दूसरी मशीन पर भी चल सकता है। यह सर्वर हॉस्ट ऑपरेटिंग सिस्टम या नेटर्वक फाइल सर्वर हो सकता है। सर्वर को फिर File System सेवाएं तथा एप्लीकेशन प्रदान किया जाता है तथा कुछ स्थितियो मे कोई दूसरा डेक्सटॉप मशीन एप्लीकेशन सेवाएं प्रदान करता है।

सर्वर प्रक्रिया एक सॉफ़्टवेयर इंजन के रूप में कार्य करती है जो शेयर संसाधनों जैसे डेटाबेस, प्रिंटर, संचार लिंक या उच्च संचालित प्रोसेसर प्रबंधित करती है। सर्वर प्रक्रिया बैक-एंड कार्यों को निष्पादित करती है जो समान अनुप्रयोगों के लिए आम हैं।

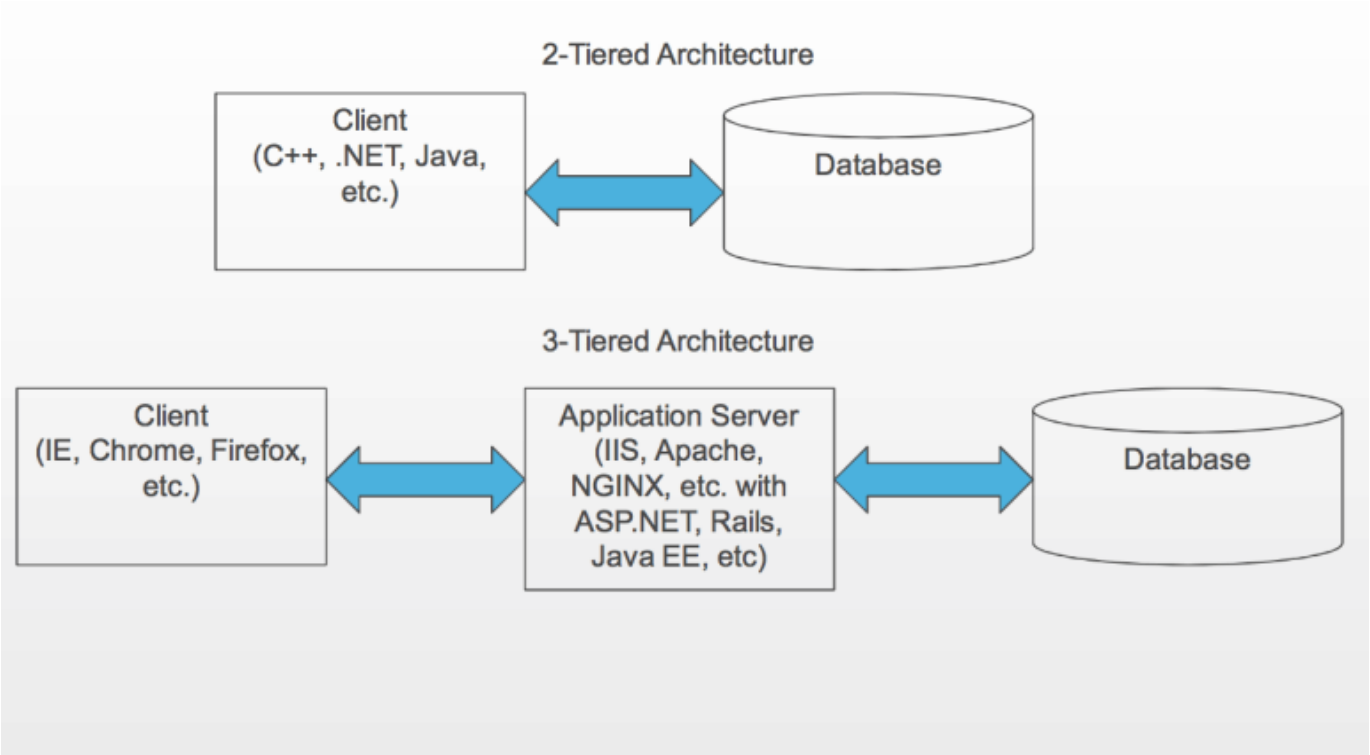
क्लाइंट / सर्वर आर्किटेक्चर के उदाहरण निम्न हैं।

Two tier Architecture

Two tier Architecture वह जगह है जहां कोई क्लाइंट बिना किसी हस्तक्षेप के किसी सर्वर पर सीधे बातचीत नहीं करता है, यह आमतौर पर छोटे वातावरण (50 से कम उपयोगकर्ताओं) में उपयोग किया जाता है। Two tier Architecture में, User interface उपयोगकर्ता के डेस्कटॉप वातावरण पर रखा जाता है और डेटाबेस प्रबंधन सिस्टम सेवाएं आमतौर पर एक सर्वर में होती हैं जो एक से अधिक शक्तिशाली मशीन होती है जो कई क्लाइंट्स को सेवाएं प्रदान करती है। सूचना प्रोसेस user system interface environment और database management server environment के बीच विभाजित है।

Three tier Architecture

Two tier Architecture की कमी को दूर करने के लिए Three tier Architecture को बनाया गया हैं| Three tier Architecture में, उपयोगकर्ता सिस्टम इंटरफ़ेस क्लाइंट पर्यावरण और डेटाबेस प्रबंधन सर्वर वातावरण के बीच एक मिडलवेयर का उपयोग किया जाता है। इन मिडलवेयर को विभिन्न तरीकों से कार्यान्वित किया जाता है जैसे कि लेनदेन प्रसंस्करण मॉनीटर, संदेश सर्वर या एप्लिकेशन सर्वर। मिडलवेयर क्यूइंग, एप्लिकेशन निष्पादन और डेटाबेस स्टेजिंग का कार्य करता है। इसके अलावा मिडलवेयर प्रगति पर काम के लिए शेड्यूलिंग और प्राथमिकता जोड़ता है। Three tier client/ server Architecture का उपयोग बड़ी संख्या में उपयोगकर्ताओं के प्रदर्शन में सुधार के लिए किया जाता है और two tier Architecture की तुलना में लचीलापन में भी सुधार करता है।



Advantages of Client Server Architecture (क्लाइंट सर्वर आर्किटेक्चर के लाभ)

प्रत्येक क्लाइंट को टर्मिनल मोड या प्रोसेसर में लॉग इन करने की आवश्यकता को समाप्त करने के लिए डेस्कटॉप इंटरफ़ेस के माध्यम से कॉर्पोरेट जानकारी तक पहुंचने का अवसर दिया जाता है।

क्लाइंट-सर्वर मॉडल के लिए उपयोग किया जाने वाला एप्लिकेशन हार्डवेयर प्लेटफॉर्म या हकदार सॉफ़्टवेयर (ऑपरेटिंग सिस्टम सॉफ़्टवेयर) की तकनीकी पृष्ठभूमि के बावजूद बनाया गया है जो कंप्यूटिंग पर्यावरण प्रदान करता है, जिससे उपयोगकर्ताओं को क्लाइंट्स और सर्वर (डेटाबेस, एप्लिकेशन और संचार सेवाओं) की सेवाएं प्राप्त करने के लिए मजबूर किया जाता है।

क्लाइंट-सर्वर उपयोगकर्ता प्रोसेसर के स्थान या तकनीक के बावजूद सीधे सिस्टम में लॉग इन कर सकते हैं।

क्लाइंट-सर्वर आर्किटेक्चर को नेटवर्क में एकीकृत स्वतंत्र कंप्यूटरों के बीच फैलाने वाली जिम्मेदारियों का प्रतिनिधित्व करने वाला मॉडल वितरित किया जाता है। इसलिए, क्लाइंट को अप्रभावित बनाते समय सर्वर को प्रतिस्थापित करना, मरम्मत करना, अपग्रेड करना और स्थानांतरित करना आसान है। इस अनजान परिवर्तन को Encapsulation के रूप में जाना जाता है।

सर्वरों के पास बेहतर नियंत्रण पहुंच और संसाधन हैं ताकि यह सुनिश्चित किया जा सके कि केवल अधिकृत क्लाइंट डेटा तक पहुंच या कुशलतापूर्वक उपयोग कर सकें और सर्वर अपडेट प्रभावी ढंग से प्रशासित होते हैं।

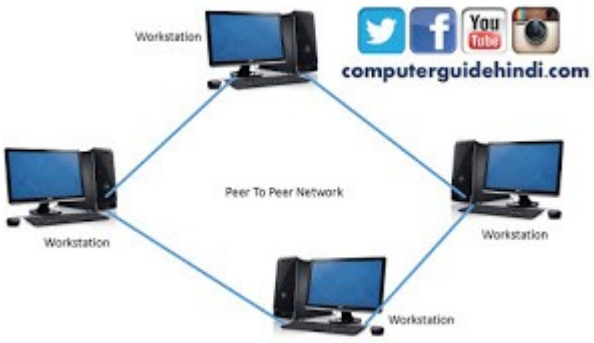
फ्रंट एंड टास्क और बैक-एंड टास्क में प्रोसेसर की गति, मेमोरी, डिस्क की गति और क्षमताओं, और इनपुट / आउटपुट डिवाइस जैसे कंप्यूटिंग के लिए मौलिक रूप से अलग-अलग आवश्यकताएं हैं।

क्लाइंट-सर्वर सिस्टम की एक महत्वपूर्ण विशेषता स्केलेबिलिटी है। उन्हें क्षैतिज या लंबवत स्केल किया जा सकता है। क्षैतिज स्केलिंग का मतलब केवल कुछ मामूली प्रदर्शन प्रभाव के साथ क्लाइंट वर्कस्टेशंस को जोड़ना या निकालना है। लंबवत स्केलिंग का मतलब है एक बड़ी और तेज़ सर्वर मशीन या मल्टीसेवर में माइग्रेट करना।

PEER TO PEER NETWORK : पीयर टू पीयर नेटवर्क

सामन्यतः पियर तो पियर कंप्यूटर नेटवर्क में क्लाइंट या सर्वर निर्धारित नही होता है . लेकिन इनमे प्रत्येक पियर नेटवर्क पर स्वयं ही क्लाइंट क्लाइंट या सर्वर कार्य करता है नेटवर्क का यह रूप क्लाइंट - सर्वर मॉडल से भिन्न होता है . इसमे कोए भी नोड नेटवर्क पर किसी भी प्रकिर्या को शुरू या समाप्त करने में सक्षम होता है पियर नोड लोकल कांफिगुरेसन , प्रोसेसिंग स्पीड , नेटवर्क बैंडविड्थ और स्टोरेज छमता में भिन्न हो सकते है इस ब्यवस्था में कंप्यूटर को आपस में में जोड़ा जाता है लेकिन यह अधिक Computers के लिए उपयोगी नहीं है , बल्कि इनमे सामान्यतः 10 computers को जोड़ा जा सकता है इसमे कोए फाइल या प्रिंट सर्वर भी बनाने की आवश्यकता नहीं होती है पिअर टू पियर का मुख्या कार्य फाइल को शेयर करने का होता है

सामान्तः दो या दो से अधिक computers को आपस में जोड़कर उनकी फाइल्स एवं प्रिंटर को शेयर करना ही पियर टू पियर नेटवर्क का उदाहरण है पियर टू पियर में प्रत्येक कंप्यूटर अपनी सुरक्षा का स्वयं जिम्मेदार होता है यूजर डाटाबेस भी प्रतेयक कंप्यूटर पर अलग अलग होता है अर्थात decentralize होता है . अतः पियर टू पियर नेटवर्क को किसी सिंगल लोकेशन से मैनेज नहीं किया जा सकता है , पियर टू पियर का सेटअप सामान्यतः छोटी संश्था , जैसे सायबर कैफ़े में किया जा सकता है जहा नेटवर्क सिक्यूरिटी प्राथमिक नहीं होती है



टोपोलॉजी क्या हैं? (What is Topology)

टोपोलॉजी नेटवर्क की आकृति या लेआउट को कहा जाता है | नेटवर्क के विभिन्न नोड किस प्रकार एक दुसरे से जुड़े होते है तथा कैसे एक दुसरे के साथ कम्युनिकेशन स्थापित करते है, उस नेटवर्क को टोपोलॉजी ही निर्धारित करता है टोपोलॉजी फिजिकल या लौजिकल होता है| Computers को आपस में जोडने एवं उसमें डाटा Flow की विधि टोपोलॉजी कहलाती है। टोपोलॉजी किसी नेटवर्क में कम्प्यूटर के ज्यामिति व्यवस्था (Geometric arrangement) को कहते है |"Topology is a Layout of Networks"

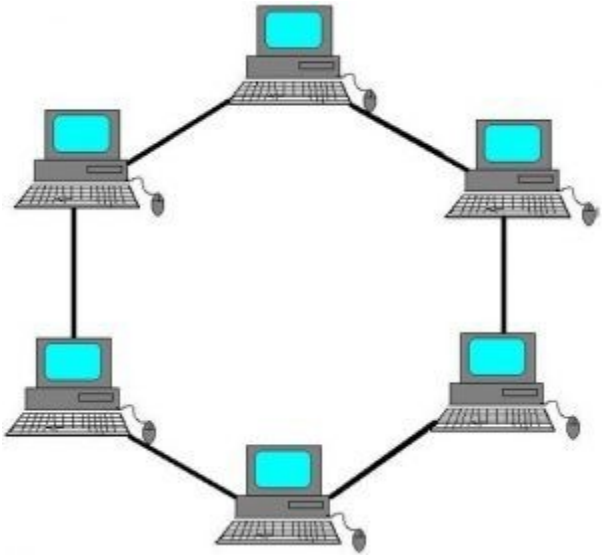
टोपोलॉजी के प्रकार (Types of topology)

नेटवर्क टोपोलॉजी सामान्यत: निम्नलिखित प्रकार की होती है:-

रिंग टोपोलॉजी (Ring Topology)
बस टोपोलॉजी (Bus Topology)
स्टार टोपोलॉजी (Star Topology)
मेश टोपोलॉजी (Mesh Topology)
ट्री टोपोलॉजी (Tree Topology)

रिंग टोपोलॉजी (Ring Topology)

इस कम्प्यूटर में कोई होस्ट, मुख्य या कंट्रोलिंग कम्प्यूटर नही होता | इसमें सभी कम्प्यूटर एक गोलाकार आकृति में लगे होते है प्रत्येक कम्प्यूटर अपने अधीनस्थ (Subordinate) कम्प्यूटर से जुड़े होते है, किन्तु इसमें कोई भी कम्प्यूटर स्वामी नही होता है | इसे सर्कुलर (Circular) भी कहा जाता है |



Ring

रिंग नेटवर्क (Ring Network) में साधारण गति से डाटा का आदान-प्रदान होता है तथा एक कम्प्यूटर से किसी दुसरे कम्प्यूटर को डाटा (Data) प्राप्त करने पर उसके मध्य के अन्य कंप्यूटरो को यह निर्धारित

करना होता है कि उक्त डाटा उनके लिए है या नही | यदि यह डाटा उसके लिए नही है तो उस डाटा को अन्य कम्प्यूटर में आगे (Pass) कर दिया जाता है |

लाभ (Advantages) –

यह नेटवर्क अधिक कुशलता से कार्य करता है, क्योकि इसमें कोई होस्ट (Host) यह कंट्रोलिंग कम्प्यूटर (Controlling Computer) नही होता |

यह स्टार से अधिक विश्वसनीय है, क्योकि यह किसी एक कम्प्यूटर पर निर्भर नही होता है |

इस नेटवर्क की यदि एक लाइन या कम्प्यूटर कार्य करना बंद कर दे तो दुसरी दिशा की लाइन के द्वारा काम किया **जा सकता है |**

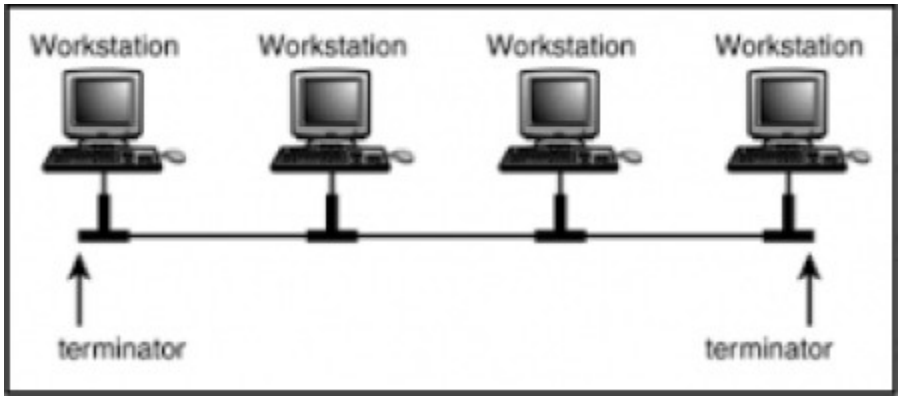
हानि (Disadvantages) –

इसकी गति नेटवर्क में लगे कम्प्यूटरो पर निर्भर करती है | यदि कम्प्यूटर कम है तो गति अधिक होती है और यदि कंप्यूटरो की संख्या अधिक है तो गति कम होती है |

यह स्टार नेटवर्क की तुलना में कम प्रचलित है, क्योकि इस नेटवर्क पर कार्य करने के लिए अत्यंत जटिल साफ्टवेयर की आवश्यकता होती है |

बस टोपोलॉजी (Bus Topology)

बस टोपोलॉजी (Bus Topology) में एक ही तार (Cable) का प्रयोग होता है और सभी कम्प्यूटरो को एक ही तार से एक ही क्रम में जोड़ा जाता है | तार के प्रारम्भ तथा अंत में एक विशेष प्रकार का संयंत्र (Device) लगा होता है जिसे टर्मिनेटर (Terminator) कहते है | इसका कार्य संकेतो (Signals) को नियंत्रण करना होता है |



लाभ (Advantages) –

बस टोपोलॉजी को स्थापित (Install) करना आसान होता है

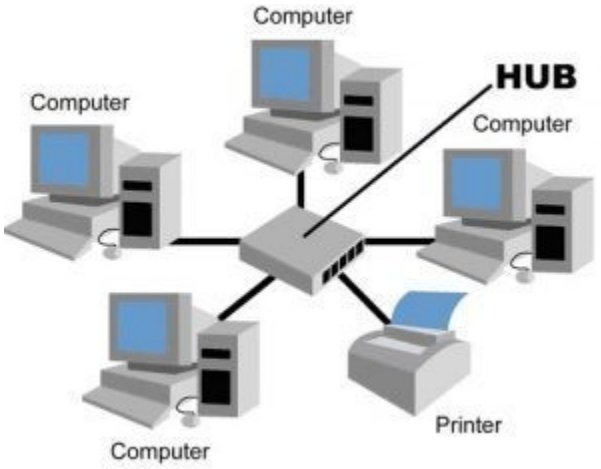
इसमें स्टार व ट्री टोपोलॉजी की तुलना में कम केबिल उपयोगी होता है |

हानि (Disadvantages) –

किसी एक कम्प्यूटर की खराबी से सारा डाटा संचार रुक जाता है |
बाद में किसी कम्प्यूटर को जोड़ना अपेक्षाकृत कठिन है |

स्टार टोपोलॉजी (Star Topology)

इस नेटवर्क में एक होस्ट कम्प्यूटर होता है जिसे सीधे विभिन्न लोकल कंप्यूटरो से जोड़ दिया जाता है | लोकल कम्प्यूटर आपस में एक-दुसरे से नही जुड़े होते हैं इनको आपस में होस्ट कम्प्यूटर द्वारा जोड़ा जाता है | होस्ट कम्प्यूटर द्वारा ही पूरे नेटवर्क को कंट्रोल किया जाता है |



लाभ (Advantages) –

इस नेटवर्क टोपोलॉजी में एक कम्प्यूटर से होस्ट (Host) कम्प्यूटर को जोड़ने में लाइन बिछाने की लागत कम आती है|

इसमें लोकल कम्प्यूटर की संख्या बढाये जाने पर एक कम्प्यूटर से दुसरे कम्प्यूटर पर सूचनाओ के आदान-प्रदान की गति प्रभावित नही होती है, इसके कार्य करने की गति कम हो जाती है क्योकि दो कम्प्यूटर के बीच केवल होस्ट (Host) कम्प्यूटर ही होता है|

यदि कोई लोकल कम्प्यूटर ख़राब होता है तो शेष नेटवर्क इससे प्रभावित नही होता है|

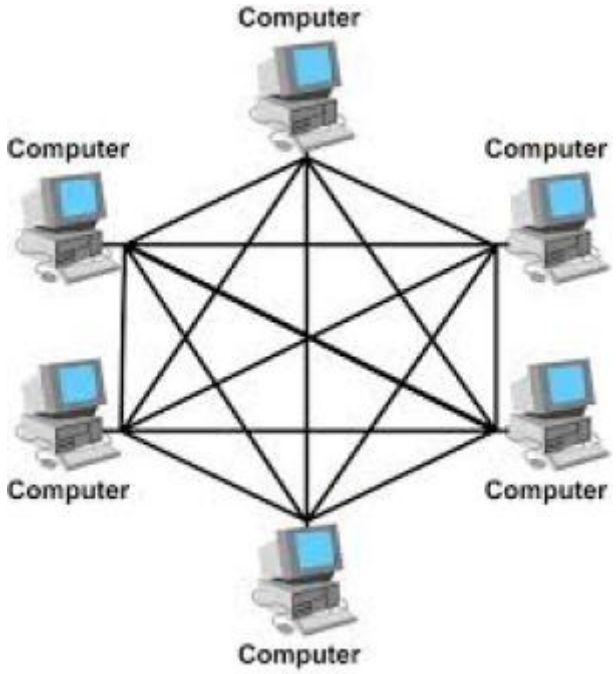
हानि (Disadvantages) –

यह पूरा तंत्र होस्ट कम्प्यूटर पर निर्भर होता है | यदि होस्ट कम्प्यूटर ख़राब हो जाय तो पूरा का पूरा नेटवर्क फेल हो जाता हैं |

मेश टोपोलॉजी (Mesh Topology)

मेश टोपोलॉजी को मेश नेटवर्क (Mesh Network) या मेश भी कहा जाता है | मेश एक नेटवर्क टोपोलॉजी है जिसमे संयंत्र (Devices) नेटवर्क नोड (Nodes) के मध्य कई अतिरिक्त अंत: सम्बन्ध (Interconnections) से जुड़े होते है | अर्थात मेश टोपोलॉजी में प्रत्येक नोड नेटवर्क के अन्य सभी नोड से जुड़े होते है |मेश टोपोलॉजी में सारे कंप्यूटर कही न कही एक दूसरे से जुड़े रहते हैं और एक दूसरे से जुड़े

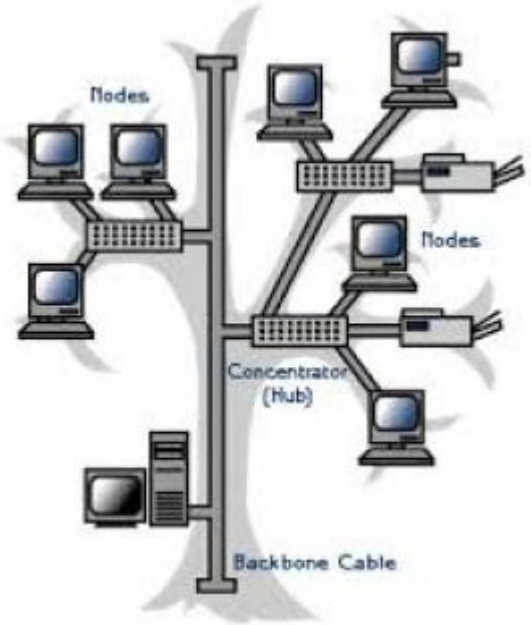
होने के कारण ये अपनी सूचनाओ का आदान प्रदान आसानी से कर सकते हैं | इसमें कोई होस्ट कंप्यूटर



नहीं होता हैं|

ट्री टोपोलॉजी (Tree Topology)

ट्री टोपोलॉजी में स्टार तथा बस दोनों टोपोलॉजी के लक्षण विधमान होते है | इसमें स्टार टोपोलॉजी की तरह एक होस्ट कंप्यूटर होता है और बस टोपोलॉजी की तरह सारे कंप्यूटर एक ही केबल से जुड़े रहते हैं | यह नेटवर्क एक पेड़ के समान दिखाई देता हैं |



लाभ (Advantages) –

प्रत्येक खण्ड (Segment) के लिए प्वाइन्ट तार बिछाया जाता है |

कई हार्डवेयर तथा साफ्टवेयर विक्रेताओ के द्वारा सपोर्ट किया जाता है |

हानि (Disadvantages) –

प्रत्येक खण्ड (Segment) का कुल लम्बाई प्रयोग में लाये गए तार के द्वारा सीमित होती है |

यदि बैकबोन लाइन टूट जाती है तो पूरा खण्ड (Segment) रुक जाता है |

अन्य टोपोलॉजी की अपेक्षा इसमें तार बिछाना तथा इसे कन्फीगर (Configure) करना कठिन होता है |

NETWORK CATEGORIES

नेटवर्क के प्रकार (Types of Network)

LAN (Local Area Network) :-

इसका पूरा नाम Local Area Network है यह एक ऐसा नेटवर्क है जिसका प्रयोग दो या दो से अधिक कंप्यूटर को जोड़ने के लिए किया जाता है| लोकल एरिया नेटवर्क स्थानीय स्तर पर काम करने वाला नेटवर्क है इसे संक्षेप में लेन कहा जाता हैं| यह एक ऐसा कंप्यूटर नेटवर्क है जो स्थानीय इलाकों जैसे- घर, कार्यालय, या भवन समूहों को कवर करता है|

विशेषतायें:-

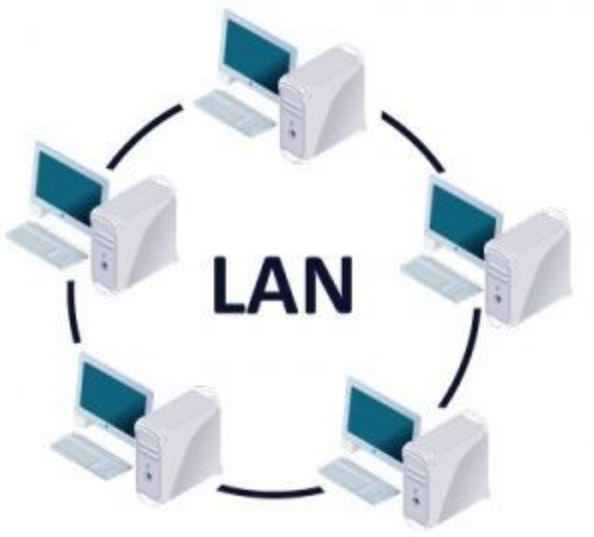
यह एक कमरे या एक बिल्डिंग तक सीमित रहता है |

इसकी डाटा हस्तांतरित (Data Transfer) Speed अधिक होती है |

इसमें बाहरी नेटवर्क को किराये पर नहीं लेना पड़ता है |

इसमें डाटा सुरक्षित रहता है |

इसमें डाटा को व्यवस्थित करना आसान होता है |



MAN (Metropolitan Area Network) :-

इसका पूरा नाम Metropolitan Area Network हैं यह एक ऐसा उच्च गति वाला नेटवर्क है जो आवाज, डाटा और इमेज को 200 मेगाबाइट प्रति सेकंड या इससे अधिक गति से डाटा को 75 कि.मी. की दूरी तक ले जा सकता है| यह लेन (LAN) से बड़ा तथा वेन (WAN) से छोटा नेटवर्क होता है | इस नेटवर्क के द्वारा एक शहर को दूसरे शहर से जोड़ा जाता है |

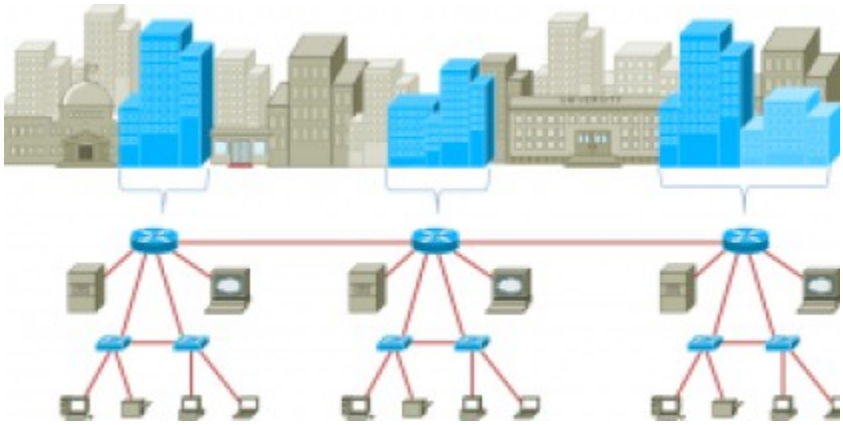
इसके अंतर्गत दो या दो से अधिक लोकल एरिया नेटवर्क एक साथ जुड़े होते हैं. यह एक शहर के सीमाओ के भीतर का स्थित कंप्यूटर नेटवर्क होता हैं. राउटर, स्विच और हब्स मिलकर एक मेट्रोपोलिटन एरिया नेटवर्क का निर्माण करता हैं|

विशेषताये:-

इसका रखरखाव कठिन होता है |

इसकी गति उच्च होती है |

यह 75 कि.मी. की दूरी तक फैला रहता है |



WAN (Wide area Network) :-

इसका पूरा नाम Wide Area Network होता है | यह क्षेत्रफल की द्रष्टि से बड़ा नेटवर्क होता है| यह नेटवर्क न केवल एक बिल्डिंग, न केवल एक शहर तक सीमित रहता है बल्कि यह पूरे विश्व को जोड़ने का कार्य करता है अर्थात् यह सबसे बड़ा नेटवर्क होता है इसमें डाटा को सुरक्षित भेजा और प्राप्त किया जाता है |

इस नेटवर्क मे कंप्यूटर आपस मे लीज्ड लाइन या स्विच सर्किट के दुवारा जुड़े रहते हैं. इस नेटवर्क की भौगोलिक परिधि बड़ी होती है जैसे पूरा शहर, देश या महादेश मे फैला नेटवर्क का जाल. इन्टरनेट इसका एक अच्छा उदाहरण हैं. बैंको का ATM सुविधा वाईड एरिया नेटवर्क का उदाहरण हैं

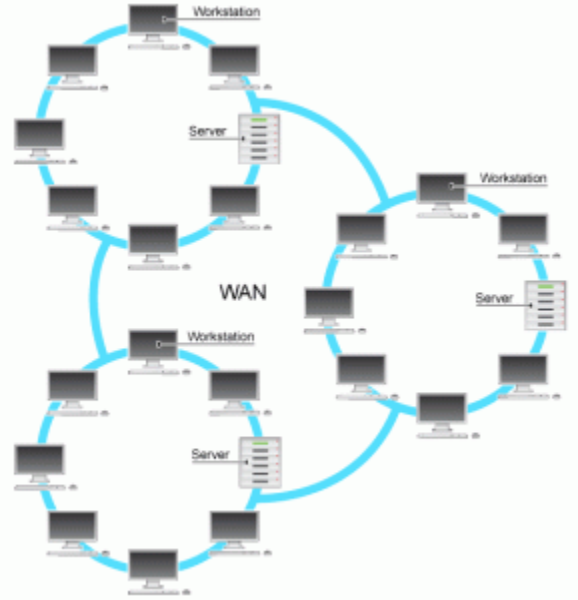
विशेषताये:-

यह तार रहित नेटवर्क होता है|

इसमें डाटा को संकेतो (Signals) या उपग्रह (Sate light) के द्वारा भेजा और प्राप्त किया जा सकता है |

यह सबसे बड़ा नेटवर्क होता है |

इसके द्वारा हम पूरी दुनिया में डाटा ट्रान्सफर कर सकते है |



लेन, मेन और वैन का तुलना चार्ट

तुलना का आधार	LAN	MAN	WAN
फुल फॉर्म	लोकल एरिया नेटवर्क	मेट्रोपॉलिटन एरिया नेटवर्क	वाइड एरिया नेटवर्क
अर्थ	यह नेटवर्क एक छोटे भौगोलिक क्षेत्र में कम्प्यूटर्स को ग्रुप में जोड़कर रखता है| जैसे – बिल्डिंग	यह नेटवर्क एक बड़े क्षेत्र को कवर करता है जैसे – सिटी, टाउन	यह नेटवर्क बहुत बड़े क्षेत्र को कवर करता है और एक कंट्री को दूसरी कंट्री के साथ जोड़कर रखता है| जैसे वर्ल्ड
नेटवर्क का मालिक	प्राइवेट	प्राइवेट और पब्लिक	प्राइवेट और पब्लिक
नेटवर्क को डिज़ाइन और प्रबंधन करना	यह आसान होता है|	यह कठिन होता है|	यह कठिन होता है|
स्पीड	ज्यादा	मध्यम	कम
नेटवर्क्स के बीच ट्रैफिक	कम	ज्यादा	ज्यादा
नेटवर्क का इस्तेमाल	कॉलेज , स्कूल , अस्पताल	शहर, टाउन	देशो और महादीपो
सहनशीलता	कम	ज्यादा	ज्यादा

नेटवर्क सर्विस के प्रकार (types of network services)

नेटवर्क में कंप्यूटर के विभिन्न रिसोर्सेस जैसे हार्ड-डिस्क ,सीडी-ड्राइव,प्रिंटर आदि को शेयर करने के लिए नेटवर्क सर्विस ही जिम्मेदार होतीं हैं

नेटवर्क में प्रयोग होने वाली प्रमुख सर्विसेस निम्न हैं-

१- फाइल सर्विस

२- प्रिंट सर्विस

३- मेसेज सर्विस

४- डाटाबेस सर्विस

५- एप्लीकेशन सर्विस

फाइल सर्विस- नेटवर्क में किसी फाइल को एक कंप्यूटर से दुसरे कंप्यूटर पर ट्रान्सफर ,मूव या कॉपी करने के लिए फाइल सर्विस प्रयोग में आती है । फाइल सर्विस ही नेटवर्क में बैकप की सुविधा प्रदान करती है । फाइल सर्विस स्टोरेज डिवाइस को प्रभावी तरीके से प्रयोग करती है ।

प्रिंट सर्विस- प्रिंट सर्विस का कार्य नेटवर्क में किसी एक कंप्यूटर पर लगे प्रिंटर को नेटवर्क के अन्य कंप्यूटर के लिए उपलब्ध करवाना होता है । अर्थात प्रिंट सर्विस के कारण ही एक प्रिंटर का प्रयोग नेटवर्क के सभी यूजर कर पाते हैं । प्रिंट सर्विस का कार्य नेटवर्क में प्रिंटर की संख्या को कम करना होता है । इस सर्विस के कारण ही नेटवर्क में प्रिंटर को कहीं भी इस्थापित किया जा सकता है । इसकी वजह से ही प्रिंट जोब्स एक पंक्ति में रहते हैं । इसके द्वारा ही प्रिंटर को नेटवर्क में एक्सेस कण्ट्रोल व मैनेज किया जा सकता है ।

मेसेज सर्विस- जैसा की हम नाम से ही समझ सकते है । की मेसेज सर्विस का कार्य एक कंप्यूटर का मेसेज दूसरे कंप्यूटर तक पहुचना होता है । इसके साथ साथ हम डाटा ऑडियो विडियो टेक्स्ट आदि भी भेज सकते हैं । एक प्रकार से मेसेज सर्विस फाइल सर्विस की तरह ही कार्य करती है । लेकिन यह डाइरेक्ट कंप्यूटर के बीच कार्य न करके यूजर अप्लिकेसन के बीच कार्य करती है । इ-मेल व वोइस-मेल इसके ही उदहारण हैं ।

डाटाबेस सर्विस- यह सर्विस नेटवर्क में सर्वर आधारित डाटाबेस की सुविधा प्रदान करती है । अर्थात नेटवर्क में जब कोई क्लाइंट रिक्वेस्ट करता है तो उसे आवश्यक जानकारी डाटाबेस सर्वर के द्वारा प्रदान कर दी जाती है । यह सर्विस डाटा सिक्योरिटी प्रदान करती है । और इसके कारण ही डाटाबेस की लोकेसन केन्द्रित हो पति है ।

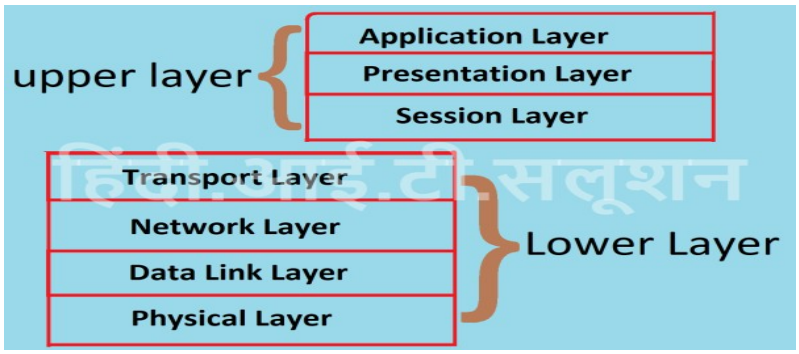
एप्लीकेशन सर्विस- नेटवर्क में वे सर्विस जो नेटवर्क क्लाइंट के लिए सोफ्टवेयर चलाती हैं । एप्लीकेशन सर्विस कहलाती हैं । यह सर्विस केवल डाटा ही नहीं शेयर करती बल्कि उनकी प्रोसस्सिंग पॉवर भी शेयर करने की अनुमति प्रदान करती है । इसका सबसे अच्छा उदाहरण लैन गेमिंग है । जिसमे एक गेम को कई यूजर एक साथ खेलते हैं ।

OSI MODEL

OSI Model का पूरा Name Open System interconnection है ! यहाँ Open System Interconnection से मतलब है की जो भी Network hardware Company अपना कोई भी hardware develop करेगी जो Company OSI model को Follow करते हुए अपने Network Hardware Develop करेगी उनके Devices आपस में Connect हो सकेंगे ! OSI model आने से पहले जो भी Hardware Company जब कोई Hardware बनाती तो वो उसमे अपने द्वारा ही बनाये गए Network Standard और Protocol को यूज़ करते थे जिससे Only उसी Company के द्वारा बनाये गए Hardware Connect हो सकते थे और जब कोई IT Company अलग-अलग Wanders से Hardware ख़रीद लेती तो उसको आपस में Computer को interconnect करने में परेशानी होती थी इसी समस्या के Solution के लिए एक ऐसे Network Standard की आवस्य्क्ता महसूस हुई की वह किसी भी प्रकार के Hardware से Connect हो सके ! OSI Model को ISO(International standardized Organization)ने 1984 में Publish किया गया जबकि इसको 1977 में establish कर लिया गया था ISO ने एक कमेटी बनाई और उसको यह Responsibility दी गई की एक Open Standard Develop किया जाये और इसी कमेटी के Reference से 1984 में OSI Mobel को Approve किया गया और जब से OSI model बना है तब से लेकर आजतक हर Company इसको Follow करते हुए अपनेComputer Network Hardware बना रही है ! यह एक Reference model है !इसके Reference को ध्यान में रखकर ही कम्पनिया अपने Device Develop करती रहेगी हालाँकि आज कल जो हम Network device या Computer को जो यूज़ करते है उनकी Working इसके ऊपर नहीं होती है ! हम जो आज Networking Device यूज़ करते है उनकी Working में TCP /IP Model यूज़ होता है ! OSI model के Reference से Network की Understanding बहुध ही अछि तरह से होती है इस Model का उद्देस्य Network की traveling को समझना है ! अर्थात Network में data को एक Node से दूसरे Node तक जाने में किस तरह की यात्रा करनी पड़ती है ! हम अन्य सरल सब्दो में कह सकते है की OSI Model एक Complex Network task को 7 Parts में divide कर देता है जिसको समझने में बहुध ही आसानी होती है OSI Model में 7 Layers होती है ! जिसमे हर Layer का अपने आप में यूनिक work होता है जिसको यहाँ हम विस्तार से समझेंगे यह 7 layer receiver से Sender की तरफ और Sender से Receiver की तरफ दोनों तरफ होती है. OSI का real life में कोई यूज़ नहीं होता है। Real life में आप इसी के base पर बना हुआ TCP/IP (Transmission control protocol/ Internet Protocol) model यूज़ करते है।

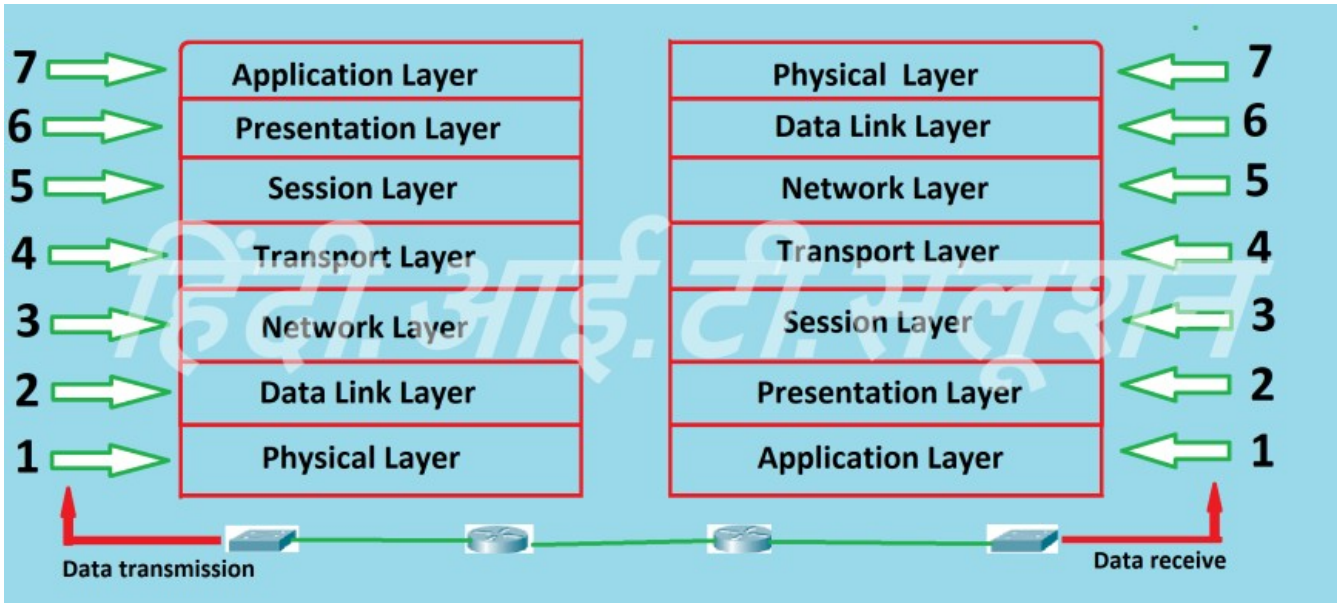
Classification of OSI Model

OSI Model के reference में Network की एक Complex task को 7 parts में divide किया जिसमे Network को आसानी से समझाजा सकता है इसलिए इसको Teaching model के नाम से भी जाना जाता है! osi model में 1st layer Physical Layer है 2nd Data link Layer, 3rd Layer Network layer ,4th Layer Transport layer ,5th session Layer ,6th Presentation Layer , 7th Application Layer है इन 7 layers को OSI Stack भी कहते है ! इस Model को 2 parts में Divide किया गया है



Upper layer-Upper Layer में Application layer , Presentation layer और Session Layer को रखा गया है ! इन तीनो Layer पर Perform होने वाले Networking task Application Specific होते है

Lower Layer- lower layer में Network Specific Function वाली Task perform होती है-
Routhng ,Addressing ,Controlling , जैसे Specific Function इसमें Perform होते है



OSI Reference Model का उद्देश्य:

OSI मॉडल सात लेयर के एक स्ट्रक्चर्ड सेट को रिप्रेजेंट करता हैं, जो एक दूसरे के साथ कनेक्ट होते है। इस मॉडल में प्रत्येक लेयर को डिवाइसेस, कंप्यूटर और नेटवर्क सेग्मेंट्स को कनेक्ट करने की क्षमता बनाए रखने के लिए डेवलप किया गया था।

सॉफ्टवेयर डेवलपर्स और हार्डवेयर के लिए एक कॉमन प्लेटफ़ॉर्म बनाना, ताकि ऐसे नेटवर्किंग प्रॉडक्ट के निर्माण को प्रोत्साहित किया जा सके जो नेटवर्क पर एक दूसरे के साथ कम्यूनिकेट कर सकते हैं।

छोटे सेग्मेंट्स में बड़ी डेटा एक्सचेंज प्रोसेस को विभाजित करके नेटवर्क एडमिनिस्ट्रेटर्स को सहायता करने के लिए यह लेयर बनाए गए हैं। छोटे सेग्मेंट्स समझने, मैनेज करने और ट्रबलशूट के लिए आसान है। लेयर्स में डिवाइड होने से केवल वही डिवाइसेस को ट्रबलशूट करना होगा जो फॉल्टी लेयर में काम कर रहे हैं।

OSI रेफरेंस मॉडल का उद्देश्य वेंडर्स और डेवलपर्स को मार्गदर्शन करना है ताकि डिजिटल कम्युनिकेशन प्रॉडक्ट और सॉफ्टवेयर प्रोग्राम तैयार किए जा सकें, और कम्युनिकेशन टूल्स के बीच स्पष्ट तुलना की सुविधा प्रदान कि जा सकें। टेलीकम्युनिकशन्स में शामिल अधिकांश विक्रेता, OSI मॉडल के संबंध में अपने प्रॉटक्ट और सर्विसेस का वर्णन करने का प्रयास करते हैं। यद्यपि डिस्कशन और मूल्यांकन मार्गदर्शन के लिए OSI मॉडल उपयोगी है, लेकिन OSI शायद ही कभी लागू किया जाता है, क्योंकि कुछ नेटवर्क प्रॉडक्ट या स्टैंडर्ड टूल्स सभी रिलेटेड फंक्शन को मॉडल से संबंधित सभी डिफाइन लेयर में एक साथ रखते हैं।

मॉडल एक विशेष नेटवर्किंग सिस्टम के साथ क्या चल रहा है इसका एक दृश्य विवरण देने के लिए लेयर का उपयोग करता है। यह नेटवर्क मैनेजर्स और कंप्यूटर प्रोग्रामर्स को समस्या को कम करने में मदद कर सकता है।

The 7 Layers of the OSI

OSI के लेयर अवधारणात्मक रूप से समान फंक्शन का एक संग्रह है जो इसके ऊपर की लेयर को सर्विस प्रदान करती है और नीचे कि लेयर से सर्विस को प्राप्त करती है।OSI का मुख्य कांसेप्ट यह है कि टेलीकम्युनिकशन्स नेटवर्क में दो एंडपॉइंट के बीच कम्युनिकेशन की प्रोसेस को संबंधित फंक्शन के सात अलग-अलग लेयर में डिवाइड किया जा सके। प्रत्येक कम्युनिकेटिंग यूजर या प्रोग्राम उस कंप्यूटर पर है जो फ़ंक्शन के उन सात लेयर प्रदान कर सकता है। इसलिए यूजर्स के बीच किसी दिए गए मैसेजेस में, सोर्स कंप्यूटर में लेयर्स के माध्यम से डेटा फ्लो नीचे कि और होता हैं और फिर रिसिविंग कंप्यूटर में लेयर्स के माध्यम से ऊपर कि और होता हैं।

फ़ंक्शन के सात लेयर ऐप्लीकेशन, ऑपरेटिंग सिस्टम, नेटवर्क कार्ड डिवाइस ड्राइवरों और नेटवर्किंग हार्डवेयर के कॉम्बिनेशन द्वारा प्रोवाइड किए जाते हैं जो एक नेटवर्क केबल या वाई-फाई या अन्य वायरलेस प्रोटोकॉल पर सिग्नल भेजने के लिए सक्षम होते हैं।

OSI मॉडल में, कंट्रोल एक लेवल से दूसरे तक, एक स्टेशन पर ऐप्लीकेशन लेयर (लेयर 7) से शुरू होता है, और नीचे की तरफ जाता है, चैनल पर अगले स्टेशन पर जाता है और हाइरार्की का बैकअप लिया जाता है। OSI मॉडल इंटर-नेटवर्किंग के टास्क को लेता है और इसे उस हिस्से में विभाजित करता है जिसे वर्टीकल स्टैक के रूप में रेफर किया जाता है जिसमें निम्नलिखित 7 लेयर शामिल हैं-

1) Physical Layer

Physical layer OSI model की 1st layer है। इस layer में data bits में convert हो जाता है। इस layer के द्वारा डेटा physical mediums के द्वारा transfer किया जाता है जैसे की Cables आदि यह डिवाइसेस के बीच वास्तविक फिजिकल कनेक्शन के लिए ज़िम्मेदार है। डेटा प्राप्त करते समय, इस लेयर को सिग्नल प्राप्त होते हैं। इसके बाद यह लेयर इसे 0 और 1 में कनवर्ट करता हैं और उन्हें Data Link layer पर भेज देता हैं।Physical Layer के उदाहरणों में ईथरनेट केबल्स और टोकन रिंग नेटवर्क शामिल हैं इसके अतिरिक्त, हब और अन्य रिपिटर्स स्टैंडर्ड नेटवर्क डिवाइस होते हैं जो कि Physical Layer पर कार्य करते हैं, जैसे केबल कनेक्टर हैं।

यह लेयर फिजिकल तथा इलेक्ट्रिकल कनेक्शन के लिए Responsible रहता है जैसे: – वोल्टेज, डेटा रेट्स आदि। इस लेयर में Digital signal, Electrical signal में बदल जाते है। इस लेयर में Network के लेआउट अर्थात Network की टोपोलॉजी का कार्य भी होता है।Physical Layer पर, फिजिकल मेडियम द्वारा सपोर्टेड सिग्नल के टाइप का उपयोग करके डेटा ट्रांसमिट किया जाता है: इलेक्ट्रिक वोल्टेज, रेडियो फ्रीक्वेंसी, या इंफ्रारेड या आर्डिनरी लाइट के पल्स।

Key Points of Physical Layer:

यह फिजिकल कनेक्शन को एक्टिवेट करता है, मेंटेन रखता है और डिएक्टिवेट करता है।

यह नेटवर्क पर अनस्ट्रक्चर्ड रॉ डेटा के ट्रांसमिशन और रिसेप्शन के लिए जिम्मेदार है।

ट्रांसमिशन के लिए आवश्यक वोल्टेज और डाटा रेट फिजिकल लेयर में डिफाइन किए जाते है।

यह डिजिटल सिग्नल या ऑप्टिकल सिग्नल में डिजिटल / एनालॉग बिट्स को कन्वर्ट करता है।

डाटा एन्कोडिंग भी इस लेयर में किया जाता है।

2) Data Link Layer

Data link layer OSI model की 2nd layer है। ये layer network के अंदर data को transport करने के लिए responsible होती है। Data link layer की 2 sub layers होती है।

Logical link control – LLC sub-layer physical layer और बाकी ऊपर की layers के बीच में एक link establish करती है।

Media access control – MAC sub layer physical medium के access को control करती है।

Data link layer नेटवर्क लेयर के data को frames में पैक करती है। Data link layer में डेटा frames में convert हो जाता है।ताकि data को किसी physical medium के through भेजा जा सके। ये process framing कहलाती है। Frames source और destination devices के hardware address contain करते है।

किसी network में host को uniquely identify करने के लिए hardware address यूज़ किया जाता है। सबसे common hardware address Ethernet का MAC address होता है।

Key Points of Link Layer:

Data link layer उस इनफॉर्मेशन को सिंक्रनाइज़ करता है जो फिजिकल लेयर पर ट्रांसमिट होती है।

इस लेयर का मुख्य कार्य यह सुनिश्चित करना है कि फिजिकल लेयर पर एक नोड से दूसरे में डेटा ट्रांसफर एरर फ्री हो।

अनुक्रमिक रूप से प्राप्त ट्रांसमिशन और डेटा फ्रेम्स इस लेयर द्वारा मैनेज किया जाता है।

3) Network Layer

यह layer OSI model की 3rd layer होती है। ये layer network communication के लिए responsible होती है। Network layer में data packets में convert हो जाता है। Network layer के 2 प्रमुख काम होते है जो नीचे दिए जा रहे है।

- Logical addressing – Network layer डेटा को network में travel करने के लिए IP address provide करती है ये IP address डेटा को destination तक पहुचने के लिए responsible होती है।
- Routing – Data को एक network से दूसरे network में भेजना भी network layer की जिम्मेदारी होती है।

Network layer पर IP (Internet Protocol) यूज़ किया जाता है।

Key Points of Network Layer:

यह एक नोड से अन्य नोड तक विभिन्न चैनलों के माध्यम से सिग्नल को राउट करता है।

यह एक नेटवर्क कंट्रोलर के रूप में कार्य करता है। यह सबनेट ट्रैफिक मैनेज करता है।

यह तय करता है कि डेटा को किस रूट को लेना चाहिए।

यह आउटगोइंग मैसेजेस को पैकेट में बांटता है और इनकमिंग पैकेट को हाइर लेवर के लिए मैसेजेस को अस्सेम्बल करता है।

4) Transport Layer

Transport layer OSI model की 4th layer होती है। ये layer data के reliable transfer के लिए responsible होती है। Data order में और error free पहुंचे ये इसी layer की जिम्मेदारी होती है। Transport layer 2 तरह से communicate करती है connectionless और connection oriented।Connectionless communication के लिए UDP और connection orientated के लिए TCP/IP protocols यूज़ किये जाते है।

Connectionless communication fast होता है लेकिन ये डेटा के error free होने और सही ढंग से पहुचने की guarantee नहीं देता है।

Connection oriented communication data के error free होने और ढंग से पहुचने की guarantee देता है।

ये communication कुछ services प्रोवाइड करता है –

- Segmentation – Data को भेजने से पहले छोटे छोटे segments में convert किया जाता है।
- Sequencing – हर segment को एक sequence number दिया जाता है।
- Connection establishment – Data को भेजने से पहले sender और receiver के बीच connection establish किया जाता है।
- Acknowledgment – जब segment पहुचता है तो उसका acknowledgment आता है की इतने number का segment आ चूका है उसे दुबारा भेजने की जरुरत नही है।
- Flow control – Data की transfer rate को confirm किया जाता है।

Key Points of Transport Layer:

एंड सिस्टम के बीच डेटा के ट्रांसपरेंट ट्रांसफर के लिए जिम्मेदार।

एंड-टू-एंड एरर रिवकरी और फ्लो कंट्रोल के लिए जिम्मेदार।

संपूर्ण डेटा ट्रांसफर के लिए जिम्मेदार।

यहां SPX, TCP, UDP जैसे प्रोटोकॉल काम करते हैं।

5) Session Layer

जब दो डिवाइसेस, कंप्यूटर या सर्वर को एक-दूसरे के साथ कम्युनिकेट की आवश्यकता होती है, तो session बनाना आवश्यकता होता है, और यह Session Layer पर किया जाता है। इस लेयर के फंक्शन में सेटअप, कोआर्डिनेशन (उदाहरण के लिए रिस्पॉस के लिए सिस्टम को कितनी कितनी देर तक प्रतीक्षा करनी होगी) और सेशन के प्रत्येक एंड पर ऐप्लीकेशन के बीच टर्मिनेशन शामिल हैं।

Key Points of Session Layer:

ऐप्लीकेशन के बीच एस्टैब्लिशमेंन्ट, मैनेजमेंट और कनेक्शन के टर्मिनेशन के लिए जिम्मेदार।

Session layer प्रत्येक एंड पर एप्लिकेशन के बीच कोऑर्डिनेशन, एक्सचेंज और डाइलॉग सेटअप करता है।

यह सेशन और कनेक्शन कोऑर्डिनेशन के साथ काम करता है।

इस लेयर पर NFS, NetBios names, RPC, SQL जैसे प्रोटोकॉल काम करते हैं।

6) Presentation Layer

Presentation layer को Translation layer भी कहा जाता है। Presentation layer OSI model की 6th layer होती है। ये layer data के presentation के लिए responsible होती है।ये layer ये verify करती है की जो data sender भेज रहा है वो receiver side के समझ में आये।इसके लिए दोनों receiver और sender कुछ data standards follow करते है।

DATA STANDARDS

Text – RTF, ASCII, EBCDIC

Images – JPG, GIF

Audio – MP3, WAV

Movies – AVI, MPE

ये कुछ common data standards है जिन पर दोनों side agree करती है। उदाहरण के लिए यदि sender कोई image भेज रहा है तो वह JPG format में होनी चाहिए ताकि receiver उसे देख सके।

ये layer data की formatting करती है। इस layer से data सीधा application layer पर जाता है, जँहा वो यूज़र को show होता है।इसलिए ये सारी जिम्मेदारी presentation layer की होती है की data यूज़र को कैसे present होगा। यदि sender और receiver एक ही format को support नहीं करते है तो presentation layer translation और conversion की services भी प्रोवाइड करती है।

Presentation layer के कुछ functions नीचे दिए जा रहे है।

- Raw data को translate करती है।
- उसे encrypt करती है।
- और उस data को compress करती है।

Key Points of Presentation Layer:

Presentation layer यह ध्यान रखता है कि डेटा इस तरह से भेजा जाएं, ताकि रिसिवर इनफॉर्मेशन (डेटा) को समझ सके और डेटा का उपयोग करने में सक्षम हो।

डेटा प्राप्त करते समय, presentation layer ऐपलीकेशन लेयर के लिए डेटा ट्रांसफॉर्म कर रेडी करता हैं।

दो कम्युनिकेशन सिस्टम में लैग्वेज (सिंटैक्स) भिन्न हो सकती हैं। इस स्थिति के अंतर्गत presentation layer ट्रांसलेटर की भूमिका निभाता है।

यह डाटा कंप्रेशन, डाटा एन्क्रिप्शन, डेटा कन्वर्शन इत्यादि परफॉर्म करता है।

7) Application Layer

OSI Reference Model के टॉप पर Application layer होता हैं, जो नेटवर्क ऐप्लीकेशन द्वारा इम्प्लीमेंट किया जाता है। यह ऐप्लीकेशन डेटा को प्रोडयुस करते हैं, जिसे नेटवर्क पर ट्रांसफर किया जाता हैं।

यह लेयर नेटवर्क एक्सेस के लिए ऐप्लीकेशन सर्विसेस के लिए विंडो के रूप में कार्य करता हैं और यूजर्स को प्राप्त इनफॉर्मेशन को दिखाता हैं।

वेब ब्राउज़र (गूगल क्रोम, फायरफॉक्स, सफारी, आदि) या अन्य ऐप - स्काइप, आउटलुक, ऑफि सवेब ब्राउज़र (Internet explorer, Mozilla firefox, chrome) या कोई ईमेल क्लाइंट (Outlook, Thunderbird) आदि यह सभी लेयर 7 एप्लीकेशन के उदाहरण हैं।

Key Points of Application Layer:

एप्लिकेशन लेयर ऐप्लीकेशन, ऐप्स और एंड यूजर्स प्रोसेसेस को सपोर्ट करता है।

सर्विस कि क्वालिटी।

यह लेयर फ़ाइल ट्रांसफर, ई-मेल और अन्य नेटवर्क सॉफ़्टवेयर सर्विसेस के लिए एप्लिकेशन सर्विसेस के लिए ज़िम्मेदार है।

इस लेयर पर Telnet, FTP, HTTP जैसे प्रोटोकॉल काम करते हैं।

The TCP/IP Model

Protocol नियमो एवं प्रतिक्रियाओ के समूह को कहा जाता है जिन्हें सफलता पूर्वक कम्युनिकेशन करने के लिए device को फॉलो करना पड़ता है. Protocol का कार्य नेटवर्क से जुड़े सभी प्रकार के device के मध्य संचार को स्थापित करना तथा सूचनाओ के आदान - प्रदान को नियंत्रण करना होता है. इसके लिए TCP/IP का प्रयोग किया जाता है जो सूचनाओ को एक कंप्यूटर से दुसरे कंप्यूटर में पैकेट के रूप में भेजने के लिए स्टैण्डर्ड Protocol होता है.

TCP/IP का Full Form TCP के लिए Transmission Control Protocol और IP के लिए Internet Protocol हैं, TCP/IP को "the language of the Internet." के नाम से भी जाना जाता हैं। TCP/IP WWW का एक Protocol है, जिसके द्वारा हम किसी भी Computer में आसानी से Internet Access करने के लिए Use करते है। अगर किसी नेटवर्क में दो Devices है तो उन्हें आपस में Communicate करने के लिए Common Protocol की जरुरत होगी। TCP/IP Model(Protocol) end-to-end Communication उपलब्ध कराता है। आज के Internet का विकास ARPAnet के रूप में हुआ जब, Advanced Research Projects Agency (ARPA) ने 1969 में Cold war (During 1945 to 1990 Between USA and USSR (Soviet Union)) के समय हुआ था जब उन्हें लगा की कोई ऐसा कम्युनिकेशन System हो जो Nuclear War में भी use किया जा सके।

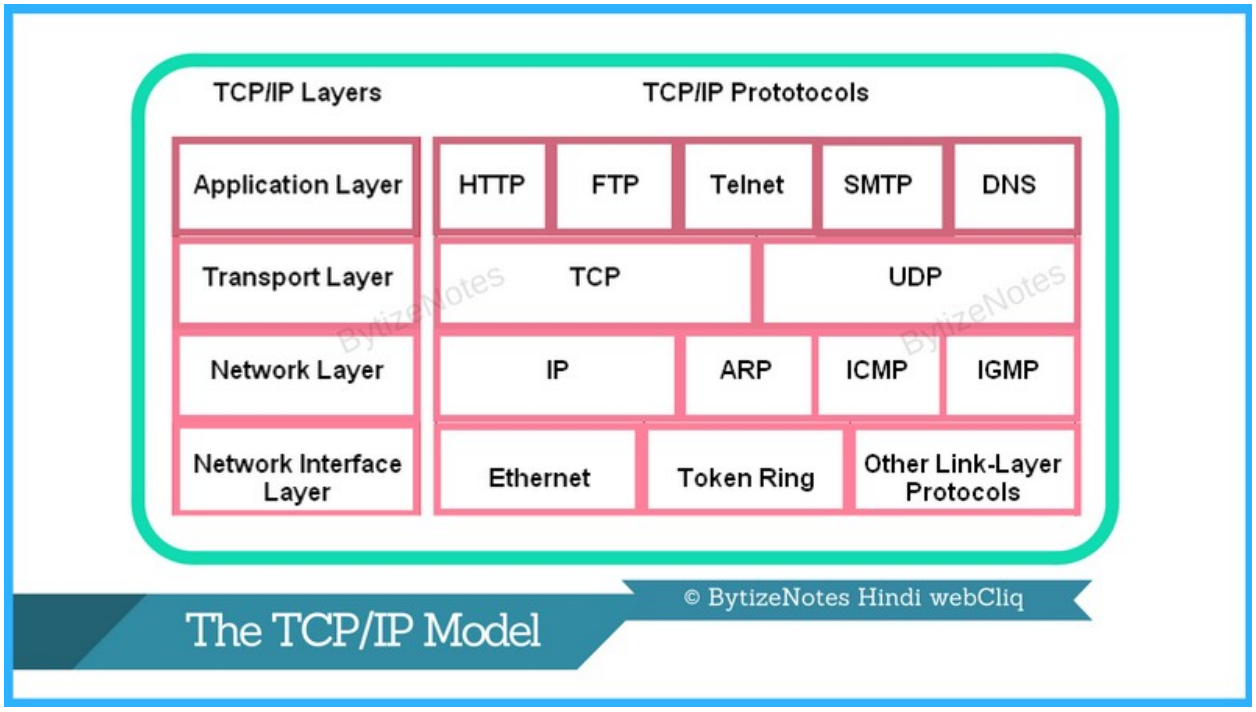
TCP/IP History

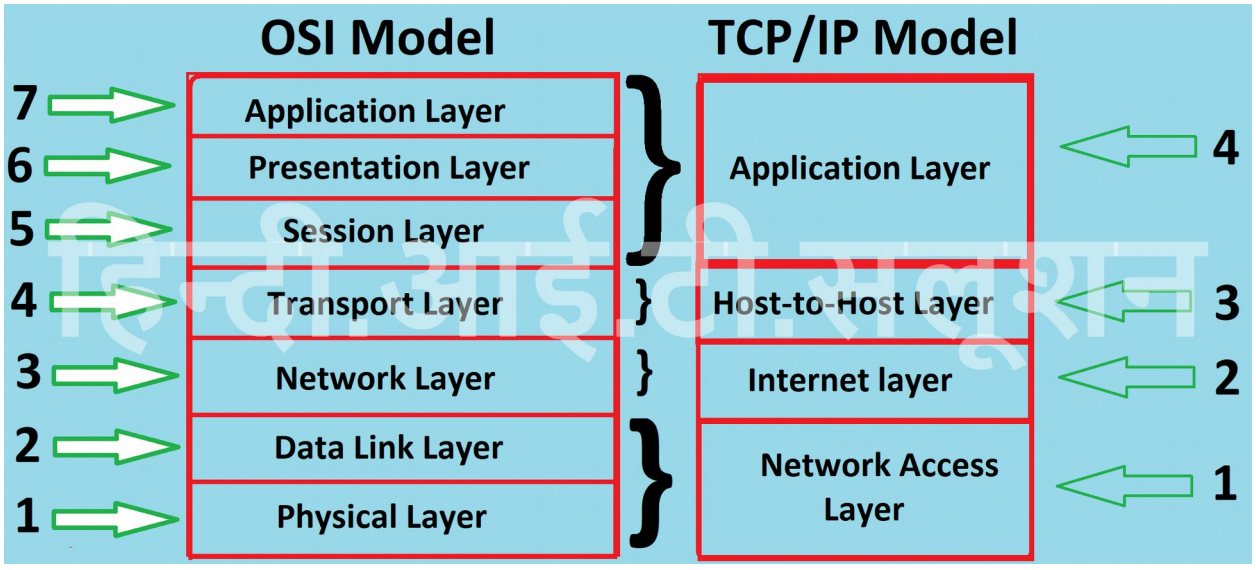
ARPAnet में जिस Protocol का Use हुआ उसे Network Control Protocol (NCP) कहा गया। बाद में जब इसकी जरुरत बढ़ी और ये जब एक बड़े नेटवर्क को connect करने में असफल हो रहा था, तब 1974 में Vint Cerf और Bob Kahn ने एक नई टेक्नोलॉजी को Introduced किया, जिसे Transmission Control Protocol (TCP) कहा गया जो जल्द ही NCP को Replace करता, तभी साल 1978 में कुछ नए Development के बाद एक नये Protocol Suite को Introduce किया गया जिसे Transmission Control Protocol/Internet Protocol (TCP/IP) कहा गया। फिर उसके बाद 1982 में ये dicide हुआ की अब NCP को TCP/IP से बदला जायेगा,जिसे ARPAnet का Standard Lanugage के रूप में। इस प्रकार से 1983 में ARPAnet को TCP/IP से बदल दिया गया और Network का विकास बहुत तेजी से हुआ। तो इसी आधार पर हम कह सकते है कि आज के TCP/IP Model का विकास ARPAnet से हुआ।

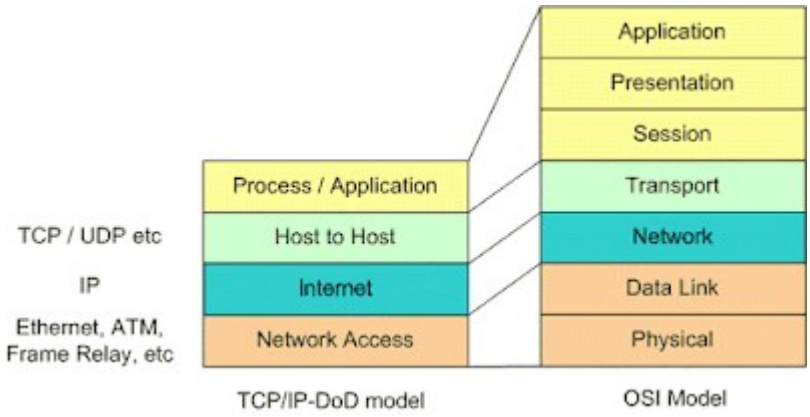
TCP/IP Reference Models:

TCP/IP दो Computers के बीच Information Transfer और Communication को Possible करता है । इसका प्रयोग Data को सुरक्षित ढंग से भेजने के लिए किया जाता है । TCP की भूमिका DATA को छोटे-छोटे भागों (Packets) में बाँटने की होती है और IP इन Packets का Address मुहैया कराता है । TCP/IP Network Protocol

Internet पर एक साथ भिन्न आकार और विभिन्न प्रकार के Systems Network से Connect करने की इसकी क्षमता के कारण सफल है। TCP/IP का Implementation लगभग सभी प्रकार के Hardware व Operating System के लिए समान रूप से काम करता है इसलिए सभी प्रकार के Networks TCP/IP के प्रयोग द्वारा आपस में Connect हो सकते हैं।







TCP/IP Protocol में 4 Layer होती है जो निम्न है:-

01). Network Access layer (Network Interface Layer):- यह TCP/IP मॉडल की सबसे निम्नतम लेयर है। TCP/IP का Network Layer, OSI Reffrence Models के पहले तीन निचले Layers (i.e ... Network, Data Link, and Physical) के सभी function को Complete करता है। नेटवर्क एक्सेस लेयर यह describe करती है कि किस प्रकार से किसी भी IP Data Gram को नेटवर्क में sent करना है। Network Layer में जो Data होता है वह Packet (Data के समूह) के रूप में होता है और इन पैकेटों को source से destination तक पहुँचाने का काम Network Layer का होता है। Network layer जैसे ही किसी नई Hardware को Detect करती हैं, नए Network Acsess Protocoal को विकसित करती है ताकि टीसीपी / आईपी नेटवर्क नए हार्डवेयर का इस्तेमाल आसानी से कर सकें।

02). Internet layer (Network Layer) :- TCP/IP Model में Internet लेयर का काम OSI Refrence Model के Layer 3 की तरह ही काम करता हैं, यह लेयर ट्रांसपोर्ट लेयर तथा एप्लीकेशन लेयर के मध्य स्थित होती है। यह लेयर नेटवर्क में connectionless कम्युनिकेशन उपलब्ध कराती है। इसमें डेटा को IP datagrams के रूप में पैकेज किया जाता है यह datagram source तथा destination IP एड्रेस को contain किये रहते है जिससे कि डेटा को आसानी से sent तथा receive किया जा सकें। TCP/IP Internet Layer's के अंतर्गत आने वाले Major Protocols है :- Internet Protocol (IP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP) और Internet Group Management Protocol (IGMP).

03). Transport layer:- TCP/IP Model का Transport layer Data के Transmission के लिए जिम्मेदार होती है यह लेयर एप्लीकेशन लेयर तथा इंटरनेट लेयर के मध्य स्थित होती है। Transport layer में Error checking, flow control भी होता हैं ताकि दो Communiction के बीच कोई भी डाटा अपने सही Reciver और Sender तक पहुँच सके, अगर में आसान शब्दों में कहें, तो ये Multiplexing और De-Multiplexing के Process के लिए जिम्मेवार होता हैं। इस लेयर में दो मुख्य प्रोटोकॉल कार्य करते है:-

Transmission control protocol(TCP)

04). Application layer:- TCP/IP Protocol की सबसे उच्चतम layer को Application Layer कहते है। यह Layer Applications को Network Services उपलब्ध करने से सम्बंधित होती है। इस Layer का सम्बन्ध किसी भी Data के formation, Encapsulation और Transmission से होता हैं। ये Layer Human Interaction का काम करती हैं जैसे: Web-browser, Email तथा अन्य Application के लिए Window उपलब्ध कराना. इस Layer का काम Transport Layer को Data भेजना और उससे Data को Receive करना । Application Layer में होने वाले कुछ Protocols निम्न प्रकार से है:-

Hypertext Transfer Protocol (HTTP)

Simple Mail Transfer Protocol (SMTP)

Dynamic Host Configuration Protocol (DHCP)

Domain Name System (DNS)

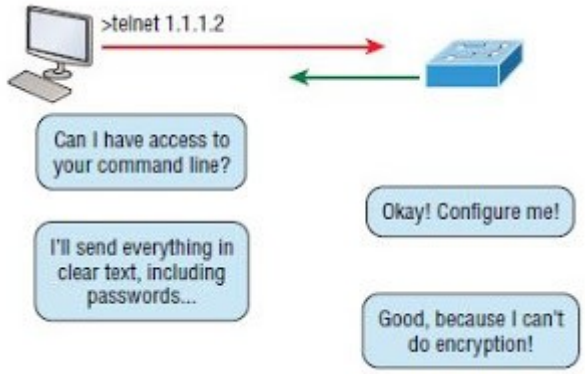
Simple Network Management Protocol (SNMP)

File Transfer Protocol (FTP)

एप्लीकेशन लेयर के कुछ प्रोटोकॉल्स

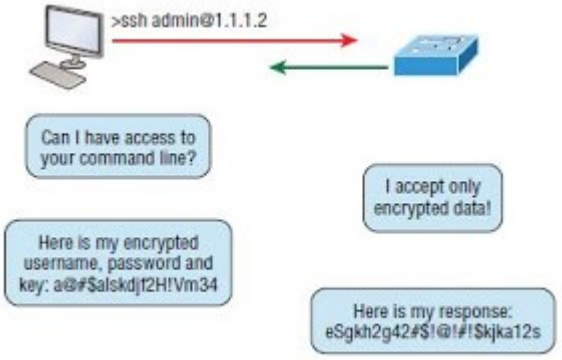
Telnet

telnet इन्टरनेट का पहला प्रोटोकॉल है जो 1969 में डेवेलोप किया गया था | इसके द्वारा एक सिस्टम से दुसरे सिस्टम को एक्सेस किया जा सकता है जो किसी दूसरी लोकेशन पर रखा हुआ है | एक्सेस करने वाला telnet क्लाइंट और एक्सेस होने वाला telnet सर्वर कहलाता है | telnet का उपयोग command line interface (cmd) केद्वारा किया जा सकता है |



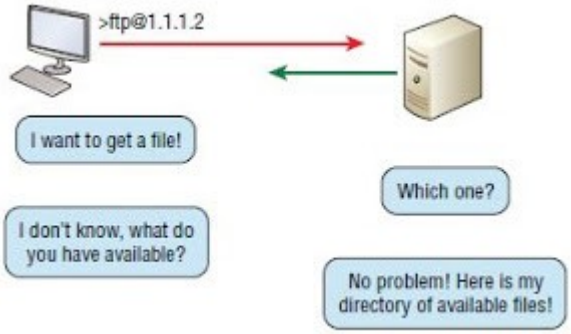
Secure Shell

ये भी telnet के जैसा ही है पर tcp/ip के द्वारा ये सिक्योर सेशंस बनाता है | इसके द्वारा और भी काम करवाए जाते है जैसे - रिमोट सिस्टम पर लॉगिंग करना, उन पर प्रोग्राम्स रन करना और फाइल्स को मूव करना | इन सभी कामों में डाटा को एन्क्रिप्टेड करके सेंड किया जाता है |



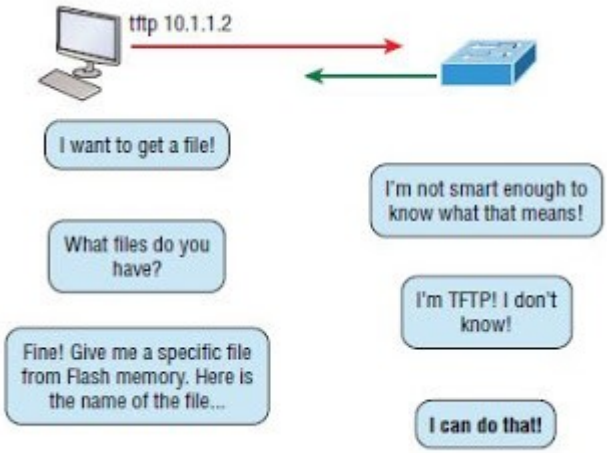
FTP

फाइल ट्रांसफर प्रोटोकॉल का इस्तेमाल किसी दो सिस्टम्स के बीच फाइल्स के ट्रांसफर में किया जाता है | ftp सिर्फ एक प्रोटोकॉल ही नहीं है ये एक प्रोग्राम भी है जो एप्लीकेशन के द्वारा काम में लिया जाता है | ftp के द्वारा एम्प्लोयी के द्वारा फाइल ट्रांसफर हाथो से किया जाता है |



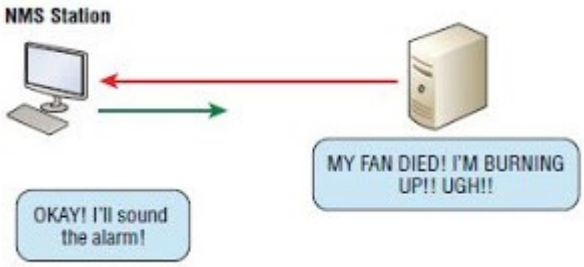
TFTP

tftp, ftp का कम फीचर वाला वर्शन है | अगर आप जानते है की कैसे और क्या करना है तो आप इसका इस्तेमाल कर सकते है, ये आसान और फ़ास्ट है | इसका ज्यादा इस्तेमाल सिस्को devices में सिस्टम को मेनेज करने में किया जाता है |



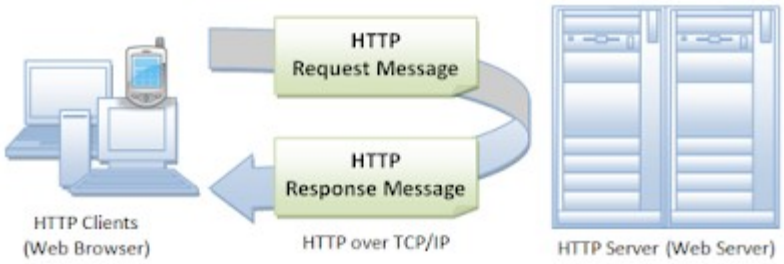
SNMP- (Simple Network Management Protocol)

इस प्रोटोकॉल का काम, नेटवर्क में हो रहे काम की इनफार्मेशन को कलेक्ट करना है | नेटवर्क में किसी भी तरह की प्रॉब्लम आने पर उसको इनफार्मेशन इसी के द्वारा दी जाती है |



Hypertext Transfer Protocol (HTTP)

आपने बहुत सारी बहुत तेज़ वेबसाइट देखीं होंगी जोकि ग्राफ़िक्स, लिंक्स, text और ऐड और भी काफी चीज़े मिलाकर बनती है और बनने के बाद इसको चलने का काम एचटीटीपी के ऊपर ही निर्भर करता है |



आपके वेब ब्राउज़र और वेब सर्वर के बीच में कम्युनिकेशन बनाये रखता है और आप जिस भी लिंक पर क्लिक करते है उससे सम्बंधित सही जानकारी आप तक पहुंचाने की जिम्मेदारी इसी की है | और यहाँ कितना सटीक होना चाहिए आप समझ सकते है क्यों आजकल इतनी वेबसाइट है और एक वेबसाइट एक बार में पता नहीं कितने लोगो से कनेक्ट रहती है उदाहण के तौर पर गूगल या फिर फेसबुक को देख लीजिये |

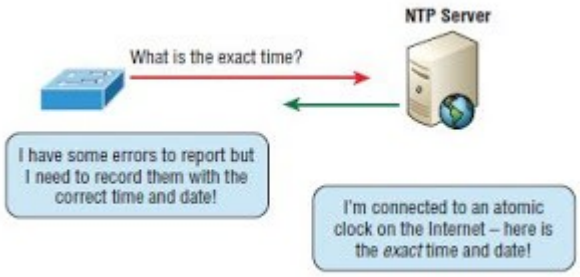
Hypertext Transfer Protocol Secure (HTTPS)

hypertext transfer protocol भी सिक्योर HTTPS की तरह जाना जाता है | ये secure socket layer (ssl) का इस्तेमाल करता है | वैसे तो काफी सरे तथ्य है इसके पर उन सब के अलावा आपको बस ये जान लेना चाहिए की ये प्रोटोकल आपके वेब कम्युनिकेशन को सुरक्षित करता है | जैसे आप देख सकते है आजकल बैंक्स की साइट्स सिक्योर होती है |

NetworkTimeProtocol (NTP)

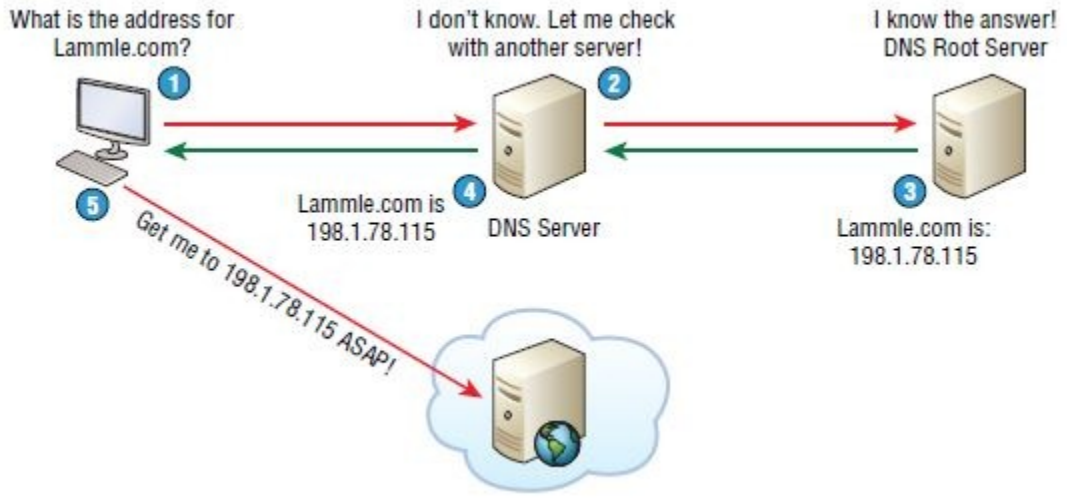
जैसा की आप जानते होंगे की ये प्रोटोकॉल आपके कंप्यूटर के टाइम को औटोमिक क्लॉक सर्वर से सिंक्रोनाइज करता है और आपके कंप्यूटर पर बिक्लकुल सही समय दीखता है | वैसे तो ये साधारण लगता है कि इसका क्या

काम होता होगा पर टेक्नोलॉजी में इसका बड़ा योगदान है | आप देखिये अगर टाइम सिंक नहीं होगा तो आपका बैंक से कोई भी ट्रान्सफर नही कर पाएंगे | आपने देखा होगा की सिक्योर ट्रांसफर कितना तेज़ी से होता है तो ntp वहां पर बहुत बड़ा रोल निभा रहा होता है |



Domain Name Service (DNS)

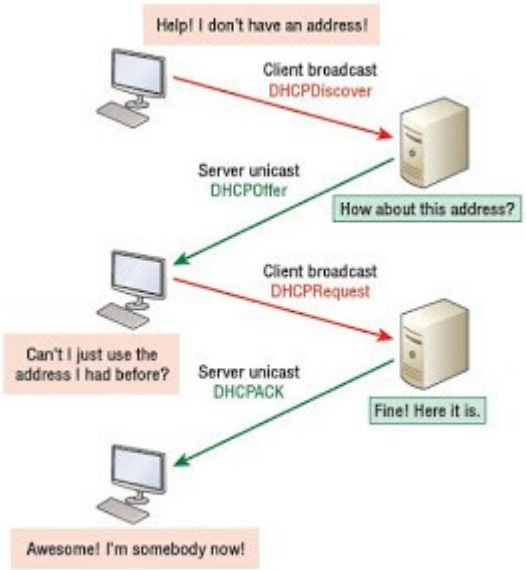
DNS का काम नाम बदलना है, खास करके इन्टनेट नेम्स (WWW) से शुरू होने वाले | पर इसको आपको अपने हाथो से इस्तेमाल करने की जरुरत नहीं है | जैसे ही आप Cisco.com पिंग करेंगे तो dns अपने आप ही इसको बदल कर इसका IP एड्रेस दिखा देखा | dns ने इन्टरनेट को बहुत ही आसान कर दिया है | जिस तरह से आप अपने मोबाइल पर हर मोबाइल नंबर याद नहीं रख सकते और नंबर की जगह आप जिसका नंबर है उसका नाम लिख देते है और आपको सर्च करने में आसानी होती है उसी तरह से dns काम करता है जब आप किसी भी साईट का नाम टाइप करते है तो dns उस नाम से जुड़े हुए IP एड्रेस को इन्टरनेट पर सर्च करके अपने आप खोल देता है |



Dynamic Host Configuration Protocol (DHCP)/Bootstrap Protocol (BootP)

DHCP का काम होस्ट्स हो ip एड्रेस देना है | ये सभी कंपनियों के लिए, फिर वो चाहे छोटी हो या फिर बड़ी काम को और भी आसान बनाने का काम करता है | dhcp सर्वर के लिए बहुत सारे हार्डवेयर काम में लिए जाते है उनमे से एक cisco के राऊटर भी है | dhcp, bootp से बिलकुल अलग है | bootp होस्ट्स हो एड्रेस तो प्रोवाइड करा देता है पर होस्ट्स का हार्डवेयर एड्रेस bootp की टेबल में मैन्युअली डालना पड़ता है | आप dhcp को डायनामिक bootp की तरह देख सकते है | पर आपको बता दू कि bootp ऑपरेटिंग सिस्टम भेजने का काम भी करता है जिससे क्लाइंट बूट कर सकते है | काफी चीज़े है जो dhcp प्रोवाइड करवाता है उनमे से ये कुछ खास है -

1. IP एड्रेस
2. Subnet Mask
3. Domain Name
4. Default Gateway (Routers)
5. DNS Server Address
6. Wins Server Address



Automatic Private IP Addressing (APIPA)

ओके, सोचिये क्या हो अगर आपके पास एक स्विच हो और उस स्विच से कुछ सिस्टम्स कनेक्टेड हो और आपके पास dhcp सर्वर न हो ? तो आप static ip addressing कॉन्फ़िगर कर सकते है | पर आपको ये करने की जरुरत नहीं पड़ेगी क्योंकि माइक्रोसॉफ्ट एक सर्विस प्रोवाइड करवाता है जिसको apipa कहते है | इसके अतर्गत अगर dhcp सर्वर ना हो तो माइक्रोसॉफ्ट ऑपरेटिंग सिस्टम अपने आप ही सभी सिस्टम आपस में कॉन्फ़िगर कर देता है अपनी ip रेंज में से सभी सिस्टम्स को ip लगाकर | The IP address range for APIPA is 169.254.0.1 through 169.254.255.254.

Host to Host Layer/Transport Layer के कुछ प्रोटोकॉल्स

ये लेयर डाटा को सेंड करने लिए तेयार करता है | इस लेयर में 2 प्रकार के प्रोटोकॉल्स आते है :-

1. Transmission Control Protocol (TCP)

2. User Data gram Protocol (UDP)

1. Transmission Control Protocol (TCP)

टी सी पी प्रोटोकॉल एप्लीकेशन से भारी मात्रा में डाटा को उठाता है और उसको छोटे छोटे सेगमेंट में बांटता है | ये हर एक सेगमेंट को एक नंबर लगाकर आगे भेजता है ताकि रिसीव करने वाले को भी सीक्वेंस से ही डाटा मिले और डाटा में कोई गड़बड़ ना हो | एक सेगमेंट सेंड करने के बाद रिसीवर के द्वारा acknowledgement का वेट करता है acknowledgment मिलने के बाद ही दूसरा सेगमेंट सेंड किया जाता है | इस प्रकार के प्रोतोकोल में डाटा पहुंचा या नहीं इसकी इनफार्मेशन पहले ली जाती है | इसलिए इस प्रकार का कनेक्शन connection ओरिएंटेड की केटेगरी में आता है |

2. User Data gram Protocol (UDP)

udp टी सी पी सेर थोडा अलग प्रोटोकल है | ये टी सी पी की तरह सेगमेंट की सीक्वेंस नहीं करता है और ना ही ध्यान रखता है की कौनसा पैकेट पहले आ रहा है और कौनसा पैकेट बाद में | UDP बस सेगमेंट को सेंड करता है और भूल जाता है | डाटा पहुंचा या नहीं इसकी भी इनफार्मेशन ये नहीं लेता है | क्योंकि ये unreliable प्रोटोकॉल की केटेगरी में आता है | पर इसका मतलब ये नहीं है की ये बेकार है और इफेक्टिव नहीं है | ये टी सी पी की जैसे वर्चुअल सर्किट भी नहीं बनाता और ना ही डाटा भेजने से पहले डेस्टिनेशन सिस्टम से कांटेक्ट करता है | तो इन प्रोसेस के ना होने की वजह से ही ये प्रोटोकॉल टी सी पी से बहुत तेज़ है | इसलिए जब भी कभी ऐसा एप्लीकेशन जिसमे तेज़ी के साथ डाटा सेंड किया जाना है तो UDP को ही इस्तेमाल किया जाता है |

The Internet Layer Protocols

dod मॉडल में इन्टरनेट लेयर को 2 मुख्य कारणों से काम में लिया जाता है एक तो रूटिंग के लिए और दूसरा ऊपर की लेयर को सिंगल नेटवर्क इंटरफ़ेस प्रोवाइड करवाने के लिए | इन्टरनेट लेयर बाकि सभी प्रोटोकॉल को भी जोड़े रखने का काम भी करती है | इन्टरनेट लेयर के कुछ मुख्य प्रोटोकॉल्स है जो इस प्रकार है :-

1.Internet Protocol (IP)
2.Internet Control Message Protocol (ICMP)
3.Address Resolution Protocol (ARP)

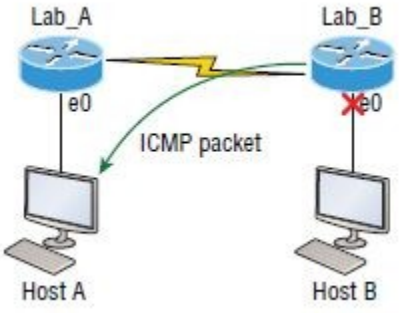
1. Internet Protocol (IP)

इस लेयर में मुख्य प्रोटोकॉल ip है और बाकी प्रोटोकॉल्स इसको सपोर्ट करने के लिए है | ip बहुत बड़ा है और ये सभी को आपस में जोड़ कर रखता है | ip हर पैकेट के एड्रेस में पाया जाता है इसी की वजह से रूटिंग टेबल में पता लगाया जाता है कि किसी भी पैकेट को कौनसी दिशा में भेजना है | नेटवर्क में किसी भी डिवाइस की पहचान के लिए फिजिकल और लॉजिकल दोनों ही प्रकार के एड्रेस के आवश्यकता पड़ती है | राऊटर के द्वारा प्राप्त किये जाने वाले पैकेट को आगे भेजने के लिए लिए जाने वाले डिसिशन ip के ऊपर ही होते है |

2.Internet Control Message Protocol (ICMP)

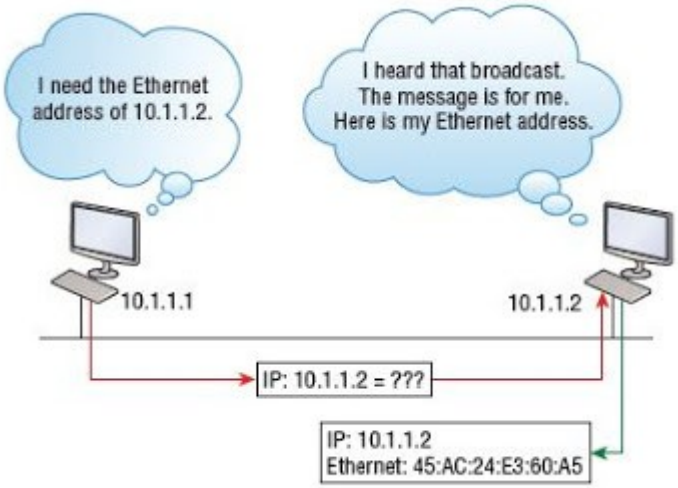
ये प्रोटोकॉल नेटवर्क लेयर पर काम करता है और इसका IP के द्वारा इस्तेमाल किया जाता है | ये साधारणतया मेनेजमेंट और मेसेंज़िंग प्रोटोकॉल है | ये प्रोटोकॉल, नेटवर्क में एरर होने पर एक मेसेज होस्ट तक पहुचाने का काम करता है |

Destination Unreachable - अगर राऊटर किसी ip डाटाग्राम को आगे भेजने में सक्षम नहीं हो पता तो वो वापस होस्ट को एक रिवर्स मेसेज सेंड करता है कि वो डाटा को आगे नहीं भेज पा रहा है या फिर डेस्टिनेशन अवेलेबल नहीं है |



3.Address Resolution Protocol (ARP)

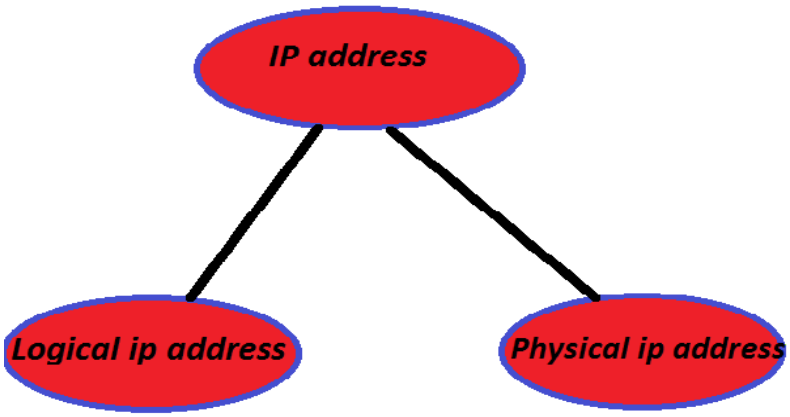
arp किसी भी नेटवर्क में ip एड्रेस से किसी भी होस्ट का हार्डवेयर एड्रेस फाइंड करने का काम करता है | याद रखे ऊपर की लेयर के द्वारा किसी भी डाटा को आगे भेजने के लिए पहले ही डेस्टिनेशन ip एड्रेस बता दिया जाता है लेकिन अगर किसी कारण वश ip एड्रेस नहीं मिलता तो arp टेबल का इस्तेमाल किया जाता है इसके द्वारा एक ब्रॉडकास्ट मेसेज सभी होस्ट हो भेजा जाता है जिसमे उनको ip एड्रेस बता कर उनका हार्डवेयर एड्रेस पुचा जाता है ताकि डाटा जिसका है उसी के पास भेजा जा सके |


I need the Ethernet address of 10.1.1.2.
I heard that broadcast. The message is for me. Here is my Ethernet address.
10.1.1.1
10.1.1.2
IP: 10.1.1.2 = ???
IP: 10.1.1.2
Ethernet: 45:AC:24:E3:60:A5

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

Concept of physical and logical addressing

IP Address (Internet protocol address) किसी system या Devise पर work करता है! IP Address किसी भी device का एक Networking पता होता है जिसके through वह Network को एक्सेस करता है और उस Devices को Verify करता है की Network or internet से connected है एक तरह से हम यह भी कह सकते है की IP Address उस अमुक उपकरण(devices) का Address होता है जो किसी internet या Network को access कर रहा होता है IP address नेटवर्क पर विशेष Device के लिए डेटा भेजने के लिए Network से Connected प्रत्येक Device -जैसे, कंप्यूटर, सर्वर, प्रिंटर, स्मार्टफ़ोन का एक यूनिक एड्रेस होता है और Communication के लिए Internet protocol का उपयोग करते हैं।



ip address

IP Address मुख्य रूप से दो प्रकार के होते है

1- logical IP address

2 - physical IP address

Logical IP address हमेसा बदलता रहता है यह dynamic होता है परन्तु Physical IP address static होता है ये world में किसी भी devise के लिए यूनिक रहता है ! हालाँकि hacking के वक्त hacker अपना Physical IP address change कर दे ते है Physical IP Address को Make Address के नाम से भी जाना जाता है

1 -Logical IP Address

OSI model के अनुसार देखे तो network layer में logical addressing यूज़ की जाती है। Logical addresses एक network को दूसरे network से separate भी करते है। Logical addresses fix नहीं होते है इन्हे change भी किया जा सकता है। Logical addresses को IP address कहते है। IP address की size 32 bit होती है। एक IP address 2 parts में divided होता है। पहला part होता है network ID जिससे ये identify किया जाता है की host का network क्या है।

दूसरा part होता है host ID जिससे से host को uniquely identify किया जाता है।

Logical addressing के लिए Internet Protocol (IP) responsible होता है। Internet protocol 2 tasks perform करता है।पहला logical addressing और दूसरा routing। Routing के माध्यम से एक packet को सही network में forward किया जाता है। Internet protocol 2 तरह की addressing provide करता है। एक IPV4 addressing और दूसरी IPV6 addressing होती है।

IPv4

IPV4 addressing में 32 bit addresses assign किये जाते है। इस तरह के IP address में 8 bits के चार octet होते है।

IP4 में 4 digit होती है जिसको Point के बाद हर Digit ओक्टेट के नाम से जाना जाता है उदारणत: 192.168.23.4 ये एक ipv4 का IP Address है यह एक सामान्य उदाहरण है। सबसे आसानी से पहचाने जाने वाली आईपी रेंज 192.168.0.1 – 192.168.0.255 हैं, क्योंकि इन एड्रेस को हम घर या ऑफिस कॉलेज आदि पर उपयोग करते हैं| IPV4 32 Bit का होता है! यह IP Address मुख्य रूप से 5 Class में divide होता है A ,B ,C ,D .E जिसमे D और E Class reserve होती है इनको publicly use नही किया जाता है IPV4 के हर Address के साथ सबनेट मास्क (Subnet mask) जुड़ा होता है जिसको देख कर यह आसानी से पता लगाया जा सकता है की कोनसा एड्रेस Host Address और कोनसा Network Address है और broad cast address है इसके बारे में हम next Tutorial में पढ़ेंगे की कैसे IP Address का Binary conversion किया जाता है और उनको छोटे पार्ट्स sub network में कैसे किया जाता है Subset mask के through

NO	Number of Class	Discretion about IP address
1	CLASS A(0-126)	exp. 10.22.23.7 submit mask (255.0.0.0)
2	CLASS B(127-191)	exp. 132.15.29.7 submit mask (255.255.0.0)
3	CLASS C(192-223)	exp.193.123,142,10 submit mask (255.255.255.0)
4	CLASS D	(224-239) this ip is used in gaming and multi-casting area
5	CLASS E(240- 255)	this ip is reserve in research area

(note-Windows operating System में अपना Ip address देख ने के लिए Follow करे Windows + R key >just type in Run windows >Cmd then command prompt open Command prompt में टाइप करे >ipconfig)

Class	Class A	Class B	Class C	Class D	Class E
नेटवर्क नंबर बिट फिल्ड	8	16	24	not defined	not defined
नेटवर्क कि संख्या	128 (27)	16,384 (214)	2,097,152 (221	not defined	not defined
एड्रेस रेंज	0.0.0.0 to 127.255.255.255	128.0.0.0 to 191.255.255.255	192.0.0.0 to 223.255.255.255	224.0.0.0 to 239.255.255.255	240.0.0.0 to 254.255.255.254
सपोर्ट	प्रत्येक 126 नेटवर्क पर 16 लाख होस्ट को सपोर्ट करता हैं।	प्रत्येक 16,000 नेटवर्क पर 65,000 होस्ट को सपोर्ट करता हैं।	प्रत्येक 2 लाख नेटवर्क पर 254 होस्ट को सपोर्ट करता हैं।	बहु प्रसारण के लिए आरक्षित।	भविष्य में उपयोग के लिए आरक्षित, या रिसर्च और डेवलपमेंट के लिए आरक्षित।

The classes of IPv4 addresses

The different classes of the IPv4 address are the following:

1) Class A address

2) Class B address

3) Class C address

4) Class D address

5) Class E address

Class A Address

The first bit of the first octet is always set to zero. So that the first octet ranges from 1 – 127. The class A address only include IP starting from 1.x.x.x to 126.x.x.x. The IP range 127.x.x.x is reserved for loop back IP addresses. The default subnet mask for class A IP address is 255.0.0.0. This means it can have 126 networks (27-2) and 16777214 hosts (224-2). Class A IP address format is thus: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH.

Class B Address

Here the first two bits in the first two bits is set to zero. Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has 16384 (214) Network addresses and 65534 (216-2) Host addresses. Class B IP address format is: 10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of this class has its first 3 bits set to 110. Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x. Class C gives 2097152 (221) Network addresses and 254 (28-2) Host addresses. Class C IP address format is: 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

Class D Address

The first four bits of the first octet in class D IP address are set to 1110. Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not intended

for a particular host, but multiple ones. That is why there is no need to extract host address from the class D IP addresses. The Class D does not have any subnet mask.

Class E Address

The class E IP addresses are reserved for experimental purpose only for R&D or study. IP addresses in the class E ranges from 240.0.0.0 to 255.255.255.254. This class too is not equipped with any subnet mask.

IPv6

IPv6 Internet Engineering Task Force द्वारा बनाया गया है यह IPv4 के साथ भी Work करता है IPV6 भविष्य के लिए reserve है IPv6 128 बिट्स लंबा होता हैं। इसलिए, यह 2 ^ 128 इंटरनेट एड्रेस को सपोर्ट करता हैं, जो 340.282.366.920.938.000.000.000.000.000.000.000.000 एड्रेस के बराबर हैं|यह एक इतना बड़ा IP Address होता है की World के हर person को लगफग 20,000 IP address मिल सकता है तो इसके Digit के कम पड़ने का सवाल ही नही उठता है यह बहुत सारे address हैं और वे बहुत लंबे समय तक internet operation जारी रखने के लिए पर्याप्त से अधिक हैं।जहा IPv4 point के through 4 डिजिट Group में define किया जाता है वही IPv6 hexadecimal number में 8 group में define या Represent किया जाता है

2- Physical IP Address / hardware address

Physical IP address को Mack Address के नाम से भी जाना जाता है यह वर्ल्ड की हर device का एक unique IP Address होता है यह पूरी तरह से static ip address हो ता है इसको कभी भी permanently change नही किया जासकता है Windows operating system में mac address देखने के लिए c ommand promp में /getmac command का प्रयोग कर देखा जा सकता है. OSI model के अनुसार देखे तो layer 2 (Data link layer) पर hardware addressing यूज़ की जाती है। Hardware address को MAC (Media Access Control) address भी कहते है। MAC address को network interface cards (NIC) पर hard-code किया जाता है। MAC address की size 48 bits होती है। एक MAC address hexadecimal form में represent किया जाता है। इसका उदाहरण नीचे दिया जा रहा है।

MAC address की पहली 6 digits से NIC (Network Interface Card) के manufacturer को identify किया जाता है।इन शुरुआती 6 bits को OUI (Organizational Unique Identifier) भी कहते है। बाकी की 6 digits host को network में uniquely identify करने के लिए यूज़ की जाती है।इन last 6 digits को host id कहते है। MAC address के अंदर एक कमी होती है इससे से आप network को नहीं identify कर सकते है।

Subnetting

subnetting एक ऐसी विधि है िजसमें एक बड़े नेटवक को दो या दो से अधिक छोटे लॉजकल नेटवरक में विभाजत किया जाता है. इन छोटे नेटवर्क को subnetwork या subnet कहा जाता है. इन subnetwork या subnet का अपना अलग-अलग address होता है. इन छोटे network को बनाने के लए subnet mask का प्रयोग किया जाता है. subnet mask को IP एड्रेस में network address तथा host address के बीच differentiate (अतर) करने के लिए प्रयोग किया जाता है. subnet mask का केवल एक मुख्य उद्देश्य होता है यह identify करना क IP address का कौन सा भाग network address है और कौन सा भाग host address.

. **subnet (sub network**

सुपरनेटिंग सबनेटिंग के विपरीत है। सबनेटिंग में, एक बड़े नेटवर्क को कई छोटे subnet में विभाजित किया जाता है। सुपरनेटिंग में, कई नेटवर्क को एक बड़े नेटवर्क में जोड़ दिया जाता है जिसे सुपरन नेटवर्क या सुपरनेट कहा जाता है। एक सबनेट IP network के कई छोटे नेटवर्क segment का एक logical विभाजन है। इसका उपयोग आमतौर पर बड़े नेटवर्क को छोटे, more efficient कार्य करने में किया जाता है। each subnet का own subnet adress होता है इन छोटे network को बनाने के लिए subnet mask का प्रयोग किया जाता है.

subnet mask को IP address में network address तथा host address के बीच differentiate करने के लिए किया जाता है

subnet mask का केवल एक ही मुख्य उद्देश्य होता है यह identify करना कि IP address का कौन सा भाग network address है और कौन सा भाग host address.

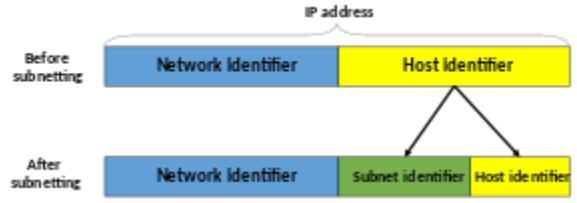
इंटरनेट कई नेटवर्क से बना है जो कई organizations द्वारा चलाए जाते हैं। प्रत्येक organizations का नेटवर्क कई छोटे नेटवर्क या सबनेट से बना हो सकता है तथा devices को एक दूसरे के साथ communicate करने की अनुमति देता है . subnet के बीच communicate करने के लिए routers का उपयोग किया जाता है। सबनेट का आकार कनेक्टिविटी आवश्यकताओं और employed network technology पर निर्भर करता है . point-to-point subnet दो डिवाइस को कनेक्ट करने की अनुमति देता है, जबकि एक data center subnet में एक से अधिक devices कनेक्ट करने के लिए डिज़ाइन किया जा सकता है।

प्रत्येक organization अपने उपयोग के लिए available address space की सीमा के भीतर, जो भी सबनेट बनाता है तो number and size of the subnets निर्धारित करने के लिए जिम्मेदार होता है.

किसी organization के भीतर सबनेट विभाजन का विवरण उस organization के लिए local रहता है। internet में मौजूद किसी organization के Network devices को other organizations के subnet segmentation की details जानने की आवश्यकता नहीं है .

why use subnetting

इसकी जरूरत इसलिए पड़ी जब इंटरनेट popular हुआ तो सभी IP adress consume होने वाले थे अर्थात उस समय IP adress shortage (कमी) हो गयी थी जससे इंटरनेट का भविष्य खतरे में था और यह खतम हो जाता. इसी परेशानी से बचने के लिए subnetting को बनाया गया.



Subnetting Benefits

Improve network performance and speed

Reduce network congestion

Boost network security

Control network growth

Ease administration

subnets also helpful to minimize the size of the routing tables on the internet

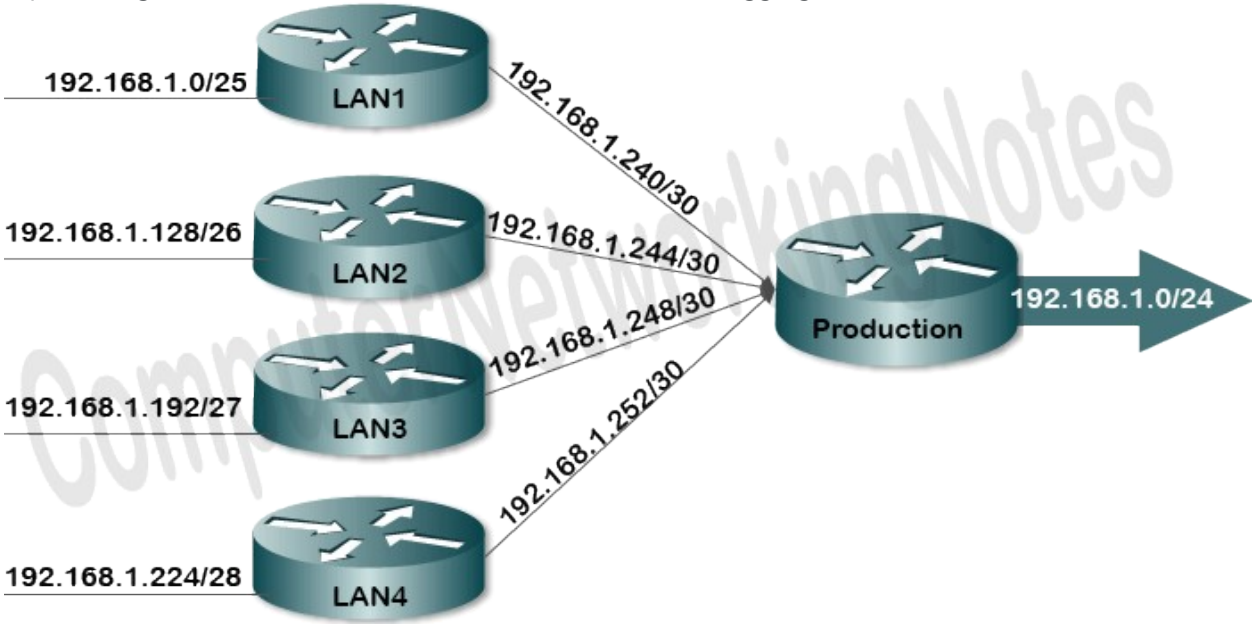
Disadvantage

Subnetting decreases the total number of IP addresses in the network but may need buying additional hardware such as a router. So, it may cost lots of money.

subnets को मैनेज करने के लिए experienced administrative की जरूरत होती है

Supernetting

सुपरनेटिंग सबनेटिंग के विपरीत है। सबनेटिंग में, एक बड़े नेटवर्क को कई छोटे सबनेटवर्क में विभाजित किया जाता है। सुपरनेटिंग में, कई नेटवर्क को एक बड़े नेटवर्क में जोड़ दिया जाता है जिसे सुपरन नेटवर्क या सुपरनेट कहा जाता है।
Supernetting is also known as route summarization and route aggregation.



In above example, 8 subnets are summarized in single subnet.

Supernetting का उपयोग मुख्य रूप से Route Summarization,में किया जाता है, जहां समान network prefixes वाले कई नेटवर्कों के मार्गों को single routing entry में जोड़ा जाता है, रूटिंग एंट्री के साथ एक सुपर नेटवर्क की ओर इशारा करते हुए, सभी नेटवर्क शामिल हैं। यह बदले में रूटिंग तालिकाओं के आकार को कम करता है और राउटिंग प्रोटोकॉल द्वारा एक्सचेंज किए गए राउटिंग अपडेट के आकार को भी कम करता है।
सुपरनेटिंग एक एड्रेसिंग स्कीम है जिसमें कई श्रेणी के सी ब्लॉक को मिलाकर एक बड़ी रेंज बनाई जा सकती है

उदाहरण के लिए, एक organization जिसे 1,000 addresses की आवश्यकता होती है, उसे चार contiguous class C ब्लॉक दिए जा सकते हैं। organization तब इन पते का उपयोग कर एक सुपरनोटवर्क बना सकता है।

Advantages of Supernetting

- The size of the router memory table is minimized by summarizing several routing information entries into a single entry.
- It also increases the speed of routing table lookup.
- Provision for the router to isolate the topology changes from the other routers.
- It also reduces the network traffic.
  - It reduces the size of routing updates.
  - It provides a better overview of network.
  - It decreases the use of resources such as Memory and CPU.
  - It decreases the required time in rebuilding the routing tables.

Disadvantages of Supernetting

- The combination of blocks should be made in power 2; alternatively, if the three blocks are required, then there must be assigned four blocks.
- The whole network should exist in the same class.
- When merged, it lacks covering different areas.

BASIS FOR COMPARISON	SUBNETTING	SUPERNETTING
Basic	A process of dividing a network into subnetworks.	A process of combining small networks into a larger network.
Procedure	The number of bits of network addresses is increased.	The number of bits of host addresses is increased.
Mask bits are moved towards	Right of the default mask.	Left of the default mask.
Implementation	VLSM (Variable-length	CIDR (Classless interdomain

BASIS FOR COMPARISON	SUBNETTING	SUPERNETTING
	subnet masking).	routing).
Purpose	Used to reduce the address depletion.	To simplify and fasten the routing process.