IRJC
International Journal of Social Science & Interdisciplinary Research
Vol.1 Issue 11, November 2012, ISSN 2277 3630

FUNDAMENTALS OF COMPUTER NETWORKS

DR. K.V.S.N. JAWAHAR BABU*; MR. S. MUNIKUMAR**

* Principal
K M M Institute Of Technology & Science
Ramireddipalle, Tirupati, Andhra Pradesh, India

** Assistant Professor
Dept. Of Computer Science & Engineering
K M M Institute Of Technology & Science
Ramireddipalle, Tirupati, Andhra Pradesh, India

ABSTRACT

A computer network, often simply referred to as a network, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information. Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. Simply, more than one computer interconnected through a communication medium for information interchange is called a computer network. Networks may be classified according to a wide variety of characteristics, such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope. Communications protocols define the rules and data formats for exchanging information in a computer network, and provide the basis for network programming. Well-known communications protocols include Ethernet, a hardware and link layer standard that is ubiquitous in local area networks, and the Internet protocol suite, which defines a set of protocols for internetworking, i.e. for data communication between multiple networks, as well as host-to-host data transfer, and application-specific data transmission formats.

KEYWORDS: configuration, computers, communication, network, protocols, transmission.

---

1. INTRODUCTION

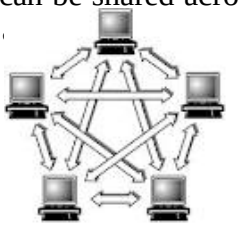
Computer networks that were based upon some type of telecommunications system, communication between calculation machines and early computers was performed by human users by carrying instructions between them. A computer network consists of a collection of computers, printers and other equipment that is connected together so that they can communicate with each other. There are two types of network configuration, Peer-to-Peer networks and Client/Server networks.

Using a network, people can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing. In a network environment, authorized users may access data and information stored on other computers on the network. The

capability of providing access to data and information on shared storage devices is an important feature of many networks.

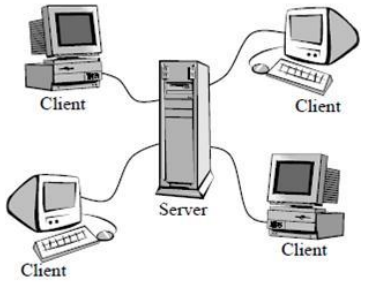
A computer network may be used by computer hackers to deploy computer viruses or computer worms on devices connected to the network, or to prevent these devices from normally accessing the network. Power line communication strongly disturbs certain forms of radio communication. It may also interfere with last mile access technologies such as ADSL and VDSL. A complex computer network may be difficult to set up. It may also be very costly to set up an effective computer network in a large organization or company.

Peer-to-peer networks are more commonly implemented where less then ten computers are involved and where strict security is not necessary. All computers have the same status, hence the term 'peer', and they communicate with each other on an equal footing. Files, such as word processing or spreadsheet documents, can be shared across the network and all the computers on the network can share devices, such as printers, which are connected to any one computer.



Peer to Peer

Client/Server Networks are more suitable for larger networks. A central computer, or 'server', acts as the storage location for files and applications shared on the network. Usually the server is a higher than average performance computer. The server also controls the network access of the other computers which are referred to as the 'client' computers. Typically, Faculty and students in a College will use the client computers for their work and only the network administrator (Chairman or Principal) will have



Client/Server

CATEGORIES OF NETWORKS

Local Area Network:

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-T G.hn also provide a way to create a wired LAN using existing home wires (coaxial cables, phone lines and power lines).

Typical library network, in a branching tree topology and controlled access to resources

A sample LAN is depicted in the accompanying diagram. All interconnected devices must understand the network layer (layer 3), because they are handling multiple subnets (the different colors). Those inside the library, which have only 10/100 Mbit/s Ethernet connections to the user device and a Gigabit Ethernet connection to the central router, could be called "layer 3 switches" because they only have Ethernet interfaces and must understand IP. It would be more correct to call them access routers, where the router at the top is a distribution router that connects to the Internet and academic networks' customer access routers.

The defining characteristics of LANs, in contrast to WANs (Wide Area Networks), include their higher data transfer rates, smaller geographic range, and no need for leased telecommunication lines. Current Ethernet or other IEEE 802.3 LAN technologies operate at data transfer rates up to 10 Gbit/s. IEEE has projects investigating the standardization of 40 and 100 Gbit/s. LANs can be connected to Wide area network by using routers.

Metropolitan Area Network:

A metropolitan area network (MAN) is a computer network that usually spans a city or a large campus. A MAN usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks (or WAN) and the Internet.

The IEEE 802-2002 standard describes a MAN as being

A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for internetworking of local networks.

A Metropolitan Area Network (MAN) is a large computer network that spans a metropolitan area or campus. Its geographic scope falls between a WAN and LAN. MANs provide Internet connectivity for LANs in a metropolitan region, and connect them to wider area networks like the Internet.

It can also be used in cable television.

Wide Area Network

A Wide Area Network (WAN) is a telecommunication network that covers a broad area (i.e., any network that links across metropolitan, regional, or national boundaries). Business and government entities utilize WANs to relay data among employees, clients, buyers, and suppliers from various geographical locations. In essence this mode of telecommunication allows a business to effectively carry out its daily function regardless of location.

This is in contrast with personal area networks (PANs), local area networks (LANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area (e.g., a city) respectively.

Virtual private network

A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features,

such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

Home area network

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

Storage area network

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

Campus area network

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

In the case of a university campus-based campus network, the network is likely to link a variety of campus buildings including, for example, academic colleges or departments, the university library, and student residence halls.

Backbone network

A backbone network is part of a computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the backbone's capacity is greater than that of the networks connected to it.

A large corporation which has many locations may have a backbone network that ties all of these locations together, for example, if a server cluster needs to be accessed by different departments of a company which are located at different geographical locations. The equipment which ties these departments together constitute the network backbone. Network performance management including network congestion are critical parameters taken into account when designing a network backbone.

A specific case of a backbone network is the Internet backbone, which is the set of wide-area network connections and core routers that interconnect all networks connected to the Internet.

NETWORK TOPOLOGY

Common layouts:

A Network Topology is the layout of the interconnections of the nodes of a computer network. Common layouts are:

A Bus Network: all nodes are connected to a common medium along this medium. This was the layout used in the original Ethernet, called 10BASE5 and 10BASE2.

A Star Network: all nodes are connected to a special central node. This is the typical layout found in a Wireless LAN, where each wireless client connects to the central Wireless access point.

A Ring Network: each node is connected to its left and right neighbour node, such that all nodes are connected and that each node can reach each other node by traversing nodes left- or rightwards. The Fiber Distributed Data Interface (FDDI) made use of such a topology.

A Mesh Network: each node is connected to an arbitrary number of neighbours in such a way that there is at least one traversal from any node to any other.

A fully connected network: each node is connected to every other node in the network.

Note that the physical layout of the nodes in a network may not necessarily reflect the network topology. As an example, with FDDI, the network topology is a ring (actually two counter-rotating rings), but the physical topology is a star, because all neighboring connections are routed via a central physical location.

Overlay network

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay are connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may (and often does) differ from that of the underlying one.

A sample overlay network: IP over SONET over Optical

For example, many peer-to-peer networks are overlay networks because they are organized as nodes of a virtual system of links run on top of the Internet. The Internet was initially built as an overlay on the telephone network.

The most striking example of an overlay network, however, is the Internet itself: At the IP layer, each node can reach any other by a direct connection to the desired IP address, thereby creating a fully connected network; the underlying network, however, is composed of a mesh-like interconnect of subnetworks of varying topologies (and, in fact, technologies). Address resolution and routing are the means which allows the mapping of the fully connected IP overlay network to the underlying ones.

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

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

Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees to achieve higher-quality streaming media. Previous proposals such as IntServ, DiffServ, and IP Multicast have not seen wide acceptance largely because they require modification of all routers in the network. On the other hand, an overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. The overlay has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes a message traverses before reaching its destination.

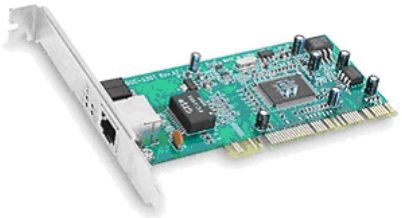
BASIC HARDWARE COMPONENTS

The physical communications media themselves as described above, networks comprise additional basic hardware building blocks interconnecting their terminals, such as network interface cards (NICs), hubs, bridges, switches, and routers.

Network interface cards

A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to physically access a networking medium. It provides a low-level addressing system through the use of MAC addresses.

Each Ethernet network interface has a unique MAC address which is usually stored in a small memory device on the card, allowing any device to connect to the network without creating an address conflict. Ethernet MAC addresses are composed of six octets. Uniqueness is maintained by the IEEE, which manages the Ethernet address space by assigning 3-octet prefixes to equipment manufacturers. The list of prefixes is publicly available. Each manufacturer is then obliged to both use only their assigned prefix(es) and to uniquely set the 3-octet suffix of every Ethernet interface they produce.



Repeaters and hubs

A repeater is an electronic device that receives a signal, cleans it of unnecessary noise, regenerates it, and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. A repeater with multiple ports is known as a hub. Repeaters work on the Physical Layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row (e.g. Ethernet's 5-4-3 rule).

Today, repeaters and hubs have been made mostly obsolete by switches.

Bridges

A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges broadcast to all ports except the port on which the broadcast was received. However, bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address to that port only.

Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

Bridges come in three basic types:

Local bridges: Directly connect LANs

Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.

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

Switches

A network switch is a device that forwards and filters OSI layer 2 datagrams (chunks of data communication) between ports (connected cables) based on the MAC addresses in the packets. A switch is distinct from a hub in that it only forwards the frames to the ports involved in the communication rather than all ports connected. A switch breaks the collision domain but represents itself as a broadcast domain. Switches make forwarding decisions of frames on the basis of MAC addresses. A switch normally has numerous ports, facilitating a star topology for devices, and cascading additional switches. Some switches are capable of routing based on Layer 3 addressing or additional logical levels; these are called multi-layer switches. The term switch is used loosely in marketing to encompass devices including routers and bridges, as well as devices that may distribute traffic on load or by application content (e.g., a Web URL identifier).

Routers

A router is an internetworking device that forwards packets between networks by processing information found in the datagram or packet (Internet protocol information from Layer 3 of the OSI Model). In many situations, this information is processed in conjunction with the routing table (also known as forwarding table). Routers use routing tables to determine what interface to forward packets (this can include the "null" also known as the "black hole" interface because data can go into it, however, no further processing is done for said data).

Firewalls

A firewall is an important aspect of a network with respect to security. It typically rejects access requests from unsafe sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in 'cyber' attacks for the purpose of stealing/corrupting data, planting viruses, etc.

NETWORK PERFORMANCE

Network performance refers to the service quality of a telecommunications product as seen by the customer. It should not be seen merely as an attempt to get "more through" the network.

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

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

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

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modelled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

NETWORK SECURITY

In the field of networking, the area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. Network security is the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. Network Security covers a variety of computer networks, both public and private that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

VIEWS OF NETWORKS

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

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

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

Unofficially, the Internet is the set of users, enterprises, and content providers that are interconnected by Internet Service Providers (ISP). From an engineering viewpoint, the Internet is the set of subnets, and aggregates of subnets, which share the registered IP address space and exchange information about the reachability of those IP addresses using the Border Gateway Protocol. Typically, the human-readable names of servers are translated to IP addresses, transparently to users, via the directory function of the Domain Name System (DNS).

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

References

1. Computer network definition, http://www.atis.org/glossary/definition.aspx?id=6555, retrieved 2011-11-12
2. Michael A. Banks (2008). On the way to the web: the secret history of the internet and its founders. Apress. p. 1. ISBN 978-1-4302-0869-3. http://books.google.com/books?id=P9wbSjO9WMMC&pg=PA1.
3. Christos J. P. Moschovitis (1998). History of the Internet: a chronology, 1843 to the present. ABC-CLIO. p. 36. ISBN 978-1-57607-118-2. http://books.google.com/?id=Hu5SAAAAMAAJ&dq=intitle%3A%22history+of+the+internet%22+sage+sabre&q=sage+sabre%27s#search_anchor.
4. Chris Sutton. "Internet Began 35 Years Ago at UCLA with First Message Ever Sent Between Two Computers". UCLA. Archived from the original on March 8, 2008. http://web.archive.org/web/20080308120314/http://www.engineer.ucla.edu/stories/2004/Internet35.htm.
5. Broadband Over Powerline, The National Association for Amateur Radio, http://www.arrl.org/broadband-over-powerline-bpl, retrieved 2011-11-12
6. "The Likelihood and Extent of Radio Frequency Interference from In-Home PLT Devices". Ofcom. http://stakeholders.ofcom.org.uk/binaries/research/technology-research/pltreport.pdf. Retrieved 18 June 2011.

7. "Mobile Broadband Wireless connections (MBWA)". http://grouper.ieee.org/groups/802/20/. Retrieved 2011-11-12.
8. Bergen Linux User Group's CPIP Implementation
9. A. Hooke (September 2000), Interplanetary Internet, Third Annual International Symposium on Advanced Radio Technologies, http://www.ipnsig.org/reports/ISART9-2000.pdf, retrieved 2011-11-12
10. Martin, Thomas. "Design Principles for DSL-Based Access Solutions". http://www.gsi.dit.upm.es/~legf/Varios/XDSL_MARTI.PDF. Retrieved 18 June 2011.
11. "personal area network (PAN)". http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci546288,00.html. Retrieved January 29, 2011.
12. New global standard for fully networked home, ITU-T, 2008-12-12, http://www.itu.int/ITU-T/newslog/New+Global+Standard+For+Fully+Networked+Home.aspx, retrieved 2011-11-12
13. IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force, http://www.ieee802.org/3/ba/, retrieved 2011-11-12
14. D. Andersen; H. Balakrishnan; M. Kaashoek; R. Morris (10-2001), Resilient Overlay Networks], Association for Computing Machinery, http://nms.lcs.mit.edu/papers/ron-sosp2001.html, retrieved 2011-11-12
15. "Define switch.". WWW.Wikipedia.com. http://www.webopedia.com/TERM/s/switch.html. Retrieved April 8, 2008.
16. "Basic Components of a Local Area Network (LAN)". NetworkBits.net. http://networkbits.net/lan-components/local-area-network-lan-basic-components/. Retrieved April 8, 2008.
17. Teletraffic Engineering Handbook, ITU-T Study Group 2, archived from the original on 2007-01-11, http://web.archive.org/web/20070111015452/http://oldwww.com.dtu.dk/teletraffic/handbook/telenook.pdf
18. Telecommunications Magazine Online, Americas January 2003, Issue Highlights, Online Exclusive: Broadband Access Maximum Performance, Retrieved on February 13, 2005.
19. "State Transition Diagrams". http://cne.gmu.edu/modules/os_perf/std.t.html. Retrieved July 13, 2003.
20. Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317–323. doi:10.1007/978-3-540-30176-9_41. ISBN 978-3-540-23659-7.
21. "Definitions: Resilience". ResiliNets Research Initiative. http://wiki.ittc.ku.edu/resilinets_wiki/index.php/Definitions#Resilience. Retrieved 2011-11-12.