PART I

BASIC NETWORKING

CHAPTER 1

INTRODUCTION TO COMPUTER NETWORKS

1.0

The world of computer networks and data communications is a surprisingly vast and increasingly significant field of study. Once considered primarily the domain of network specialists and technicians, computer networks now involve business managers, computer programmers, system designers, office managers, home computer users, and everyday citizens. It is virtually impossible for the average person on the street to spend 24 hours without directly or indirectly using some form of computer network.

Ask any group, "Has anyone used a computer network today?" and more than one-half of the people may answer, "Yes." Then ask the others: "How did you get to work, school, or the store today if you did not use a computer network?" Most transportation systems abroad use extensive communication networks to monitor the flow of vehicles and trains. Expressways and highways have computerized systems for controlling traffic signals and limiting access during peak traffic times. Some major cities are placing the appropriate hardware inside city buses so that the precise location of each bus is known. This information enables the transportation systems to keep the buses evenly spaced and more punctual.

In addition, a satellite system exists that, if you become lost while driving, will tell you precisely where your automobile is and give you directions. This system also can unlock your car doors if you leave your keys in the ignition, and it can locate your car in a crowded parking lot, then beep the horn and flash the headlights if you can't remember where you parked.

Businesses are able to order parts and inventory on demand and build products to customer-designed specifications, all electronically, without the need for paper. Online retail outlets can track every item you look at or purchase. Using this data, they can make recommendations of similar products and inform you in the future when a similar new product becomes available. Twenty-four-hour banking machines can verify the user's identity by taking the user's thumbprint.

In addition, cable television continues to expand, offering extensive programming, pay-per-view options, video recording, digital television and music, and multi-megabit connectivity to the Internet. The telephone system, the oldest and most extensive network of communicating devices, continues to become more of a computer network every day. Cellular telephone systems cover virtually the entire Ghana and include systems that allow users to upload and download data to and from the Internet, send and receive images, and download streaming video such as television programs.

Welcome to the amazing world of computer networks!

Unless you have spent the last 24 hours in complete isolation, it is nearly impossible to *not* have used some form of computer networks and data communications.

A computer network is an interconnection of computers and computing equipment using either wires or radio waves over a small or large geographic areas. Computer networks that use microwaves are termed wireless networks and can involve broadcast radio, microwaves or satellite transmissions.

1.2 Benefits and Uses of Networks

Networks have several uses and benefits such as sharing of data, sharing peripherals, sharing applications, provision of system resilience, security etc. These benefits are explained in detail below

1.2.1 Shared Data

One of the principal benefits of networking is the ability to share. Whether the data is a word processing document or a corporate database system, the ability to share the data is essential. Networks enable multiple users to access the same disk or disk system. A single copy of a file can be held on a central server rather than duplicating the file on each workstation. Facilities such as file and record locking ensure it is impossible for two users to simultaneously access the same piece of data.

This is one of the prime benefits of a network. Once there is a network, data in which ever form; word processing document, corporate database system, can be shared. It allows multiple users to access the same disk or disk system. A single copy of the file can be held on a central computer (server) rather than duplicating the file on each workstation. Security facilities such as file and record locking ensures that it is impossible for two users to access simultaneously the same file.

1.2.2 Sharing Peripherals

Networks allow users to share devices such as printers, scanners, modems, fax systems and CD-ROMs. Sharing can provide several benefits

- Fewer devices have to be purchased and maintained. The devices that are purchased can be of a higher specification and sharing this equipment between many users ensures it is used more efficiently
- Providing shared modems and fax systems allows system administrators to monitor and control the use of the facilities.

1.2.3 Sharing Applications

Some network applications can be configured with the program files located on a central server and just small numbers of files loaded onto the user's workstation or personal directory. Shared software can reduce administration time as upgrades can be implemented on the server with minimal changes required for each user. It also allows a system administrator to implement a standard configuration that reduces support costs and may simplify the control of software licenses. Its disadvantages lie in the increase in network traffic generated and the inability to work when the server is down.

Electronic messaging

Electronic mail (email) is one of the most common network applications. The messaging server acts as the central repository for messages. Users can submit messages to another user who is not currently connected to the network and the message waits at the server until the user connects to view his or her messages. The client messaging software is used to compose and address the message.
Widely used LAN-based messaging systems include Microsoft Exchange, Lotus Notes and Novell GroupWise.

Workgroup applications

Workgroup applications are designed to allow two or more users to improve their productivity by communicating and sharing information across a network. Oftan these Explications are based on messaging systems that have been enhanced to provide extra facilities. The most common example is scheduling applications. These enable users to view the appointment books of other users and schedule meetings. Examples of these include; Microsoft Outlook, Microsoft Schedule+ and Lotus Organizer.

Client-server applications

Older network applications were designed so that most of the processing effort was performed by the client machine. These applications are described as client-based. For example, in a database application, the server acted as a repository for the database (a shared file containing the data), while the client-based application performs all the queries and operations on the data. In this situation, the server is a passive participant.

A number of systems have been developed where both client and server are active participants. In a client-server system, the sewer performs most of the data manipulation and provides the client with the information requested. The server is typically a more powerful machine than the client computer. The reason for this is because it holds data locally and does not have to request information across the network. As a result, client-server systems generally provide better performance. The client machines can be of a lower specification because they are only required to make requests and display the results.

In essence, a client-server based system is one where the application's components are distributed amongst both clients and servers. Examples of client-server systems include; SQL Server pronounced "sequel server"), Oracle and Microsoft Exchange

1.2.4 Provision Of System Resilience

Local area networks can be used to provide system resilience. Centralized tape backup systems ensure data can be recovered after a disaster. Disk arrays using RAID technology allow the system to continue operating when a disk fails. For example, a mirrored hard drive duplicates data onto two hard drives, with the 'good' hard drive continuing to operate until the other can be replaced. Replication of data between servers allows them to act as a backup for each other, and

modern cluster technology provides grouping of servers so that the others can take over in the event of failure. The addition of another server to a cluster improves performance when the load becomes too great for the existing configuration.

Networks are especially vulnerable to virus infection, but have the advantage that a centralized virus policy can be implemented to protect all servers and workstations. By ensuring all servers and workstations hold an up-to-date version of the virus software, a administrator can minimize the risk to data. Virus software vendors provide software that automatically downloads the latest copy of the virus database to a workstation when an update is required.

1.2.5 Security

Local area networks offer varying levels of security. Simple network systems may use a password to control access to resources, while the more sophisticated systems control access by a user name. User names are an important part of network security and many network systems deny access until the user is provided a valid user name and password

1.3 Classification of Computer Networks

Computer networks can be classified under any of the following criteris depending on what is being discussed or considered;

- Scale
- Connection method
- Functional relationship (Network Architectures)
- Network topology
- Protocol
- Layers

By scale

Computer networks may be classified according to the scale: Personal area network (PAN), Local Area Network (LAN), Campus Area Network (CAN), Metropolitan area network (MAN), or Wide area network (WAN).

As Ethernet increasingly is the standard interface for networks, these distinctions are more important to the network administrator than the user. Network administrators may have to tune the network, to correct delay issues and achieve the desired performance level.

Network coverage ranges from small geographical size, such as around an individual, to very large areas such as spanning the whole world. The type of network depends solely on the range of the network. A breakdown of the various types is as indicated in the Table 1.1 below

Table 1.1

Network Type	**Descriptions**
Personal Area Network (PAN)	Networks spanning in the areas of several meters around an individual e.g. Personal Digital Assistants, Laptops
Local Area Network (LAN)	Networks with a wider range spanning a room, floor of a building or even within a building. Does not exceed a distance of 1.25 miles or 2km from end to end.
Campus Area Network (CAN)	This network is limited in scope to a

	single geographical area such as within a school campus, large company with several buildings,
Metropolitan Area Network (MAN)	This is a network that covers an area the size of a city or metropolis. It spans no more than tens of miles or kilometers. It can operate at speeds that are comparable to LANs
Wide Area Network (WAN)	These are wide networks encompassing parts of regions, multiple regions, countries-wide, inter-countries and inter-continents as well as world wide

By connection method

Computer networks can also be classified according to the hardware technology that is used to connect the individual devices in the network such as Optical fibre, Ethernet, Wireless LAN, HomePNA, or Power line communication.

Ethernets use physical wiring to connect devices. Often they employ hubs, switches, bridges, and/or routers.

Wireless LAN technology is built to connect devices without wiring. These devices use a radio frequency to connect.

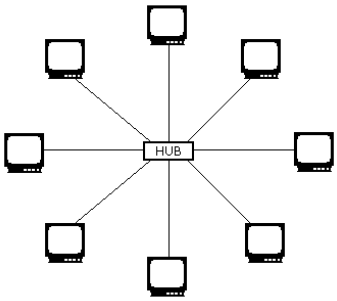
By functional relationship (Network Architectures)

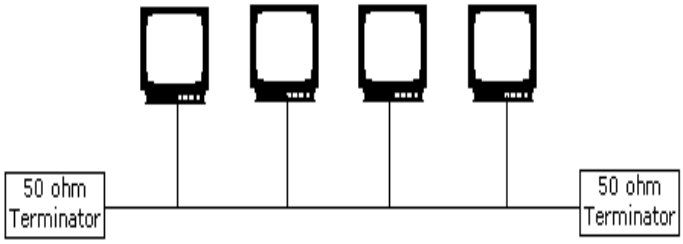
Computer networks may be classified according to the functional relationships which exist between the elements of the network, e.g., Active Networking, Client-server and Peer-to-peer (workgroup) architecture.

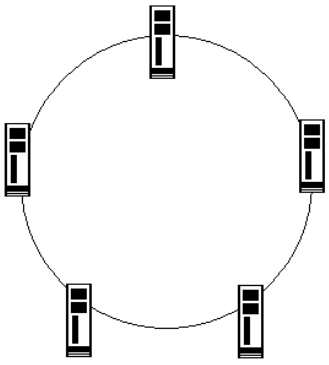
By network topology

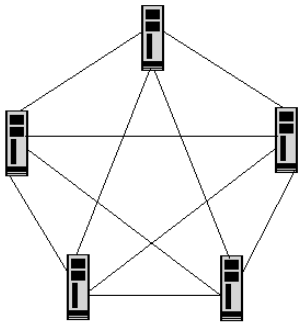
Computer networks may be classified according to the network topology upon which the network is based, such as Bus network, Star network, Ring network, Mesh network, Star-bus network, Tree or Hierarchical topology network, etc.

Network Topology signifies the way in which intelligent devices in the network see their logical relations to one another. The use of the term "logical" here is significant. That is, network topology is independent of the "physical" layout of the network. Even if networked computers are physically placed in a linear arrangement, if they are connected via a hub, the network has a Star topology, rather than a Bus Topology. In this regard the visual and operational characteristics of a network are distinct; the logical network topology is not necessarily the same as the physical layout.









By protocol

Computer networks may be classified according to the communications protocol that is being used on the network.

By layers

Networks may be classified by the network layer at which they operate according to basic reference models considered as standards in the industry, such as the five-layer Internet Protocol Suite model. While the seven-layer Open Systems Interconnection (OSI) reference model is better known in academia, the majority of networks use the Internet Protocol Suite (IP).

These networks are often made to enable data and resource sharing by transmitting signal s from one point to the other across a medium of connection which could be either cable or wireless as noted earlier. It is also important to understand that data and signals are not the same thing. Data is information that has been translated into a form that is more conducive to storage, transmission and calculation, whereas signals are is used to transmit data. Both can be analogue or digital. These shall be discussed into details in a later chapter.

Chapter 2

Terms and concepts

Internet: This a world wide network of networks that is based on TCP/IP protocols. The internet is not owned by a single company or organization. The term could also be used to describe any series of interconnected networks.

Intranet: An intranet uses the same technologies as the internet, but it is owned and managed by a company or organization. An intranet is typically implemented as a LAN or WAN

Internetwork: An internetwork is a series of networks joined to each other by routers. The internet is the largest example of an internetwork.

Protocol (computing)

In computing, a protocol is a convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints. In its simplest form, a protocol can be defined as the rules governing the syntax, semantics, and synchronization of communication. Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection.

Typical properties

It is difficult to generalize about protocols because they vary so greatly in purpose and sophistication. Most protocols specify one or more of the following properties:

- Detection of the underlying physical connection (wired or wireless), or the existence of the other endpoint or node

- Handshaking
- Negotiation of various connection characteristics
- How to start and end a message
- How to format a message
- What to do with corrupted or improperly formatted messages (error correction)
- How to detect unexpected loss of the connection, and what to do next
- Termination of the session or connection.

Importance

The widespread use and expansion of communications protocols is both a prerequisite for the Internet, and a major contributor to its power and success. The pair of Internet Protocol (or IP) and Transmission Control Protocol (or TCP) are the most important of these, and the term TCP/IP refers to a collection (or protocol suite) of its most used protocols. Most of the Internet's communication protocols are described in the RFC documents of the Internet Engineering Task Force (or IETF).

The protocols in human communication are separate rules about appearance, speaking, listening and understanding. All these rules, also called protocols of conversation, represent different layers of communication. They work together to help people successfully communicate. The need for protocols also applies to network devices. Computers have no way of learning protocols, so network engineers have written rules for communication that must be strictly followed for successful host-to-host communication. These rules apply to different layers of sophistication such as which physical connections to use, how hosts listen, how to interrupt, how to say good-bye, in short how to communicate, what language to use and many others. These rules, or protocols, that work together to ensure successful communication are groups into what is known as a protocol suite.

Object-oriented programming has extended the use of the term to include the programming protocols available for connections and communication between objects.

Generally, only the simplest protocols are used alone. Most protocols, especially in the context of communications or networking, are layered together into protocol stacks where the various tasks listed above are divided among different protocols in the stack.

Whereas the protocol stack denotes a specific combination of protocols that work together, a reference model is a software architecture that lists each layer and the services each should offer. The classic seven-layer reference model is the OSI model, which is used for conceptualizing protocol stacks and peer entities. This reference model also provides an opportunity to teach more general software engineering concepts like hiding, modularity, and delegation of tasks. This model has endured in spite of the demise of many of its protocols (and protocol stacks) originally sanctioned by the ISO. The OSI model is not the only reference model however.

Common protocols

- IP (Internet Protocol)
- UDP (User Datagram Protocol)
- TCP (Transmission Control Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- HTTP (Hypertext Transfer Protocol)
- FTP (File Transfer Protocol)
- Telnet (Telnet Remote Protocol)
- SSH (Secure Shell Remote Protocol)
- POP3 (Post Office Protocol 3)

- SMTP (Simple Mail Transfer Protocol)
- IMAP (Internet Message Access Protocol)

Protocol testing

In general, protocol testers work by capturing the information exchanged between a Device Under Test (DUT) and a reference device known to operate properly. In the example of a manufacturer producing a new keyboard for a personal computer, the Device Under Test would be the keyboard and the reference device, the PC. The information exchanged between the two devices is governed by rules set out in a technical specification called a "communication protocol". Both the nature of the communication and the actual data exchanged are defined by the specification. Since communication protocols are state-dependent (what should happen next depends on what previously happened), specifications are complex and the documents describing them can be hundreds of pages.

The captured information is decoded from raw digital form into a human-readable format that permits users of the protocol tester to easily review the exchanged information. Protocol testers vary in their abilities to display data in multiple views, automatically detect errors, determine the root causes of errors, generate timing diagrams, etc.

Some protocol testers can also generate traffic and thus act as the reference device. Such testers generate protocol-correct traffic for functional testing, and may also have the ability to deliberately introduce errors to test for the DUT's ability to deal with error conditions.

Protocol testing is an essential step towards commercialization of standards-based products. It help ensure that products from different manufacturers will operate together properly ("interoperate") and so satisfy customer expectations. This type of testing is of particular importance for new emerging communication technologies.

INTERNET PROTOCOL SUITE

The Internet protocol suite (commonly TCP/IP) is the set of communications protocols that implement the protocol stack on which the Internet and most commercial networks run. It is named for two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were also the first two networking protocols defined. Today's IP networking represents a synthesis of two developments that began to evolve in the 1960s and 1970s, namely LANs (Local Area Networks) and the Internet, which, together with the invention of the World Wide Web by Sir Tim Berners-Lee in 1989, have revolutionized computing.

The Internet protocol suite—like many protocol suites—can be viewed as a set of layers. Each layer solves a set of problems involving the transmission of data, and provides a well-defined service to the upper layer protocols based on using services from some lower layers. Upper layers are logically closer to the user and deal with more abstract data, relying on lower layer protocols to translate data into forms that can eventually be physically transmitted. The TCP/IP reference model consists of four layers. From lowest to highest, these are the link layer, the network layer, the transport layer, and the application layer.

History

The Internet protocol suite came from work done by Defense Advanced Research Projects Agency (DARPA) in the early 1970s. After building the pioneering ARPANET in the late 1960s, DARPA started work on a number of other data transmission technologies. In 1972, Robert E. Kahn was hired at the DARPA Information Processing Technology Office, where he worked on both satellite packet networks and ground-based radio packet networks, and recognized the

value of being able to communicate across them. In the spring of 1973, Vinton Cerf, the developer of the existing ARPANET Network Control Program (NCP) protocol, joined Kahn to work on open-architecture interconnection models with the goal of designing the next protocol for the ARPANET.

By the summer of 1973, Kahn and Cerf had soon worked out a fundamental reformulation, where the differences between network protocols were hidden by using a common internetwork protocol, and instead of the network being responsible for reliability, as in the ARPANET, the hosts became responsible. (Cerf credits Hubert Zimmerman and Louis Pouzin [designer of the CYCLADES network] with important influences on this design.)

With the role of the network reduced to the bare minimum, it became possible to join almost any networks together, no matter what their characteristics were, thereby solving Kahn's initial problem. One popular saying has it that TCP/IP, the eventual product of Cerf and Kahn's work, will run over "two tin cans and a string." There is even an implementation designed to run using homing pigeons, IP over Avian Carriers (documented in Request for Comments 1149).

A computer called a router (a name changed from gateway to avoid confusion with other types of gateway) is provided with an interface to each network, and forwards packets back and forth between them. Requirements for routers are defined in (Request for Comments 1812).

The idea was worked out in more detailed form by Cerf's networking research group at Stanford in the 1973–74 period, resulting in the first TCP specification (Request for Comments 675) (The early networking work at Xerox PARC, which produced the PARC Universal Packet protocol suite, much of which existed around the same period of time (i.e. contemporaneous), was also a significant technical influence; people moved between the two).

DARPA then contracted with BBN Technologies, Stanford University, and the University College London to develop operational versions of the protocol on

different hardware platforms. Four versions were developed: TCP v1, TCP v2, a split into TCP v3 and IP v3 in the spring of 1978, and then stability with TCP/IP v4 — the standard protocol still in use on the Internet today.

In 1975, a two-network TCP/IP communications test was performed between Stanford and University College London (UCL). In November, 1977, a three-network TCP/IP test was conducted between the U.S., UK, and Norway. Between 1978 and 1983, several other TCP/IP prototypes were developed at multiple research centers. A full switchover to TCP/IP on the ARPANET took place January 1, 1983.

In March 1982, the US Department of Defense made TCP/IP the standard for all military computer networking. In 1985, the Internet Architecture Board held a three day workshop on TCP/IP for the computer industry, attended by 250 vendor representatives, helping popularize the protocol and leading to its increasing commercial use.

Layers in the Internet protocol suite

The IP suite uses encapsulation to provide abstraction of protocols and services. Generally a protocol at a higher level uses a protocol at a lower level to help accomplish its aims. The Internet protocol stack has never been altered, by the Internet Engineering Task Force (IETF), from the four layers defined in RFC 1122. The IETF makes no effort to follow the seven-layer OSI model and does not refer to it in standards-track protocol specifications and other architectural documents.

Some textbooks have attempted to map the Internet protocol suite model onto the seven layer OSI Model. The mapping often splits the Internet protocol suite's

Network access layer into a Data link layer on top of a Physical layer, and the **Internet layer** is mapped to the OSI's Network layer. These textbooks are secondary sources that contravene the intent of RFC 1122 and other IETF primary sources. The IETF has repeatedly stated that Internet protocol and architecture development is not intended to be OSI-compliant.

RFC 3439, on Internet architecture, contains a section entitled: "Layering Considered Harmful": *Emphasizing layering as the key driver of architecture is not a feature of the TCP/IP model, but rather of OSI. Much confusion comes from attempts to force OSI-like layering onto an architecture that minimizes their use.*

Implementations

Today, most commercial operating systems include and install the TCP/IP stack by default. For most users, there is no need to look for implementations. TCP/IP is included in all commercial Unix systems, Mac OS X, and all free-software Unix-like systems such as Linux distributions and BSD systems, as well as Microsoft Windows.

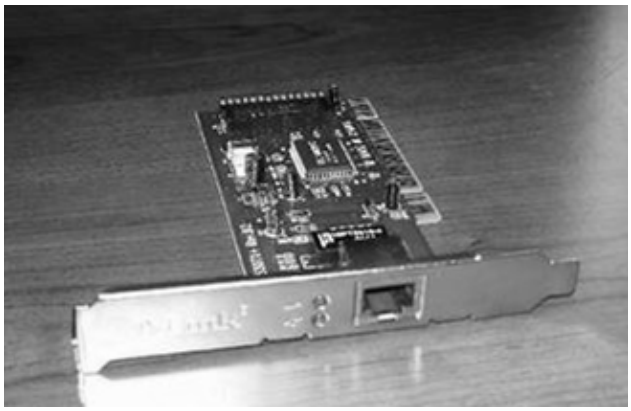
Unique implementations include Lightweight TCP/IP, an open source stack designed for embedded systems and KA9Q NOS, a stack and associated protocols for amateur packet radio systems and personal computers connected via serial lines.

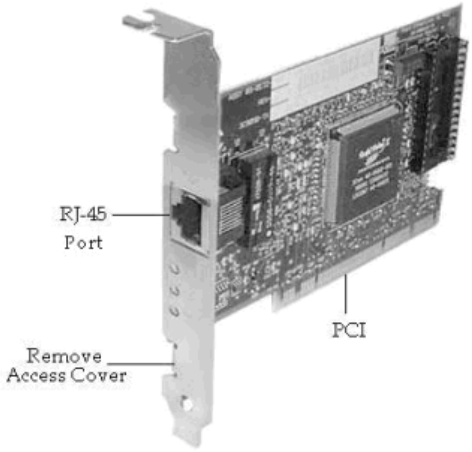
CHAPTER 3
NETWORK HARDWARE

All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers. In addition, some method of connecting these building blocks is required, usually in the form of galvanic cable (most commonly Category 5 cable). Less common are microwave links (as in IEEE 802.11) or optical cable ("optical fiber").

Network Interface Cards

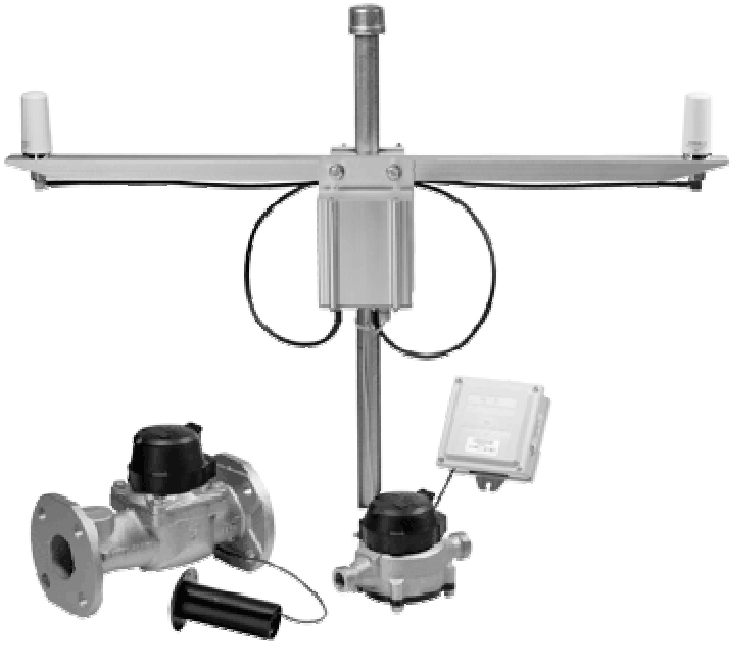
A network card, network adapter or NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.





Repeaters

A repeater is an electronic device that receives a signal and retransmits it at a higher level or higher power, or onto 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 runs longer than 100 meters away from the computer.



Hubs

A hub contains multiple ports. When a packet arrives at one port, it is copied to all the ports of the hub for transmission. When the packets are copied, the destination address in the frame does not change to a broadcast address. It does this in a rudimentary way, it simply copies the data to all of the Nodes connected to the hub.

Bridges

A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. 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 only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received.

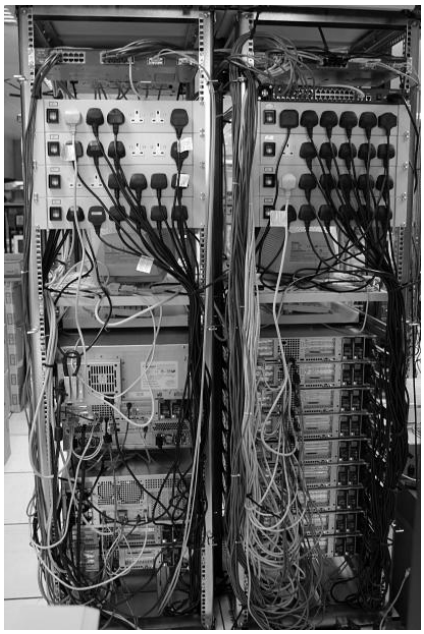
Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown 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 local area networks (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 by routers.
- Wireless bridges: Can be used to join LANs or connect remote stations to LANs.

Switches

A switch is a device that performs switching. Specifically, it forwards and filters OSI layer 2 datagram's (chunk of data communication) between ports (connected cables) based on the Mac-Addresses in the packets. This is distinct from a hub in that it only forwards the datagram's to the ports involved in the communications rather than all ports connected. Strictly speaking, a switch is not capable of routing traffic based on IP address (layer 3) which is necessary for communicating between network segments or within a large or complex LAN. Some switches are capable of routing based on IP addresses but are still called switches as a marketing term. A switch normally has numerous ports with the intention that most or all of the network be connected directly to a switch, or another switch that is in turn connected to a switch.



Switches is a marketing term that encompasses routers and bridges, as well as devices that may distribute traffic on load or by application content (e.g., a Web URL identifier). Switches may operate at one or more OSI layers, including physical, data link, network, or transport (i.e., end-to-end). A

device that operates simultaneously at more than one of these layers is called a multilayer switch.

Overemphasizing the ill-defined term "switch" often leads to confusion when first trying to understand networking. Many experienced network designers and operators recommend starting with the logic of devices dealing with only one protocol level, not all of which are covered by OSI. Multilayer device selection is an advanced topic that may lead to selecting particular implementations, but multilayer switching is simply not a real-world design concept.

Routers

Routers are networking devices that forward data packets between networks using headers and forwarding tables to determine the best path to forward the packets. Routers work at the network layer of the TCP/IP model or layer 3 of the OSI model. Routers also provide interconnectivity between like and unlike media (RFC 1812). This is accomplished by examining the Header of a data packet, and making a decision on the next hop to which it should be sent (RFC 1812). They use preconfigured static routes, status of their hardware interfaces, and routing protocols to select the best route between any two subnets. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Some DSL and cable modems, for home (and even office) use, have been integrated with routers to allow multiple home/office computers to access the Internet through the same connection. Many of these new devices also consist of wireless access points (waps) or wireless routers to allow for IEEE 802.11b/g wireless enabled devices to connect to the network without the need for a cabled connection.


ROUTERS
Cisco 2851
Cisco 3825
Cisco 7603
Cisco 2821
Cisco 3845
Cisco 7604
Cisco 2811
Cisco 7201
Cisco 2801
Cisco 7204 VXR
Cisco 7606
Cisco 7206 VXR
Cisco 7609
Cisco 7613


LINKSYS

NETWORK MEDIA

The world of computer networks would not exist if there were no medium by which to transfer data. All communication media can be divided into two categories:

- Physical or conducted media such as telephone lines, fibreoptic cable, coaxial cables, UTP and STP
- Radiated or wireless media such as Bluetooth, satellite systems, radio waves etc.

The choice of which medium of transmission to use depends on so many factors including;

- Area covered by network
- Security requirements
- Cost

CHAPTER 4

CONDUCTED AND WIRELESS MEDIA

4.1 Conducted Media

4.2 Wireless Media

4.3 Media Connectors

A variety of media connectors are used in a network. A media connector attaches to the transmission media and allows the physical connection into the computing devices. It is necessary to identify the connectors associated with the specific media. Some of the media connectors are described below:

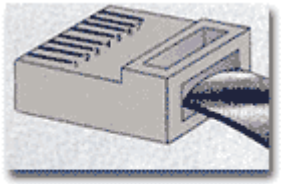
RJ-11 (Registered Jack)

RJ-11 is the most familiar of the registered jack connectors. RJ-11 type of connector is most often used for telephone wire terminals. An RJ-11 connector has only four conductors. It is used to connect telephone cables to a telephone set or to a modem. RJ-11 connectors are used with two standard varieties of wirings-untwisted (flat-satin cable) and Unshielded Twisted Pair (UTP).

RJ-45 (Registered Jack)

RJ-45 is a type of connector similar to an RJ-11 telephone connector but is larger in size because it has eight conductors. An unshielded twisted-pair (UTP)

connection uses an RJ-45 connector and is used in computer networks.



RJ-45

F-Type

An F-type connector is a threaded medium performance coaxial signal connector, which is used in TVs and VCRs. The pin of the connector is actually the center conductor of the coaxial cable. It is an inexpensive connector.

F-type

ST (Straight Tip)

A straight tip (ST) connector is a fiber-optic connector used with multimode fiber. An ST connector has a 2.5mm shaft and bayonet locking ring, and allows quick connect and disconnect of 125 micron multi-mode fiber.

ST

SC (Subscriber Connector or Standard Connector)

A subscriber connector (SC) is a fiber-optic connector used with multimode fiber. It is a square shaped connector used for terminating fiber optic cables.

SC

IEEE 1394 (FireWire)

The IEEE 1394 (FireWire) connector is used with the FireWire serial bus. FireWire can transmit data at a very high speed of 400Mbps. Two types of connectors are available in this category, namely 4-pin and 6-pin.

IEEE1394 6-Pin FireWire

IEEE1394 4-Pin FireWire

Fiber LC (Local Connector)

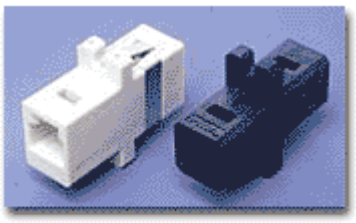
The LC connector was developed to meet the need for small and easier-to-use fiber optic connectors. The LC connector reduces space required on panels by 50%.

Fiber LC

MT-RJ (Mechanical Transfer Registered Jack)

The MT-RJ connector is the most recent type of small form factor fiber optic connector. The MT-RJ fiber connector is less than half the size of the SC duplex

connector and transceiver, so it doubles the port density of fiber-optic LAN equipment. The connector is a 2-fiber connector and takes up no more room than an RJ-45 jack.



MT-RJ

USB (Universal Serial Bus)

A Universal Serial Bus (USB) connector is used with the USB cable for connecting various electronic devices to a computer. USB supports a data speed of up to 12 megabits per second. Two types of connectors are used with USB, namely USB-A Type and USB-B Type.

USB-A Type

USB-B Type