COMPUTER NETWORKS
Contents

1.COMPUTER NETWORKS

Definition

A computer network allows computers to communicate with many other and to share resources and information.

5.1 Types of networks

Personal area network

A Personal area network (PAN) is a computer network used for communication among computer devices close to one person. Some examples of devices that are used in a PAN are printers, fax machines, telephones, PDAs and scanners. The reach of a PAN is typically about 20-30 feet (approximately 6-9 meters), but this is expected to increase with technology improvements.

Local Area Network (LAN)

A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet.

In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

Campus area network

A campus area network (CAN) is a computer network made up of an interconnection of local area networks (LANs), but smaller than MAN, within a limited geographical area. It can be considered one form of a metropolitan area network, specific to an academic setting.

Metropolitan area network

A metropolitan area network (MAN) is a network that connects two or more local area networks or campus area networks together but does not extend beyond the boundaries of the immediate town/city. Routers, switches and hubs are connected to create a metropolitan area network.

Wide Area Network (WAN)

A WAN is a data communications network that covers a relatively broad geographic area (i.e. one city to another and one country to another country) and that often uses transmission facilities provided by common carriers, such as telephone companies. The **Internet** is the largest WAN, spanning the Earth. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer. WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.

WAN is a geographically-dispersed collection of LANs. A network device called a **router** connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.

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.

A VPN allows computer users to appear to be editing from an IP address location other than the one which connects the actual computer to the Internet.

5.2 Network Topologies

It is the geometric arrangement of a computer system. It is the way in which the network nodes are linked together. Network topologies like bus, ring and star are basic Topologies. More complex networks can be built as hybrids of two or more of the above basic topologies.

Some of the other topologies are also explained in detail below.

Point-to-point

The simplest topology is a permanent link between two endpoints.

Switched point-to-point topologies are the basic model of conventional telephony. The value of a permanent point-to-point network is the value of guaranteed, or nearly so, communications between the two endpoints. The value of an on-demand point-to-point connection is proportional to the number of potential pairs of subscribers.

Permanent (dedicated):

It is a point-to-point communications channel that appears, to the user, to be permanently associated with the two endpoints. The link is permanently linked.

Switched:

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

Bus Topology

In local area networks where bus technology is used, each machine is connected to a single cable. Each computer or server is connected to the single bus cable through some kind of connector. A terminator is required at each end of the bus cable to prevent the signal from bouncing back and forth on the bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the MAC address or IP address on the network that is the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data does match the machine address, the data is accepted.

Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable breaks, the entire network will be down, since there is only one cable. Since there is one cable, the transfer speeds between the computers on the network is faster.

Ring Topology

In a ring network, every device has exactly two neighbors for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise"). To implement a ring network, one typically uses **FDDI, SONET, or Token Ring technology**. Ring topologies are found in some office buildings or school campuses.

The machines or computers connected to the ring act as signal boosters or repeaters which strengthen the signals that transverse the network. The primary disadvantage of ring topology is the failure of one machine will cause the entire network to fail.

Star Topology

Many home networks use the star topology. A star network features a central connection point called a "hub" that may be a hub, switch or router. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet.

An advantage of the star topology is the simplicity of adding other machines. Compared to the bus topology, a star network generally requires more cable, but a failure in any star network cable will only take down one computer's network access and not the entire LAN. (If the hub fails, however, the entire network also fails.)

Tree Topology

It is also known as a **hierarchical network**. Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus and each hub functions as the "root" of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub connection points) alone.

Mesh Topology

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. (Recall that even in a ring, although two cable paths exist, messages can only travel in one direction.) Some WANs, most notably the Internet, employ mesh routing. A mesh network in which every device connects to every other is called a full mesh.

5.3 Basic hardware components

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 802.12) or optical cable ("optical fiber"). An Ethernet card may also be required.

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.

Repeaters

A repeater is an electronic device that receives a signal 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 which runs longer than 100 meters.

Hubs

A network hub contains multiple ports. When a packet arrives at one port, it is copied unmodified to all ports of the hub for transmission. The destination address in the frame is not changed to a broadcast address.

Bridges

A bridge is a device that allows segmenting a large network into two smaller, more efficient networks. Bridges reduce the amount of traffic on a LAN by dividing it into two segments. Bridges inspect incoming traffic and decide whether to forward or discard it.

A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can "listen" to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

Bridges can be used to connect different types of cabling, or different types of topologies. Bridges must be used between networks with the same protocol, however.

Switches

A **network switch** is a small hardware device that joins multiple computers together within one local area network (LAN). Technically, network switches operate at Data Link Layer of the OSI model.

Network switches appear nearly identical to network hubs, but a switch generally contains more intelligence (and a slightly higher price tag) than a hub. Unlike hubs, network switches are capable of inspecting data packets as they are received, determining the source and destination device of each packet, and forwarding them appropriately. By delivering messages only to the connected device intended, a network switch conserves network bandwidth and offers generally better performance than a hub.

Routers

It is an electronic device used to connect two or more computers or other electronic devices to each other, and usually to the Internet, by wire or radio signals. This allows several computers to communicate with each other and to the Internet at the same time.

A router is a networking device that forwards packets between networks using information in protocol headers and forwarding tables to determine the best next router for each packet. Routers work at the Network Layer of the OSI model and the Internet Layer of TCP/IP.

Gateway:

Gateways are the components used to achieve communications between terminals connected to heterogeneous networks that use different protocols and have different network characteristics. A network gateway provides the connectivity between remote systems.

5.4 Communication

Network Protocol

Network protocols defines a language of rules and conventions for communication between network devices .A **protocol** is a set of rules which is used by computers to communicate with each other across a network. A protocol is a convention or standard that controls or enables the connection, communication, and data transfer between 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. The most popular protocols are TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), Token ring, Ethernet and many more.

The ISO/OSI Reference Model

The International Standards Organization (ISO) Open Systems Interconnect (OSI) Reference Model defines seven layers of communications types, and the interfaces among them. Each layer depends on the services provided by the layer below it, all the way down to the physical network hardware, such as the computer's network interface card, and the wires that connect the cards together.

Physical Layer

This layer deals with the physical plugs and sockets and electrical specification of signals. This is the medium over which the digital signals are transmitted. It can be twisted pair, coaxial cable, optical fiber, wireless, or other transmission media.

Data Link Layer

Transforms basic physical services to enable the transmission of units of data called frames. Frames carry data between two points on the same type of physical network, and maybe relayed if the network is extended. They normally contain low level addressing information and some error checking. This layer may be involved in arbitrating access to the physical network. The Data Link layer detects, and possibly corrects errors in the physical layer

Network Layer

It controls routing of data by providing an address domain, and in consequence the routing of messages. This addressing is separate from the hardware which implements the network connections. i.e. specifies how addresses are assigned and how packets are forwarded from one end of the network to another.

Transport Layer

It provides an interface for the upper layers to communications facilities. The presence of this layer obscures the underlying network hardware and topology from the applications. A very complex set of protocols are required for this layer. This layer is responsible for delivering data to the appropriate process on the host computer.

Session Layer

The protocols for this layer specify how to establish a communication session with a remote System (e.g., How to login to a remote timesharing computer). Specifications for security details such as authentication using passwords are described in this layer.

Presentation Layer

Layer 6 protocols specify how to represent data. Such protocols are needed because different brands of computer use different internal representation for integer and characters. Thus layer 6 protocols are needed to translate from the representation on one computer to the representation on another.

Application Layer

This is where the application using the network resides. Common network applications include remote login, file transfer, e-mail, and web page browsing.

Internetwork

An Internetwork is the connection of two or more distinct computer networks or network segments via a common routing technology. The result is called an Internetwork. Two or more networks or network segments connected using devices that operate at layer 3 (the 'network' layer) of the OSI Basic Reference Model, such as a router. Any interconnection among or between public, private, commercial, industrial, or governmental networks may also be defined as an Internetwork.

In modern practice, interconnected networks use the Internet Protocol. There are at least three variants of Internetwork, depending on who administers and who participates in them:

- Intranet
- Extranet
- Internet

Intranets and extranets may or may not have connections to the Internet. If connected to the Internet, the intranet or extranet is normally protected from being accessed from the Internet without proper authorization. The Internet is not considered to be a part of the intranet or extranet, although it may serve as a portal for access to portions of an extranet.

Intranet

An intranet is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer an application that is under the control of a single administrative entity. That administrative entity closes the intranet to all but specific, authorized users. Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information.

Extranet

An extranet is a network or Internetwork that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities (e.g., a company's customers may be given access to some part of its intranet creating in this way an extranet, while at the same time the customers may not be considered 'trusted' from a security standpoint). Technically, an extranet may also be categorized as a CAN, MAN, WAN, or other type of network, although, by

definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

Internet

The Internet consists of a worldwide interconnection of governmental, academic, public, and private networks based upon the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the U.S. Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW).