

# Chapter 2

## Computer Networks

**Abstract** A computer network, in general, comprises of numerous computers that are linked together to communicate with each other. The goal of a computer network is to enable two or more computers to share and exchange data with one another for various purposes. Users can access remote resources by either logging into the appropriate remote computer or transfer data from the remote computer to their own computers. To understand what a network is all about, this chapter provides details on topologies, design, and usage of a network. Furthermore, since present network demands future technologies to be self-adaptive and self-healed, the chapter provides details on issues and challenges faced by it. Additionally, the chapter provides ground details on the future of networking technologies.

### 2.1 Introduction

As individual microchips in high-performance computing systems reach evermore prominent speed, execution starts to depend less on the rate of processors and more on the framework that supplies them with information. This framework is the network system, a regularly overlooked yet essential piece of any complex computer (Osborn 2015). Network system administration is to a great degree a wide subject in data science which calculates itself regarding profundity and significance. Taken just, on the other hand, a network system is close to a framework by which one can handle components and send data to another. Accordingly, the discriminating parameter of a network system is to measure the data stream. One essential metric is the transmission capacity or *bandwidth*, or the greatest rate at which a system can move data over a line that partitions the hubs/nodes into two equivalent gatherings. Generally, as essential for firmly coupled multiprocessing, the time needed to exchange a message between hubs is called the *latency*. An extensive and consistent examination exertion devotes itself to enhance these two numbers, bringing about a tremendous scope of way to deal with network system outline.

A network, in general, is formed by a collection of people, devices, and agents where the agents communicate with each other to share and gain resources.

A computer network is a collection of two or more devices connected for the purpose of sharing resources. Devices can include computers, printers, fax machines, and Internet communication hardware. In addition to hardware devices, software is also used to provide additional capabilities such as security (privacy and protection of network traffic) and enhanced services such as Internet browsing, print queue management, etc. These devices can be connected through wires (cables) or wireless technologies (radio or infrared).

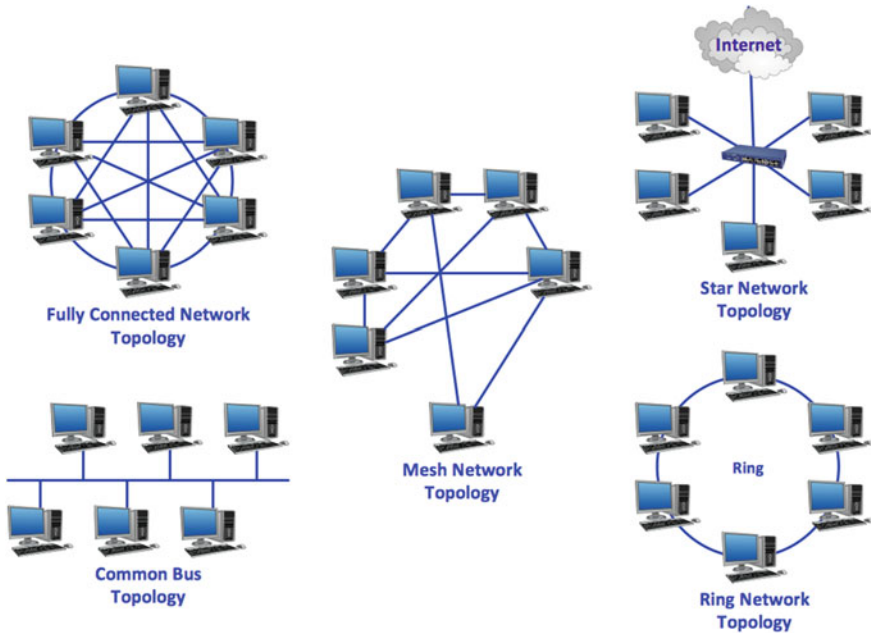
## 2.2 Network Topologies, Types, and Design Strategies

While designing a network structure, network topologies, type, and design strategies play a very important role. Customarily, numerous individuals have thought that it was valuable to separate all the topologies into two vast gatherings, saying that a system is either static or dynamic. This is to some degree deluding on the grounds that not many genuine topologies submit to such simple characterization, rather falling some place on an expansive range in the middle of static and dynamic. A static system topology is supposed on the grounds, that it tries to give perpetual information ways that fit the correspondence needs of the application. In a consummately static topology, the system itself is a sensibly inactive gadget that essentially gives a gathering of channels with known and true endpoints. The perfect static system is a totally joined chart, where a committed channel exists in the middle of every single pair of hubs. For this situation, the system does no routing, and the sending node places the message on the right channel or the destination node. Involving the inverse end of the range are dynamic systems, which make altogether different suppositions about the system's part in taking care of messages. Dynamic systems endeavor to utilize adaption and intervention to share a littler number of physical connections among more nodes. A basic transport topology is a bus topology, which has precisely one physical channel that is shared by every single appended node. Given that both static and dynamic procedures have distinct tradeoffs, most real frameworks pick some all-around adjusted center ground. The following section presents details on various network topological designs and types.

### 2.2.1 Network Topologies

Topology refers to the shape of the network or in other terms it is the network layout. The way the computers in a network are physically linked to each other and how they communicate with each other is determined by the network topology as shown in Fig. 2.1. Topologies are either physical or logical such as:

- (a) *Mesh Topology*: The simplest network connecting two computers A and B is an electrical link directly from one to the other. In a mesh topology, every



**Fig. 2.1** Different network topologies

computer has a connection to every other computer in the network. Each computer has a network interface card (NIC) with a transmitter and a receiver. A packet is transmitted by one computer as a sequence of bits and received by the other in the same order. Depending on the times it takes to transmit one bit, the link has a capacity of bandwidth or bits per second. Mesh topology is preferred where dedicated connection is required and time is more important than infrastructure, cost of laying, and maintenance of physical or wireless media. This type of interconnection enables every computer to have  $(N - 1)$  NICs and  $N(N - 1)/2$  total number of links, where  $N$  is the number of computers.

- (b) *Star Topology:* All the devices are connected to a central hub. Nodes communicate across the network by passing through the hub. To reduce the number of links, every node is connected to one central node in the star topology. A packet between any two nodes may need two hops via the central node. If the central node is the source or the destination, only one hop is required. The central node is a single point whose failure renders the entire network inoperative. In cases, where most communication is between one server and its clients, the star topology is especially useful.
- (c) *Ring Topology:* The single point of failure can be avoided using the ring or bus topology. In the ring, every device is attached to a circular cable, so that each device is connected directly to two other devices, one on either side of it. As a packet circulates around the ring, every node can receive it. To avoid packet

circulating indefinitely, the transmitting node removes it after one round. In order to handle these functions, the attachment is through an electronic circuit called a transceiver.

- (d) *Bus Topology*: In the bus topology, all nodes are connected to a single cable, called the bus or backbone, with no active devices. All the nodes in the system are directly connected to that link (the bus), which may be organized as a straight line. The sites can communicate with each other directly through this link. Each node is connected to it by a single tap. This can be very reliable and inexpensive. The failure of one side does not affect communication among the rest of the sites. However, if the link fails, the network is partitioned completely. The bus is the most popular topology for local area networks (LAN) due to its simplicity and reliability. Initially, the most widely used LAN Ethernet uses the bus topology. Like the ring, the bus also has the broadcast property, i.e., as a packet propagates down the bus to its ends, it can be received by every node. In the mesh and star topologies sending the same packet to every node requires that  $N - 1$  copies of the packet be separately transmitted.
- (e) *Tree Topology*: Tree topology can be derived from the star topology. Tree has a hierarchy of various hubs, like we have branches in a tree. In this case, every node is connected to some hub or switch.

### 2.2.2 Network Types

The network computers may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams. There are three basic types of computer networks:

- Local area networks (LAN)
- Metropolitan area network (MAN)
- Wide area network (WAN)

#### (a) Local Area Network

A local area network is normally a privately owned network within a single office, building, or campus covering a distance over a few kilometers. In a typical LAN configuration, one computer is designated as the file server. It stores all the software that controls the network as well as the software that can be shared by the computers attached to the network. Computer connected to the file server are called as workstations. In most of the LANs, cables are used to connect the NIC in each computer. Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but is also able to access data and devices anywhere on the LAN. The users can share expensive devices such as laser printers, communicate with each other by sending emails, or engage in chat sessions. The following characteristics differentiate one LAN from another:

- *Topology*: The geometric arrangement of devices on the network. For example, devices can be arranged in a ring or in a straight line.
- *Protocols*: The rules and encoding specifications for sending data. The protocols also determine whether the network uses peer-to-peer (P2P) or client–server architecture.
- *Media*: Devices can be connected by twisted-pair wire, coaxial cables, or fiber optic cables. Some networks communicate without connecting media altogether, instead, doing so through radio waves.

LANs are capable of transmitting data at very fast rates, much faster than data that can be transmitted over a telephone line, limitation being the number of computers attached to a single LAN. A LAN can be configured either as a client–server LAN or a P2P LAN as shown in Fig. 2.2.

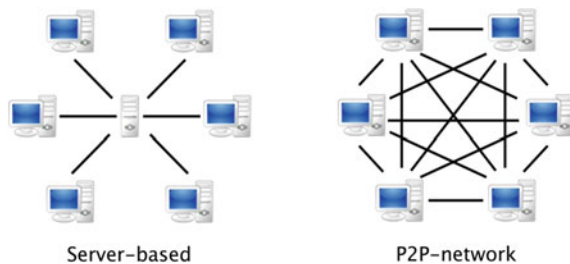
*Peer-to-Peer Model*: P2P networks are the simplest and least expensive networks to set up. P2P networks are simple in the sense that the computers are connected directly to each other and share the same level of access on the network. Computer A will connect directly to computer B and will share all files with the appropriate security or sharing rights. If many computers are connected, a hub may be used to connect all these devices.

*Client-Server Model*: The most common LAN types used by companies today are the “client-server model,” since they consist of the server (storing the files and running applications) and the client machines (computers used by the workers). Using a client–server setup can be helpful in many ways. It can free up disk space by providing a central location for all the files to be stored ensuring that the most recent file is available to all. A server can act as a mail server (collecting and sending the mails) or a print server (performing print jobs), thus freeing computing power on the client machine to continue working.

#### (b) Metropolitan Area Network

A metropolitan area network (MAN) covers larger geographical areas such as cities or districts. A system of LANs connected through telephone lines and radio waves is called as MAN. The connectivity lies among cities or districts where cities cannot lay a private network all around in the city.

**Fig. 2.2** Client–server model versus peer-to-peer Model



### (c) Wide Area Network

Wide area networks (WANs) are huge compared to a LAN or a MAN and span across cities, state, country, continent, or even the whole world. WANs connect larger geographical areas such as India, the United States, or the world. The satellite uplinks may be used to connect this type of network. A WAN provides long-distance transmission of data, voice, image, and video information. Using a WAN, people in India can communicate with places like Tokyo in a matter of minutes, without paying enormous phone bills. WAN technologies use multiplexers to connect local and metropolitan networks like the Internet.

### (d) Internetworks

When two or more networks are connected, they become an Internetwork, or Internet. Individual networks are joined into Internetworks by the use of Internetworking devices. These devices include routers and gateways.

## 2.2.3 Design Strategies for Communications

A network allows one computer to send electrical signals to another computer. These signals have to be interpreted as a stream of bits. The stream of bits has different meaning depending on the application. If one computer sends a binary file and the other expects to receive an e-mail message, clearly communication will not take place. In order to communicate, both parties must agree on a set of conversions such as signals that constitute a 1 or a 0, such a set of conventions is a *protocol*.

A network may include computers manufactured by different vendors with software from various sources. For these to be able to communicate, the protocols must be agreed upon by all the manufacturers, i.e., *standards* are required. For instance, RS-232C is a standard protocol for transmission of a stream of bytes that is widely used for sending data between computers and peripherals such as printers and modems. TCP is a standard protocol used for reliable transmission of arbitrary data between computers in the Internet.

While designing a communication network, the systems on the networks agree on a protocol or a set of protocol for determining host names, locating hosts on the network, establishing connections, and so on. The design strategy should be simplified by partitioning the problem into several layers. Each layer on one system communicates with the equivalent layer on the other system. Each layer has its own protocols or logical segmentation. The protocols may be implemented in hardware or software. The logical communication between two computers can be implemented in three layers. The lowermost layer defines the electrical characteristics of the link, the representation of bits, and the mechanical details of connectors and cable. The middle layer handles the sending and reception of packets. At the highest layer is the protocol for actually transferring the complete file. Layering of protocols serves another purpose: it is possible for different vendors to implement different

layers and for these to interoperate provided they all conform to a standard layering. One such standard for layering is the International Standards Organization (ISO) reference model for Open Systems Interconnection (OSI).

### OSI Reference Model

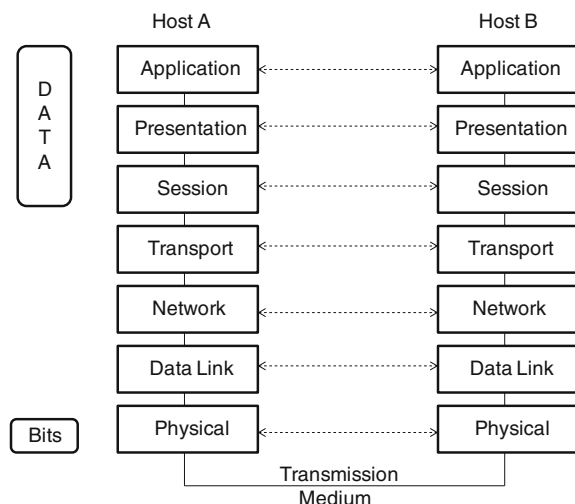
The OSI reference model provides a means of understanding the fundamentals of networking. It describes how data flows across a network. It helps in making better decisions about equipment purchases and configurations. It has the following seven layers with their basic tasks described below (Fig. 2.3):

*Application layer:* The application layer is responsible for a set of functions commonly required by various applications. It uses a set of protocols for carrying out these functions. Examples of some application layer protocols include HTTP, FTP, TELNET. Virtual terminal emulation and similar functionality are included in the list of responsibilities of the application layer.

*Presentation Layer:* The presentation layer is responsible for another set of functions commonly required by various applications sitting in the application layer. It is primarily concerned with the syntax and semantics of the information required to be transmitted over the network. Examples of some of the activities of this layer include data or information encoding in a manner a priori agreed between the sending and receiving parties. For instance, an ASCII system talking to an EBCDIC system may use services of this layer.

*Session Layer:* The session layer is responsible for establishment of one or more sessions between two or more users or applications working on different member systems of a network. Examples of some of the activities of this layer include selective flow of traffic in either directions, session control by token circulation, and synchronization of status information, etc.

**Fig. 2.3** The OSI reference model



*Transport Layer:* The transport layer is responsible for receiving the data from the upper layer, i.e., the session layer and dividing it into manageable chunks for the purpose of further processing and onward transmission to network layer after prefixing its own header to the processed data. At the other end, this operation is reversed when this layer receives data from the network layer and after due processing passes it on to its upper layer. Other activities of this layer include creation of network connections as per the transport connection requests by the upper layer.

*Network Layer:* The network layer is responsible for receiving the data from the transport layer, process it for finding out the required resources, and divide the data into fragmented units. Thereafter, decide the route to be taken by the respective data units and pass the data to the lower (data link) layer after prefixing its own header to it. At the other end, this operation is reversed. Routing decision can be based on a fixed or static routing policy or a dynamic (situation dependent) routing policy. Other functions of the network layer include congestion control, address resolution, protocol translation, and resource usage accounting.

*Data Link Layer:* The data link layer is responsible for receiving the data from the network layer, process it, insert the processed data into data frame, add control information to it by prefixing a header, and suffixing a trailer to the processed data to pass it on to the physical layer for actual transmission in signal form. Examples of some of the other activities of this layer include data link layer protocol translation in required cases, ensuring acceptably error-free transmission, flow control, traffic direction regulation, and media access control in case of shared media systems.

*Physical Layer:* The physical layer is responsible for receiving the data from the data link layer, converting it into equivalent signal (representing the data in bits), and transmitting these signals in the desired manner over a shared or dedicated transmission link. Apart from the electrical characteristics, this layer is also concerned with the mechanical issues like connector dimensions, interpin distance, mechanical strength needed, etc. Issues like physical connection establishment, direction of transmission, frequency usage, and other procedural matters are under its purview.

## 2.3 Wireless Networking

Although the origins of radio frequency-based wireless networking can be traced back to the University of Hawaii's ALOHANET research project in the 1970s, the key events that led to wireless networking becoming one of the fastest growing technologies of the early twenty first century have been the ratification of the IEEE 802.11 standard in 1997, and the subsequent development of interoperability certification by the Wi-Fi Alliance (formerly WECA).



From the early 1970s to the early 1990s, the growing demand for wireless connectivity could not be met by a narrow range of expensive hardware, based on proprietary technologies, which offered no interoperability of equipment from different manufacturers, no security mechanisms, and poor performance compared to the standard 10 Mbps wired Ethernet.

The 802.11 standard stands as a major milestone in the development of wireless networking and the starting point for a strong and recognizable brand Wi-Fi. This provides a focus for the work of equipment developers and service providers and is as much a contributor to the growth of wireless networking as the power of the underlying technologies.

With the various Wi-Fi variants that have emerged from the original, 802.11 standard have grabbed most of the headlines in the last decade; other wireless networking technologies have followed a similar timeline, with the first IrDA specification being published in 1994, the same year when Ericsson started research on connectivity between mobile phones and accessories that led to the adoption of bluetooth by the IEEE 802.15.1 Working Group in 1999. Various 802 working groups are shown in Table 2.1 (Wikipedia 2015).

**Table 2.1** IEEE 802 standards

Number	Topic
802.1	Overview and architecture of LANs
802.2	Logical link control
802.3	Ethernet
802.4	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6	Dual queue dual bus (early metropolitan area network)
802.7	Technical advisory group on broadband technologies
802.8	Technical advisory group on fiber-optic technologies
802.9	Isochronous LANs for real time applications
802.10	Virtual LANs and security
802.11	Wireless LANs
802.12	Demand priority (Hewlett Packard's AnyLAN)
802.14	Cable modems
802.15	Personal area network (Bluetooth)
802.16	Broadband wireless access (WiMAX)
802.17	Resilient packet ring
802.18	Technical advisory group on radio regulation
802.19	Technical advisory group on coexistence
802.20	Mobile broadband wireless access
802.21	Media independent handoff
802.22	Wireless regional area network
802.23	Emergency services working group

## 2.4 Usage of Networking

In general, computer communication and networking enables sharing of peripherals and resources which may be data, information, and supports communication among people. Some common usage of networks lies in remote login, file access, electronic mail, information access, remote printing.

- (a) *Remote Login and File Access*: Network systems allow a user to issue commands for accessing remotely located computer. Furthermore, a user from any of the several client computers can read or modify files on single server computer. Thus, a group of people working on a common task can easily share data, documents, and programs.
- (b) *Remote Printing*: The network enables use of a remote printer from any other computer without physically moving either the printer or the files.
- (c) *Electronic Mail*: It enables a fast and convenient alternative to traditional post and telephone for inter person communication.
- (d) *Information Access*: It ensures searching of databases which are available on remote machines. The development of World Wide Web (WWW) is one of the rapidly growing technologies of present network systems.
- (e) *Storage Capacity*: Since there is more than one computer on a network system which can, without much of a stretch, offer documents, the issue of capacity limit gets set out all the things considered. A stand-alone computer may miss the mark concerning stockpiling memory, however, when numerous computer are on a network system, the memory of diverse computer can be utilized as a part of such case. One can likewise outline a stockpiling server on the system keeping in mind the end goal to have an immense stockpiling limit (Buzzle 2015).
- (f) *Resource Sharing*: Resource sharing is another vital advantage of a computer network. For instance, if there are 12 representatives in an association, every individual has their own particular computer; they will oblige 12 modems and 12 printers on the off chance that they need to utilize the assets in the meantime. A computer network gives a less-expensive option by the procurement of asset sharing. Each computer can be interconnected utilizing a system and only one modem and printer can effectively give the administrations to each of the 12 clients (Kozierok 2015).
- (g) *Economical Setup*: Shared assets mean decrease in equipment costs. Shared documents mean decrease in memory prerequisite, which in a roundabout way implies lessening in record stockpiling costs. A specific programming can be introduced just once on the server and made accessible over every single associated computer without a moment's delay. This spares the cost of purchasing and introduces the same programming the same number of times for the same number of clients.
- (h) *Performance Enhancement and Balancing*: Under a few circumstances, a system can be utilized to upgrade the general execution of a few applications by conveying the calculation errands to different computer on the system.

Besides all the above-mentioned advantages, networking can be utilized in resolving various issues which the single stand-alone system cannot do.

## 2.5 Challenges and Issues of Networking

The development of network systems has encountered a few noteworthy steps, and the research center of every stride has been continuously changing and advancing, from ARPANET to OSI/RM, then high speed networking (HSN) and high-performance computing (HPN) (Gu and Luo 2006). Amid the development, network systems have gained incredible ground and increased extraordinary achievement. On the other hand, with the appearance and escalation of tussle, alongside the three troublesome issues (service customizing, resource control, and user management) of the current system, it is found that conventional Internet and its building design no more meet the prerequisites of cutting edge system. In this way, it is the next generation network which the present Internet must develop to. With the mentality of accomplishing significant direction for exploration on next generation system, this section breaks down a few quandaries confronting the current system situation.

### 2.5.1 Quality of Service

Quality of service (QoS) is a dynamic, broad topic which has significant origination since appearance. It is an imperative metric and a requirement parameter set comprising of data transfer capacity (bandwidth), delay, jitter, packet loss ration, and nature of voice/video. While the customary Internet can just give best effort transmission, the necessities of brilliant multimedia (voice and video) transmission cannot be fulfilled. Consequently, it prompts the significance of the powerful QoS ensured. IETF has advanced numerous administration models and components to meet distinctive QoS necessities, for example, IntServ/RSVP, DiffServ, traffic engineering, and QoS-based routing.

IntServ gives three sorts of administration models: *guaranteed service*, *controllable-load service*, and *committed rate service*. Notwithstanding, IntServ cannot be deployed on a vast scale on the grounds that each system hub needs to store numerous streams state (Xiao and Ni 1999). In this manner, DiffServ is advanced to defeat the confinement of IntServ, which is to give basic, adaptable, and separated administrations in Internet (Nichols et al. 1998; Carlson et al. 1998). However, DiffServ does not simplify QoS-guaranteed, but rather in the interim gives relative QoS-guaranteed to stream flow. The two administrations, IntServ and DiffServ, supplement and support one another in diverse applications. IntServ can be sent at the system edge or get to network to satisfy adaptable admission control and

resource reservation. DiffServ works as a spine system of human body to satisfy productive information transmission.

Traffic engineering ensures QoS-guaranteed administrations by solving the unbalanced activity due to traffic circulation issue brought by routing protocol, and in addition the blockage issue created by improper resource utilization, hence giving QoS-guaranteed administrations to benefits. Likewise, QoS-based routing can fulfill distinctive QoS necessities (Mazumdar et al. 1991). In QoS-based routing system, path selection depends on QoS necessity of the accessible resource and data flow, which offers route of end-to-end limitation for more flows. QoS-based routing takes care of the issue that, path selection is just taking into account, single metric without considering the accessibility of resources (Crawley et al. 1998). Also, route change can help to adjust on the single system connection and enhance the productivity of system resource usage (Chen and Nahrstedt 1998).

### ***2.5.2 Connectivity, Manageability, and Scalability***

Performance degradation alludes to issues including loss of speed and information uprightness because of poor transmissions and connectivity (IT Direct 2015). While each network system is inclined to execution issues, extensive systems are particularly powerless because of the extra separation, endpoints, and extra devices at midpoints.

Solutions for performance degradation are not appallingly troublesome. The primary step is to buy the best quality computer hardware equipment one can manage. Every single other arrangement expands upon a strong establishment of good system equipment. Of all the things considered, network performance is just tantamount to the parts of which it is created.

Albeit quality matters, for this situation, scalability can likewise be an issue. Systems without enough routers, switches, and bridges are practically identical to pumping water from a city well with a straw. Starting with satisfactory, quality equipment is an important aspect, however, that still is insufficient. Equipment is pointless without fitting setup.

It is crucial to guarantee all computers and system “pipes” are appropriately associated (with quality cabling) and arranged properly. This incorporates confirming system settings in server and desktop system design applications furthermore checking settings in the firmware of systems administration parts (switches, routers, firewalls, etc.). Each device joined on the system ought to be at first and routinely checked for issues, as computers tainted with viruses, spyware, and malware can squander data transmission and surprisingly more dreadful, contaminate different frameworks.

### **2.5.3 *Network Security***

Network system security issues include keeping up system integrity, keeping unapproved clients from invading the framework (survey/taking delicate information, passwords, and so forth.), and ensuring the system denial of service attack.

These issues are significantly amplified as systems increment in size. Bigger network systems are more helpless to assault in light of the fact that they offer more powerless focuses at which interlopers can obtain entrance. More clients, more passwords, and more equipment mean more places, an intruder can attempt to get in. Barrier against these issues incorporate utilizing firewalls and proxies, introducing solid antivirus programming, installing strong antivirus software, making utilization of system investigation programming, physically securing computer organizing resources, and summoning methods that compartmentalize an extensive system with inside limits. These three issues, as comprehensively including as they may be, can be overpowering for little to average-sized business to handle all alone.

### **2.5.4 *Network Congestion***

Numerous system interferences connected with network demands are identified with signaling overload and data transmission overburden/bandwidth utilization. It is imperative to comprehend and have the capacity to scale and improve the signaling in the network system guaranteeing that the unlimited number of devices and applications are not bringing on pointless clog or in other terms, network congestion. Spectrum is the most profitable resource in the network domain. Spectrum increments are basic to network scope and to have the adaptability to meet the regularly extending number of users and data transmission requests. An expanded and well-utilized spectrum will convey better client experience. Measured performance execution of the system sign is imperative to the client experience. Network planning and tuning can convey up to three times the change in bandwidth. Calibrating the system through expert administrations is generally as critical as the equipment. Moreover, reconfiguring the systems rapidly (utilizing virtualization and a software-defined networking methodology) to rapidly test new administrations can rapidly scale it to millions. There is no more the need to contribute months of operational arranging to trial and offer service. The OpenDaylight project has given an open-source stage where individuals team up to build common software-defined networking infrastructure. Ericsson's commitment to the joint effort is centered around extending this insight from the data center into the network system—giving a more incorporated and less-difficult improvement environment.

## 2.6 Future of Networking

The era of modern business systems started more than a quarter century and was stamped by the public packet mode network as an alternative option for leased line-based wide area networks (WANs). Frame Relay formed the first epoch of this new era. It rose to prominence in the mid-1990s when organizations were saddled with numerous, merchant particular systems supporting centralized computer and customer/server situations. Frame Relay was intended to be convention straightforward and utilized supplant-isolated leased line WANs with a single multiprotocol packet network.

Before the end of the 1990s, Microsoft-controlled PCs and LANs were pervasive crosswise over organizations pushing out other exclusive network systems. At the same time, the Internet was prospering and TCP/IP turned into the overwhelming route to join branch, campus, and datacenter LANs together. The second age of cutting edge organizing, i.e., LAN internetworking was borne.

Today, IP-based devices are quickly multiplying inside and outside the four dividers of organizations making systems progressively hard to scale, manage, secure, and adjust.

Likewise, with most engineering issues, all aspects of system configuration present tradeoffs. It is troublesome, hence, to focus the essential heading of current network system research, on the grounds that it is assaulting numerous fronts at the same time. Regardless, there is adequate opportunity to get better on advanced system frameworks. Indeed, even the quickest systems are significantly slower than as far as possible forced by the rate of light, and enhancements in this idleness would have an awesome impact on multiprocessing execution. There is likewise the likelihood that new strategies for parallelizing applications will lead the network organization in already unexplored headings. Regardless, networking technology is in no way, shape or form a depleted science, and much work stays to be finished.

When we glance back at every age of cutting edge organizing, we see a watch's change at every move. Network technology has shown phenomenal growth in the today's global developing scenario. The network system should be adaptive and healed in such a way that if there are any catastrophic errors at one end, it should not affect the overall network performance. The network should show minimal errors with maximum output.

## 2.7 Summary

The union of computing and network systems administration is more apparent than in the amazing development of the WWW. In another sense, however, network systems administration is being pulled in two inverse directions. From one perspective, the Web's prominence and development have been powered to a great extent by desktop applications expanding transfer speed concentrated pictures and

videos. From the other perspective, thin-client computers are turning out to be all the more generally utilized as edge-of-network system devices, frequently associated by wireless technology. There is likewise an expanding befuddling between fiber-optic transmission data transfer capacities and computer speed, pushing the processing further far from the system center. Based on it, this chapter provides details on network structure, type, and topology and the issues pertaining to the present network scenario. Furthermore, the chapter provides insights on the issues and challenges of networking.

## References

- Buzzle. (2015). *Advantages and disadvantages of computer networks*. <http://www.buzzle.com/articles/advantages-and-disadvantages-of-computer-networks.html>. Accessed September 29, 2015.
- Carlson, M., Davies, E., Nortel, U. K., Wang, Z., & Weiss, W. (1998). *An architecture for differentiated services*.
- Chen, S., & Nahrstedt, K. (1998). An overview of quality of service routing for next-generation high-speed networks: problems and solutions. *Network IEEE*, 12(6), 64–79.
- Crawley, E., Sandick, H., Nair, R., & Rajagopalan, B. (1998). *A framework for QoS-based routing in the internet*.
- Gu, G. Q., & Luo, J. Z. (2006). Some issues on computer networks: Architecture and key technologies. *Journal of Computer Science and technology*, 21(5), 708–722.
- IT Direct. (2015). <http://www.gettingyouconnected.com/the-top-3-issues-affecting-todays-large-computer-networks/>. Accessed September 28, 2015.
- Kozierok, C. M. (2015). [http://www.tcpipguide.com/free/t\\_TheAdvantagesBenefitsofNetworking.htm](http://www.tcpipguide.com/free/t_TheAdvantagesBenefitsofNetworking.htm). Accessed September 29, 2015.
- Mazumdar, R., Mason, L. G., & Douligeris, C. (1991). Fairness in network optimal flow control: Optimality of product forms. *IEEE Transactions on Communications*, 39(5), 775–782.
- Nichols, K., Black, D. L., Blake, S., & Baker, F. (1998). *Definition of the differentiated services field (DS field) in the IPv4 and IPv6 headers*.
- Osborn, C. (2015). *A networking overview*. <http://www.ai.mit.edu/projects/aries/course/notes/networkpaper.pdf>. Accessed September 29, 2015.
- Wikipedia. (2015). [https://en.wikipedia.org/wiki/IEEE\\_802](https://en.wikipedia.org/wiki/IEEE_802). Accessed September 29, 2015.
- Xiao, X., & Ni, L. M. (1999). Internet QoS: A big picture. *Network IEEE*, 13(2), 8–18.

Mapping Biological Systems to Network Systems

Rathore, H.

2016, IX, 196 p. 107 illus., 37 illus. in color., Hardcover

ISBN: 978-3-319-29780-4