1

Introduction to Network Routing

1.1 Introduction to Networks

A computer network supports data communication between two or more devices over a transmission medium. The transmission medium can either be wired or wireless. The network is established and data is transmitted over it with the support of networking hardware and the software running on the hardware. Network hardware comprises equipment that generates the signal at the source, transmits the signal over the transmission medium, and receives and processes the signal at the destination. The software comprises protocols, standards, instructions, and algorithms that support transmission services over the network. The essentiality of networks has increased over time, along with advancement in network hardware, software, and support applications. There are huge variations in the size of a network in use; there can be small networks confined to an office or home, and at the same time there are networks spread across cities and countries. The spread of the network can be described in various terms, such as distance covered and the number of computers and other resources connected to the network. A local area network confined to a building may connect thousands of computers, such as in a software development center, a call center, or a stock exchange. Alternatively, a network spread across continents may connect only a handful of computers; for example, a network from a country to its base station in Antarctica may cover a few thousand miles but connect only a few computers.

The purpose of a network is to enable transmission of information between two or more networked nodes. The networked nodes can be computing devices, storages,

Network Routing: Fundamentals, Applications, and Emerging Technologies, First Edition.
Sudip Misra and Sumit Goswami.

Companion website: www.wiley.com/go/misra2204

networking devices, or network-enabled peripherals. The computing devices can be desktop computers, laptops, or servers. Network-enabled peripherals can be printers, FAX, or scanners, and the networking devices are switches, routers, or gateways. Any other network-enabled device capable of sending or receiving data over the transmission medium can be a part of the network. A network system comprises a source, a destination, and the transmission system in-between. The source prepares data for transmission over the transmission medium. The preparation involves transformation of data, striping it into smaller parts, encapsulation, encoding, modulation, and multiplexing for converting bit streams into electrical signals or electromagnetic or radio waves. The transmission medium comprises the network connecting different nodes. The transmission medium can support unidirectional flow of data (simplex), bidirectional flow of data (duplex), or flow of data in either direction at one time (half-duplex). It can also be wired or wireless, providing point-to-point connectivity, or it can work in a one-to-many broadcast mode. The transmission medium may directly connect the source to destination, or it may be through intermediate network nodes. Thus, a transmission medium can be in various forms, utilizing different technologies and encompassing a variety of architectures. The destination receives data from the transmission medium, demultiplexes, demodulates, and retrieves the original data after decoding, rearranging, and merging. The transmission medium is a complex system as it can be shared between various network devices and has to run identification, channel utilization, security, congestion control, and bandwidth assurance services on it.

In addition to the source, destination, and transmission medium, a network system also comprises a few services such as exchange management, error detection and correction, flow control, addressing and routing, recovery, message formatting, and network management [1]. *Exchange management* deals with the mutually agreed conventions for data format and transmission rules between the sender and the receiver. The network system is prone to errors due to signal distortion, introduction of noise in the data signal, and bit flips during transmission, which may lead to receiving incorrect data, data loss, and data alteration. These are handled by *error detection and correction* techniques. *Recovery* is the process through which a network system is able to resume its activity even after a failure. The recovery may be from the point of failure or from a restore point prior to the failure. *Flow control* helps in synchronizing the rate of transmission from the sender, its flow through the network, and the rate at which the data is received. Flow control ensures that the data is transmitted at a mutually agreed rate to take care of the difference in the processing speed or variation in the network bandwidth of the sender and the receiver. *Addressing* is used uniquely to identify a network resource, and *routing* helps in deciding the optimum path for the data to flow from the source to the destination through the intermediate network. *Message formats* are the mutually agreed form of data. *Network management* is to monitor the network system, detect points of failure, and monitor the health of the system in terms of bandwidth utilization and load on network nodes. This helps to predict probable points of failure in future and enables enhancement or change in resources to avoid any network outage. The network management system also helps in version control of the software running on the nodes, its centralized upgradation, patch management, and inventory control of software and hardware.

The Internet is the largest network in terms of its geographical spread as well as the number of connected computers. The Internet has become the de facto network for people as well as organizations worldwide owing to its capability to act as a connectivity medium across geographical regions. The common applications running over the

Internet are electronic mail, electronic commerce, and Web access. In the 1960s, when the networks were being conceptualized and experimented, vendors designed and developed proprietary network equipment and protocols. This led to competitiveness among the vendors for faster development of network protocols and devices for having a competitive edge by providing an advanced and more scalable network. However, it restricted interconnectivity among networks from different vendors such as Microsoft, Novell, Banyan, Xerox, IBM, and DEC. A network based on equipment and software of one vendor could not connect or exchange data with a network based on the products of another vendor. Thus, if some computers in an organization were on the Novell network, they could not share data with other computers of the same organization that were on the IBM network.

Introduction of the seven-layered open system interconnection (OSI) as an implementation of the ISO standard led to the establishment of a framework for multivendor network compatibility, connectivity, and interoperability. Based on the ISO standard, the vendors provided interconnectivity options over their proprietary networking protocols. However, the Transmission Control Protocol/Internet Protocol (TCP/IP) became a de facto network connectivity standard preferred over interconnection suites of the proprietary networks, and slowly the vendors moved on to support TCP/IP [2]. TCP/IP was an outcome of research in ARPANET, a United States Department of Defense (DoD) project and hence sometimes known as the 'DoD model'. TCP/IP is also commonly known as the 'public networking model', as the Internet Engineering Task Force (IETF) maintains the protocol with the involvement of representatives from various networking companies for evolution of TCP/IP standards. The Internet is built on TCP/IP providing connectivity between heterogeneous physical networks and protocols.

The present-day network is used for transmission of data, voice, video, and share resources. With time, there has been a rapid increase in the bandwidth supported by wired as well as wireless networks. The bandwidth availability has increased to cater for data sharing between computers and servers with high memory and processing power as well as voice and video applications. Concurrently, the problem of traffic congestion is evident owing to an increasing demand for network bandwidth. Congestion is also caused by scaling of the network without considering the available network resources in place. There has been a reduction in the cost of networking devices as well as computing devices. So, a faster and scalable network can be established at a much lower cost. However, the reduction in computing cost and increase in the number and type of computer applications lead to increase in the rate at which the devices push data into the network. Convergence of voice, video, and data into a single application and its transmission through a common integrated channel also increases the bandwidth utilization. With a high degree of office automation and dependence on the network for real-time or near-real-time data transmission and updates, slow and congested networks are unacceptable.

In order to avoid congestion, a network is generally broken down into smaller segments using networking devices called bridges, switches, and routers. The contents of the data being transmitted over a network are not of any interest to these networking devices. These networking devices look only into the origin, destination, and control information related to the data in transit so as to enable its effective delivery to the destination [3]. The effectiveness of the delivery varies with the application and may be optimized in terms of transmission time, secured delivery, reliable delivery, acknowledgement, delivery only through a dedicated path, or assurance of a minimum bandwidth throughout the transmission link, ensuring quality of service (QoS).

A network is generally gauged by three major criteria – performance, reliability, and security [4]. The performance of a network is dependent on a number of factors, such as the number of nodes connected to the network, the bandwidth of the transmission medium, the protocol used, the software overlay, and the amount of memory and processing capability of the networking hardware and the nodes. The network performance is evaluated in terms of throughput and delay, which are inversely proportional to each other. Transit time and response time are the two parameters used to measure the performance of the network. Transit time is the amount of time a message spends in the network after its transmission from the source until it reaches the destination. Response time is the total time between sending a query through the network and receiving its response. Reliability relates to the duration for which a network remains operational without failure, which is different from availability. A network that goes down every hour just for a second will be highly available, but its reliability will be low. Thus, reliability can be measured with the help of mean time between failures (MTBF). Network security relates to implementation of access policies, restricting the data from unauthorized access, protection from change of data (integrity), preventing damage or loss of data, detection of security breaches, and procedures for data and network recovery in case of security attack.

1.2 Network Architecture and Standards

Network architecture is the logical and structural layout of the network that assists and guides the network designer in implementing an optimum network. The network architecture also supports the network administrator in managing the network and troubleshooting the point of failure in case of a breakdown. The network architecture is an essential component for working on the security of the network and implementing access policies. Network communication is a multilayer task wherein each activity is accomplished at a particular layer of the architecture. The layering makes the architecture simple to develop and implement. Each product and protocol is designed to work in a particular layer or across a few layers with standard interlayer interfaces supporting interoperability among the products and protocols. Although a network may be designed and implemented in various forms, the OSI layer divides it into three basic categories. The data transmission uses the physical layer of the OSI model, the network devices operate at the data link layer and network layer, and the applications use the session layer, presentation layer, and application layer of the OSI model.

The network architecture is closely associated with the topology of the network. The topology is the logical design of the network, showing the interconnection of the networked nodes. The topology planned for a network is based on cost, scalability, application, criticality, size, and type of network. The commonly used topologies are star, bus, ring, and mesh. Various combinations or minor modifications of these common topologies can be used to evolve other topologies such as tree, distributed bus, extended star, distributed star, partial mesh, or hybrid.

In a star topology, the network nodes have a point-to-point connection with the central hub. In a bus topology, also known as a line network, each network node is connected to a single cable. In a ring topology, the network nodes are set up in a circular fashion in which the data transmission takes place around a ring in one direction and each

neighboring node, either to the left or to the right, works as a repeater in order to maintain the strength of the signal as it is transmitted in a loop. This topology is also known as a loop network. In a mesh network, each node is connected point-to-point with all other nodes in the network. When every node is connected to all the other nodes in the network, it is known as a complete mesh. When some of the links in a complete mesh network are removed to reduce redundancy, this leads to the creation of a partial mesh.

Visual representation of the common topologies is given in Figures 1.1 to 1.4.

Each topology has its advantages, disadvantages, and applications, which are set out in Table 1.1.

A network is also classified according to the geographical spread of the nodes. Based on size, the classical types of network are typically the local area network (LAN), the metropolitan area network (MAN), and the wide area network (WAN). A LAN connects the networking devices within a short span of area and is generally controlled, maintained, and administered by a single person or a company. A MAN is an

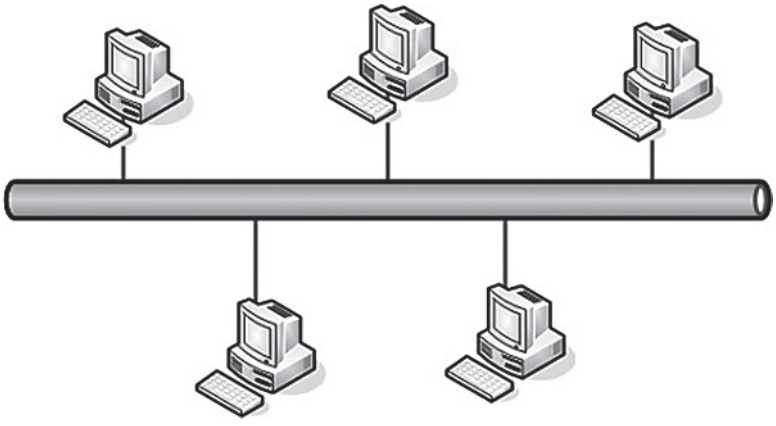

Figure 1.1 Bus topology.

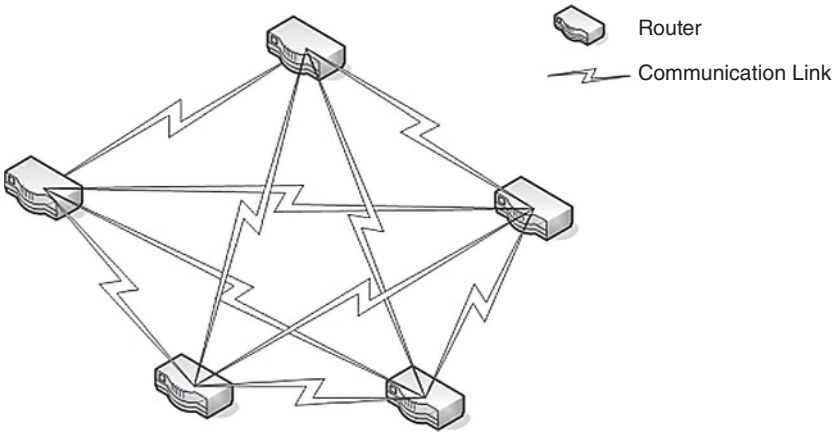

Figure 1.2 Mesh topology.

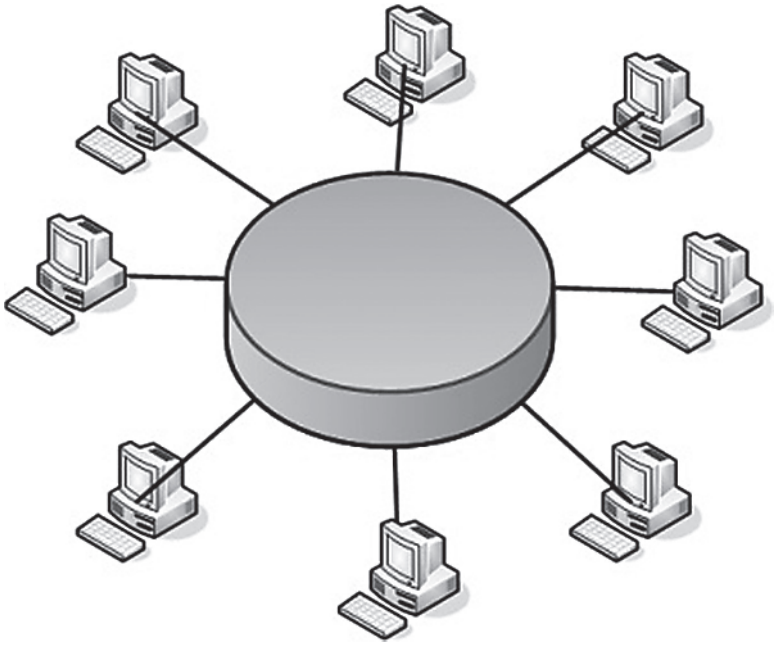

Figure 1.3 Ring topology.

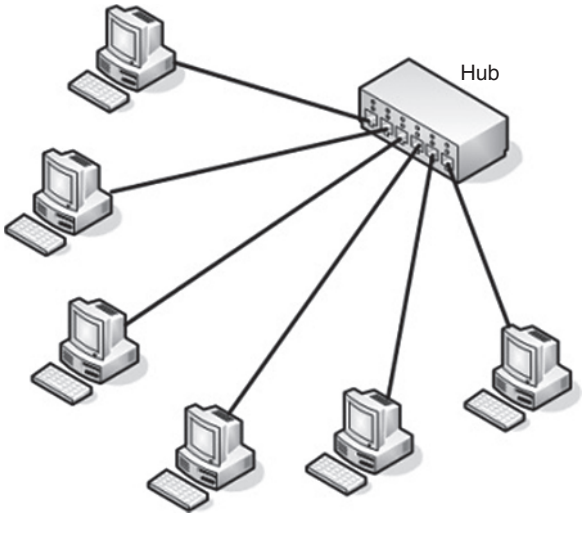

Figure 1.4 Star topology.

intermediate-sized network and in terms of outreach can be placed between a LAN and a WAN as it covers a large span of physical area such as a metropolitan city, which is larger in size than a LAN but smaller than a WAN. A WAN connects the networking devices and a collection of LANs that are distributed over a large geographical area, which may spread across cities or even continents. In addition to the classical types of

Table 1.1 Comparison of network topologies.

Topology	Architecture	Operation	Scalability	Point of failures	Advantage	Disadvantage
Bus	Each node is connected to a single backbone cable.	Information is transmitted from one node to another through the backbone cable.	High scalability at low cost as a node has to be directly connected to the backbone cable.	A break in the backbone cable disrupts the entire network.	Easy to install and cost effective.	Only one node can transmit at a time.
Star	Each node is connected to a central hub.	Information passes from one node to another through the central hub.	High scalability at optimum cost as a node has to be directly connected to the hub.	Failure of the hub disrupts the entire network.	Easy to install and cost effective; if a switch is used as a central node, multiple nodes can communicate with each other concurrently.	Single point of failure.
Ring	Each node is connected to a single backbone cable configured as a ring.	Information moves from the source node in a unidirectional manner along the ring until it reaches the destination.	Generally implemented using fiber cables. Hence relatively higher cost.	Even if there is a break in the cable, information can be transmitted through the rest of the ring.	Avoids a single point of failure as the data can move in another direction to reach the destination from any source in the case of a break in the ring.	Not in common use.
Mesh	Each node is connected to every other node.	Information is directly transmitted from source to destination without intermediate nodes and in a single hop.	Limited scalability as each new node has to be connected to every other existing node.	A cable break will disrupt the direct connectivity only between a pair of nodes. However, alternative routes will exist.	Highly redundant, and reliable and fast network.	Implementation is costly and complicated.

network, a few more network types have now emerged, which are defined according to the size and application domain of the network. Some of these are as follows:

Campus area network (CAN). These are the networks spread across the campus of large institutes, academic centers, research organizations, or industrial complexes.

System area network (SyAN). These networks connect the high-performance systems in a network. The network has low latency and high speed of the order of 1 GB/s. These are also known as cluster area networks as they provide a high-speed data and communication interconnection framework to workstations and PC clusters [5].

Storage area network (SAN). SAN is a network of storage devices and associated servers redundantly interconnected with switches using fiber connectivity providing high bandwidth and parallel links. The storage media has information redundancy at its own level. The SAN provides consolidated high-volume storage accessible by the computational devices over the network.

Personal area network (PAN). The coverage of the network ranges from only a few centimeters to a few meters and is capable of connecting various devices used as personal assistants to individuals or located near to their area of presence. The personal area network can be wired and supported by USB or Firewire. It can be wireless and supported by ZigBee, 6LoWPAN, Bluetooth, or Z-Wave.

In addition to these common types of network, a number of other networks have also been introduced, based on scale of extent and purpose. Some examples of these special and new types of network are the near field network (NFC), Internalnet, the body area network (BAN), the near-me network (NAN), the home area network (HAN), and the interplanetary Internet.

Based on the services concept, the network architecture can be broadly grouped into the following two categories:

Client–server architecture. The system is decomposed into two entities classified as the client and the server. The client and the server may be the processors (computers) or the processes. A producer providing the appropriate resources and services is termed the 'server', and the consumer using the provided services is termed the 'client'. There exists a relationship between multiple clients and multiple servers. The client–server architecture model works in a 'tier' approach, separating the functionality of the tiers on the basis of the concept of the services provided.

Peer-to-peer architecture. In this model, all the network nodes are believed to have equivalent computational power and resources and have equal capabilities and responsibilities in terms of service provision.

There can be instances where a combination of peer-to-peer architecture is embedded in client–server architecture. The client–server architecture distributes the system in tiers, and each tier can further have a peer-to-peer architecture running within it.

The network architecture can also be designed with an attempt to separate application from data so as to enhance security as well as accessibility. Such architecture has three tiers [6] – the Web tier (referred as the demilitarized zone), the application tier, and the data tier. The description of each of these tiers is as follows:

Demilitarized zone (DMZ). The demilitarized zone is the topmost level of the application in the network's hierarchy and is also known as the Web tier. It provides an interface to the external network for accessing data and utilizing the services of the applications and resources lying in the militarized zone without directly interacting with the internal system in a network. The functional implementation of the demilitarized zone is created using firewalls. A DMZ is categorized as the part of the network that is layered between a trusted internal network and an untrusted external network.

Application tier. The application tier is also known as the business logic layer. This is the middle layer between the demilitarized zone and the data tier. The application tier accesses the data tier to retrieve or modify data from the data tier and sends the processed data to the devices in the DMZ tier. Direct access to the application tier is not permissible to the users.

Data tier. The data tier is the innermost (i.e. core) tier of the network's architecture. This tier hosts the databases and database servers that store and access information of the systems. This tier is responsible for maintaining the neutrality and the independency of the data from application servers and business logic. Direct access to the data tier is not permissible to the users. This layer is also known as the database tier or intranet zone.

Setting up network standards facilitates the interoperability of network technologies and systems. A standard in the field of the networks can be proprietary, open, or de facto. The open standards generally emerge from the efforts of a consortium of industries, which are generally non-profit organizations. Some of the standards organizations in the field of networks are as follows:

- International Organization for Standardization (ISO),
- American National Standards Institute (ANSI),
- Institute of Electrical and Electronics Engineers (IEEE),
- Electronic Industries Alliance (EIA),
- Telecommunications Industry Association (TIA),
- International Telecommunication Union – Telecommunication Standardization Sector (ITU-T),
- European Telecommunications Standards Institute (ETSI).

Unlike international standards organizations, which generally work on open standards, there are also networking industry groups that work on creating, upgrading or promoting standards. However, they develop and promote specific standards that are generally product oriented. With the wide spread and usage of the Internet, a few Internet standards organizations [7] have also taken responsibility to develop policies, standards, and architecture related to the Internet. Some of these organizations are as follows:

- Internet Society (ISOC),
- Internet Architecture Board (IAB),
- Internet Engineering Task Force (IETF),
- Internet Research Task Force (IRTF),
- Internet Engineering Steering Group (IESG),
- Internet Research Steering Group (IRSG).

Table 1.2 A few major networks standardized by IEEE.

IEEE standard	Network/system standardized
802.1	Procedures for bridging and managing network
802.1 Q	Virtual LANs (VLANs) over Ethernet network
802.3	Physical layer and media access control layer of wired Ethernet
802.4	Token-passing bus
802.5	Token ring
802.6	Distributed queue dual bus (DQDB)
802.7	Broadband LAN
802.11	Wireless networking and Wi-Fi certification
802.15	Wireless PAN
802.20	Mobile broadband wireless access

Many networking standards set by IEEE are in common use, and the major ones are listed in Table 1.2.

The 802.11 standard includes 802.11a, 802.11b, and 802.11 g, the details of which are as follows:

802.11a. The 802.11a standard [8] sets the protocols in the data link layer and an orthogonal frequency-division multiplexing (OFDM)-based physical layer. It operates in a bandwidth spectrum of 5 GHz with a maximum data flow rate of 54 Mb/s and includes error correction procedures.

802.11b. The 802.11b standard uses the media access method and has a maximum data flow rate of 11 Mb/s. The 802.11b standard extends the modulation technique of the 802.11 standard directly.

802.11 g. The 802.11 g standard works on a bandwidth of 2.4 GHz and uses the OFDM-based physical layer scheme for data transmission. It has a maximum data flow rate of 54 Mb/s, exclusive of error correction codes.

Networking standards set by EIA: EIA-485 is a standard that defines the characteristics and electrical properties of drivers and receivers that are to be used in a balanced digital multipoint circumvented system. Digital communication networks possessing the EIA-485 standard can be used for long-range networks that can work effectively in an environment with electrical interference or other noise.

Networking standards set by ITU-T: ITU-T is a standard that defines the characteristics of an optical transport network (OTN), and hence this standard has played a characteristic role in transforming the Internet's bandwidth and spectrum capabilities.

Networking standards set by the International Organization for Standardization: In the networking area, ISO sets the standards for the implementation of an OSI reference model. This model defines and lays the networking framework for network protocol implementation in the seven distributed layers of the network. Control is passed in the network via these seven layers, starting from the topmost to the bottom-most layers, which are as follows:

Table 1.3 Layer-wise protocols in the ISO OSI model.

Layer	Protocols
Application (layer 7)	COPS, FANP, FTP, HTTP, IPDC, IMAP4, IRC, ISAKMP, NTP, POP3, RLOGIN, RTSP, SCTP, SLP, SMTP, SNMP, TELNET, WCCP
Presentation (layer 6)	BGP4, EGP, HSRP, EIGRP, TGRP, NARP, NHRP
Session (layer 5)	BGMP, DIS, DNS, ISAKMP/IKE, ISCSI, LDAP, MZAP, NetBIOS/IP
Transport (layer 4)	ISTP, Mobile IP, RUDP, TALI, TCP, UDP, Van Jacobson, XOT
Network (layer 3)	DVMRP, ICMP, IGMP, IP, IPv6, MARS, PIM, RIP2, RSVP, VRRP
Data link (layer 2)	ARP/RARP, MPLS, PPP, FDDI, SLIP
Physical (layer 1)	ATMP, L2F, L2TP, PPTP

Application (layer 7). This layer is application specific and provides services such as file transfers, email, and other network services and supports end-user processes.

Presentation (layer 6). This layer provides the representation of data by application to network format translation, and vice versa. This layer is also responsible for encryption and decryption.

Session (layer 5). This layer is responsible for establishing, managing, and terminating the network connections between applications.

Transport (layer 4). This layer provides the effective and fault-free transfer of data between end systems and is responsible for error recovery and control of flow so as to ensure complete data transfer.

Network (layer 3). This layer provides the switching and routing techniques to transmit the data from source node to destination node in a network.

Data link (layer 2). At this layer the encoding and decoding of data packets into bits take place.

Physical (layer 1). The bit stream, in the form of electrical impulse, light or radio waves, is transmitted through the network. It provides a hardware means of sending and receiving data on a carrier.

A list of selected protocols in the various layers of the ISO OSI model is given in Table 1.3.

1.3 Glimpse at the Network Layer

The network layer is also referred as the internet layer or the internetworking layer. It is designed for data delivery across the nodes in the network. It also performs device addressing, packet sequencing, path determination, congestion control, and error handling. The network layer operates over the physical layer and the data link layer. While the lower layers provide a mechanism for data transfer within the same network, the network layer has protocols for support, with due consideration for QoS, and data transfer across various interconnected networks or the internetwork and even the

Internet. The main network equipment operating in this layer is the router, which is used for routing packets and message forwarding within an internetwork. A few common protocols of the network layer are as follows:

- Internet Protocol (IPv4/IPv6),
- Internet Control Message Protocol (ICMP),
- Internet Group Management Protocol (IGMP),
- Internet Protocol security (IPsec),
- Internetwork Packet Exchange (IPX),
- Routing Information Protocol (RIP).

The need for the network layer [4] can be explained with a simple example of an internetwork connecting a few local area networks (LANs). When the source and destination are within the same LAN interconnected by a switch, the delivery of the packet can be achieved using the physical layer and the data link layer, employing the media access control (MAC) addresses of the source and destination available in the frame. However, to achieve data delivery across LANs connected by a router, as shown in Figure 1.5, the lower layers cannot provide information regarding forwarding of the frames to the appropriate interface on the router, as they lack the routing information. The network layer provides information regarding the link and interface on which a packet should be forwarded for delivery to the destination.

The network layer is responsible for host-to-host delivery and performs necessary functionality at the source, router, and destination [4]. At the source, which is the transmission end, the network layer creates packets from the data received from higher layers, such as the transport layer or any other appropriate layer in the protocol stack being used. For delivery of the packet across various links, a logical address of the destination is required, which is handled by the network layer. As logical addressing is handled at the network layer, the necessary information for routing, which also includes the source and destination addresses, is put in the network layer header to assist routing. Other information available in the header includes packet checksum

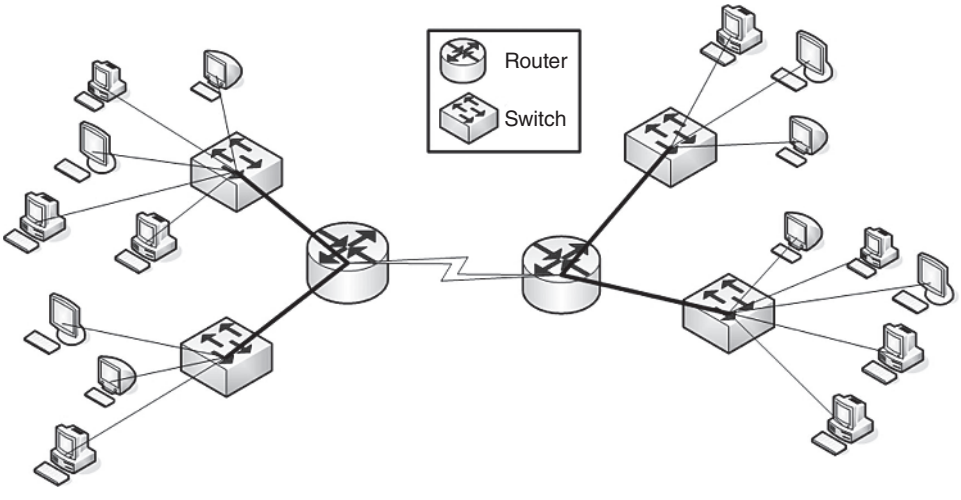

Figure 1.5 A network with two routers and two LANs connected to each router.

information for facilitating error detection, an identifier for the higher-level protocol being used, and some administrative data and some optional padded-out fields. Thereafter it adds the network layer header to the data packet and fragments the data packet if the size is larger than the maximum transmission unit (MTU). The network layer is responsible for maintaining the routing table, which contains information related to the interfaces through which a packet should be forwarded for a particular destination. The network layer refers to this routing table available at the source and determines the interface at the source through which the data packet should be forwarded out of the source. With this exit interface information, the data packet is sent to the lower layers for delivery.

Each protocol has an MTU, which is the maximum packet size that it can handle and transfer. When the network receives a data packet that is larger than its MTU, it has to fragment the data packet for transmission and then reassemble the data packet from the fragments at the destination. The format of a fragment, as well as that of a much larger data packet, is the same so as to support the reassembly. The header of the fragment contains information for identification of the fragment, i.e. the identification field to locate the packet to which the fragment belongs, as well as that for its reassembly, i.e. the fragmentation offset to identify the location of the fragment in the packet [9]. A 'More Fragments' flag field acts as a counter to indicate the assembly of all the fragments of the packet.

When the data packet reaches the router through any of its interfaces, it looks at the network header to read the destination address. If the packet is not meant for the router, then it looks up its routing table to search for a suitable exit interface for the destination address of the arrived packet and thereafter forwards the packet through that interface for framing at the lower layer and further delivery. During this process, necessary modifications are made in the network header to support a number of other functionalities of the network layer. The actual delivery of the packet to its destination is based on the MAC address. The network layer facilitates mapping of the MAC address with the logical address generally at the time of network connection. If a suitable entry corresponding to the destination address cannot be located in the routing table, then the packet is dropped.

At the destination, the network layer ensures that the delivered packed is meant for it. The identification is based on the destination address in the data packet header. As the network layer may not be connection oriented, this may lead to the arrival of fragments through different links and in a different sequence to that in which they were transmitted. The network layer assembles all the fragmented packets and arranges them sequentially. The reassembled fragments are then sent to the upper protocol layer.

There are two types of packet in the network layer – data packets and route update packets. Data packets are used to transmit the data received from the higher layers for transmission across the internetwork. These packets belong to any of the protocols, such as IP or IPX, that support routing of the packets across the routers. Such types of protocol are known as 'routed protocols.' The route update packets are generated by the routers to make the network aware of its interfaces and connected networks and enable the recipient routers to build, maintain, and update the routing table. The packets may be transmitted only to neighbors or to the entire internetwork, depending on the routing protocol in use. Protocols such as RIP and OSPF that transmit these route update packets are known as 'routing protocols.'

Connection-oriented vs connectionless network service. A network layer service can be connection oriented or connectionless, based on the specific protocol being used, the supported application, the type of network, and a few other related parameters. In a connection-oriented network service, a virtual path [4] is established between the source and the destination before initiation of the packet transmission, and so this is also known as the virtual circuit approach of packet switching. Once the path is established, all the packets are transmitted from the source to the destination using the same path, and the packets are transmitted in sequence. The transmission is reliable, and all the packets follow the same path. They arrive at the destination in the same sequence in which they were transmitted. The connection is terminated only after the entire message has been transmitted. Asynchronous transfer mode (ATM) and frame relay use the virtual circuit approach for packet switching.

In a connectionless network service, the path of each data packet is determined separately. The network header of each packet is read for its destination address along with the other network layer parameters. The destination address is then looked up in the routing table to determine the exit interface for forwarding the packet. As the routing table may be dynamic in nature and can change with time owing to change in the network parameters, this can lead to a different exit interface for the packets to the same destination address. Thus, the packets from a source to the same destination can travel across different links and reach the destination in a different sequence from the one in which they were transmitted. This type of service, which is also known as packet switching using the datagram approach, is commonly used on the Internet.

1.4 Addressing in TCP/IP Networks

TCP/IP is the basic communication language or protocol that enables computers to communicate over the network. Created by an agency of the United States Department of Defense, DAPRA, TCP/IP is an industry standard suite of protocols describing a set of guidelines and specifications to provide communication in a heterogeneous environment. It provides a routable, enterprise networking protocol and access to the Internet and its resources. In TCP/IP, a session is established between the sender and receiver before transmission of the actual data, thus making it a connection-oriented protocol. The end-to-end connection is established using the port numbers at the endpoints. The reliability of the delivery of data to the destination is ensured by using the sequence number in the data packets and acknowledgement from the destination.

The TCP specifications were first laid down in 1974, and the IP standard was published in 1981 in the form of RFC-791. TCP/IP is a bilayer standard. In the higher layer is the Transmission Control Protocol, which manages the assembling and reassembling of the packets that are transmitted over the network for communication. The received packets are converted into the original message. Thus, a TCP header primarily comprises the source port, the destination port, the sequence number, the acknowledgement number, the data offset, the flag bits, the window size, and the checksum. In the lower layer the Internet Protocol manages the address of each packet so that it goes to the right destination. It follows a point-to-point communication in which the message is transmitted from a point in the source computer to the destination computer. For the delivery of every TCP segment there is a TCP port, and the commonly used port

numbers are: 20 for File Transfer Protocol (FTP) (data channel), 21 for FTP (control channel), 23 for Telnet, 25 for Simple Mail Transfer Protocol (SMTP) (for email), 80 for Hypertext Transfer Protocol (HTTP) used for the WWW, and 139 for the Net BIOS Session Service. The IP header mainly comprises time to live (TTL), the protocol, the header checksum, the source IP address, and the destination IP address.

The network nodes, such as computers, servers, routers, and other network-enabled devices, have a unique IP address. Internet Protocol Version 4 (IPv4) uses a 32 bit addressing scheme, limiting the number of uniquely addressable devices to 2^{32}, i.e. 4 294 967 296. The 32 bit IP address is represented in the form of four octets (8 bit field). Each octet, being 8 bit, represents a decimal number in the range 0–255. This format of representing the IP address as four decimal numbers in the range 0–255, each separated by a dot, is called dotted decimal notation. For example, an IPv4 address represented in binary form can be 10000010.01101111.00000010.00001100, the dotted decimal notation of which is 130.111.2.12

Classful Addressing

Originally, IP addresses were divided into two parts, namely the network ID and the host ID. The former used the first octet of the address, and the latter occupied the remainder of the address. This led to the development of only 256 networks. Later on, classes of network were created of higher-order octet. This type of class-based IP address was known as classful networking [7,10]. For the purpose of network identification, the classes A, B, and C had different bit lengths for both network ID and host ID, as shown in Table 1.4.

Subnetting

A network may be small and does not require the entire available host IDs to address its nodes. Alternatively, the organization may be willing to divide its network into a number of smaller networks based on the applications or physical distribution and would be interested in restricting the traffic flow within the smaller network unless specified. A subnet divides the host address space into smaller groups for preservation of address space, reduction in traffic congestion in the network, and enhancement of security. A subnet reduces the network traffic by limiting the broadcast domain within the subnet. A subnet address is created using the initial bits of the host ID, thus reducing the number of hosts that can be accommodated in the subnet.

Table 1.4 IP address class.

Class	Bits in network number	Bits in host number	Initial bits
Class A	8	24	0
Class B	16	16	10
Class C	24	8	110
Extended addressing			111
Class D	Not defined	Not defined	1110
Class E	Not defined	Not defined	1111

In a classful address [3], the host computer knows which initial bits of the address represent the network ID, and the remaining bits represent the host ID. However, in the case of subnet addressing, the same information is sent to the host computer using subnet masking, as it is not predefined. Like an IP address, the subnet mask is a 32 bit address with the initial bits as 1 and the trailing bits as 0. The 1 s in the subnet mask indicate the bits that will represent the subnet or the network ID in the IP address. The default subnet mask for class A, B, and C addresses is 255.0.0.0, 255.255.0.0, and 255.255.255.0 respectively. The number of bits available in class A, B, and C addresses for subnetting is 24, 16, and 8 respectively. Thus, in a class C address, the subnet masks in the fourth octet can be 10000000 (128), 11000000 (192), 11100000 (224), 11110000 (240), 11111000 (248), 11111100 (252), and 11111110 (254), which are created by increasing the masking by 1 bit successively. The subnet mask of 11111110 (254) cannot address any host computer, as all 0 s in the host ID represent the network or the subnet and all 1 s are reserved for broadcast. However, RFC 3021 uses a 31 bit subnet mask for a point-to-point link where network and broadcast addresses are not necessary. In a similar manner, the subnet mask of class B and A addresses can vary from 1000000.00000000 to 11111111.11111110 and from 1000000.00000000.000000 to 11111111.11111111.11111110 respectively. Consider a class C address with a subnet mask as 11000000 (192). Here, the two bits with value 1 represent the subnet and the six bits with value 0 represent the host. Thus, the subnet can have the values 00, 01, 10, and 11. For the subnet 01, the first host ID will be 000000, i.e. the network address (**01**000000), the next host ID will be 000001, i.e. the first valid host (**01**000001), up to the last valid host (**01**111110), followed by the broadcast ID (**01**111111111).

Classless interdomain routing (CIDR) is used to assign blocks of IP addresses with consecutive addresses within an address bit boundary. CIDR is represented using an IP address followed by a decimal number with a slash (/) in-between. The decimal number when converted into binary gives the sequence of leading 1 s, which represent the initial bits that cannot be changed in the address chunk. The trailing 0 s represent the bits that can be changed to obtain a sequence of IP addresses in the address block. Thus, a block with an IP address represented as 192.168.13.32/28 represents a subnet mask of 255.255.266.240. The default subnet mask in a class C address is 255.255.255.0, and a class C address, e.g. 192.168.13.70, with a default subnet mask can be represented in CIDR slash notation as 192.168.13.70/24 because 24 bits of 1 s followed by 0 s translate to 11111111 11111111 11111111 00000000, i.e. 255.255.255.0.

Variable-length subnet mask (VLSM). The conventional classful addressing scheme was a two-level addressing scheme with a network ID and a host ID. Subnetting converted this addressing to a three-level scheme, adding an extra level of subnet giving the network designer the liberty to divide a huge network or a large address space into smaller equisized addressing chunks. However, the equisized address blocks sometimes prove to be a bottleneck, as the subnet is generally determined by the size of the biggest chunk, thereby wasting address space in the smaller subnetworks.

The subnet masking will be inefficient when a network is divided into two or more parts with a huge variation in the number of host computers in the two networks. This can be explained with an example of a network with, say, 200 nodes that can be easily addressed by class C addressing. Now, if this network is to be divided into five subnetworks accommodating 6, 14, 30, 50, and 100 nodes each, it requires 3 bits in the subnet for the creation of five subnets. Now, with 5 bits left for the host ID, it will not be enough to address the nodes in the networks with 50 and 100 hosts, even though the addresses

will be unused in the subnets with 6, 14, and 30 nodes. Using the conventional classful method, this would be resolved by taking one more block of class C address and dividing it into only two subnets, each accommodating 100 and 50 nodes respectively. This would effectively mean using an address space of 255 + 255, i.e. 510 nodes to address 200 nodes. The reason for the wastage is that subnetting creates only equisized subnetworks. Variable-length subnet masking [7] enables the creation of subnetworks of varying size. This is achieved by splitting a subnet further into smaller subnets, which can further be split into even smaller subnets until a subnet of an appropriate size is achieved. Thus, to accommodate 200 nodes in the example above, a class C address space (/24 network) will be split into subnetworks accommodating 126 hosts (/25 network), 62 hosts (/26 network), 30 hosts (/27 network), 14 hosts (/28 network), and six hosts (/29 network).

IPv6. IPv4 has an address space of 2^{32}, i.e. 4.29 billion, and every node on the Internet has to be given a unique address to enable its communication with others. Network address translation (NAT) is a technique to map a public IP with a number of private IPs, thus reducing the requirement of the number of unique IP addresses over the Internet. Still, as reported by the Asia-Pacific Network Information Center (APNIC) [11], 'the primary supply of unallocated IPv4 addresses was exhausted' by the Internet Assigned Numbers Authority (IANA) in February 2011. To cope with the shortage of IPv4 address space envisaged by IETF, it introduced IPv6 as the new protocol for Internet communication.

The protocol has an address length of 128 bits and has enhanced features of security, mobility, QoS, end-to-end connectivity, scalability, and autoconfiguration over IPv4. IPv6 has provided expansion of the available network addresses, and it has catered for the various demands of technological enhancements of IPv4, which has been in use for more than two decades. This is one of the reasons for NAT not being able to handle the address space problem and magnify the requirement of IPv6. As the existing networks are on IPv4, and the upcoming networks would be using IPv6, compatibility among IPv4 and IPv6 networks would be achieved using dual-stack translation or tunneling.

IPv6 is 128 bits (16 bytes) long and hence can address 2^{128} nodes. The address is represented as b_1:b_2:b_3:b_4:b_5:b_6:b_7:b_8, where b_i is a 16 bit binary number represented in hexadecimal form and thus requires only four digits. For example, 2012:0000:0000:9876:0000:0000:0000:9ABC:1234 is an IPv6 address. Some of the addressing rules [12,13] in IPv6 are as follows:

- Leading zeros in the address are optional
  2012:0000:0000:0076:0000:0000:0000:9ABC:1234
  →2012:0:0:076:0:0:0:9ABC:1234
- The address is case insensitive
  2012:0000:0000:0076:0000:0000:0000:9ABC:1234
  →2012:0000:0000:0076:0000:0000:0000:9abc:1234
- Once in an address, fields with successive 0 s can be represented as "::"
  2012:0000:0000:0076:0000:0000:0000:9ABC:1234
  →2012:0:0:076:0:0:0:9ABC:1234
  →2012:0:0:076::9ABC:1234
- In an URL, it is enclosed in a bracket
  http://[2012:0:0:076::9ABC:1234]:8080/index.html
- It should use a fully qualified domain name (FQDN)

In IPv6 address structuring, Internet service providers (ISPs) are assigned a /32 IPv6 address, customer sites are assigned a /48 address, /64 is used for subnets, and /128 is used for devices. Unlike IPv4, which had a unicast and broadcast address, IPv6 supports unicast, multicast, and anycast (one-to-one-to-one-…, leading to many by delivery to the nearest).

1.5 Overview of Routing

The routing calculates a route between the source and destination node so as to enable proficient utilization of the intermediate network connecting the source and destination. The parameters for proficiency vary with the algorithm used for routing and may be associated with the bandwidth utilization, the time delay, the number of hops across the intermediate routers in the network, the congestion in the network, or a combination of these. The simplest performance criterion to evaluate the proficiency of the routing algorithm is the hop count, which gives an idea of the number of intermediate links traversed by the packet. The overhead associated with counting the hop is also less, as each intermediate node has to change the hop counter by 1 and does not involve any detailed calculations, leading to minimum processing time and minimum resource consumption. However, hop count is an effective performance criterion if the links are similar in terms of bandwidth. The number of hops determines the 'cost' of the route and the routing algorithm attempts to achieve the minimum-cost route. If the links are of different bandwidth, the least hop count may not be the most efficient performance criterion as it may not give the least time delay path between the source and the destination. So, to improve the routing efficiency of the algorithm, the cost may depend on other parameters and may be directly or inversely proportional to the parameter. The routing algorithms are designed on the least-cost approach, and the costing parameters vary with the algorithm or the network parameters. The cost parameters may either be predefined in the algorithm or may be defined at the time of configuring the routing algorithm in the network to make it suite the network environment and parameters.

The routing decisions can be differentiated on the basis of the time when the decision is taken and the place where the decision is taken. The routing decision can be taken before initiation of the actual data transfer between the nodes or during the actual data transfer. In the case of a datagram network where packet switching takes place, the routing decision is taken throughout the path in which the packet is in transit, as each node decides on the next-hop node. In contrast to this, in virtual-circuit-based networks the virtual circuit is established before data transmission, and hence the entire path through which the data packets will traverse is decided at the time of establishment of the virtual circuit. Thus, in the case of packet switching networks, the routing decisions are taken throughout the duration when the packet is in transit, while in virtual-circuit-based networks, the routing decision is taken before the transmission of the packet. However, in advanced routing methodologies, a virtual circuit may be established before the transmission of the packets, but the virtual circuit may reconfigure itself during the process of data transmission. The reconfiguration of the virtual path depends on link congestion, link failure, or the introduction of new and better links. So, in such routing decisions, the time of decision is prior to as well as during the network transmission.

The 'decision place' of routing is a variable that tells the location of decision-making for routing a packet. The most commonly used, but relatively complex, strategy is *distributed decision-making*, where each intermediate node decides on the next link to which the packet should be forwarded. Each decision-making node should have complete or partial information about the network. The failure of a few intermediate nodes does not drastically affect the performance of the network, as the packet is forwarded through some alternative route. An alternative to this is the *centralized routing decision*, in which there is a centralized control node that takes all routing decisions. The control node has a view of the entire network topology and controls the routing of the packet through the network. The drawback of such a routing design is failure of the network routing in the case of failure of the control node. The control node is computationally overloaded, as it has to administer the entire network and may become a computational bottleneck for the network, and also leads to congestion of the links connecting the control node. A minor design improvement can be achieved by designating a few nodes as the network controllers instead of a central node.

The third policy of routing based on place of decision is *source routing*. In source routing the path of packet forwarding is decided by the source node and intimated to the network for data delivery. This routing strategy helps in deciding the route by the source on the basis of the parameters that the source may feel to be significant for that data delivery.

1.6 Delivery, Forwarding, Routing, and Switching

Delivery [4] refers to the handling of a packet under the supervision of the network layer to ensure it reaches the destination. The delivery of the packet is elaborated under two different concepts – connection type and the method of delivery. The connection types are handled by the data link layer in terms of two different types of switching – packet switching and circuit switching. The methods of delivery are direct delivery and indirect delivery.

Direct delivery can be achieved when two nodes are connected point-to-point on the same physical network and the packet can reach from the source to the destination in a single hop without any routers in-between. If the source and destination are connected through a wide area network and there are a number of routers in the path between the source and destination, leading to a multihop delivery, the last hop in which the packet is transmitted from the last/peripheral router to the destination is also known as direct delivery. The source node, looking at the network address of the destination, can determine before data transmission whether the packet will reach the destination by direct delivery, because if they have the same network address it will be sent using direct delivery.

When the source and the destination nodes are not on the same network, the packet has to pass through one or more routers in-between. The method of delivery from the source node to the router or between two intermediate routers is known as indirect delivery. Thus, a delivery will always involve at least one direct delivery and zero or more indirect deliveries, which is explained in Figure 1.6.

A message to be transmitted over the network is broken down into packets. Each packet contains some user data and the packet header, which has the control information such as source address and destination address. Each switch follows a

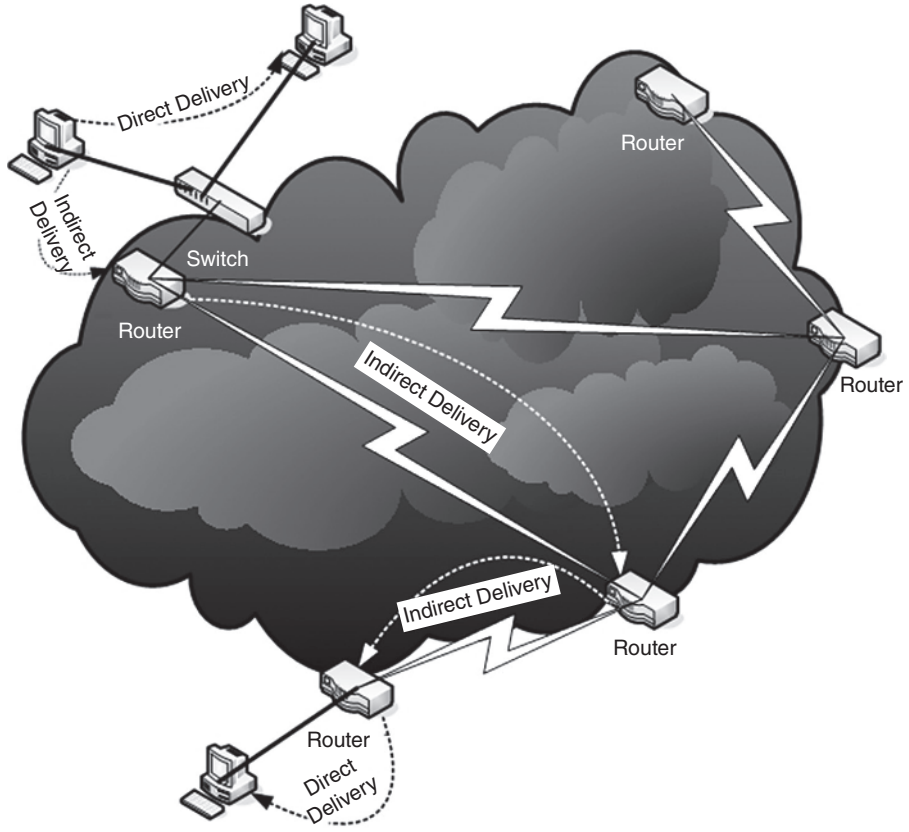

Figure 1.6 Methods of delivery.

store-and-forward technique, where it initially receives the packet which it may store in its buffer and then pass to the next network node. According to the type of switching, the network can be classified into two categories – the packet switching network and the circuit switching network.

A packet switching network is also known as the datagram approach, where each packet is treated independently. For each packet, the route through which it will travel in the network is decided independently and is not dependent on the preceding or the succeeding packet. Each packet can follow a different network route. Thus, the packets may become out of transmission order, and to reassemble the packet in proper sequence, a sequence number is used in the packet header as control information. In contrast to packet switching, in circuit switching a virtual circuit is established between the source and the destination before the exchange of data. As all the packets are transmitted over this virtual circuit, they reach the destination in the same sequence in which they were transmitted. Circuit switching does not require routing decisions for the packets, and thus it is fast. However, it takes time to establish a circuit, and once a circuit has been established between the source and the destination, the packets cannot take an alternative route if the channel is congested or fails, and no other packet meant for some other destination can be transmitted using the virtual circuit even if the circuit in underutilized.

Forwarding [4] is the process of determining the next hop for a packet in a network and placing it in the appropriate link for further transmission and delivery. Forwarding is done with the help of a routing table. The source node as well as all the intermediate routers perform the task of forwarding. The node consults the routing table before taking a decision concerning the link through which it should be forwarded. However, with an increasing number of nodes in the network and the Internet, a routing table cannot have entries of all the network nodes, and thus the routing table cannot be used for direct mapping of the address of the destination node and the related forwarding path. To cater for this requirement, various techniques are used to support forwarding with a minimal size of the routing table.

It is generally believed that a routing table should contain the entire route, i.e. details of all the intermediate nodes through which a packet should be forwarded to reach any destination from the forwarding node. This requires entry of all the host computers and routers in the routing table, along with the exact path that should be followed to reach the destination node from the node referring to its routing table. In the next hop method, the routing table maintains the information only about the next hop instead of the entire route through which the packet should be forwarded in order to enable the data to reach its destination network. In the network-specific method, the routing table contains route information for the networks and not for specific hosts. Thus, to forward a packet, the network ID of the destination is retrieved from the destination IP, and that network ID is searched in the routing table for a match to determine the next hop to which the packet should be forwarded.

The default forwarding method is used to forward the packets to a default link when the router is aware that the destination cannot be reached through any of its other available links. The default route is used for all those packets for which the related entries cannot be found in the routing table, and the default route link is connected to a much larger network, which may help in determining the exact path to the destination.

Routing aims to find the minimum cost path within the network so as to efficiently transmit data packets from the source node to the destination node. The parameters for cost and efficiency vary with the type of routing algorithm used. The cost and efficiency may be measured in terms of time taken in the transition, number of intermediate routers used (hops), time taken by the router to decide the next hop, time taken by the router to build the routing table on booting and rebuild the same in case of change of network topology.

1.7 Routing Taxonomy

Routing algorithms can be classified on the basis of two different criteria:

1) Global information vs decentralized information with the routing nodes.
2) Static information vs dynamic information in routing tables.

Algorithms that possess global information are aware of the topology of the entire network and the associated link costs. The routing node has information about all the links and the neighbors connected to the routing node. It also has information about all other nodes that are available in the network and indirectly connected to this routing node through one or more intermediate routers. It may also possess information about

nodes that were once connected to the network but may not be available in the network presently. Algorithms with decentralized information have partial information about the network. They possess information about themselves and all their neighbors to which they are directly connected, along with associated link cost.

Algorithms with static information are those in which the routing table once created in the routing node is rarely changed. Algorithms with static information are suitable for those networks in which the topology does not change frequently, links are reliable, and the type of links between all the nodes is known. Static algorithms require less computational power at the routing nodes, as they do not require calculation of the network topology or frequent building of the routing table. They simply have to look up the static routing table for a suitable entry and forward the packet to the appropriate link. It is easy to implement static routing in small networks, but difficult in huge networks. However, once a static routing table has been built for a network, small or big, static routing is faster than dynamic routing.

Dynamic routing is more suitable for networks in which there are links and nodes that often fail and where frequent rebuilding of the routes is required for successful transmission of the packets from source to destination or between two routing nodes. In algorithms with dynamic information, the nodes regularly share with their neighbors information about all the links connected to them. By accumulating all such information, a routing node can have a fair idea about the entire network. In the case of a link or node failure, all nodes become aware of it from updates received directly or indirectly from neighbors concerning failed nodes. Algorithms with dynamic information have to rebuild the routing table if they receive from a neighbor an update that is different from its previous update.

Thus, in the case of a huge network, with links frequently going up and down, the dynamic algorithm may keep the routing node computationally busy. However, as this algorithm has updated information about the network topology, it can avoid transmitting packets on routes with congested or failed links.

The routing algorithms can also be classified into the following categories:

a) adaptive routing,
b) non-adaptive routing,
c) multipath routing,
d) hierarchical routing.

a. Adaptive routing. Adaptive routing algorithms are dynamic in nature and they recalculate the routing tables whenever there is a change in network topology in terms of available links and variation in link costs. The routing node may receive information about topological changes either from its neighbors or from any other routing node connected to the network. An adaptive routing algorithm can be centralized, isolated, or distributed.

In a centralized mode of operation, there can be one or more centralized nodes in the network that get information from all the routing nodes about their link states, link condition, and cost. Based on this input, the centralized node updates a routing table. The routing table either may be shared by the centralized node with all other routing nodes or the routing nodes may refer to the centralized node to make routing decisions without getting a copy of the routing table. The advantage of centralized adaptive routing is that

there is only a central node that has to do all the computation related to routing. As all the nodes transmit their routing table with neighbor information only to a centralized node instead of flooding the network to send it to all other nodes, the network traffic is reduced. However, in the case of failure of the central node, the entire network is down.

An isolated routing algorithm does not require the routing nodes to share any information with other nodes. Every routing node takes a forwarding decision either based on the condition of its links or based on the information about the network it collects from the incoming packets using backward learning. The decision to forward a packet to a particular link may be based on the fact that the packet is forwarded to the link with the highest bandwidth, lowest congestion, or minimum queue length. Alternatively, in backward learning, the routing node uses backward learning on the incoming packets to gain an insight into the path followed by it, rebuilding the information about the available routing nodes in the network and the number of hops those routing nodes are away from this routing node. The routing node keeps updating this information based on the information retrieved from each incoming packet.

The distributed adaptive routing algorithm is the most commonly used routing technique, where every node receives information from its neighbors about the links connected to them. Based on this information, the routing node updates its routing table. Route table updates are exchanged between neighbors either in the case of change in the state of any of its links or at a regular frequency. The advantage of the algorithm is that it can take an optimized routing decision; its disadvantage is that the algorithm is computationally expensive and generates network traffic for exchange of routing tables.

b. Non-adaptive routing. Non-adaptive routing algorithms are static routing algorithms that do not calculate the route based on any of the changing characteristics of the network or traffic patterns such as link failures and congestion. The simplest implementation of the algorithm is by 'flooding'. A routing node receiving a packet on any of its links forwards it to all other links. Flooding may lead to packets going in infinite loops in the network, leading to congestion. Looping of the packets is avoided by using a sequence number, hop count, or spanning tree. A packet is assigned a unique sequence number by the source.

Each intermediate node maintains a list of source ID and the sequence number of all the packets forwarded by it. When the routing node receives a packet, it checks the source ID and sequence number from its list of forwarded packets and drops the packet if it has already forwarded it before. In the hop count method, the packet may be assigned an optimum hop count based on the number of hops required by the packet to travel from source to destination, which may be separated by the maximum number of hops. The hop count assigned to the packet by the source node is reduced by 1 by every routing node from which the packet is forwarded. If the hop count becomes 0, the packet is dropped. A spanning tree can be used in non-adaptive routing if the intermediate nodes between source and destination are aware of the entire network topology. This helps to create a spanning tree from source to destination without loops. Instead of flooding, the algorithm may forward the packet 'randomly' to any of its links except the one from which it received the packet. The outgoing link may also be selected on the basis of certain criteria, such as the link with the maximum available bandwidth or minimum queue length.

c. Multipath routing. There may be more than one route between the source and the destination. All the routes may be of equal cost or with variation in cost. In case of cost

variation, each route between a source–destination pair is assigned a weight based on its relative cost. The routing table maintains information not only on a single route between the source and the destination but also on a number of other routes with equal cost or with varying costs, along with the associated weight. A path is selected based on a random number generator, which uses the weights of the routes as probabilities. The routing table with weights assigned to the alternative routes is generally static and computed manually.

d. Hierarchical routing. Hierarchal routing is best suited for networks with a tree topology. Although it can be used for wired networks, this is a common routing algorithm used in wireless sensor networks and mobile networks where a cluster of nodes elect a cluster head and this cluster head in turn communicates with the upper level. Thus, in hierarchical routing, the network is divided into hierarchical clusters. The information can be transmitted only through the intermediate cluster heads enabling a node to transmit and receive from a node just one level above or below it in the hierarchy.

1.8 Host Mobility and Routing

Host mobility has become an area of research and technological development to support wireless and mobile networking. The host may not only change its location between two consecutive communication sessions but also change its location during an established session involving transfer of data. The host mobility approaches have to consider factors such as scalability, hand-off, rate of movement, computational requirements, traffic generation, connection blackouts, and byzantine failures. There are a number of protocols that support host mobility. Mobile IP, I-TCP, end-to-end solution, and cellular IP are some of the protocols that handle host mobility.

Mobile IP keeps the mobility of the source and the receiver transparent with minimum overhead. The host is assigned a permanent IP address known as the home address, and this IP is known to the home agent of the host. The home agent is deployed in the home network of the mobile host, and all the data packets meant for the mobile host are sent through its home agent. When the mobile agent changes its network, it gets a new temporary IP from the foreign agent after the mobile host has performed agent discovery for the foreign host. The foreign agent resides in the network to which the mobile host has currently shifted. The address assigned by the foreign agent to the mobile host is known as the care-of-address. The foreign agent then updates the home agent of the mobile host about its presence in the foreign network. Thus, the home agent is able to keep a record of the location of the mobile agent. When a packet reaches the home agent for delivery to the mobile host, the home agent forwards it to the mobile node using the care-of-address. The forwarding to care-of-address is done by encapsulating the packet with a new IP header, which is the care-of-address of the mobile host. As the mobile host keeps moving, changing its locations, it discovers new foreign agents and gets a new care-of-address, and the home agent is kept updated about its latest location, which it duly acknowledges to the mobile host through its foreign agent.

In indirect TCP (I-TCP), an intermediate mobile support router (MSR) is used to support the communication between the mobile host and the fixed host. I-TCP divides the communication between the mobile and the fixed host into two parts, the first between the mobile host on the mobile network and the second between the MSR and

the fixed host in the wired network. Thus, the problem related to host mobility and routing in a wireless network is confined only to one part of the network, and the other part uses fast and reliable connectivity with the TCP/IP network. I-TCP uses a variant of the mobile IP in the wireless network for communication between the mobile host and MSR. As the mobile agent moves, its MSR is changed. MSRs coordinate with each other to hand over the mobile host among themselves. They also keep the mobility of the mobile host transparent to the fixed host.

The end-to-end host mobility [14] approach does not provide transparency to the mobility, unlike mobile IP and I-TCP. The approach uses the Domain Name System (DNS) to update the new IP address of the mobile host as it leaves its home network and enters a foreign network, acquiring a new address. As the mobile node keeps changing its location, it keeps the DNS updated of its latest IP address. The migration from one network to another when a connection is already established and with data transfer in progress is supported by a new migrate TCP option by changing the method of handling sync packets.

Cellular IP uses a combination of the technology of mobile IP and cellular communication. Mobile IP is used for transmission of data packets to the mobile host. However, unlike mobile IP, the foreign agent from the care-of-address of the mobile host does not directly send the data packet to the home network of the mobile agent. The foreign agent sends the packet to its base station using a wireless access network. The foreign agent's base station then forwards it to the base station of the mobile host's home network. The base stations have the routing information for path determination. The mobility of the node from the cellular area of one base station to another base station is supported by the hand-off between the base stations.

For routing, mobile IP, I-TCP, and cellular IP use intermediate devices, namely foreign/home agents, MSRs, and base stations respectively. This leads to a delay in the routing and failure of the mobile hosts to communicate with each other in the region in the case of failure of the intermediate device. Two mobile nodes in close proximity cannot communicate directly and have to use the services of an intermediate device, which may be placed far away. There are improvements in all the protocols to overcome the drawbacks. In mobile IP, the sender is also informed of the care-of-address of the mobile host so that it can directly communicate with the mobile host. The packet is sent to the home agent only if the sender does not have the latest care-of-address of the mobile host. The end-to-end host mobility supports direct communication between the source and the destination. A separate mobile routing algorithm is not required for the same, as the sender looks for the latest address of the destination in the DNS and establishes a connection with the mobile host. As the connectivity is point-to-point, it is secured and fast. The method requires optimization only when the mobile host has just moved and the source has received its old IP address from the DNS before it could be updated with the new one.

References

1 W. Stallings. *Data and Computer Communications*. Prentice Hall of India Publication, 8th edition, 2007.

2 W. Odom. *Computer Networking First Step*. Cisco Press, 2004.

3 T. Lammle. *Cisco Certified Network Associate Study Guide*. BPB Publishers, 4th edition, 2003.
4 B. A. Forouzan. *Data Communications and Networking*. McGraw-Hill Publication, 4th edition, 2006.
5 Description of system area networks, Microsoft. http://support.microsoft.com/kb/260176.
6 Network architecture standard. http://www.servicecatalog.dts.ca.gov/docs/3117_Network_Architecture_Standard.pdf.
7 C. M. Kozierok. *TCP/IP Guide, Volume 3.0*. No Starch Press, 2005.
8 IEEE 802.11. http://standards.ieee.org/about/get/802/802.11.html.
9 C. Hunt. *TCP/IP Network Administration*. O'Reilly & Associates, Inc., 2nd edition, 1998.
10 Internet Protocol, RFC 791. http://www.ietf.org/rfc/rfc791.txt, September 1981.
11 Asia Pacific Network Information Center (APNIC). http://labs.apnic.net/blabs/.
12 S. Deering and R. Hinden. Internet Protocol, version 6 (IPv6) specification, RFC 1883. https://tools.ietf.org/html/rfc1883, 1995.
13 S. Deering and R. Hinden. Internet Protocol, version 6 (IPv6) specification, RFC 2460. https://tools.ietf.org/html/rfc2460, 1998.
14 A. C. Snoeren and H. Balakrishnan. An end-to-end approach to host mobility. 6th ACM MOBICOM, 2000.

Abbreviations/Terminologies

ANSI	American National Standards Institute
APNIC	Asia-Pacific Network Information Center
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
ATM	Asynchronous Transfer Mode
ATMP	Ascend Tunnel Management Protocol
BAN	Body Area Network
BGMP	Border Gateway Multicast Protocol
CAN	Campus Area Network
CIDR	Classless Interdomain Routing
COPS	Common Open Policy Service
DIS	Distributed Interactive Simulation
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
DQDB	Distributed Queue Dual Bus
DVMRP	Distance Vector Multicast Routing Protocol
EGP	Exterior Gateway Protocol
EIA	Electronic Industries Alliance
EIGRP	Enhanced Interior Gateway Routing Protocol
ETSI	European Telecommunications Standards Institute
FANP	Flow Attribute Notification Protocol
FDDI	Fiber Distributed Data Interface

FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HAN	Home Area Network
HSRP	Hot Standby Router Protocol
HTTP	Hypertext Transfer Protocol
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IMAP	Internet Message Access Protocol
IPDC	Internet Protocol Device Control
IPsec	Internet Protocol security
IPX	Internetwork Packet Exchange
IRC	Internet Relay Chat
IRTF	Internet Research Task Force
IRSG	Internet Research Steering Group
ISAKMP	Internet Security Association and Key Management Protocol
ISCSI	Internet Small Computer Systems Interface
ISO	International Organization for Standardization
ISOC	Internet Society
ISP	Internet Service Provider
ISTP	Internet Signaling Transport Protocol
I-TCP	Indirect TCP
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MAN	Metropolitan Area Network
MARS	Multicast Address Resolution Server
MPLS	Multiprotocol Label Switching
MSR	Mobile Support Router
MTBF	Mean Time Between Failures
MTU	Maximum Transmission Unit
MZAP	Multicast-Scope Zone Announcement Protocol
NAN	Near-me Network
NARP	NBMA Address Resolution Protocol
NAT	Network Address Translation
NFN	Near Field Network
NHRP	Next Hop Resolution Protocol
NTP	Network Time Protocol

OFDM	Orthogonal Frequency-Division Multiplexing
OSI	Open System Interconnection
OSPF	Open Shortest Path First
OTN	Optical Transport Network
PAN	Personal Area Network
PIM	Protocol Independent Multicast
POP	Post Office Protocol
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RIP	Routing Information Protocol
RSVP	Resource Reservation Protocol
RTSP	Real-Time Streaming Protocol
RUDP	Reliable User Datagram Protocol
SAN	Storage Area Network
SCTP	Stream Control Transmission Protocol
SLP	Service Location Protocol
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SyAN	System Area Network
TALI	Transport Adapter Layer Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
TGRP	Trunk Group Routing Protocol
TIA	Telecommunications Industry Association
TTL	Time To Live
UDP	User Datagram Protocol
VLAN	Virtual LAN
VLSM	Variable-Length Subnet Mask
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WCCP	Web Cache Communication Protocol
XOT	X.25 over TCP

Questions

1 Why are standards required for networking? What were the difficulties being faced with proprietary products and protocols?

2 State the difference between reliability and availability.

3 Name and then draw at least four network topologies that can be created from the basic network topologies, i.e. star, bus, ring, and mesh. Also mention the advantages and disadvantages of the network topologies drawn.

4 Explain the requirement of network address translation in IPv4.

5 What problems are faced in using a static routing algorithm for huge and scaling networks with regular link failures?

6 What are the disadvantages of a distributed routing algorithm compared with centralized routing?

7 How does a three-tier architecture with a demilitarized zone at the first layer enhance the security of the data and application?

8 Study from the Internet about the special and new types of network, such as the near field network (NFC), Internalnet, near-me network (NAN), home area network (HAN), and interplanetary Internet. Mention the basic features in terms of bandwidth, distance covered, and application of each of these.

9 Explain the following:
- **A** personal area network,
- **B** client–server architecture,
- **C** ISO OSI network layer,
- **D** classless interdomain routing,
- **E** variable-length subnet mask.

10 Differentiate between the following:
- **A** storage area network and system area network,
- **B** ISO OSI presentation layer and session layer,
- **C** routing protocols and routed protocols,
- **D** IPv4 and IPv6,
- **E** direct delivery and indirect delivery.

11 State whetherthe following statements are true or false and give reasons for the answer:
- **A** Mobile IP, I-TCP, end-to-end solution, and cellular IP are the protocols that support host mobility.
- **B** The end-to-end host mobility approach uses the care-of-address.
- **C** In multipath routing, the various routes between the source and the destination may be of different cost.
- **D** Static routing uses flooding to get information about the network nodes and the link status.
- **E** SNMP is an ISO OSI layer 4 protocol.
- **F** IEEE 802.15 defines standards for wireless personal area networks.
- **G** TCP/IP is known as the 'DoD model' as well as the 'public networking model'.
- **H** Non-adaptive routing algorithms calculate the route based on the changing characteristics of the network or traffic pattern.
- **I** 10.192.172.13 is a class A address.

Exercises

1 Assume a simple network with three nodes: A, B, and C. A is connected to B, B is connected to C, and C is connected to A. Node A has to transfer 800 GB of data to node B, and node B has to send 1 TB of data to node A [B = bytes, b = bits, K = kilo (1000), M = mega (1000 000), G = giga (1000 000 000)].
   - **i** Assume that the network between node A and node B is on fiber (separate channels for transmit and receive) and has a full duplex communication capability, where node A can communicate with node B at an effective bandwidth (after removing bandwidth utilization for overhead processing) of 0.8 Gb/s, and at the same time node B can communicate with node A at 0.8 Gb/s. How much time will be required to transfer the total data between the two nodes.
   - **ii** Now assume that the network between node A and node B is on copper wire with an effective bandwidth of 0.8 Gb/s and the transmission can only be one way at a time, with negligible time for switchover from one direction to the other direction of transmission. How much time will now be required to transfer the total data between the two nodes?
   - **iii** What is the time required for the transmission over the copper wire if transmission of only 50 GB is permissible towards one direction and then the transmission starts in the other direction if some data is waiting in the other direction to be transmitted. The time required for pre-emption and processing for change in direction is 2 ms.
   - **iv** What will be the total time required if the network allows only a simplex mode of communication from node A to node B and from node B to node C and from node C to node A. Node C has a processing time of 10 μs for receiving and forwarding each GB of data.

2 Hashing/checksum is a technique that can be used to check any change in values in a file. Consider a text file having a few hundred characters in it. Write a function to generate a hash value/checksum of blocks of 100 characters and insert the values just after each block or in a separate file. Also write a function to validate using the hash value/checksum if any character in the document has been changed. Can the exact location also be detected where the character has been changed?

3 A network router 'Alpha' had been operating for 1 year. During the year it failed only once, and it took just 1 day to repair and put back into operation. Another network router 'Bravo', which is installed in the shaft of the building, gets switched off once every weekend owing to removal of power cables caused by movement of rats. It takes 5 min to detect the failure through NMS and make it operational again by plugging in the power cable. Which network router has more availability and by how much percentage?

4 An organization has bought 50 network switches and it is open to implement any type of network topology for connecting these switches. Before selection of the topology, it wants to see the requirement of cables and connectors for each topology only in terms of numbers and irrespective of the type of cable or connecter. Calculate the number of cable and connectors required if the 50 network switches are connected in:

i bus,
ii single star with a separate core-switch in the center,
iii ring,
iv complete mesh,
v partial mesh where each switch is connected to two other switches,
vi binary tree.

If the number of nodes is denoted by n, can any formula be derived in terms of n to calculate the number of cables or connectors for the different topologies?

5 The railway station of a big city has an area of 500 m × 500 m. Wireless network accessibility has to be provided throughout the station. One wireless router has a range of 100 m.

i A minimum of how many routers will be required to cover the entire area of the station under wireless communication so that no area is left without wireless signal coverage?
ii If it is told that there should be no area with overlapping signals from two different wireless routers, even if certain areas in the station are left without the wireless signals, what is the maximum number of routers that can be deployed and what is the minimum percentage area of the station that will exist without a network signal?

6 A network has to be set up in a building. There are ten floors in the building, each floor has an area of 30 m × 20 m, and there will be 20 computers installed across each floor. Design the network architecture for the building along with the subnet masking scheme. The designed network will fall under which topology? What changes will have to be incorporated in the network and the subnet mask scheme if the number of computers in each floor has to be scaled up to 150?

7 Router 'Alpha' is connected to router 'Bravo' through router 'Charlie', 'Delta', and 'Echo' in-between. There are 20 hosts connected to router 'Alpha' and 15 computers connected to router 'Bravo'. Each of the 35 hosts sends one data packet to two other hosts in the same network and to any two hosts connected to the other network. What will be the total number of direct delivery hops and indirect delivery hops during this complete process of data transfer.

8 A travel agency has one office in the capital cities of 15 different countries. Each city office has seven computers. Design the network for the travel agency. What should be the preferred IP addresses for the computers on the LAN? What subnet mask should be preferred over the LAN and over the WAN? Which type of routing would be most preferred in this network?

9 The backup of SAN has to be taken from the data center to the disaster recovery data center, which are connected to each other on a 2 Mb/s link. The SAN has 35 Tb of data stored in it. Assume that 15% of the bandwidth is consumed for overheads, headers, and call set-up, and only 85% of the channel capacity can be used for actual data transmission. How much time will it take to take the backup of the SAN? What will be the reduction in time if the bandwidth is increased to 34 Mb/s or to 155 Mb/s?

10 Your organizational network was established a few years back. The network has catered for the expansion of the organization over the past few years by enhancing the capacity with additional network devices and is now not further scalable owing to difficulties in managing the infrastructure and lower bandwidth. Better security solutions also cannot be implemented over the network as it lacks proper design after the expansion. Design a new network for your organization to provide connectivity to all the existing devices and with a scalability of 25%. What is the topology of this newly designed network? Explain the subnetting that is being planned for the network and the type of routing that will be most suitable for this network?