LECTURE NOTES ON COMPUTER NETWORKS (CSC 403)

1. OVERVIEW OF COMPUTER NETWORKS

A computer network is a system that connects two or more computing devices for transmitting and sharing information. The computing devices include everything from a mobile phone to a server. These devices are connected with physical cables or by wireless. The first working network, ARPANET, created in the 1960s was used to share information among government researchers but the computers were large and difficult to move. Today, the Internet is a network of networks that connects billions of devices worldwide. Organizations can now setup up networks to connect employees via their devices and share resources such as printers both locally and over the internet. Teams are now able to collaborate using cloud-based platforms such as Google Drive to share documents with colleagues and work remotely. Every form of interaction where people make voice/video calls, stream movies, share files, chat with instant messages, or browse the internet all shows that the computer network is at work.

1.1. Network Devices

A network device is a piece of hardware or software integral to communication between a computer and an internet network. Network devices play two roles. The first is establishing a network connection, as a router or a modem does. The second one is maintaining, protecting and enhancing that connection, as with a hub, repeater, switch or gateway. Many types of network devices go into creating a network. Some are necessary for connections, while others are enhancers. Below is a list of network devices that can play a role in enabling your organization to transfer information as securely as possible:

(i) Switches:

A network switch connects devices within a network (often a local area network) and forwards data packets to and from those devices. Unlike a router, a switch only sends data to the single device it is intended for (which may be another switch, a router, or a user's computer), not to networks of multiple devices. Switches forward data based on the destination MAC address or the IP address.

(ii) Bridges

A network bridge is a device that divides a network into segments. Each segment represents a separate collision domain, so the number of collisions on the network is reduced. Also, because each collision domain has its own separate bandwidth, a bridge also improves the overall network performance. A bridge works at the Data link layer (Layer 2) of the OSI model, just like a switch does. It inspects incoming traffic and decides whether to forward it or filter it. Each incoming Ethernet frame is inspected for the destination MAC address. If the bridge determines that the destination host is on another segment of the network, it forwards the frame to that segment.

(iii) Routers

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. It is known as an intelligent device as it can calculate the best route to pass the network packets from the source to the destination automatically.

(iv) Firewalls

A firewall restricts the internet traffic of a private network, controlling what goes in and out. They analyze and restrict data packets based on programmed parameters, either whitelists or blacklists. Whitelists only allow information that falls within a certain set of parameters, while blacklists deny all information that falls inside the parameters. Firewalls are essential for private networks, especially those operating with sensitive information. They are also used within internal networks to block access between subgroups, such as a sales department being denied access to files pertaining to IT or HR.

(v) Repeaters

A repeater is an electronic device that works at the physical layer of the OSI model to amplify a received signal. It receives a signal and retransmits it at a higher level or higher power. As a result, the signal covers longer distances, sometimes more than 100 meters for standard LAN cables. Repeaters are useful for anyone working in a large facility where the Wi-Fi might be spotty in the outer reaches of the space. Large office buildings, warehouses, laboratories and campuses are all locations that can benefit from repeaters.

(vi) Gateways

Gateways connect networks operating on different protocols so data can transfer between destinations. These devices normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors, and gateways help deal with them. Gateways translate between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). Because of this, gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies. They perform all of the functions of routers and more. In fact, a router with added translation functionality is a gateway.

(vii) Hubs

Hubs connect multiple computer networking devices, working only on the Physical layer of the OSI. Hubs do not perform packet filtering or addressing functions. Instead, they send data packets to all connected devices. A hub also acts as a repeater, amplifying signals that deteriorate after traveling long distances over connecting cables. A hub is the most straightforward network connecting device because it connects LAN components with identical protocols. A hub can be used with digital and analog data, provided its settings are configured to prepare for the formatting of the incoming data. For example, if the incoming data is in digital format, the hub must pass it on as packets. But if the incoming data is analog, it passes it on in signal form.

(viii) Modems

A modem (modulator-demodulator) converts digital signals into analog signals of different frequencies and transmits them to a modem at the receiving location. The receiving modem performs the reverse transformation and provides a digital output to a device connected to a modem, usually a computer. The digital data is usually transferred to or from the modem over a serial line through an industry-standard interface, RS-232.

(ix) Network interface cards (NICs)

A network interface card is an internal hardware chip that connects a device to the internet. At the TCP/IP layer, the NIC connects a device to a network. At the physical layer, the NIC transmits a signal that sends information to the network layer. Then all data passes through the NIC to the server and back to the device. There are two main types of NICs: Ethernet NIC and Wi-Fi NIC. An Ethernet NIC comes with an 8P8C socket for connecting an ethernet cable. A Wi-Fi NIC connects to a wireless network. Mobile devices have only a wireless NIC, but most computers still incorporate an Ethernet chip. Ethernet ports are more reliable but limit a user’s mobility while handling the device.

(x) Wireless access points (WAPs)

A wireless access point consists of a transceiver (transmitter and receiver) device used to create a wireless LAN (WLAN). WAPs are separate network devices with a built-in antenna, transmitter and adapter. WAPs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired ethernet LAN. They also have several ports, allowing you to expand the network to support additional clients. Depending on the size of the network, one or more WAPs might be required to provide full coverage. Additional WAPs allow access to more wireless clients and expand the wireless network range. Each WAP is limited by its transmission range — the distance a client can be from an WAP and still obtain a reasonable signal and data process speed. The distance depends on the wireless standard, the obstructions and the environmental conditions between the client and the WAP. Higher-end WAPs have high-powered antennas, enabling them to extend how far the wireless signal can travel.

1.2 Types of Computer Networks

Computer networks can be classified based on several criteria, such as the transmission medium, the network size, the topology, and organizational intent. Based on a geographical scale, the different types of networks are:

1. **Nanoscale networks**: These networks enable communication between minuscule sensors and actuators.
2. **Personal area network (PAN)**: PAN refers to a network used by just one person to connect multiple devices, such as laptops to scanners, etc.
3. **Local area network (LAN)**: The local area network connects devices within a limited geographical area, such as schools, hospitals, or office buildings.
4. **Storage area network (SAN)**: SAN is a dedicated network that facilitates block-level data storage. This is used in storage devices such as disk arrays and tape libraries.
5. **Campus area network (CAN)**: Campus area networks are a collection of interconnected LANs. They are used by larger entities such as universities and governments.
6. **Metropolitan area network (MAN)**: MAN is a large computer network that spans across a city.
7. **Wide area network (WAN)**: Wide area networks cover larger areas such as large cities, states, and even countries.
8. **Enterprise private network (EPN):** An enterprise private network is a single network that a large organization uses to connect its multiple office locations.
9. **Virtual private network (VPN)**: VPN is an overlay private network stretched on top of a public network.

10. **Cloud network**: Technically, a cloud network is a WAN whose infrastructure is delivered via cloud services.

Based on organizational intent, networks can be classified as:

1. **Intranet**: An intranet is a set of networks that are maintained and controlled by a single entity. It is generally the most secure type of network, with access to authorized users alone. An intranet usually exists behind the router in a local area network.
2. **Internet**: The internet (or the internetwork) is a collection of multiple networks connected by routers and layered by networking software. This is a global system that connects governments, researchers, corporates, the public, and individual computer networks.
3. **Extranet**: An extranet is similar to the intranet but with connections to particular external networks. It is generally used to share resources with partners, customers, or remote employees.
4. **Darknet**: The darknet is an overlay network that runs on the internet and can only be accessed by specialized software. It uses unique, customized communication protocols.

1.3 Key Objectives of Creating and Deploying a Computer Network

There is no industry—education, retail, finance, tech, government, or healthcare—that can survive without well-designed computer networks. The bigger an organization, the more complex the network becomes. Before taking on the onerous task of creating and deploying a computer network, here are some key objectives that must be considered.

(i) Resource sharing

Today’s enterprises are spread across the globe, with critical assets being shared across departments, geographies, and time zones. Clients are no more bound by location. A network allows data and hardware to be accessible to every pertinent user. This also helps with interdepartmental data processing. For example, the marketing team analyzes customer data and product development cycles to enable executive decisions at the top level.

(ii) Resource availability & reliability

A network ensures that resources are not present in inaccessible silos and are available from multiple points. The high reliability comes from the fact that there are usually different supply authorities. Important resources must be backed up across multiple machines to be accessible in case of incidents such as hardware outages.

(iii) Performance management

A company’s workload only increases as it grows. When one or more processors are added to the network, it improves the system’s overall performance and accommodates this growth. Saving data in well-architected databases can drastically improve lookup and fetch times.

(iv) Cost savings

Huge mainframe computers are an expensive investment, and it makes more sense to add processors at strategic points in the system. This not only improves performance but also saves money. Since it enables employees to access information in seconds, networks save operational time, and subsequently, costs. Centralized network administration also means that fewer investments need to be made for IT support.

(v) Increased storage capacity

Network-attached storage devices are a boon for employees who work with high volumes of data. For example, every member in the data science team does not need individual data stores for the huge number of records they crunch. Centralized repositories get the job done in an even more efficient way. With businesses seeing record levels of customer data flowing into their systems, the ability to increase storage capacity is necessary in today’s world.

(vi) Streamlined collaboration & communication

Networks have a major impact on the day-to-day functioning of a company. Employees can share files, view each other’s work, sync their calendars, and exchange ideas more effectively. Every modern enterprise runs on internal messaging systems such as Slack for the uninhibited flow of information and conversations. However, emails are still the formal mode of communication with clients, partners, and vendors.

(vii) Reduction of errors

Networks reduce errors by ensuring that all involved parties acquire information from a single source, even if they are viewing it from different locations. Backed-up data provides consistency and continuity. Standard versions of customer and employee manuals can be made available to a large number of people without much hassle.

(viii) Secured remote access

Computer networks promote flexibility, which is important in uncertain times like now when natural disasters and pandemics are ravaging the world. A secure network ensures that users have a safe way of accessing and working on sensitive data, even when they're away from the company premises. Mobile handheld devices registered to the network even enable multiple layers of authentication to ensure that no bad actors can access the system.

1.4 Computer Network Management

Network management is the process of configuring, monitoring, and troubleshooting everything that pertains to a network, be it hardware, software, or connections. The five functional areas of network management are fault management, configuration management, performance management, security management, and (user) accounting management.

Computer networks can quickly become unruly mammoths if not designed and maintained from the beginning. Here are the top 10 practices for proper computer network management.

(i) Pick the right topology

Network topology is the pattern or hierarchy in which nodes are connected to each other. The topology can speed up, slow down, or even break the network based on the company's infrastructure and requirements. Before setting up a network from scratch, network architects must choose the right one. Some common topologies include:

a) **Bus network**: Each node is linked to only one other node.

b) **Ring network**: Each node is linked to two other nodes, thus forming a ring.

c) **Mesh network**: Each node must strive to be connected to every other node in the system.

d) **Star network**: A central node server is linked to multiple other nodes. This is faster since data doesn't have to travel through each node.

e) **Tree network**: Here, nodes are arranged in hierarchies.

(ii) Document and update constantly

Documentation of the network is vital since it is the backbone of operations. The documentation must include:

a) Technical specifications of equipment, including wires, cables, and connectors

b) Hardware

c) The software used to enable the hardware and the smooth and secure flow of data

d) Firmware

e) A formal record of policies and procedures with respect to network operators and users

This must be audited at scheduled intervals or during rehauls. Not only does this make network management easier, but it also allows for smoother compliance audits.

(iii) Use the right tools

The network topology is just the first step toward building a robust network. To manage a highly available and reliant network, the appropriate tools must be placed at the right locations. Must-have tools in a network are:

a) **Network monitoring solutions**: A network monitoring solution gives complete visibility into the network. Visual maps help gauge network performance. It can track packets, provide a granular look into network traffic, and help spot anomalies. Newer monitoring systems leverage artificial intelligence to predict scaling requirements and cyber threats using historic and real-time data.

b) **Configuration management tools**: A network contains many components that interface with each other. This results in a lot of configuration parameters to keep track of. Configuration management tools resolve this by providing configuration tools that span across the entire network. They also allow network managers to ensure that all compliance requirements have been fulfilled.

c) **IP address managers**: Bigger networks need to have an IP address manager (IPAM) to plan, track, and manage information associated with a network's IP addresses.

d) **Security solutions**: Firewalls, content filtering systems, intrusion detection and prevention systems—these are all tools that safeguard networks that are carrying increasingly sensitive loads. No network is complete without them. However, just acquiring these tools is not enough. They must also be properly placed within the network. For example, a firewall must be placed at every network junction. Anti-DDoS devices must be placed at the perimeters of the network. Load balancers need to be placed at strategic locations based on the infrastructure, such as before a cluster of database servers. This must be an explicit part of the network architecture.

(iv) Establish baseline network & abnormal behaviour

A baseline allows admins to know how the network normally behaves in terms of traffic, user access, etc. With an established baseline, alerts can be set up in appropriate places to flag anomalies immediately. The normal range of behaviour must be documented at both, user and organizational levels. Data required for the baseline can be acquired from routers, switches, firewalls, wireless APs, sniffers, and dedicated collectors.

(v) Protect the network from insider threats

Firewalls and intrusion prevention systems ensure that bad actors remain out of the network. However, insider threats need to be addressed as well, particularly with cybercriminals targeting those with access to the network using various social engineering ploys. One way of doing this is to operate on a least-privilege model for access management and control. Another is to use stronger authentication mechanisms such as single sign-on (SSO) and two-factor authentication (2FA). Besides this, employees also need to undergo regular training to deal with security threats. Proper escalation processes must be documented and circulated widely.

(vi) Use multiple vendors for added security

While it makes sense to stick to one hardware vendor, a diverse range of network security tools is a major plus for a large network. Security is a dynamic and ever-involving landscape. Hardware advancements are rapid and cyber threats also evolve with them. It is impossible for one vendor to be up to date on all threats. Additionally, different intrusion detection solutions use different detection algorithms. A good mix of these tools strengthens security; however, you must ensure that they are compatible and allow for common logging and interfacing.

(vii) Segregate the network

Enterprise networks can become large and clunky. Segregation allows them to be divided into logical or functional units, called zones. Segregation is usually done using switches, routers, and virtual LAN solutions. One advantage of a segregated network is that it reduces potential damage from a cyberattack and keeps critical resources out of harm’s way. Another plus is that it allows for more functional classification of networks, such as separating programmer needs from human resources needs.

(viii) Use centralized logging

Centralized logs are key to capturing an overall view of the network. Immediate log analysis can help the security team flag suspicious logins and IT admin teams to spot overwhelmed systems in the network.

(ix) Consider using honeypots & honeynets

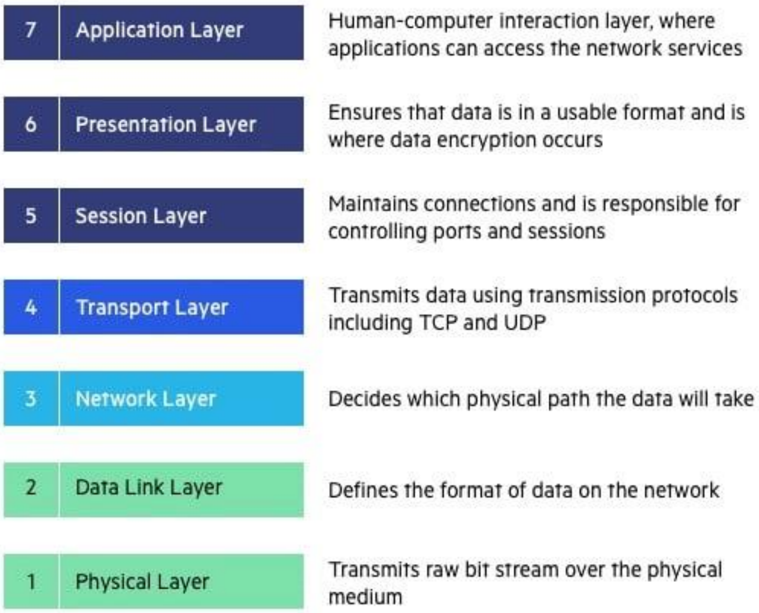
Honeypots are separate systems that appear to have legitimate processes and data but are actually a decoy for insider and outsider threats. Any breach of this system does not cause the loss of any real data. A honeynet is a fake network segment for the same cause. While this may come at an additional cost to the network, it allows the security team to keep an eye out for malicious players and make appropriate adjustments.

(x) Automate wherever possible

New devices are added to systems regularly, and old ones are retired. Users and access controls keep changing frequently. All of these must be automated to ensure that human error does not occur and there are no vulnerable zombie systems in the network, costing money and security. Automation with respect to security is also crucial. It is a good practice to automate responses to attacks, including blocking IP addresses, terminating connections, and gathering additional information about attacks.

2. OSI MODEL

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s. It has been developed by ISO – ‘International Organization for Standardization‘, in the year 1984. The OSI layers “top-down” starts from the application layer that directly serves the end user, down to the physical layer.



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Figure 1. OSI Model

2.1. Application Layer

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user. The application layer is used by end-user software and applications such as web browsers, skype messenger, and email clients.

It provides protocols that allow the software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS). The Functions of the Application Layer are

1. Network Virtual Terminal: It allows a user to log on to a remote host.
2. FTAM- File transfer access and management: This application allows a user to access files in a remote host, retrieve files in a remote host and manage or control files from a remote computer.
3. Mail Services: Provide email service.
4. Directory Services: This application provides distributed database sources and access to global information about various objects and services.

2.2. Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer. The Functions of the Presentation Layer are

1. Translation: For example, ASCII to EBCDIC.
2. Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. Compression: Reduces the number of bits that need to be transmitted on the network.

Note: Device or Protocol Use: JPEG, MPEG, GIF

2.3. Session Layer

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security. The Functions of the Session Layer

1. Session establishment, maintenance, and termination: The layer allows the two processes to establish, use and terminate a connection.
2. Synchronization: This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

Note:

1. All the below 3 layers (including Session Layer) are integrated as a single layer in the TCP/IP model as the “Application Layer”.

2. Implementation of these 3 layers is done by the network application itself. These are also known as Upper Layers or Software Layers.

3. Device or Protocol Use: NetBIOS, PPTP

Let us consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0’s and 1’s) so that it can be transmitted.

2.4. Transport Layer

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found. At the sender’s side: The transport layer receives the formatted data from the upper layers, performs Segmentation, and also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer. The sender needs to know the port number associated with the receiver’s application. Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned. At the receiver’s side: Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data. The Functions of the Transport Layer

i. Segmentation and Reassembly: This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.

ii. Service Point Addressing: To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services Provided by Transport Layer: Connection-Oriented Service and Connectionless Service

1. Connection-Oriented Service: It is a three-phase process that includes: Connection Establishment, Data Transfer and Termination/disconnection.

In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

2. Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

Note:

1. Data in the Transport Layer is called Segments.

2. Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
3. The transport layer is called as Heart of the OSI model.

4. Device or Protocol Use: TCP, UDP NetBIOS, PPTP

The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

2.5. Network Layer

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver’s IP addresses are placed in the header by the network layer. The Functions of the Network Layer are:

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.

2. **Logical Addressing:** To identify each device on Internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver’s IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Note:

1. Segment in the Network layer is referred to as **Packet**.

2. Network layer is implemented by networking devices such as routers and switches.

2.6. Data Link Layer

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address. The Data Link Layer is divided into two sublayers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of the NIC (Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header. The Receiver’s MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address. The Functions of the Data Link Layer are as follows:

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.
3. **Error control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
5. **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

Note:

1. Packet in the Data Link layer is referred to as **Frame.**

2. Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.

3. Switch & Bridge are Data Link Layer devices.

2.7. Physical Layer

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together. The Functions of the Physical Layer are as follows:

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
4. **Transmission mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

Note:

1. Hub, Repeater, Modem, and Cables are Physical Layer devices.

2. Network Layer, Data Link Layer, and Physical Layer are also known as **Lower Layers** or **Hardware Layers**

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for the transmission of the raw data, which is simply a series of 0s and 1s while taking care of bit rate control.

Table 1. OSI Model in a Nutshell

Layer No	**Layer Name**	**Responsibility**	**Information Form (Data Unit)**	**Device or Protocol**
7	Application Layer	Helps in identifying the client and synchronizing communication.	Message	SMTP
6	Presentation Layer	Data from the application layer is extracted and manipulated in the required format for transmission.	Message	JPEG, MPEG, GIF
5	Session Layer	Establishes Connection, Maintenance, Ensures Authentication, and Ensures security.	Message	Gateway
4	Transport Layer	Take Service from Network Layer and provide it to the Application Layer.	Segment	Firewall
3	Network Layer	Transmission of data from one host to another, located in different networks.	Packet	Router
2	Data Link Layer	Node to Node Delivery of Message.	Frame	Switch, Bridge
1	Physical Layer	Establishing Physical Connections between Devices.	Bits	Hub, Repeater, Modem, Cables

The modern Internet is not based on OSI but on the simpler TCP/IP model.

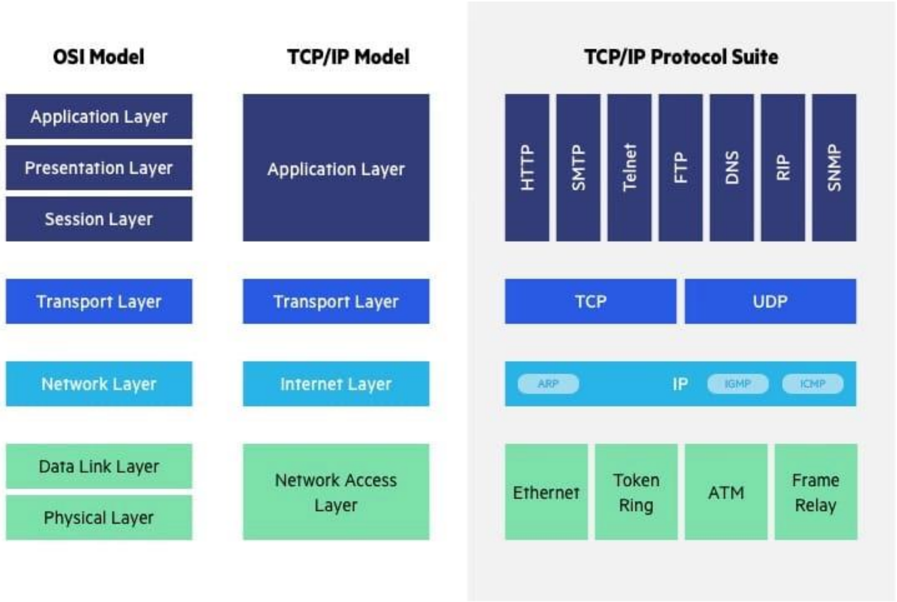


Figure 2. OSI vs. TCP/IP Model

The Transfer Control Protocol/Internet Protocol (TCP/IP) is older than the OSI model and was created by the US Department of Defense (DoD). A key difference between the models is that TCP/IP is simpler, collapsing several OSI layers into one:

1. OSI layers 5, 6, and 7 are combined into one Application Layer in TCP/IP
2. OSI layers 1, and 2 are combined into one Network Access Layer in TCP/IP – however, TCP/IP does not take responsibility for sequencing and acknowledgement functions, leaving these to the underlying transport layer.

Other important differences:

1. TCP/IP is a functional model designed to solve specific communication problems, and which is based on specific, standard protocols. OSI is a generic, protocol-independent model intended to describe all forms of network communication.

2. In TCP/IP, most applications use all the layers, while in OSI simple applications do not use all seven layers. Only layers 1, 2 and 3 are mandatory to enable any data communication.

3. NETWORK LAYER

The network layer or layer 3 of the OSI (Open Systems Interconnection) model is concerned with getting packets from the source to destination, routing, error handling and congestion control.

3.1 Function of Network Layer

The functions of the network layer are:

3.1.1 Addressing

Maintains the address at the frame header of both source and destination and performs addressing to detect various devices in the network

3.1.2 Packeting

This is performed by internet Protocol. The network layer converts the packets from its upper layer

3.1.3 Routing

It is the most important functionality. The network layer chooses the most relevant and best path for the data transmission from source to destination using a routing algorithm as follows:

1. In order to transfer the packets from source to the destination, the network layer must determine the best router through which packet can be transmitted
2. Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
3. The routing protocol is a routing algorithm that provides that best path from the source to the destination. The best path is the path that has the least-cost-path from source to the destination
4. Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm

Routing algorithm is divided into two categories:

1. Adaptive Routing Algorithm
   a. An adaptive routing algorithm is also known as dynamic routing algorithm
   b. This algorithm makes the routing decisions based on the topology and network traffic
2. Non-Adaptive Routing Algorithm
   a. Non-adaptive routing algorithm is also known as a static routing algorithm
   b. Non-adaptive routing algorithms do not take the routing decision based on the network topology or network traffic
   c. Different routing algorithms are: Shortest path algorithm, Distance vector routing, link state routing, hierarchical routing.

3.1.4 Inter-networking

It works to deliver a logical connection across multiple devices

3.2 Network layer design Issues

The network layer comes with some design issues such as store-and-forward packet switching, service to transport layer, providing connection-oriented service and providing connectionless service.

3.2.1 Store and Forward Packet Switching

The network layer operates in an environment that uses store and forward packet switching. The node which has a packet to send delivers it to the nearest router. The packet is stored in the router until it has fully arrived and its checksum is verified for error detection. Once, this is done, the packet is forwarded to the next router. Since each router needs to store the entire packet before it can forward it to the next hop, the mechanism is called store and forward switching.

3.2.2 Services to Transport Layer

The network layer provides service to its immediate upper layer (transport layer) through the network-transport layer interface. The two types of services provided are −

1. Connection-Oriented Service − In this service, a path is set up between the source and the destination, and all the data packets belonging to a message are routed along this path.
2. Connectionless Service − In this service, each packet of the message is considered as an independent entity and is individually routed from the source to the destination.

The objectives of the network layer while providing these services should be as follows −

- The services should not be dependent upon the router technology.
- The router configuration details (type, number or topology) should not be of concern to the transport layer.
- A uniform addressing plan should be made available to the transport layer, whether the network is a LAN, MAN or WAN.

3.2.3 Providing Connectionless Service

In connectionless service, packets are injected into the network individually and routed independently of each other. No advance setup is needed. In this context, each packets contains its routing information are is referred to datagram and the network is called datagram network.

3.2.4 Providing Connection-Oriented Service

In the connection-oriented service, a path from the source router to the destination router must be established before any data packets can be sent. This connection is called a virtual circuit (VC) and the network is called virtual circuit network.

This is done in either two ways:

1. Circuit switched connection - A dedicated physical path or a circuit is established between the communication nodes and then the data stream is transferred

2. Virtual Circuit switching connection – The stream is transferred over a packet switch network, in such a way that it seems to the user that there is a dedicated path connections from the sender to the receiver. A virtual path is established here. While, other connections may also be using the same path.

Table 2. Comparison of Virtual Circuit and Datagram Network

Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short CV number
State Information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set; all packets follow it
Effect of router failures	None, except for packet lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocation in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

4. TRANSPORT LAYER

The transport layer is Layer 4 of the Open Systems Interconnection (OSI) communications model. It is responsible for ensuring that the data packets arrive accurately and reliably between sender and receiver. In the OSI model, the transport layer sits between the network layer and the session layer. The network layer is responsible for taking the data packets and sending them to the correct computer. The transport layer then takes the received packets, checks them for errors and sorts them. Then, it sends them to the session layer of the correct program running on the computer. The session layer now takes the well-formatted packets and uses them for the application's data.

4.1 Transport layer functions

The overall functionality is to insulate the application layer from needing to worry about the nitty-gritty details. It does this by providing end-to-end communication, reliability, flow control, addressing and multiplexing:

(i) End-to-end communication between hosts

End-to-end communication is the ability of the transport layer to provide the application a way to send and receive a stream of data. The network layer segments the data stream into packets that are sent over the network and reconstruct the data on the other end. If the data packets arrive out of order, it can reorder them by segment numbering and present the data in the correct order.

(ii) Reliability (Data integrity and error checking)

Reliability is the ability to correct errors that can happen during data transmission over the network. If data were to be accidentally changed in transit, error-correcting and checksums would catch it. If a packet were to be lost, it would be caught and retransmitted. If a single packet were to be duplicated, it could be detected and dropped. It can also send an acknowledgement of received packets for guaranteed delivery. Some protocols send a message if a packet is not received or is corrupt.

(iii) Flow and congestion control

Flow control (congestion control) is the ability of the transport layer to avoid sending more data than can be reliably transmitted. It can buffer sending and receiving data until there is enough network capacity for it to go through. If the receiver buffer becomes full, it can reduce the sending rate. It also implements congestion control. If a network were to become flooded with too many retransmit messages, it would be overwhelmed and not able to recover. Congestion control prevents this by using dynamic retransmission timers and slow start.

(iv) Addressing

Addressing is the ability to communicate with the correct application on the computer. Addressing typically uses network ports to assign each sending and receiving application a specific port number on the machine. By combining the IP address used in the network layer and the port on the transport layer, each application can have a unique address.

(v) Multiplexing

Multiplexing is the ability for any number of applications to use any number of network connections. For example, a typical desktop computer may only have one Ethernet network connection but have several connections to the internet running at the same time, such as a web browser, video streaming and a mail client. Conversely, a large server may only have one application, such as a SQL server, but have two physical Ethernet connections to provide as much bandwidth as possible. The transport layer ensures that each application gets a fair amount of shared network connections.

4.2 Transport layer protocols

The transport layer is represented by two protocols: TCP and UDP.

(i) User Datagram Protocol (UDP)

UDP is one of the simplest transport layer protocols that provide non-sequenced data transmission functionality. It is considered a connectionless transport layer protocol and is referred to be used when speed and size are to be prioritized over reliability and security. UDP is an end-to-end transport-level protocol that adds transport-level addresses, and length information to the data from the upper layer of the OSI. UDP uses User Datagram Format has the following features:

a) The user datagram format is of a 16-byte header which consists of various components, namely:
b) Destination Port Address: The address for receiving the message from the request procedure is provided. The destination port's address is 16 bits long.
c) Checksum: The control is an error-detection field. It is 16 bit long.
d) Total Length: A 16-bit region that defines the total length of the user datagram. The length is defined in bytes.
e) Source Port Address: The address of the application process that sent the message is provided. The source port's address is 16 bits long.

(ii) Transmission Control Protocol

Transmission Control Protocol (TCP) is a transport layer protocol that is based on connections. Transport layer services are provided to applications by it. TCP is a protocol that describes how to create and manage network connections so that applications can communicate data. The Internet Protocol (IP) is used by TCP to describe how computers exchange data packets. HTTP, HTTPS, FTP, and many computer games are examples of services and programs that use TCP. TCP Segment Format is made up of:

a) Control Bits: Each control section is self-contained and functions on its own. The control bit specifies a segment's behaviour or acts as a validity check for particular fields.
b) Acknowledgement Number: Data from other communication devices is used to acknowledge data via an acknowledgement number. It is a 32-bit long field. The sequence number that the receiver expects to receive is given if ACK is set to 1.
c) Header Length: The TCP header length is 32-bit words. 5 words is the minimum size of the header while the maximum size is 15 words. The TCP header is 60 bytes long. The UDP header is 20 bytes long.
d) Source Port Numbers: It is used to specify the application's address in a source computer. It is a 16-bit space.
e) Sequence Number: TCP divides a data stream into two or more segments. The data within an original data stream is located in the 32-bit number sequence field.
f) Destination Port Address: This is used to identify the address of application software in a destination machine. It is a 16-bit field.

5. NETWORK ADDRESSING

A network address is a unique physical or logical address that distinguishes a network node or device over a computer or telecommunications network. The Network address is a numeric number or address that is assigned to any new device that seeks access to the network or is already part of the network. Network addresses are designed to be unique identifiers across the network, although some networks allow for private addresses, or locally administered addresses that may not be unique. Each computer on a network use a network address to identify, locate and address other computers. In networking technology, network address is a key component to identify and locate network node/device over a network. It has several forms, including the Internet Protocol (IP) address, media access control (MAC) address and host address. An IP address is an address used in order to uniquely identify a device on an IP network. The address is made up of 32bits number, which can be divisible into a network portion and host portion with the help of a subnet mask.

The basic concepts is as follows:

1. Network Addressing is one of the major responsibilities of the network layer.
2. Network addresses are always logical, i.e., software-based addresses.
3. A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
4. A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
5. Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

5.1 Classful Addressing

An IP address is 32-bit long. An ip address is divided into two parts: Network ID which represents the number of networks and Host ID which represents the number of hosts. An IP address is divided into sub-classes: A, B, C, D and E.

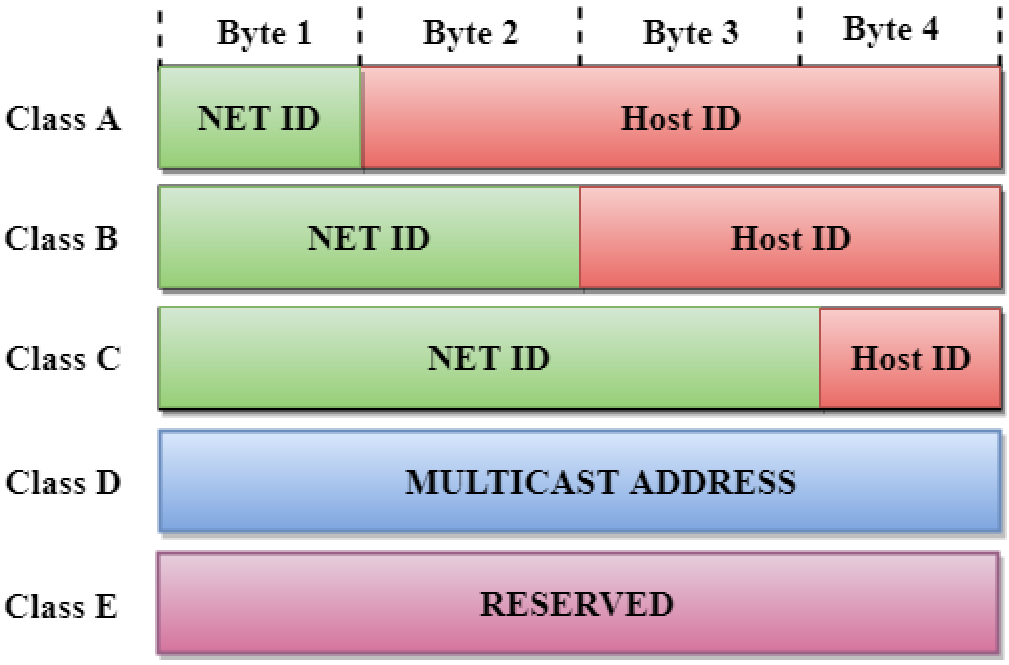
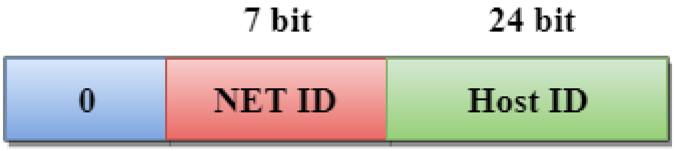


Figure 3: Classful addressing

Each class have a specific range of IP addresses as shown in the figure above. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

(i) Class A

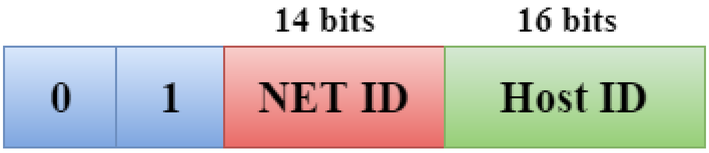
In Class A, an IP address is assigned to those networks that contain a large number of hosts. The network ID is 8 bits long. The host ID is 24 bits long. In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network. The total number of networks in Class A = 2^7 = 128 network address. The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address



(ii) Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks. The Network ID is 16 bits long. The Host ID is 16 bits long. In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID. The total number of networks in Class B = 2^{14} = 16384 network address.

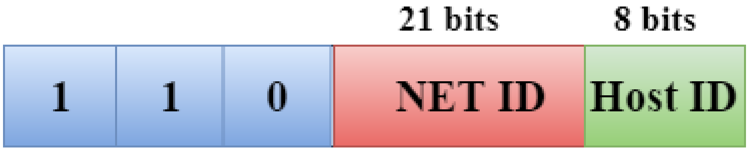
The total number of hosts in Class B = 2^{16} - 2 = 65534 host address.



(iii) Class C

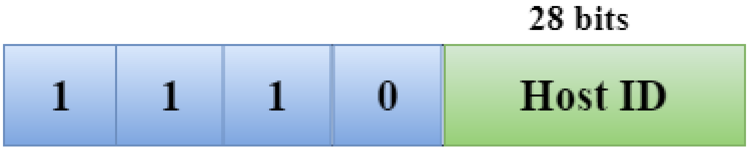
In Class C, an IP address is assigned to only small-sized networks. The Network ID is 24 bits long.

The host ID is 8 bits long. In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network. The total number of networks = 2^{21} = 2097152 network address. The total number of hosts = 2^8 - 2 = 254 host address.



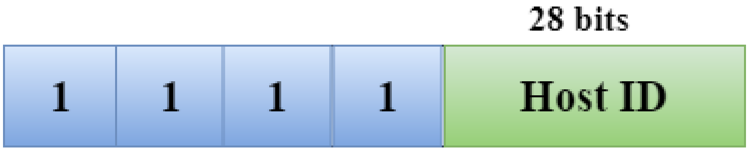
(iv) Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



(v) Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



6. NETWORK MANAGEMENT SYSTEMS

A network management system is a framework for managing the hardware and software components of a company's data network. It allows an administrator to monitor all parts of the network from a central server and can help optimize the performance of a network and improve its security. Network management systems are common in large organizations because a network administrator can use them to oversee extensive networks that include hundreds or thousands of separate components. Network management systems streamline the operations of a company's network by connecting all of its components, such as computers routers, cameras, switches, sensors and software applications. These components then provide information to the system, which collects the data in a central server. The system's network administrators can access the data and may receive alerts if the system detects a security breach or other issue within the network.

6.1 Functions of network management systems

Because network management systems have a high degree of customization, they can perform a wide range of tasks. Some common tasks perform by network management systems are as follows:

(i) Network automation

Automation is often the primary function of a network management system. Network automation allows testing, configuring and managing all devices in the network to happen automatically through software applications. While an administrator might develop the update schedule and perform tests, the system carries out updates and configurations across the devices in the network. This function allows the system to provide consistency and agility across networks of all sizes and can decrease the labour required from IT teams.

(ii) Network monitoring

Network monitoring, where a system collects data from a network's components, is another vital task for most network management systems. These systems perform regular checks on the different components of a network and create reports for the network administrator. Typically, a network administrator can access these reports on a special server or dashboard, depending on the type of management system they're using. If any component in the network malfunctions or is nearing capacity, the network administrator might also receive an alert so they can address the problem before it affects any employees or clients.

(iii) Device detection

Sometimes IT personnel may add new devices or components to a network, like new computers or tablets. A network management system with device detection can locate these new elements and integrate them into the network smoothly. This feature can also configure devices to operate efficiently with other components. Automated device detection ensures that employees can use these new devices quickly without requiring a complete system overhaul.

(iv) Performance analysis

Many network management systems monitor their network's performance over time and compare it to its current metrics. They can send these reports to network administrators and might offer strategies to increase performance if it is declining. Some systems may also recommend additional devices or components to optimize the network's functions.

(iv) Fault management

Fault management is an important part of maintaining data security and preventing network disruption. If any part of the network fails, the fault management system can often reroute traffic away from the faulty component. This can help avoid any loss of data or productivity.

(v) Data backup

Data loss can be a major disruption for companies with extensive networks. To prevent this, many network management systems can duplicate data on backup servers automatically. Network administrators might determine how often the network management system duplicates network data and how long the system stores backup information. They can often restore information from backup servers after an outage or other data loss event.

(vi) Security management

Many network management systems have security protocols to protect the network from outside security threats. They can ensure that any breaches in security immediately trigger notifications to the administrator. System administrators might add extra security protocols that suspend certain activities in case of security breaches. Some industries, like health care, have specific legal requirements regarding data security, and a network management system can make it easier for IT teams to ensure compliance.

(vii) Traffic management

For a large network to operate effectively, each component of the network handles a certain amount of stress caused by traffic. Network management systems can ensure steady service by distributing traffic evenly throughout the network's elements. Many systems also can prevent outages by diverting traffic through other systems. Network administrators might create protocols that govern how the system allocates traffic during busy periods.

6.2 Types of network management systems

Network management systems come in several configurations, including cloud-based, on-site and off-site. Here are descriptions of these three types of network management systems:

(i) Cloud-based

Some companies choose to purchase their network management systems as cloud-based services, which store data online. Cloud-based systems often offer the advantage of lower costs since they don't require the company to invest in on-site servers. They can also allow IT personnel to access their services wherever they are and may allow the provider to send automatic updates and extensions to their network when required.

(ii) On-premise

A business may choose to base its network management system on its premises. These systems may have higher startup costs but often offer improved security. On-site servers may also provide better performance for large networks, but they often require extensive maintenance from company personnel. This makes on-site network management systems more common for large enterprises that have the IT staff and facilities to house them. An enterprise may also choose to locate its network management services in an off-site data facility. This type of network management system may allow the company to save money by avoiding the cost of installing and maintaining on-site servers. It may also provide increased performance for large networks, but may not be as secure as on-site data storage.

6.3 Benefits of network management systems

Network management systems may give a business the following advantages:

(i) Lower costs

Network management systems can help to lower hiring and payroll costs by enabling a single administrator, or a small team of IT employees, to manage an entire network.

(ii) Improved network performance

Many network management systems collect and aggregate data on network performance and often offer options for improvement.

(iii) More efficient data sharing

A network management system can help a company save time by allowing each member of a team to access data from their workstations. Administrators can decide what level of access each employee requires.

(iv) Increased productivity

A network management system can immediately report any malfunction to the administrator, which can help the IT team fix any issues quickly. This can keep productivity from slowing down and prevent data loss.

(v) Enhanced data security

Administrators may resolve security threats more quickly if they have a network management system that automatically reports any breach.

(vi) Better device integration

Network administration systems can ensure that hardware and software from different vendors operate effectively together.