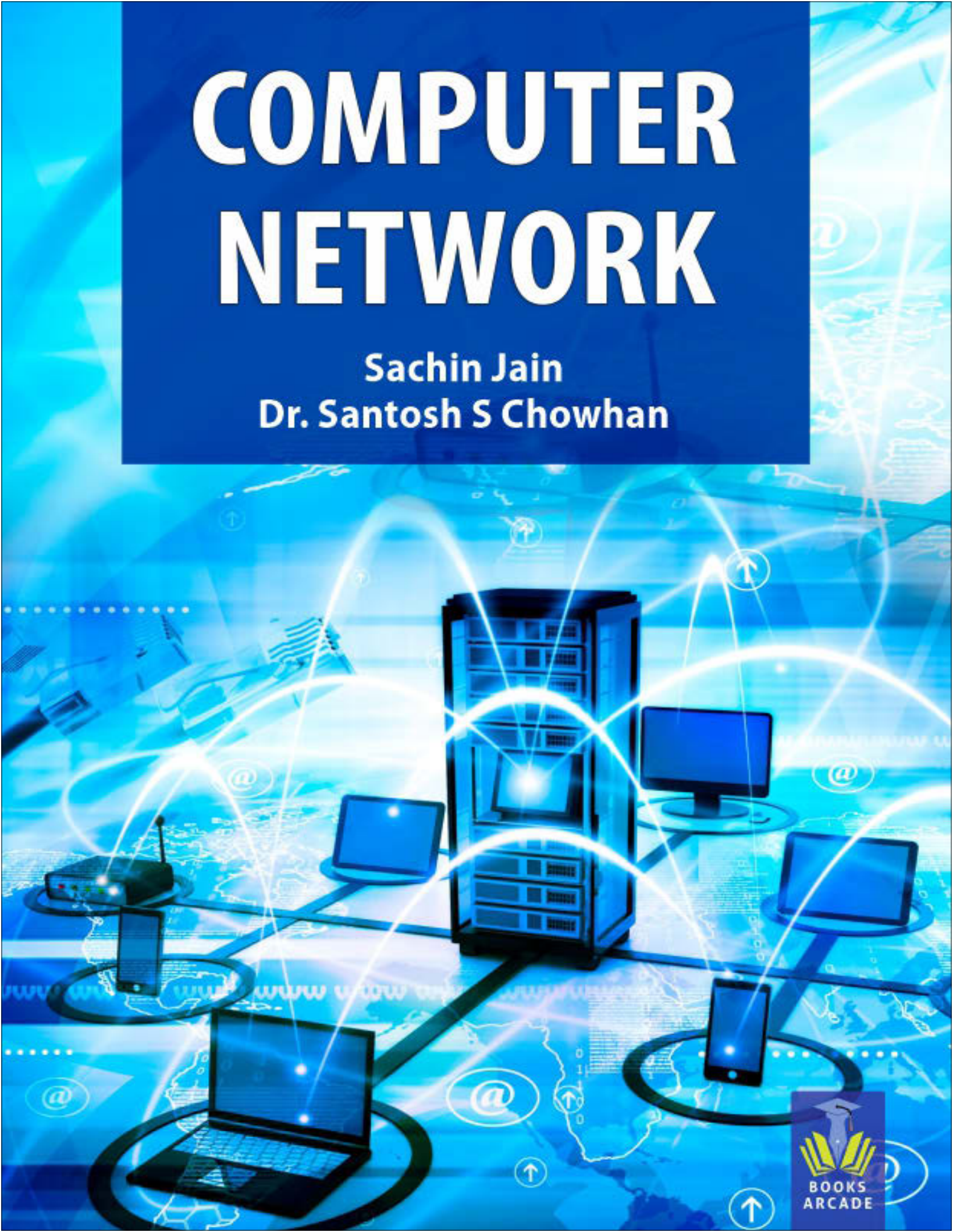
COMPUTER NETWORK

Sachin Jain
Dr. Santosh S Chowhan



BOOKS ARCADE

Computer Network

Computer Network

Sachin Jain
Dr. Santosh S Chowhan

BOOKS ARCADE
KRISHNA NAGAR, DELHI

Computer Network

Sachin Jain
Dr. Santosh S Chowhan

BOOKS ARCADE

Regd. Office:
F-10/24, East Krishna Nagar, Near Vijay Chowk, Delhi-110051
Ph. No: +91-11-79669196, +91-9899073222
E-mail: info@booksarcade.co.in, booksarcade.pub@gmail.com
Website: www.booksarcade.co.in

Year of Publication 2023

International Standard Book Number-13: 978-81-19199-20-4

CONTENTS

Chapter 1

INTRODUCTION TO COMPUTER NETWORK

Sachin Jain, Assistant Professor,
School of Computer & Systems Sciences, Jaipur National University, Jaipur, India,
Email Id-sachin.jain@jnujaipur.ac.in

A group of computers sharing resources that are available on or offered by network nodes is known as a computer network. Over digital links, the computer linked with one another using standard communication protocols. These connection is established up of telecommunication network technologies, which are based on technically wired, optical, and wireless radio-frequency means and may be set up in a number of different network topologies. Personal computers, servers, networking equipment, and other specialized or general-purpose hosts can all function as nodes in a computer network. They can have hostnames and are identifiable by network addresses. After being assigned, hostnames act as recognizable labels for the servers and are rarely updated. Network addresses are used by communication protocols like the Internet Protocol to locate and identify the nodes. Computer networks can be categorized using a variety of factors, including the bandwidth, signal transmission medium, communications protocols used to organize network traffic, topology, network size, organizational goals and traffic management system (Figure 1.1).

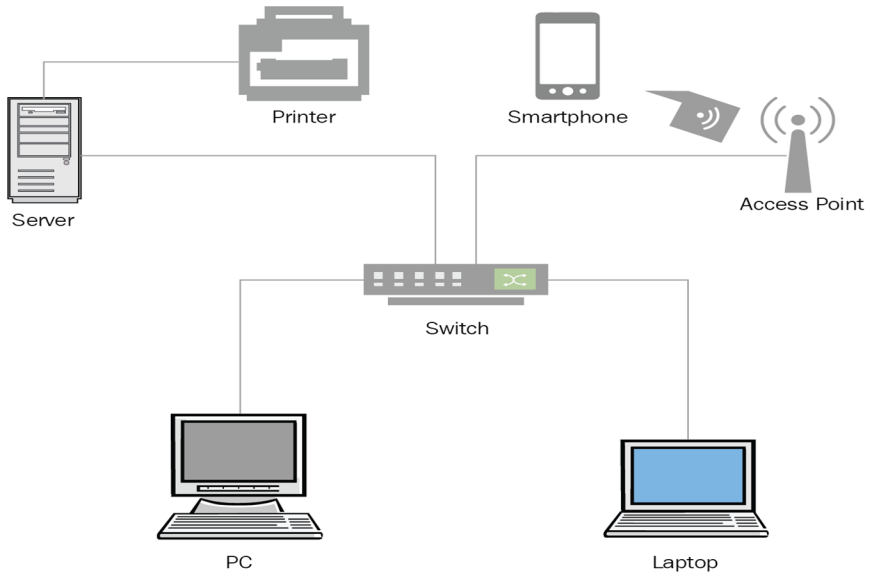


Figure 1.1: Computer Network

A computer network is a setup that joins two or more computers together to share and transport data. Mobile phones and servers are both examples of computing devices. These gadgets may be wireless or linked by physical connections like fiber optic cables. The U.S. Department of Defense provided funding for the development of the first operational network, known as ARPANET, in the late 1960s. Researchers from the government used to exchange information back when computers were bulky and difficult to carry. Today, we have advanced much from that fundamental network type. The internet, a network of networks that links billions of devices

worldwide, is the center of our modern world. Networks are used by businesses of all kinds to link the devices of their workers with common resources like printers. The traffic monitoring systems in big centers are an illustration of a broad computer network. These systems provide information on traffic flow and events to authorities and emergency personnel. A simpler example is sharing papers with coworkers who work remotely using collaboration tools like Google Drive. A computer network is in use whenever we connect through a video call, stream movies, and exchange files, communicate via instant messaging, or just access anything on the internet.

Component of the Computer Network:

A computer network is composed of five fundamental parts as shown in Figure 1.2.

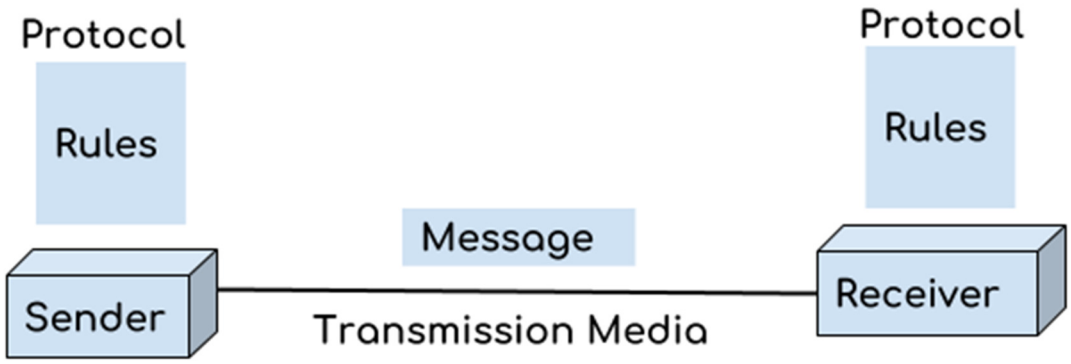


Figure 1.2: five fundamental parts.

1. **Message:**

It is the information that must be moved from one computer to another through a computer network.

2. **Sender:**

A computer that has to deliver data to another device linked to a network is a sender.

3. **Receiver:**

A device that is waiting for data from other networked devices is known as a receiver.

4. **Transmission Media:**

Data transfer requires a transmission medium, such as wires, radio waves, cables etc., in order to move data from one device to another.

5. **Protocol:**

A protocol is a set of guidelines that both the sender and the receiver agree upon; without a protocol, two devices can be linked to one another but cannot interact. A set of guidelines known as a protocol is required in order to create trustable connection or sharing of information between two separate devices. For instance, web browsers utilize the http and https protocols to download and upload data to the internet, while email services that are connected to the internet use the smtp protocol.

Important Computer Network Elements

A computer network is composed of two fundamental building blocks: nodes, or network devices, and connections. The linkages link together two or more nodes. Communication protocols specify how these networks transmit the data. The origin and destination devices, which serve as the communication endpoints, are often referred to as ports. Main Computer Network Components are

Networking Equipment

Computing devices that need to be connected to a network are known as network devices or nodes. Computers, smartphones, and other consumer electronics are examples of network devices. Users often and directly contact these endpoints. For instance, an email is created using the mail program on a laptop or smartphone.

Servers: The major computing and data storage take place on these application or storage servers. The servers receive all requests for certain operations or data.

Routers: Routing is the process of choosing the network route that data packets take to go from A to B. These packets are sent by routers across networks in order to get to their destination. They boost the effectiveness of big networks.

Switches: Repeaters are electrical devices that receive network signals and clean or amplify them. They are to networks what transformers are to electricity grids. Repeaters with several ports are called hubs. They distribute the data to any open ports there may be. Bridges are more intelligent hubs that only transmit data to the intended port. A switch is a bridge with several ports. To facilitate connectivity with several network devices, switches may accept multiple data connections.

Gateways: Hardware items known as "gateways" between two different networks. They might be servers, routers, or firewalls.

Links

Links are a kind of transmission medium that come in two varieties:

Wired: Coaxial cables, phone lines, twisted-pair cabling, and optical fibres are a few examples of wired technologies that are utilised in networks. To represent data, optical fibres transmit pulses of light.

Wireless: Radio and other electromagnetic waves may also be used to create network connections. The term "wireless" refers to this kind of communication. Cellular networks, radio and technology distributed spectrums, as well as communication satellites, are some of the most prevalent instances of wireless connectivity. Spectrum technology is used by wireless LANs to create connections in constrained spaces.

Protocols for communications

All nodes engaged in the information transmission must abide by a set of rules known as a communication protocol. The internet protocol suite (TCP/IP), IEEE 802, Ethernet, wireless LAN, and cellular standards are a few examples of popular protocols. A theoretical paradigm called TCP/IP standardizes communication in a contemporary network. It proposes that these communication linkages have four functional layers:

- Network access layer: This layer specifies the physical means of data transport. It covers the method through which hardware transmits data bits via actual cables or fibres.
- Internet layer: This layer is in charge of encapsulating data into decipherable packets and enabling data transmission and reception.
- Transport layer: By ensuring the connection is reliable and legitimate, this layer allows devices to continue talking to one another.
- Application layer: This layer specifies how advanced apps may connect to a network and start transferring data.
- The open systems interconnection (OSI) concept, which is comparable to TCP/IP but has seven layers instead of two, continues to have a significant impact on the construction of the current internet.
- Metropolitan area networks (MANs) and local area networks (LANs) are covered by the IEEE802 family of standards (MAN). The most well-known component of the IEEE 802 family is wireless LAN, sometimes referred to as WLAN or Wi-Fis.

Network Defense: While nodes, connections, and protocols serve as a network's building blocks, it is impossible for a contemporary network to function without protections. When enormous volumes of data are created, transported, and processed across networks, security is crucial. Firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), network access control (NAC), content filters, proxy servers, anti-DDoS devices, and load balancers are a few examples of network security technologies.

Computer Network Uses:

Resource sharing: Resource sharing refers to the distribution of network resources, such as software, printers, and data, among users without regard to the actual locations of the users or the resources.

Client-Server model: The server-client model makes advantage of computer networking. A server is a major computer that the system administrator maintains and uses to store data. Clients are the devices used to remotely view the data held on the server.

Communication medium: Computer networks function as a channel for users to exchange information. For instance, a business with multiple computers can have an email system that staff members utilize on a daily basis.

E-commerce: Computer networks are essential to companies. We can conduct business online. Example-amazon.com conducts business online.

Characteristics of Computer Networks:

Network enables us to communicate quickly and effectively over the network. We can have video conferences, send emails, and other things online, for instance. As a result, the computer network is a fantastic tool for exchanging information and ideas. One of the main benefits of the computer network is file sharing. The computer network enables us to share files among ourselves. It's simple to roll back and back up, as the centrally situated main server is where the files are kept. As a result, taking a backup from the primary server is simple. Applications can be installed on the primary server, allowing for centralized user access. As a result, do not need to install the software

on each computer. The same is true for sharing hardware. The network enables security by confirming that the customer has permission to access specific files and apps. Scalability refers to the network's ability to accommodate new components. The network must be expandable so that can add new devices to the network. But because the connection speed and the data transfer speed both slow down, there is a greater likelihood of an error. The router or switching devices can be used to solve this issue. In the situation of a hardware breakdown, a computer network could use a backup source to communicate data.

Computer Network Applications

The following are examples of computer network applications or usage. Networks on computers are used for

Resource Exchange: An application of a computer network is resource sharing. Sharing resources is letting numerous people utilize the same hardware and software. Hardware includes things like printers, discs, and fax machines, computer hardware. Additionally, there is software, such as Atom, Android Studio, Postman, Oracle VM Virtual Box, etc.

Information Exchange: We may communicate information across a computer network, and it offers search tools like the World Wide Web. A single piece of information may be distributed across multiple people through the network and the internet. The computer network is essential for data exchange. Data may be shared between users that are connected to the same computer network. For instance, a huge number of people may access the same database simultaneously through the Internet.

Interaction: Email, phone conversations, message broadcasts, electronic money transfer systems, etc. are all examples of communication. Through computer networks, people may connect with one another anywhere in the globe. Through various network services including email, social networking, video conferencing, groupware, wikis, blogs, and SMS services, they may communicate and exchange information with one another.

The Entertainment Sector: Computer networks are also extensively used in the entertainment business. Entertainment businesses include those for video on demand, multiplayer real-time simulation games, films and television shows, etc.

Use of distant databases: We can access the Remote Database of the different apps by the end-users thanks to computer networks. Applications include automated newspapers, automated libraries, automated hotel reservations, automated flight reservations, and home banking. Additionally, a network offers the tools needed for distant data access. By connecting to the network from any location in the globe, a user may access and update data.

Household software: The computer network is often used for domestic purposes. You may take user-to-user communication, access to distance learning, electronic commerce, and entertainment as examples. Another method involves maintaining bank accounts, sending money to other banks, and making electronic bill payments. A computer network sets up a reliable connecting system for users.

Business software: Resource sharing is the end consequence of the business application here. The idea of resource sharing is to allow any network user to access all of the data, plans, and tools without having to physically visit the resource's location. With the use of a computer network, the majority of businesses do business electronically with other businesses and customers throughout the globe.

Cellular users: Mobile devices like laptop computers and PDAs are among the computer application industries that are expanding quickly (personal digital assistants). Portable device is referred to here as mobile users. The computer network is extensively employed in modern technology, including tablets, smart watches, wearable tech, and other online transactions like buying and selling goods.

Social media: Another excellent example of a computer network application is social media. It facilitates the exchange of knowledge on political, moral, and social problems. People may find a variety of entertainment options thanks to computer networks. We can watch movies, play games, and listen to music, for instance. Online, we may also meet new pals.

Sharing Software: Application software is often deployed on a centralised machine in a computer network (Server Computer). Instead than getting each person their own copy of the programme, it may be shared via the network.

Sharing Hardware: Hardware components of a computer network include printers, access points, HDDs, SATA drives, SSDs, drivers, etc. For instance, many users may share a single network-connected printer. Sharing several devices via a network enables a business to make significant financial savings. Without the network, these devices would need to be set up individually for each user, which would be exceedingly expensive for the business.

Consolidated Software Administration: On a single server computer, all the software is installed or updated. This reduces the amount of time needed to install/update software on each networked PC. These apps may be accessed by users who are connected to the network.

Data Management and Security: Centralized data storage is provided via the computer network. It denotes that a single server houses all of the data. In a business setting, an administrator effectively controls the vital data of the organization. Anyone may simply locate the information. A system administrator has total authority and has the ability to view or modify sensitive data. A system administrator may simply take a data backup. Similarly, it is quite simple to add security protections to the data.

Saving space on a disc: The role of applications in computer networks is crucial. In a computer network, the application programs and data files are shared by all machines. These are only kept on the server computer's hard drives. It is not necessary to keep application applications and data files on a person's computer locally. Each computer's disc space is preserved in this manner.

Improvement of Performance: Distributed computing may be utilized over a network to enhance the performance of many applications. A calculation job is shared among several machines connected to a network in distributed computing. Any application's performance improves as a result.

Key Purposes for Building and Implementing a Computer Network

Without well-designed computer networks, no sector, including education, retail, banking, technology, government, or healthcare, can exist. The network gets more sophisticated as an organisation becomes larger. Here are some important goals that need to be taken into account before beginning the difficult effort of building and implementing a computer network. Deploying a Computer Network's Goals are

1. Resource exchange

Critical assets are shared across divisions, locations, and time zones in today's globalised businesses. Customers are no longer restricted by location. Every relevant user may access hardware and data thanks to a network. Processing interdepartmental data is aided by this as well. To support top-level executive choices, the marketing team, for instance, examines consumer data and product development cycles.

2. Reliability of resource availability

Resources are available from numerous places and are not kept in inaccessible silos thanks to a network. Due to the fact that there are often many supply authorities, the dependability is quite high. In order to remain available in the event of disasters like hardware failures, important resources must be backed up across many computers.

3. Performance administration

As a business expands, its burden only becomes heavier. The system's overall performance is enhanced and this expansion is accommodated when one or more processors are added to the network. Data storage in well-designed databases may significantly reduce search and retrieve times.

4. Financial savings

It makes more sense to install processors at key locations within the system than purchasing large mainframe computers, which are a costly investment. This boosts efficiency while simultaneously reducing costs. Networks save operating time and expenses by allowing staff to access information quickly. Less money needs to be invested in IT support thanks to centralized network management.

6. Enhanced storage space

Employees that deal with large amounts of data benefit greatly from network-attached storage devices. For instance, due to the enormous volume of information the data science team analyses, no individual member needs their own data repository. Using centralised repositories increases productivity even more. The ability to expand storage capacity is essential in the modern world because organisations are receiving unprecedented amounts of client data into their systems.

7. Simplified communication and cooperation

Networks significantly affect how a firm runs on a daily basis. Employees may more easily share files, observe one another's work, sync calendars, and discuss ideas. Internal chat platforms like Slack are used by every contemporary business to provide unrestricted communication and information flow. Emails remain the official channel of contact with customers, partners, and suppliers, nevertheless.

8. Error reduction

By guaranteeing that all people involved obtain information from a single source, even if they are accessing it from various places, networks minimize mistakes. Data backups provide consistency and continuity. A large number of individuals may easily be provided with standard copies of employee and customer manuals.

9. Protected online access

Computer networks encourage flexibility, which is crucial in tumultuous times like these, when pandemics and natural calamities are wreaking havoc on the globe. Even when they are outside

the company's facilities, users may access and work on important data safely thanks to a secure network. Multiple levels of authentication are also available on mobile handheld devices connected to the network to prevent unauthorized access to the system.

Computer Network Management Techniques

The process of establishing, maintaining, and troubleshooting all aspects of a network, including its connections, software, and hardware, is known as network management. Fault management, system integration, performance management, information assurance, and (user) financial accounting are the five functional components of network management.

If not built and managed properly from the start, computer networks may swiftly grow into untamed behemoths. Here are the top 10 methods for managing a computer network correctly. Best Practices for Network Management are

1. Choose the proper topology

The way nodes are linked to one another in a network is called the topology. Depending on the architecture and needs of the firm, the topology may cause the network to speed up, slow down, or even go down. Network architects must choose the best choice before starting from scratch with a network. Several prevalent topologies include:

Bus network: Only one node is connected to each node in this network.

Ring network: A ring is formed when each node is connected to two further nodes.

Mesh network: Every node in the system has to work to link to every other node.

Star network: Several additional nodes are connected to a central node server. Data doesn't have to pass via each node, hence this is quicker.

Tree network: Nodes are placed hierarchically in this network.

2. Constantly document and update

Since the network is the foundation of operations, documentation of the network is essential. The paperwork must include the following information: • Technical equipment specs, including wires, cables, and connections

Hardware, software, and firmware all work together to activate the hardware and ensure the safe and secure transfer of data.

A written record of the rules and procedures governing network users and operators

At certain periods or during rehauls, this has to be audited. This facilitates simpler network administration as well as more efficient compliance checks.

3. Use the appropriate tools.

The topology of the network is just the first stage in creating a reliable network. The proper tools must be used in the right places to manage a highly available and dependent network. The following are network essentials:

Solutions for network monitoring A network monitoring tool provides whole network visibility. Maps that show network performance are helpful. It can trace packets, provide a detailed view of network activity, and assist in identifying abnormalities. Utilizing historical and real-time data,

more recent monitoring systems use artificial intelligence to forecast scalability needs and cyber risks.

Tools for configuration management: Numerous components that interact with one another make up a network. As a consequence, there are several setup settings to remember. This problem is solved by configuration management software, which provide network-wide configuration tools. Network administrators may use them to confirm that all compliance criteria have been met.

IP address managers: To plan, monitor, and manage information related to a network's IP addresses, larger networks must have an IP address manager (IPAM).

Security measures Networks that are carrying more sensitive loads are protected by solutions like firewalls, content filtering systems, and intrusion detection and prevention systems. Without them, no network is complete. But just getting these tools is insufficient. They must be positioned correctly inside the network as well. For instance, each network intersection requires the installation of a firewall. At the boundaries of the network, anti-DDoS devices must be installed. Depending on the architecture, load balancers must be positioned in key areas, such as in front of a cluster of database servers. The network architecture must explicitly include this.

4. Establish normal and abnormal behaviour in the network

A baseline enables administrators to understand how the network typically operates in terms of user accesses, traffic, etc. With a baseline in place, it is possible to set up alerts where they are needed to quickly identify abnormalities. It is necessary to record the typical range of behaviour at both the organisational and user levels. Sniffers, specialised collectors, wireless APs, switches, firewalls, and routers may all provide the necessary data for the baseline.

5. Guard the network from insider dangers

Bad actors are kept out of the network using intrusion prevention and firewall technology. Insider risks must also be handled, especially as hackers often use social engineering techniques to target those with network access. Operating on a least-privilege paradigm for access management and control is one method to do this. One alternative is to utilise more powerful authentication methods like single sign-on (SSO) and two-factor authentication (2FA). Employees must also get ongoing training to cope with security concerns in addition to this. Escalation procedures that are appropriate must be recorded and widely disseminated.

6. Use several providers to increase security

Even while it makes sense to just use one hardware provider, a big network benefits greatly from having a wide variety of network security technologies. The world of security is dynamic and constantly changing. Rapid hardware development also hastens the evolution of cyber threats. One vendor just cannot stay current with all dangers. Furthermore, many intrusion detection tools use various detection techniques. However, you must make sure that they are interoperable and allow for shared logging and interface. A solid combination of these technologies increases security.

7. Divide the network.

Enterprise networks may become big and cumbersome. They may be split into zones, which are logical or practical units, by segregation. Typically, switches, routers, and virtual LAN technologies are used for segregation. A separated network has the benefit of minimising the possible damage from a cyberattack and protecting vital resources. Another benefit is that it

enables networks to be classified more functionally, such as by isolating the demands of programmers from those of human resources.

8. Make use of central logging

Centralized logs are essential for getting a comprehensive picture of the network. The security team can identify suspect logins with the use of immediate log analysis, and IT admin teams may identify overworked systems in the network.

9. Think about using honeypots and honey nets

A decoy for internal and external threats, honeypots are distinct systems that seem to contain genuine operations and data. Real data is not lost as a result of any system compromise. A phone network section for the same purpose is called a honey net. This may increase network costs, but it enables the security team to keep an eye out for bad actors and make the necessary corrections.

10. Automate as much as you can

Regularly, new devices are included into systems, while outdated ones are discarded. Users and access restrictions are always changing. To prevent human mistake and insecure zombie systems from entering the network and costing money and security, all of these must be automated. Security-related automation is also essential. Automating defenses against attacks, such as banning IP addresses, cutting off connections, and collecting more data about assaults, is a smart practice.

Internetwork

A computer network that has two or more LANs, WANs, or network segments linked by devices and set up using a local addressing system is called an internetwork. Internetworking is the name given to this procedure. Internetworking is the connecting of public, private, commercial, industrial, or governmental computer networks. The internet protocol is used in internetworking. Open System Interconnection is the internetworking reference model (OSI).

Internetwork Types:

Extranet: A communication network using the internet protocol, such as the Transmission Control protocol and internet protocol, is known as an extranet. It is used to exchange information. Only users with login credentials are permitted access to the extranet. The most basic kind of internetworking is an extranet. It may fall under the MAN, WAN, or other computer network categories. A single LAN is insufficient for an extranet; at the very least, it needs one link to the outside network.

Intranet: An intranet is a private network built using internet protocol standards like the Transmission Control protocol and internet protocol. An intranet that belongs to an organisation and may only be accessed by members or employees of that organisation. The intranet's primary goal is to facilitate resource and information sharing across the organization's workforce. Working in groups and doing teleconferences are both made possible by intranets.

Benefits of an intranet

Communication is made simple and inexpensively thanks to it. A company employee may contact with another employee through email or chat.

Time-saving: Because information is communicated on the intranet immediately, it saves time.

Collaboration: The intranet's most significant benefit is its ability to foster collaboration. The data is dispersed among the company's staff members and is only accessible to authorized users.

Platform independence: This design is neutral and allows for connections to other devices of various architectures.

Cost-effective: Users of the browser may access the data and documents, and the intranet is used to disseminate duplicate copies. Costs are decreased as a result of this.

Chapter 2

NETWORK

Sachin Jain, Assistant Professor,
School of Computer & Systems Sciences, Jaipur National University, Jaipur, India,
Email Id-sachin.jain@jnujaipur.ac.in

Two or more computers connected together to share resources (such printers and CDs), exchange data, or enable electronic conversations make up a network. A network's connections to its computers may be made through cables, phone lines, radio waves, satellite, or infrared laser beams. Nodes (a group of devices) or computers may link to one another via networks. A network is made up of many computers, servers, and networking equipment that are connected to each other to share resources, such as a printer or a file server. Either wireless or cable media are used to establish the connection.

Types of Network: There are many different kinds of computer networks, ranging from a room-sized network of mobile devices (such smartphones or tablets) linked by Wi-Fi or Bluetooth to the millions of computers dispersed around the world. Some connections are made wirelessly, while others need cables. Computer networks are widely categorized based on the geographic area covered and the data transmission rate as follows:

1. Networked Personal Area (PAN)

The simplest and smallest kind of computer network is this one. PAN may range in size from a few millimeters to 30 meters. PAN networks fall into one of two categories.

- PAN networks, both wired and wireless
- PAN examples include: USB, Bluetooth, and computers (Figure 2.1).

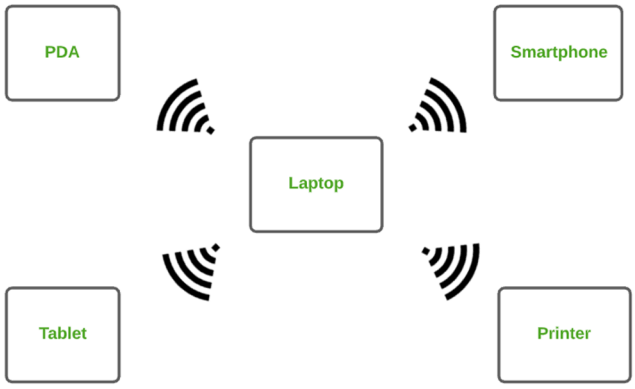


Figure 2.1: Networked Personal Area (PAN).

Benefits of PAN include: less costly, limited to a compact space, links to many devices at once

Drawbacks of PAN include: small area**,** data transmission is slowly**,** signal interference with radio.

2. Local Area Network (LANs)

A LAN is typically restricted to a single region, such as a floor, building, or other small space. Being constrained typically allows for the employment of a single transmission medium (cabling). The technology is less expensive to adopt than WAN because all of your costs are concentrated in one place, and you can typically get better speeds. They are frequently used to link computers and workstations in corporate offices and manufacturing facilities so that resources can be shared. LANs frequently employ a transmission method for connecting all of the devices. Traditional LANs operate at speeds between 10 and 100 mbps, with little delay and few mistakes. Never allow LANs to operate at a speed greater than 100 megabytes/sec (Figure 2.2).

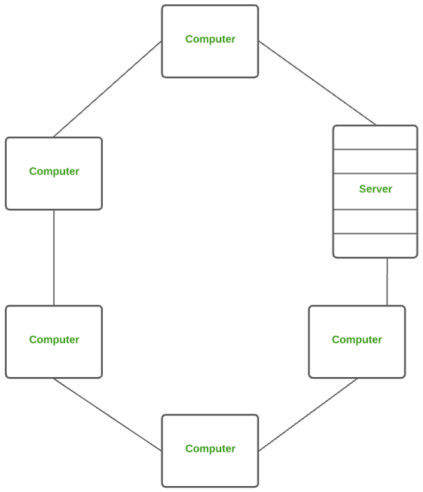


Figure 2.2: Local Area Network

LAN advantages

1. In this network, one may take on the role of a server, providing services to all the other computers, or clients. The remaining clients may utilize software that is kept on the server.
2. It is feasible to locally link every computer in a building to every other workstation even without internet connectivity.
3. With LAN, it is simple to share shared resources like printers.

LAN Disadvantages

4. The LAN administrator has the right to inspect each and every LAN user's personal data files, which is a privacy violation. Additionally, he has access to the LAN user's internet and computer use histories.
5. Data Security Threat: If the centralized data repository is not adequately protected by the LAN administrator, unauthorized users may get access to critical data of a company.
6. Limited Area: Local Area Network only covers a limited area, such as a single office, one building, or a cluster of adjacent structures.

3. Metropolitan Area Network (MANs)

Metropolitan Area Network, which often employs the same technology as LAN, is essentially a larger version of it. It might be private or public, and it could cover a city or a cluster of neighboring

business locations. On the other side, MAN is a network that spans a metropolitan area and serves as a phone service provider's backbone. A MAN does not have any switching components and only has one or two cords.

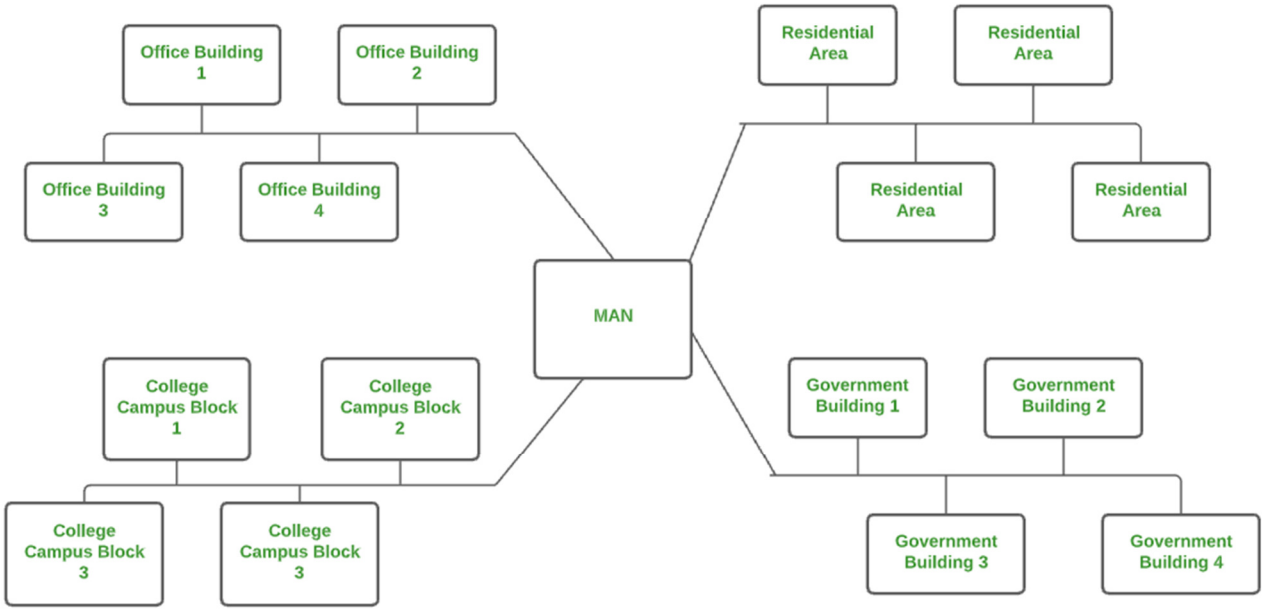


Figure 2.3: Metropolitan Area Network

Benefits of MAN

- It offers quick communication via high-speed carriers like fibre optic cables and is very effective.
- It offers better access to WANs and serves as a solid backbone for big networks.
- The dual bus employed in MAN enables simultaneous data transfer in both directions.
- A MAN often includes a complete city or a few of its blocks.

The drawbacks of MAN

- It takes more cable to link a MAN from one location to another;
- It is challenging to keep the system safe from hackers and eavesdroppers.

4. Wide Area Network (WANs)

A network that connects continents or nations is referred to as a WAN. For instance, users can access a distributed system called www from any location in the world thanks to the Internet. Switches, routers, and modems are examples of connecting equipment that the WAN connects. Typically, a LAN is privately owned by the company that uses it. Point-to-point WANs and Switched WANs are the two main types of WANs that are used nowadays (Figure 2.4).

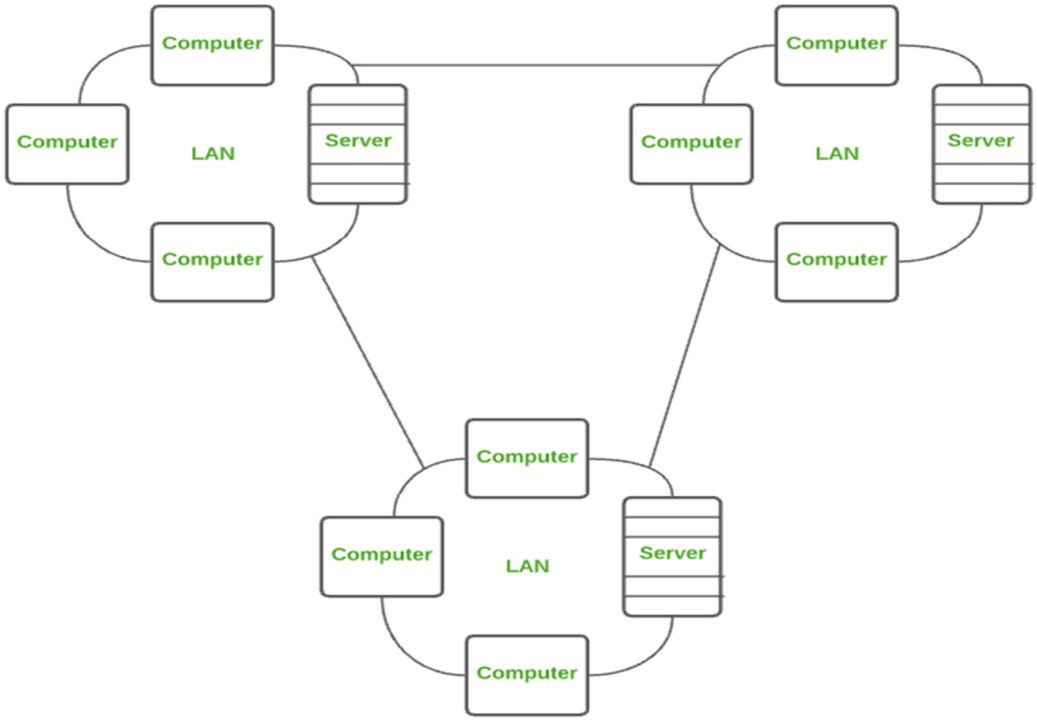


Figure 2.4: Wide Area Network

Benefits of WAN

It spans a vast geographic region and exchanges resources and software with linked workstations.

Anyone on the network may get messages extremely rapidly. These communications may also incorporate images, music, or data (called attachments).

The same data may be used by everyone on the network. By doing this, issues where some users could have older information than others are avoided.

The drawbacks of WAN

To prevent outsiders from accessing and disturbing the network, it requires a strong firewall.

After a network is installed, maintaining it is a full-time task that calls for the employment of network managers and technicians.

When multiple users may access data from other computers, security becomes a serious concern. Security against viruses and hackers increases complexity and costs

5. Wireless Local Area Network (WLAN)

WLANs are wireless and perform WAN-like tasks without wires. WLAN, which adheres to the IEEE 802.11 standard, enables wireless device connections. Laptops, cellphones, PDAs, desktop PCs, printers, and other devices are all connected through WLAN. Installing and using it are simple (Figure 2.5).

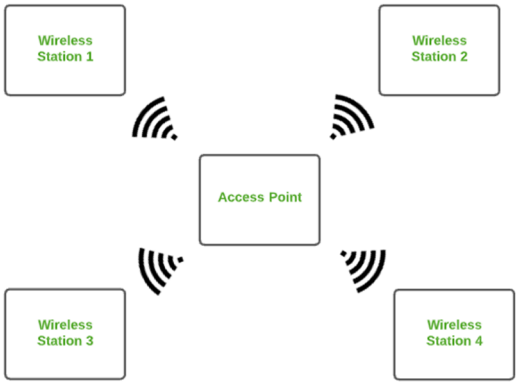


Figure 2.5: Wireless Local Area Network

The benefits of WLAN include: a reduced access area makes it more practical to utilise economically. Connectivity may be set up more easily in places where installing cables is impossible. Installation is simple since no cable configuration is required.

The drawbacks of WLAN include: It has a small coverage area. As it utilizes radio waves, it could cause interference with other devices. Data transport speed drops when more devices are linked,

6. Storage Area Network (SAN)

Small companies will benefit from this network. A SAN network is made up of several switches, storage units, and storage components that are linked to one another. LAN and WAN networks are not necessary for SAN networks (Figure 6.6).

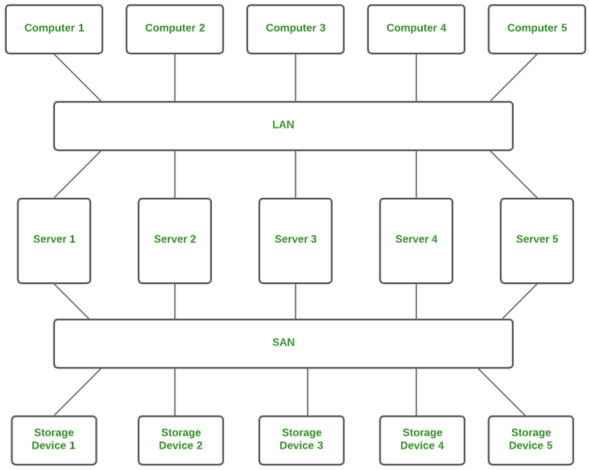


Figure 2.6: Storage Area Network

Benefits of SAN include: Inadequate Data Security. Decreases LAN bandwidth issues. Protection against dynamic failover

The drawbacks of SAN include: Expensive, Complex in nature and high maintenance

7. System-Area Network (SAN)

SAN is a collection of networks created for (server-server) mode high-speed connectivity. This quick link is established via fibre optics. Fiber channels are a few SAN examples (Figure 2.7).

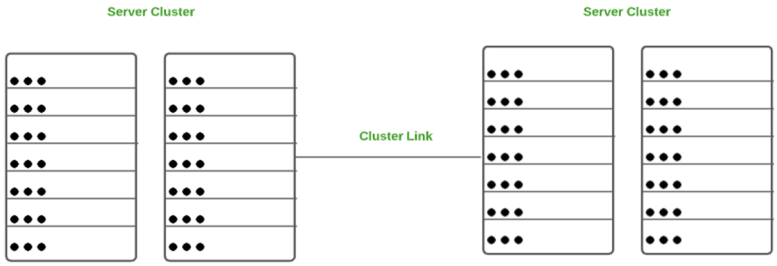


Figure 2.7: System-Area Network

Benefits of SAN include: Able to handle enormous data quantities. High-level network performance is ideal. It has a broad bandwidth.

The drawbacks of SAN include: The network is huge and complicated, making it difficult to manage. Nature's complexity. High starting price

8. Passive Optical Local Area Network (POLAN)

Similar in operation to LAN is POLAN. It is based on point-to-multipoint architecture and separates and collects optical data using optical splitters rather than electrically driven switches. Networking in medium-sized businesses, hospitals, hotels, etc. are a few examples of POLAN (Figure 2.8).

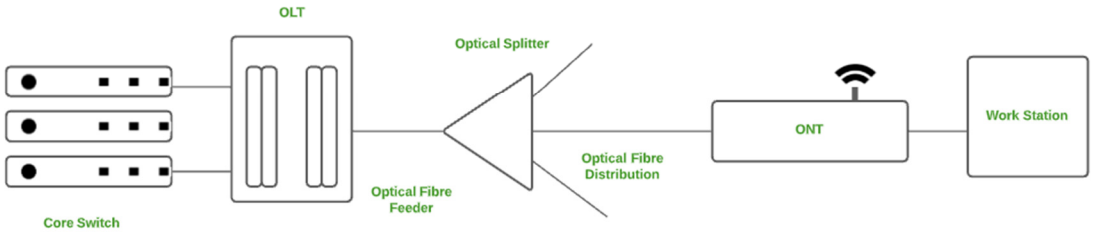


Figure 2.8: Passive Optical Local Area Network

Benefits of POLAN include: It is adaptable. Environmentally and economically friendly low energy requirements.

The drawbacks of POLAN include: difficult to identify splitters' failure. Includes costly components. Installation challenges

9. Enterprise Private Network (EPN)

Private networks known as "Enterprise Private Networks" (EPN) are often held by companies who desire to link their numerous branches in order to share computer resources. EPN examples include linking different parent business branches, facilitating communication between the headquarters and outlying offices, etc ((Figure 2.9).

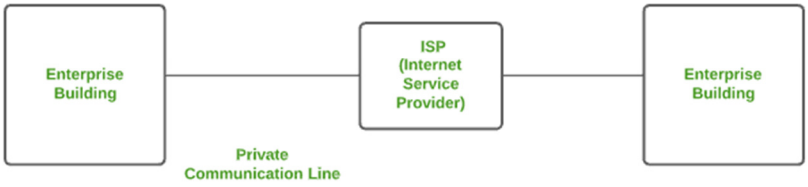


Figure 2.9: Enterprise Private Network

Benefits of EPN include: Network that is safe and secure aids in centralizing IT resources. Cost-efficient for large businesses

The drawbacks of EPN include: Costly service charges. Coverage restrictions. Arduous to set up

10. Virtual Private Network (VPN)

A virtual private network, or VPN, uses a public network to link distant people or websites. A VPN establishes a secure connection between users or websites with the same IP address using tunneling or virtual point-to-point connection technologies ((Figure 2.10).

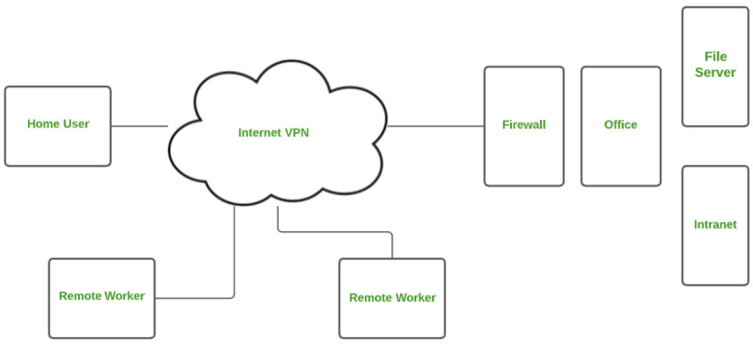


Figure 2.10: Virtual Private Network

Benefits of VPNs include: creates a fake IP address to help. Bypasses Increased online privacy thanks to geo-restrictions

VPN disadvantages include: Missing Connections. Logging data Slow connections

11. Home Area Network (HAN)

Multiple computers or peripherals used in the same household may be shared via HAN. Network address translation is performed by one device, which serves as a central hub (NAT) ((Figure 2.11). HAN includes devices like printers, gaming consoles, tablets, WiFi, etc.

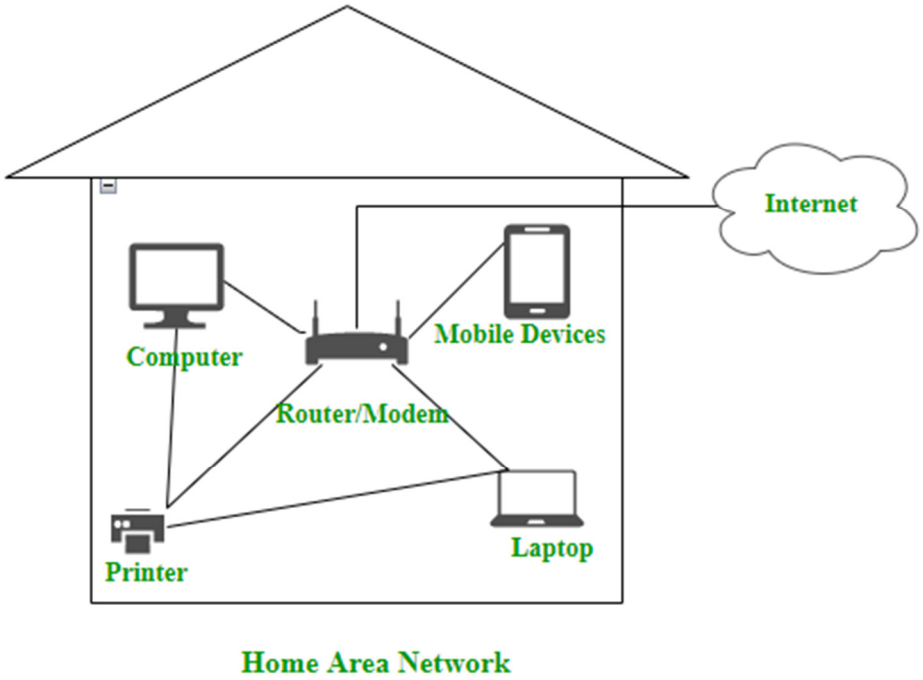


Figure 2.11: Home Area Network

Benefits of HAN include: Resource Sharing Multi-User Security.

The drawbacks of HAN include: Costly Slow Connectivity. Maximum Security

Networking Devices

All networks employ the same basic hardware to link network nodes, including Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers. Additionally, a means of linking various components of the building is required; optical fibre is less common than galvanic cable. The network devices are as follows:

Network interface card (NIC): Computer hardware that facilitates network communication between computers is known as a network card, often referred to as a network adapter or NIC (network interface card). It provides direct physical access to networking resources, and MAC addresses often act as a kind of low-level addressing. There is a unique identification for each network interface card. This information is kept on a card-attached chip (Figure 2.12).

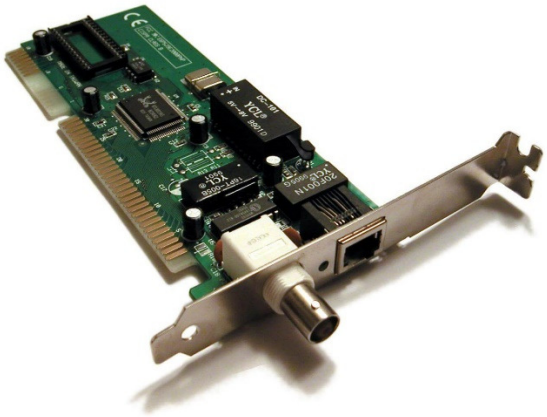


Figure 2.12: Network interface card (NIC)

Repeater: A repeater is a kind of electrical device that receives a signal, removes undesired noise from it, regenerates it, and then retransmits it at a higher power level or on the other side of an obstacle so that the signal may go further without degrading. For cable lengths more than 100 meters in certain systems, repeaters are required in the majority of twisted pair Ethernet networks. Repeaters are physics-based devices. Signals are used to transmit data through the wire. These signals have a maximum range of movement (typically 100 m). Beyond this point, signals start to deteriorate and become feeble. Original signals must be created again in these circumstances. An analogue device called a repeater uses the signals carried by the wires it is linked to function. A repeater regenerates and re-transmits the signal that is appearing on the cable (Figure 2.13).

Figure 2.13: Repeater

Hub: A hub is a piece of equipment that connects several twisted-pair or fiber-optic Ethernet components to create the appearance of a single network segment. One way to think of the gadget is as a multiport repeater. A comparatively simple broadcast device is a network hub. Hubs have no control over the traffic that travels through them; every packet that enters a port is created and disseminated out on all other ports. Every packet is sent out via every other port, which

significantly impedes the smooth flow of communication by causing packet collisions (Figure 2.14).

Figure 2.14: Hub

Bridges: Bridges broadcast data to every port, except the one on which it was received. In contrast to hubs, which duplicate messages to all ports, bridges identify which MAC addresses may be reached via certain ports. The bridge will only send traffic for that address to that port once a port and an address are linked.

Switches: In contrast to a hub, a switch just passes frames to the ports involved in the connection. It does not do this for all of the linked ports. A switch destroys the collision domain, but it presents itself as a broadcast domain. Switches rely their frame forwarding choices on MAC addresses. A network switch is used to link many computers or communication devices together, much like a hub. The switch extracts the data when it comes in the data packet's destination address and seeks it up in a database to check the destination for the package. As a result, it transmits signals to just a few devices rather than all. It is capable of simultaneously forwarding many packets. Noise- or corrupted-filled signals are not sent by a switch. Such signals are dropped, and the sender is prompted to try again. Ethernet switches are often used in homes and companies to link various devices and create LANs, as shown in Figure connect to the Internet (Figure 2.15).

Figure 2.15: Switches

Routers: Routers are networking devices that determine the best path to convey data packets across networks using headers and forwarding tables. A router is a piece of hardware used in computer networking that connects two or more networks and transfers data packets only when necessary. A router may detect if a data packet has to be carried across networks by looking at the address information in each data packet to see whether the source and destination are on the same network. Each router may create a table showing the preferred paths between any two systems on the linked networks when several routers are placed in a large collection of interconnected networks (Figure 2.16).

Figure 2.16: Routers

There are wired and wireless routers. Smartphones and other devices may get Wi-Fi connection from a wireless router. These routers often include ports that provide wired Internet connectivity. Nowadays, residential Wi-Fi routers serve as both a modem/switch and a router. These routers connect to incoming internet lines from ISPs and transform the analogue signals into digital data that can be processed by computer devices.

Gateways: A gateway may include components like protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators to ensure system compatibility. Additionally, it calls for the creation of administrative practices that both networks can agree on. A protocol translation/mapping gateway connects networks that use various network protocol technologies by performing the required protocol conversions (Figure 2.17).

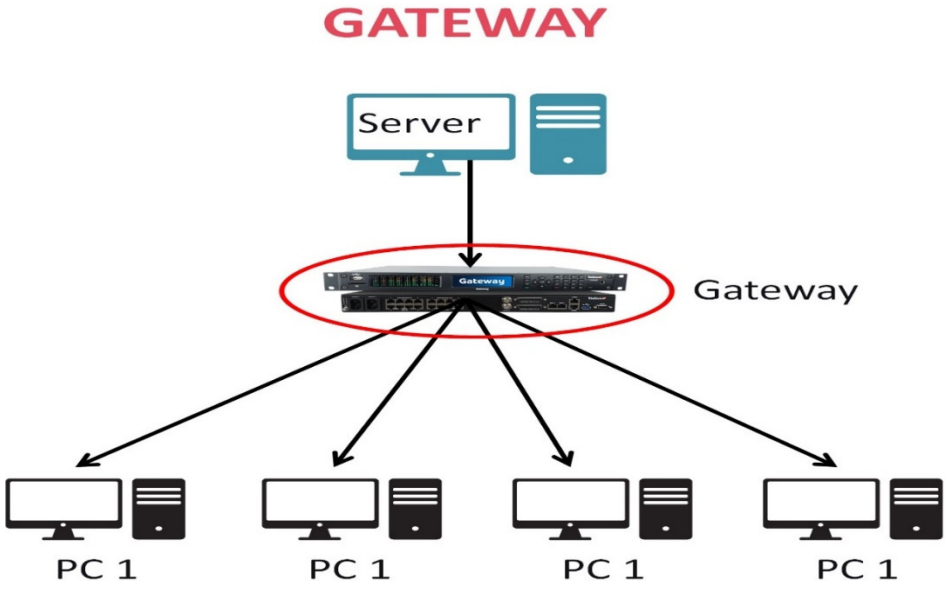


Figure 2.17: server Gateways.

Chapter 3

TOPOLOGY

Vikram Singh, Assistant Professor,
School of Computer & System Sciences, Jaipur National University, Jaipur, India,
Email Id- vikram@jnujaipur.ac.in

A network topology describes how its component parts are physically connected to one another, that a network's topology specifies its various nodes are connected to one another. A network arrangement's topology is a schematic representation that shows how different nodes (such as the sender and receiver) are connected via lines of communication. The way that nodes, connections, and other network components are connected to one another and communicate with one another is known as a network topology. A network topology can be either logical or physical; the former describes the configuration of physical devices connected to one another, while the latter shows the numerous signals present in a network or the data moving from one peripheral to another. The various types of topologies are discuses in the below.

1. P2P (Peer to Peer) Topology:

Two devices are directly attached to each other in a peer-to-peer topology. In a P2P topology, there is no distinction between a client and a server because both devices can function as either one. Since one machine may both download and upload data to another, torrent is an example of a P2P topology. These two hardware components in P2P could be two PCs, routers, switches, etc. The computer that requests the data is known as the client, and the computer that sends the requested data is known as the server. Both devices can transmit and request data in a P2P network (Figure 3.1).

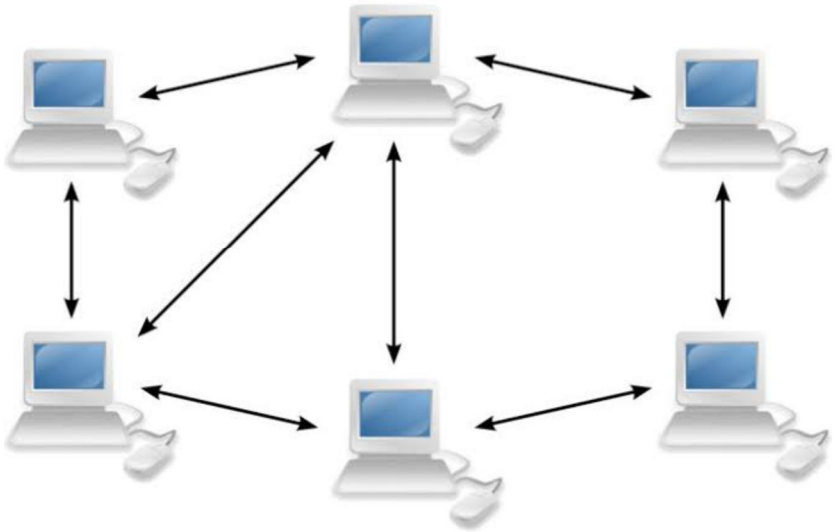


Figure 3.1:P2P (Peer to Peer) Topology

Characteristics of peer-to-peer networks: On their computers, individuals have control over who has access to the data or information. A computers (or peer's) data and resources may be directly shared between computers or made available to a group of computers. Simply setting up sharing

permissions on a computer or creating a password for things that need more restrictive access might limit access to a peer machine. While some peer-to-peer networks use a physical network to transport data or resources and a virtual network to create communication between the computers, others direct a virtual network to be superimposed on the physical network. A small number of nodes are required for the peer-to-peer network.

Benefits: Simple and rapid data and resource exchange across computers. Peer-to-peer networks nowadays are compatible with practically all types of operating systems. It is dependable to use since, unlike when a central server is unavailable, it continues to operate even when a machine fails. It offers excellent performance and lower network traffic.

Disadvantages: Because there isn't a backup on a central server, data might disappear. Because files are stored on individual computers rather than a central server, finding them might be challenging. Due to other computers accessing their data, PCs might function more slowly. Each machine need its own antivirus protection and backup, which makes maintenance more costly.

2. Bus Topology:

In a bus topology, every device utilizes a single communication wire or line. When multiple hosts are sending data at once, bus topology may have problems. Bus topology uses either CSMA/CD technology or designate one host as the Bus Master in order to solve the issue. It is one of the simple networking models where the failure of one device has no bearing on the other devices. All other gadgets, however, might stop working if the data transmission route breaks down. At both ends of the shared channel are line terminators. The data is sent via a single path, and the terminator disconnects the line when the data reaches its destination (Figure 3.2).

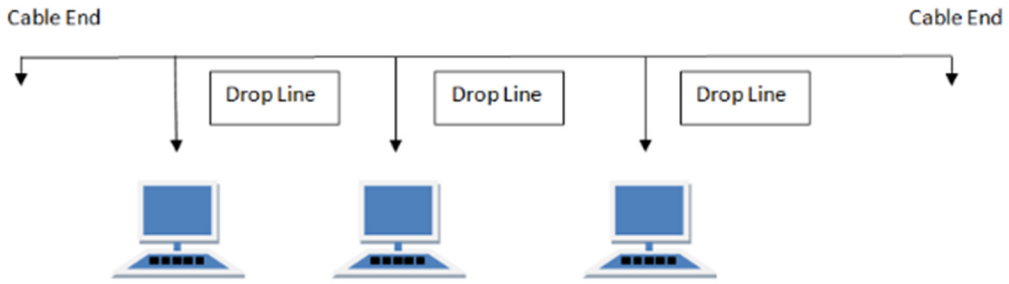


Figure 3.2: Bus Topology

Consistencies in Bus Topology: Data is only sent in one way. One cable connects all of the devices.

Benefits of a Bus Topology: It is economical. When compared to other network topologies, cable is least necessary. It used in small networks. It is simple to comprehend. Adding two wires together makes it simple to extend.

Cons of the Bus Topology: If cables break, the whole network will fail. The performance of the network declines if network traffic is high or there are more nodes. The length of cable is finite. Compared to the ring topology, it is slower.

3. Ring Topology

In a ring network, each device has precisely two neighbors with whom it can interact. It is called a ring topology because of its ring-like structure. In this topology, every computer is connected to every other computer. In this instance, the last node and the first node are linked. In this topology,

data is transferred between computers via tokens. In this architecture, all communications travel along the same path through a ring (Figure 3.3).

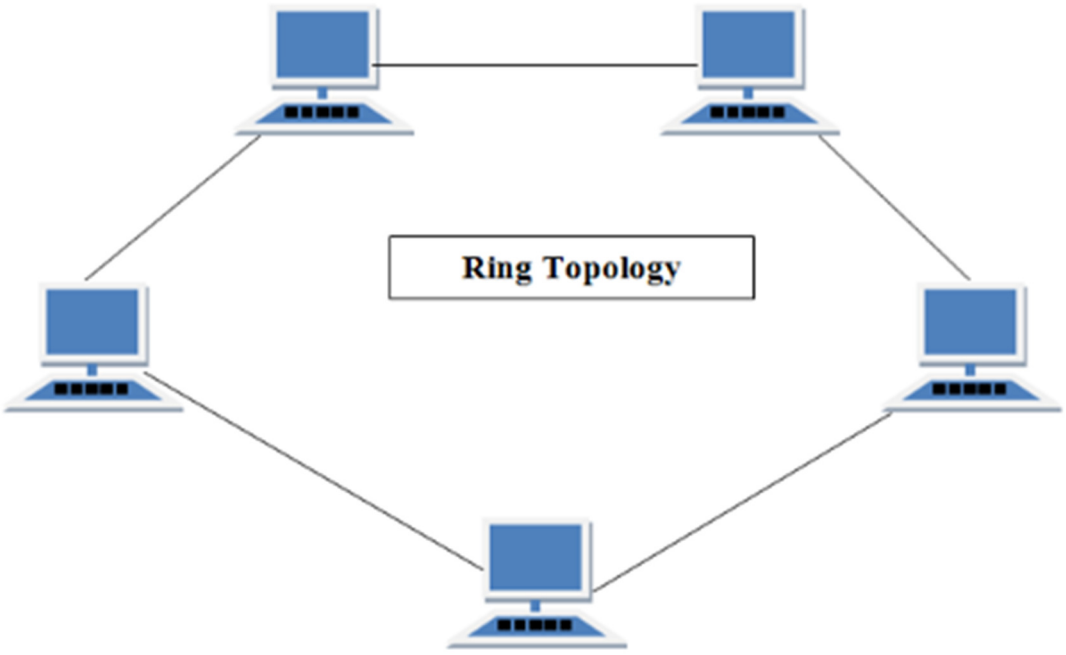


Figure 3.3: Ring Topology

Ring topology characteristics: When a ring topology has a high number of nodes, a lot of repeaters are necessary because, in order to deliver data to the final node in a ring topology with 100 nodes, the data must first transit through 99 nodes. Therefore, repeaters are utilized in the network to avoid data loss. Dual Ring Topology is a method of converting a unidirectional transmission into a bidirectional one by using two links between each Network Node. Dual Ring Topology is the formation of two ring networks with opposing data flow directions. Additionally, the second ring may serve as a fallback to keep the network operational if one ring fails. Bit by bit transfers of data take place sequentially. Each network node must pass through the sent data before it reaches its destination.

Ring topology's benefits: High traffic or the addition of new nodes have no impact on the network's ability to transfer data since only nodes with tokens are able to do so. Inexpensive to install and increase.

Negative aspects of ring topology: Ring topology is a challenging problem to solve. The network activity is disturbed when machines are added or removed. One machine failing affects the whole network.

4. Mesh Topology

A sort of network architecture known as mesh technology connects the computers using numerous redundant connections. There are various ways to move from one system to another. There is no central switch, computer, or other communications hub present. The Internet is one instance of a mesh topology. Mesh topologies are only suitable for wireless networks (Figure 3.4).

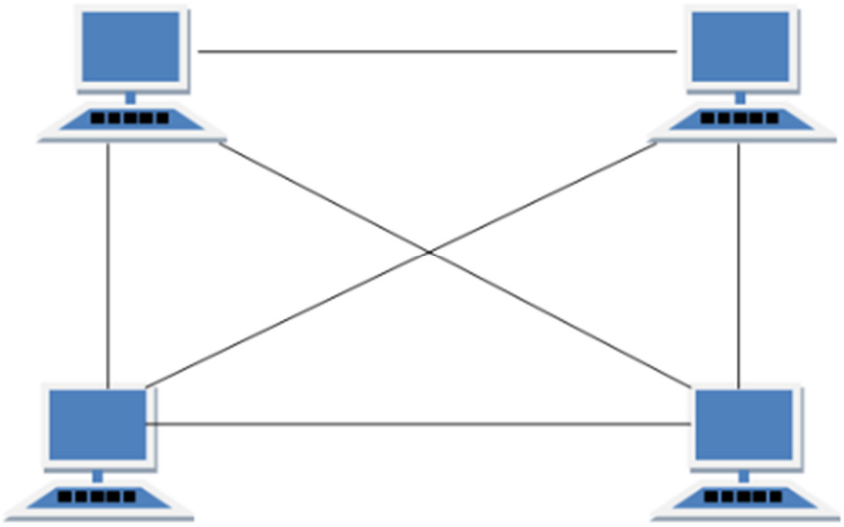


Figure 3.4: Hybrid Topology

The Mesh topology may be used with one of two methods to convey data:

Router MESH Topology: According to the needs of the network, the nodes in routing have a routing logic. Similar to routing logic, which guides data to the location via the quickest route. Or, routing logic that avoids specific nodes, etc. since it is aware of the broken connections. Even routing logic may be used to reconfigure the failing nodes.

Topology of MESH: Flooding: Flooding eliminates the need for routing logic since the identical data is sent to all network nodes. Since the network is stable, losing data is quite improbable. But it causes unnecessary network burden. The topology of mesh networks in computers

Mesh Topology Types

Partial Mesh Topology: In this topology, certain systems are linked together similarly to how mesh topology does, however some devices are only linked to two or three other systems.

Full Mesh Topology: Every node or device is linked to every other node or device in a full mesh topology.

Consistencies in Mesh Topology: completely joined. Robust. Not adaptable.

Mesh topology's benefits: A connection's individual data load may be supported. It is strong. Diagnoses of faults are simple. Offers privacy and security.

Negative aspects of mesh topology: It's challenging to install and configure. Cost of cabling is higher. Wiring in bulk is needed.

5. **Tree Topology**

Many interconnected components of a special type of structure called a tree topology are arranged like the branches of a tree. For instance, tree topologies are frequently used to organize the devices in a corporate network or the data in a database. In a tree structure, there can only be one link among any two linked nodes. Due to the fact that any network entities can only have one common link, tree topologies inherently establish a parent and child hierarchy (Figure 3.5).

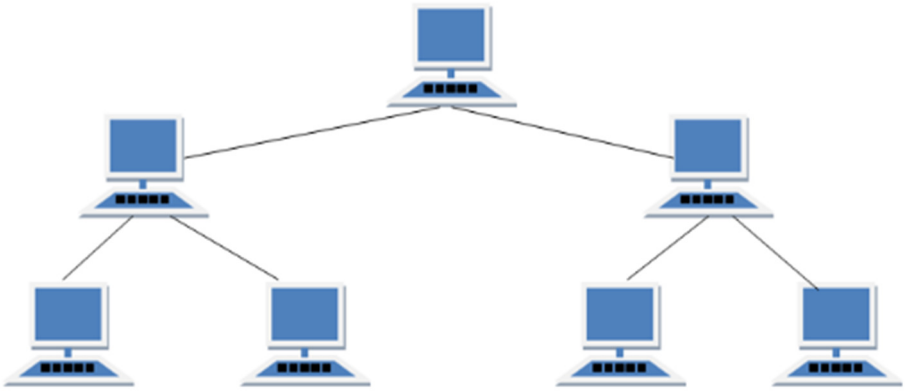


Figure 3.5: Tree Topology

Consistencies in Tree Topology: If workstations are arranged in clusters, ideal. Wide Area Network is used.

Tree topology's benefits: bus and star topologies are expanded. Node expansion is doable and simple. Simple to maintain and manage. Error detection is simple to do.

Problems with Tree Topology: strongly cabled. Costly. The difficulty of maintenance increases as nodes are added. If the central hub fails, the network will also collapse.

6. Star Topology

Each node in a star topology is connected to the central hub by a cable. This hub, which acts as the central node, is connected to all the other nodes. Unlike mesh topology, which allows for direct connections between devices, star topology necessitates the need of a hub for interaction between devices. A device must first transmit data to the hub, which then forwards it to the other device when it needs to be sent (Figure 3.6).

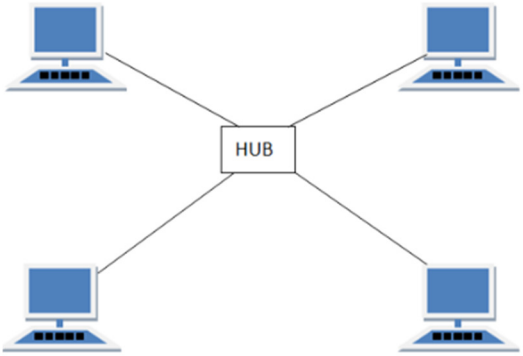


Figure 3.6: Star Topology

Consistencies in Star Topology: Each node has a separate, exclusive connection to the hub. Data flow is repeated by the hub. It may be utilized with coaxial, twisted pair, or optical fiber cables.

Benefits of the Star Topology: With few nodes and little network traffic, performance is quick. Hub may be readily updated. Simple to troubleshoot Simple to set up and change only the failing node is impacted; the other nodes continue to function normally.

Problems with Star Topology: Installation is expensive. It is costly to use. Because all nodes rely on the hub, the whole network is shut down if the hub fails. Performance is dependent on the hub's capacity, which is dependent on the hub itself.

7. Hybrid Topology

All the many topologies that have already investigated are combined in one topological technology. When the nodes have total freedom of form, it is used. This indicates that they might consist of a single topology, such as the Ring or Star topology, or they might combine several of the topologies have already seen. Each different topology is subjected to the previously discussed process (Figure 3.7).

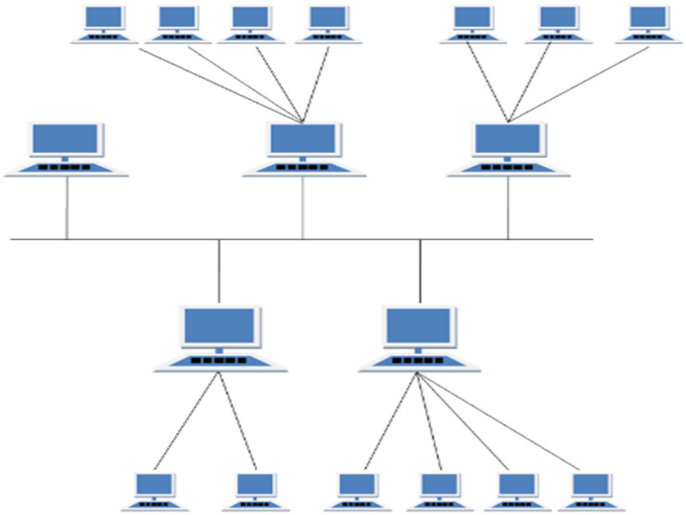


Figure 3.7: Hybrid Topology

Characteristics of Hybrid Topology: It combines two or more topologies. Carries over the benefits and drawbacks of the topologies used.

Hybrid Topology's benefits: dependable because troubleshooting errors is simple, Effective, And Scalable since size may be simply expanded. Flexible.

Issues with Hybrid Topology: Design complexity, Costly.

Networked Communication Node Identification

In order for a network device to identify the sender and receiver and choose a routing route for data transmission, each node in the network has to be individually recognized.

IP address: Device's ability to transmit or receive data packets over the internet is enabled by its IP address. It stores information about your position, enabling two-way communication via gadgets. To identify between various networks, routers, and websites on the internet, a technique is necessary. Because of this, IP addresses give the means of doing so, and they play a crucial role in how the internet functions. You'll see that the majority of IP addresses are just numerical. However, when internet use increases and the globe sees a massive increase in network users, the network engineers had to add some letters and certain addresses. A string of digits separated by periods is used to indicate an IP address (.). Four pairs are used to represent them; one example address would be 255.255.255.255; the range for each pair is 0 to 255. Creating IP addresses is not

a random process. They are created mathematically, and the IANA (Internet Assigned Numbers Authority), a division of ICANN, is responsible for assigning them. Internet Corporation for Assigned Names and Numbers, or ICANN. It is a non-profit organisation that was established in the US in 1998 with the goal of managing Internet security and making it accessible to everyone.

IP address types

Public and private addresses are depending on the network's location, with private addresses being used within networks and public addresses being used outside of networks. IP addresses often come in one of four categories:

1. Public IP Addresses

A public IP address is one where your whole network is linked to a single main address. Each connected device has the same IP address using this kind of IP address. Your ISP gives this kind of public IP address to your router.

2. Private IP Addresses

Every device that connects to your home internet network, such as laptops, tablets, and smartphones used by your family, is given a private IP address, which is a particular IP number. Additionally, it probably contains any Bluetooth devices you use, such as printers, smart gadgets like TVs, etc. You are more likely to have more private IP addresses in your house as the market for internet of things (IoT) equipment expands.

3. Dynamic IP address:

IP addresses with a dynamic nature are those that constantly change. It is transient and is given to a device each time it establishes a web connection. Dynamic IPs may be traced back to a group of IP addresses that are used by several machines. Another significant kind of internet protocol addresses is dynamic IP addresses. It has a set expiration date after which it ceases to be operational.

4. Static IP Addresses

An IP address that cannot be modified is known as a static IP address. A Dynamic Host Configuration Protocol (DHCP) server, which might change, will, nevertheless, assign a dynamic IP address. Although a static IP address is static and never changes, it may be modified as part of standard network management.

Static IP addresses are reliable since they are allocated just once and remain constant throughout time. You may get a great deal of information about a device with the aid of this kind of IP.

MAC address: Each device connected to the network is given a 12-digit hexadecimal number known as a MAC address, or media access control address. The MAC address is often located on a device's network interface card and is typically established as a distinctive identifier during device production (NIC). When attempting to find a device or running network device diagnostics, a MAC address is necessary. The MAC address is a component of the Open Systems Interconnection (OSI) model's data link layer. To assure node-to-node connectivity, each data frame's header contains the MAC addresses of the source and destination. A device may have more

than one MAC address since each network interface is given a distinct MAC address. For instance, if a laptop has both an Ethernet cable connector and integrated Wi-Fi, the system setup will display two MAC addresses.

MAC address types

MAC addresses come in three different varieties, including:

1. Unicast MAC address:

The Unicast MAC address identifies a particular network NIC. Only the interface that is allocated to a particular NIC and hence delivered to the single destination device receives a Unicast MAC address packet. If the frame is intended to only reach one destination NIC, the LSB (least significant bit) of the first octet of the address must be set to zero.

2. Multicast MAC Address:

The source device may broadcast a data frame to several other devices or NICs using a multicast MAC address. The first three bytes of the first octet of an address, or the LSB (least significant bit), in a Layer-2 (Ethernet) Multicast address are set to one and reserved for multicast addresses. The device that wishes to communicate the data in a group uses the remaining 24 bits. The prefix 01-00-5E is always the first part of the multicast address.

3. MAC address for broadcast

It stands in for all of the network's devices. Ethernet frames with one in each of the destination address's bits (FF-FF-FF-FF-FF) are referred to as broadcast addresses in broadcast MAC addresses. These bits are all the reserved broadcast addresses. Every machine in that LAN segment will receive frames with the destination MAC address FF-FF-FF-FF-FF-FF. Therefore, a source device may use the broadcast address as the destination MAC address if it wishes to deliver data to every device connected to the network.

Important distinctions between MAC addresses and IP addresses

The manufacturer of the hardware interface assigns the MAC address, but the network administrator or Internet service provider assigns the IP address (ISP).

The IP address is an address that enables you to recognize a network connection, but the MAC address is a specific hardware identification number that is allocated to a NIC (Network Interface Controller/Card).

IP address indicates how the devices are linked to the network, while Mac address specifies the identification of the device.

IP addresses, on the other hand, may be used for broadcasting or multicasting but MAC addresses cannot.

The OSI or TCP/IP reference model's Data-Link layer is where the MAC address is implemented. In contrast, the TCP/IP or OSI model's Network layer is where the IP address is implemented.

Chapter 4

NETWORK SOFTWARE ARCHITECTURE

Vikram Singh, Assistant Professor,
School of Computer & System Sciences, Jaipur National University, Jaipur, India,
Email Id- vikram@jnujaipur.ac.in

Network Architecture for Computers

Computer network architecture refers to the conception and implementation of a computer network. It is the physical and logical organisation and arrangement of various network devices (i.e., clients like PCs, desktops, laptops, mobiles, etc.) in order to meet the demands of the end user or customer. The two most well-known architectures for computer networks are:

Computer Network Types

1. The Peer-to-Peer Network

The gadgets that are directly connected to one another and have equal rights and obligations in the absence of a centralized authority are referred to as peers in this context. This design is sometimes referred to as a decentralized architecture since there isn't a single entity in charge of managing duties. Each computer has unique permissions for sharing resources, however this might pose problems if the computer holding the resource is down. Useful in settings with fewer computers and limited spaces (Figure 4.1).

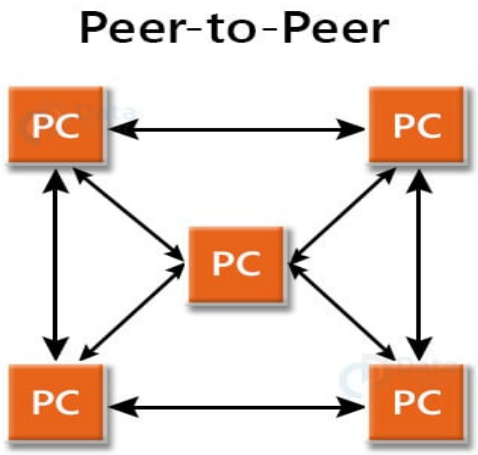


Figure 4.1: Peer-to-Peer Network

Peer-to-Peer Network Benefits: No one device serves as either a client or a server; rather, all of the devices, which also serve as clients, share the duties of servers. The lack of a centralized server makes it very easy to set up, and it also assures that all unaffected devices continue to function correctly in the event of a network loss. Each computer operates separately, making setup and maintenance easy. Peer-to-peer networks' drawbacks include: the lack of a centralized structure, which makes it difficult to maintain a backup copy of the data in case of error. Because the computers are self-managed, it has a security issue. Performance, security, and access may all experience significant problems as the number of computers on this network increases.

2. Client-Server Architecture

Because one powerful central computer handles all of the requests from the client computers, this is also known as centralized architecture. This main computer serves as a server. When the client computers need to access shared resources or shared data, they connect to the server. The server is the only place where the shared data is kept; no other computers. All of the important jobs, such network management and security, are handled by servers. Through a server, all of the clients communicate with one another (Figure 4.2).

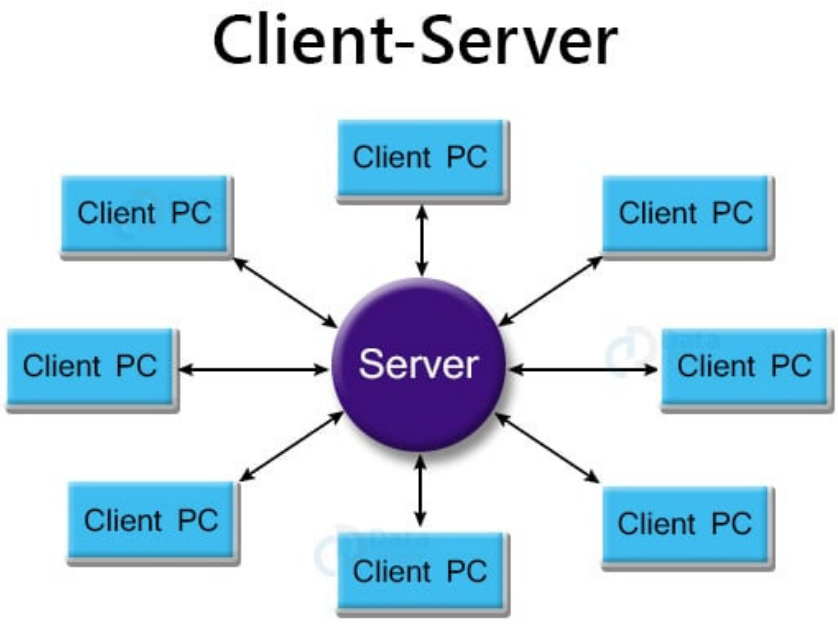


Figure 4.2: Client-Server Architecture

Client-Server Architecture Benefits: Since it is far more straightforward to add more server computers than to establish the network on each and every machine, this form of architecture is considerably easier to expand (as is the case in peer-to-peer architecture). Greatly increased network speeds. In a client/server network, security is improved since a single server controls the shared resources. Data backup is simple thanks to the centralized system. To make resources available to many users that need them, the server offers a customized Network Operating System (NOS).

Client-server architecture's drawbacks include: more prone to outages as none of the client computers can get their requests fulfilled if the server goes down. a dedicated network administrator is necessary to manage all of the resources. It costs a lot more than P2P. This is because a server with more RAM is necessary, as well as a number of networking components like hubs, routers, switches, and so on.

Additional lesser-known computer designs include:

3. Centralized Computing Architecture:

In centralized computing architecture, one powerful computer is used to support one or more low-powered systems. Under the centralized design, the nodes are not interconnected; rather, they are only linked to the server (Figure 4.3).

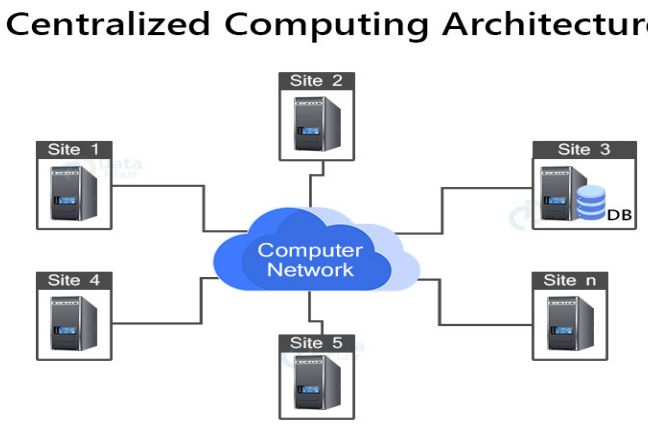


Figure 4.3: Centralized Computing Architecture

The following elements make up the centralized computing architecture: the central mainframe that does all processing. Terminals serve as input/output devices and are linked to a central computer. Using networks to connect at least two mainframe systems. Only the mainframe and never other terminals are in communication.

4. Distributed Computer Architecture:

One or more nodes, which are personal computers, are connected through a distributed architecture. It offers a wide range of features, such as network sharing, hardware sharing, and file sharing. The distributed architecture's nodes are capable of handling their own data management and relying on the network for network administration as opposed to data processing (Figure 4.4).

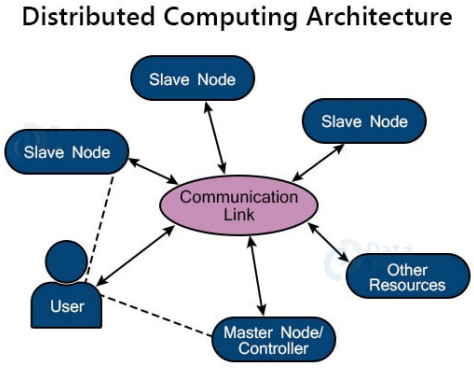


Figure 4.4: Distributed Computer Architecture

The distributed computing architecture includes the following elements: Independent performance is effective between several computers. Local task completion across several PCs. Computer networks allow for the sharing of data and services, but they do not provide processing assistance.

5. Collaborative Computing Architecture.

The architecture of collaborative computing combines centralization and decentralization. Under the collaborative paradigm, individual network members may handle the core requirements of their consumers. All database-related activities on all network nodes are monitored or managed by a database server, such as an MSSQL server or an ORACLE server, for instance. However, the model will process queries that come from outside the database.

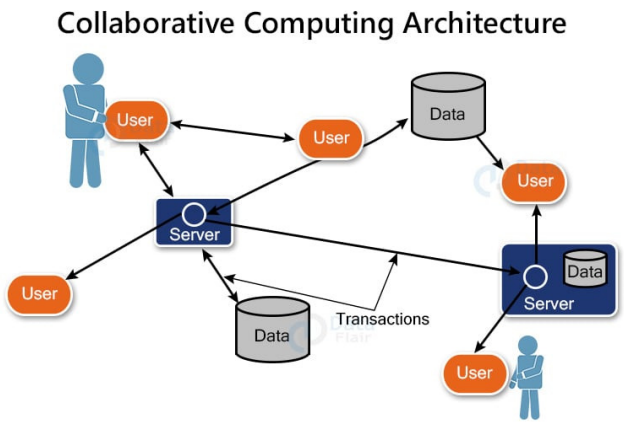


Figure 4.5: Collaborative Computing Architecture

The benefits of network architecture

Knowing the advantages and disadvantages of various network designs is essential to choose the best one for your purposes. Peer-to-peer models don't need you to spend money on a powerful server, making them often affordable and simple to set up. Theoretically, all you need to get started are some network cables or a router. It is also highly durable; even if one computer fails, the network continues to function. Additionally, the dispersed design spreads out the network load to decrease congestion risk. Peer-to-peer arrangements are more difficult to control, however. Since there is no central hub, you would have to set up security software, for example, on each machine separately. Peer-to-peer networks are hence less safe. It just takes one compromised machine to take over the network. Client/server models, on the other hand, use a centralised approach, making them simpler to administer. To increase the network's security, you may instal proxy servers, firewalls, and access restrictions. A client/server configuration is thus ideal for big networks across greater distances.

The drawback of network architecture:

The drawback of this strategy is that setting up a client/server architecture costs more money since a strong server is required to manage the network demand. Additionally, the server has to be managed by a dedicated administrator, which increases payroll. The server is a weak link in a client/server arrangement, which is its main drawback. The network stops functioning if the server crashes. As a result, security is often the strongest at and close to the server.

Layered Architecture

To divide data transmission and reception into smaller, more manageable tasks, a computer network architecture should include multiple levels. The top layer receives contributions from each lower layer, creating a vast array of services for controlling connections and powering applications. Each layer transmits and receives data from its immediately upper and lower layers, forming a network between these levels. A model's structure is made simpler by being divided into layers, which makes it simpler to spot issues when they occur. A recipient, sender, and carrier are the three main parts of a computer network model. It provides scalability and explicit interfaces, enabling communication between components. By providing services from a lower to a higher layer without mentioning how they ar implemented, it maintains layer independence. The other

layers won't be impacted by modifications to one layer. The number of layers, their purposes, and what each layer contains will vary from network to network. On the other hand, each layer's objective is to provide a services from a lower to a greater layer while concealing the details of how the operations are carried out at each layer.

Layered Computer Network Architecture's Importance:

1. The primary objective of the layered architecture is to divide the design into little components.
2. The top layer receives services from each lower layer, creating a comprehensive set of services for controlling communications and powering applications.
3. It offers modularity and accessible interfaces, enabling interactivity between components.
4. By providing services from the lowest to the highest layer without mentioning how the services are provided, it maintains layer independence. Therefore, any modifications to one layer have no impact on the other layers.
5. Each network will have a different number of layers, each with its own functions and contents. While concealing the particular of how the activities are carried out from one layer to the next, each layer's goal is to provide the resource from an upper to the lower layer [2].

Fundamental Components of Layered Architecture:

1. **Service:**

Service is a group of tasks that a layer does on behalf of a higher tier.

2. **Protocol:**

It establishes a set of guidelines that a layer utilizes to communicate with peer entities. These guidelines primarily focus on the messages' sequence and content.

3. **Interface:**

This is a channel used to transport messages from one layer to another.

The rules of a discussion are defined as a layer-n protocol in a layer-n architecture where layer n on one machine will communicate with layer n on another machine.

Characteristics of Layered Architecture:

A. In a layered architecture, layer n of one computer does not receive any data from layer n of another machine. Each layer instead communicates the data to the one immediately underneath it until the lowest layer is reached.

B. Under layer 1, there is a physical route through which genuine communication occurs.

C. In a layered architecture, unmanageable tasks are broken down into smaller, more controllable duties.

D. An interface is used to transmit data from the top layer to the lower layer. A layered design offers a clear interface, allowing for the transmission of only the most crucial information across levels. Additionally, it guarantees that the implementation of one layer may be easily modified by another.

Benefits:

A. The framework is straightforward and simple to understand and use.

B. Because each layer's function is distinct from the functions of the other levels, there is less dependence.

C. The ability to test each component separately makes testing simpler due to the distinct components.

D. Cost overheads aren't very high.

Drawbacks:

A. Scalability is challenging because the framework's structure prevents growth.

B. They can be challenging to keep up. Because the system functions as a single entity, a modification in a single layer can have an impact on the entire thing.

C. Since a layer needs the layer above it to get data, there is dependency between the layers. Processing in parallel is not feasible.

Computer Network Models

A computer network is made up of hardware and software that allows devices to communicate with one another by sending and receiving data. While software provides the sequence of commands that employ the hardware instruments for data transfer, hardware plays the job of demonstrating the physical equipment needed to send and receive data. A straightforward data transmission involves a number of processes at different computer network layers. Two models of computer networks form the foundation of the entire data transmission process.

Types of Computer Network Model

The entire data transmission process is based on two computer network models.

A. Open Systems Interconnection (OSI) Model

B. Transmission Control Protocol/Internet Protocol (TCP/IP) Model

Open Systems Interconnection (OSI) Model

The reference model known as OSI, or Open System Interconnection, explains how data from one computer's software program travels over a physical media to another computer's software application. Each of the seven OSI levels carries out a specific network function. In 1984, the International Organization for Standardization (ISO) created the OSI model, which is currently regarded as an architectural framework for inter-computer interactions. The OSI model breaks down the entire process into seven more manageable, subtasks. Each layer has a certain task assigned to it. Every layer is self-contained, allowing each layer's given work to be completed individually (Figure 4.6).

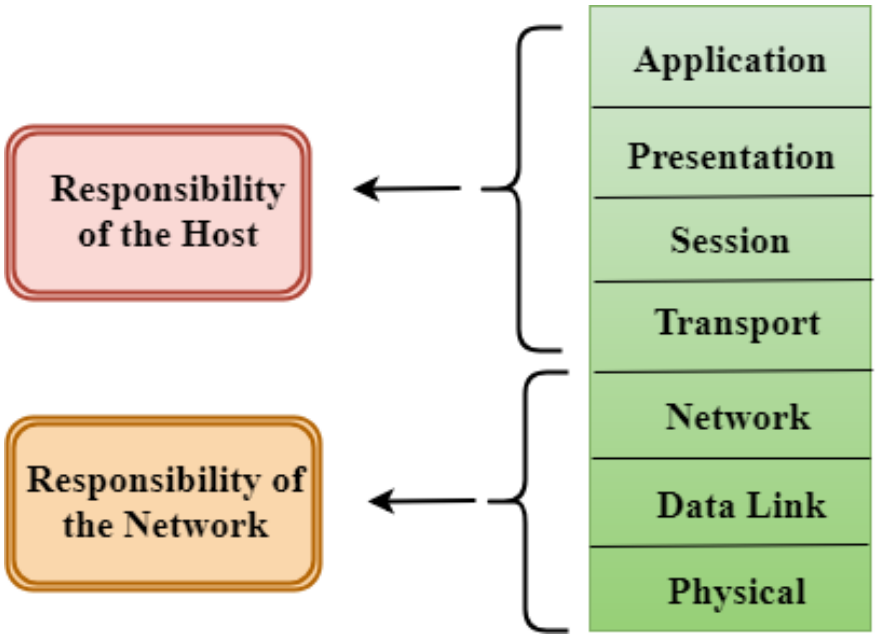


Figure 4.6: Open Systems Interconnection (OSI) Model

Physical Layer

This layer provides information regarding the hardware, wiring, power output, heart rate, and other factors.

Data-Link Layer

Information reading and writing from and onto the line is handled by the Data Link Layer. Identifying link issues occurs at this layer.

Network Layer

This layer manages of allocating addresses and contacting hosts in a network in a specific way.

Transport Layer:

End-to-end delivery among hosts is handled by the Transport Layer.

Session Layer

This layer keeps remote hosts' sessions active. For instance, after completing user/password verification, the remote host keeps this session for some time and does not request verification again during that time.

Presentation Layer

This layer specifies how information in the native format of the remote host should be displayed on the host.

Application Layer

This layer is in charge of giving program users an interface. These protocols communicate with the user directly at this layer

OSI Model Benefits in Computer Network Models:

A. The OSI model is simple and convenient to use since each layer has a distinct structure and function.
B. It serves as a general-purpose reference model and is applicable to data communication.
C. Services that require and don't require connections are supported.
D. Any type of host, hardware, or software can connect to any sort of device.

OSI Model Drawbacks in Computer Network Models:

A. This concept was replaced by the TCP/IP Internet Model since it couldn't fit protocols.
B. Less useful than other layers, the session and presentation levels do not offer high-end functionality.
C. Services that require and don't require connections are supported.
D. Any type of host, hardware, or software can connect to any sort of device [4].

- **Transmission Control Protocol/Internet Protocol (TCP/IP) Model**

The TCP/IP architecture serves as the foundation for the network of networks known as the Internet. The TCP/IP Protocol Set is another name for it as a result. It has four layers and was created especially for the internet [5].

- **Application Layer:**

The protocol that enables network communication between users is specified at the application layer. Among them are HTTP and FTP.

- **Transmission Layer:**

The Transport Layer explains how information should be transferred between hosts. The most crucial protocol at this tier is the Transmission Control Protocol (TCP). This layer is responsible of end-to-end delivery and ensures that data is delivered between hosts in the proper order.

- **Internet Layer:**

On this layer, the Internet Protocol (IP) functions. Host addressing and identification are made simpler by this layer. The routing is done by this layer.

- **Internet Protocol Layer:**

This layer provides a way to send and receive actual data.

This layer is independently of the hardware and underlying network architecture, than its OSI Model equivalent.

Router

A router can connect one or even more packet-switched networks or sub networks. It controls traffic between several networks and enables multiple devices to share an Internet connection by transmitting data packets to their intended IP addresses. Despite the fact that routers come in a vast variety, most of them transfer data among LANs (local area networks) and WANs (wide area networks). A LAN is a group of connected devices that are restricted to a specific area. A LAN typically only requires one router. A WAN, in contrast, consists of a huge network that is scattered

over a sizable geographic area. large firms and corporations having several locations across the country.

Types of Router

Depending on the functionality of the router or the number of devices that need to be connected, routers come in a wide range of sizes. A router typically belongs to one of the following groups:

Core router:

These routers transfer a lot of data packets from across network and are widely utilized by large corporations, ISPs, and cloud service providers. Sometimes, the "Internet backbone" is referred to as these central routers. They are often found working in the "core" of a network, hence their name.

Border router:

An edge router is simply the router that communicates with core routers and external networks, and it frequently located at the "edge" of a network. These networks broadcast and receive data from other LANs and WANs using the Border Gateway Protocol (BGP).

Wired router:

LAN connections for devices whose primary networking connectivity is Ethernet are frequently made possible via the Ethernet ports found on these routers. An older wired router will be used by desktop computers without wireless capability and other networking hardware in data centers.

Wireless router:

These routers have a wireless radio that, like a wired router, converts the digital impulses into radio waves. Data is typically wirelessly sent from a laptop or even other portable device to one of these routers. Wireless access point help transport data to a wired router before it is provided via the internet within a large enterprise.

Features of Router

A. A router functions at layer three (the network layer) of the OSI model, where it connects to adjacent devices using IP addresses and sub networks.
B. A router's several ports, including its fast Ethernet, gigabit, and STM link connections, provide high-speed internet connectivity.
C. It gives consumers the option to modify the network port to suit their needs.
D. The crucial components of routers are the central processing unit (CPU), interface card, non-volatile RAM, flash memory, console, RAM, and network.
E. Routers can route traffic in a large networking system by treating the sub-network as a whole network.
F. Data encapsulation and de capsulation, as well as hazardous interference filtering, are tasks carried out by routers.
G. Routers provide redundancy since they continuously run in master and slave mode.
H. Users can connect too many LAN and WAN networks thanks to it.
I. Additionally, a router creates several paths for the information to follow.

Application of the Router:

A router is used in many different contexts, including:

A. Routers are used to connect hardware equipment to remote location networks such SGSN, MGW, BSC, IN, and other servers.
B. Because it provides rapid data transmission and makes use of high STM links for connectivity, it is employed in both wired and wireless communication.
C. Access controls are offered by routers. It can be configured so that just a small number of people have full access, while everyone else can only access the data that has been defined for them.
D. Routers are also used by software testers for WAN communications. An organization might, for instance, have its executive in Pune or Bangalore and its software manager in Agra. The executive is then offered a chance to share his software tools and other programs with the management by employing WAN infrastructure to connecting their PCs to the router.
E. By setting up VPN in routers, the client-server strategy, which allows access of the internet, videos, information, audio, and hardware resources, may be used in wireless networks.

A protocol is a collection of guidelines that largely defines the language that gadgets will speak when they communicate. A wide variety of protocols are widely used in networking, and they are often implemented at different tiers. It offers a network connectivity where messages are exchanged via a certain procedure. When communication is straightforward, we can only employ one straightforward protocol. When communication is complicated, we must split the work into layers and adhere to a protocol at each level. This process is known as protocol layering. We can isolate the services from the implementation thanks to this layering. The lower layer must provide a set of services to each layer, and the top layer must receive the services from the lower layer. Any adjustment made to one layer won't have an impact on the others.

Simple Layered Architecture Elements

The following are the fundamental components of the layered architecture: Services are a group of tasks or activities sent from a lower layer to a higher tier. A protocol is a set of guidelines that a layer utilizes to communicate with a peer entity. It is worried about both the messages' substance and chronological arrangement. This is the passageway via which messages are sent from one layer to another.

Reasons: The following justifies the use of layered protocols: In order to prevent changes in one layer from affecting a neighboring one, layering of protocols creates clearly defined interfaces between the levels. A network's protocols are very complex, and layering their architecture makes it easier to implement them.

The following are layered protocol's benefits: Protocols that function at a certain layer include stated information about how they work and a clear interface to the layers above and below, which aids in protocol style. Foster's rivalry as a result of the compatibility of goods from several manufacturers. Stops changes in technology or capabilities in one layer from affecting layers above and below. Explains networking capabilities and functionalities in everyday words.

The following are layered protocol drawbacks: The primary drawbacks of layered systems are the cost in processing and message headers brought on by the separation of concerns in the levels. The overhead of such boundaries is often more than the computation being done since a message must generally transit through numerous protocol layers. Because the upper-level layers are unable to

observe what is happening in the lower levels, an application is unable to identify exactly where a problem is in a network connection or what the issue is. In order to adjust the transfer system (such as managing windowing, header compression, CRC/parity checking, etc.) or define routing, the higher-level layers must depend on the operation of the lower levels and are unable to provide alternatives when there are problems.

Chapter 5

PHYSICAL LAYER

Ram Lal Yadav, Assistant Professor,
School of Computer & Systems Sciences, Jaipur National University, Jaipur, India,
Email Id-ramlal.yadav@jnujaipur.ac.in

The physical layer of the OSI reference model is the bottom layer. It is in charge of transmitting unprocessed information over a network from one machine to another. It is concerned mainly with the establishment of the physical link to the internet and does not engage with the data contained in these bits. It functions as an interface between real hardware and signaling systems. It is in charge of creating, maintaining, and deactivation the physical connection between two separate computer devices in a network. It is the sole layer of the OSI network architecture that concerns with physical connectivity. This layer specifies the hardware components, topologies, wiring, transmission techniques, frequencies, and pulse types used it to represent binary signals, among other things.

Performing Operations by Physical Layer:

Here are some essential and fundamental tasks carried out by the Physical Layer of the OSI Model:

1. Data rate is maintained by the physical layer.
2. It executes bit synchronization.
3. It aids in choosing a transmission medium.
4. It facilitates the choice of Physical Topology.
5. It aids in making choices about Physical Medium and Interface.
6. It offers two different configuration options. Configuration options include Point to Point and Multi-Point.
7. It offers a connection point between hardware such as computers and the transmission medium.
8. It has a bit-sized protocol data unit.
9. Devices like hubs, Ethernet, etc. are utilized in this.
10. It offers a crucial feature known as modulate, which is the method of transforming data into radio signals by including the data into an optical or electrical sensory signal.
11. Additionally, it offers a switching mechanism by which packets of data can be forwarded from the sender port to the top destination port.

DIGITAL TRANSMISSION

Digital transmission is the process of transmitting information as digital signals via a physical communications medium. Transmission of signals that alternate discretely over time between two measurements of a physical variable, one of which corresponds to the binary number 0 and the other to 1. For the transmission of binary data through a communication medium like a network cable or a telecommunications link, digital signals use discrete values [2].

1. Digital-to-Digital Conversion

Digital-to-digital encoding is the expression of digital information by a digital signal. Digital-to-digital encryption is the process of transforming a computer's output of binary 1s and 0s into a sequence of output pulse that may be conveyed across a network.

2. Analog-to-Digital Conversion

Analog-to-digital conversion is the process of digitizing an analogue signal. If a human delivers a voice as an analogue signal, if the requirement to digitalize the signal to make it less susceptible to noise. In order for an analogue message to be represented in a digital stream, fewer values must be included. The information included in a sustained wave form is turned into digital pulses during the analog-to-digital conversion process.

Transmission Media

A communication channel known as "transmission media" is used to send information from a source or transmitter to a receiver. It is a physical way for electromagnetic signals to transport data. Through LAN, information is transmitted in the form of bits. It can regulate the transmission of telecommunications signals. Waves that are appropriate for the selected medium are then given signals. The physical layer that controls them is above these media.

The following elements must be taken into account while constructing the transmission media:

1. When all other elements are held constant, the bandwidth of a media determines how quickly data is sent from a signal.
2. When there is a transmission degradation, the data transmission is not the same as the one that was delivered. Signal quality will be destroyed owing to transmission problems.
3. The process of disturbing a signal as it flows over a transmission media due to the addition of an unwanted signal is known as interference.

Types of transmission Media

There are 2 types of transmission media:

1. Guided

Physical linkages are used to direct and constrain the signals that are being transmitted along a certain path. Additionally, it is known as wired or bounded communication medium. The features of the guided media Fast and Secure, used while travelling a relatively short distance.

Twisted Pair Cable:

The most common kind of transmission medium cable is twisted pair. It is made up of two separate, insulated conductor wires that have been wound around one another. Usually, many such pairs are gathered together in a protective sheath.

Twisted-pair cables come in two main categories:

Unshielded Twisted Pair: Offers a fast connection. The least expensive. Easy to set up

Possible external intervention exists.

It performs less well and has a lesser capacity than Shielded Twisted Pair.

Categories for Unshielded Twisted Pair:

Category 1: Low-speed telephone data transfer uses category 1 twisted pair wires.

Category 2: The maximum bandwidth for category 2 is 4Mbps.

Category 3: The highest bandwidth available is 16Mbps.

Category 4: It has a 20 Mbps maximum bandwidth. It is hence appropriate for long-distance communication.

Category 5: 200 Mbps is the highest bandwidth available

Advantages: It is affordable. Installing an unshielded twisted pair is easy.

It works well with high-speed LAN.

Disadvantages: This cable is used in connection solutions for short distances due to attenuation.

Shielded Twisted Pair: Manufacturing and installation both provide certain difficulties.

Pricier. It operates more effectively at higher data rates as compared to Unshielded Twisted Pair. Faster compared to it.

Characteristics: Insulated twisted pair cable is not particularly costly or inexpensive.

It attenuates more strongly. A higher data transmission rate is possible because to its shielding.

Advantages: Installation of STP is easy. Compared to unshielded twisted pair cable, it can carry more weight. Higher transmission rate.

Disadvantages: Compared to UTP and coaxial cable, it is more expensive. It attenuates at a faster pace.

Applications: Telephony Local Area Networks

Coaxial Cable: It has two parallel conductors, each with its own insulated protective cover, and an outer plastic covering. It has two modes of operation: baseband and broadband.

Applications: Cable TV and analogue television networks often employ coaxial connections.

i. Benefits: a lot of bandwidth. Less sensitive to sound. Inexpensive to install. Simple to update and install.

ii. Negative aspects: The whole network might go down if the cable fails.

c. **Fiber Optic Cable**: It operates on the idea of light reflection via a glass or plastic core. The core is enclosed by the cladding, which is a thinner layer of glass or plastic. In large-volume data transport, it is useful. The cable may have a unidirectional or bidirectional configuration.

Benefits: it has no metal, thus it cannot rust or corrode. It can send data at a fast rate of speed. It allows for high bandwidth. There is less attenuation of the signal. The ability to withstand electromagnetic interference

ii. Negative aspects: It is challenging to install and maintain. Both costly and delicate.

iii. The optical fibre cable's components:

An optical fiber's core is a thin strand of glass or plastic. The portion of the fibre that transmits light is called the core. The size of the core affects how much light is transmitted into the fibre.

Glass that is layered in a concentric pattern is referred to as cladding. The cladding's main purpose is to reduce the refractive index at the core-interface, which causes reflection within the core and permits light waves to flow through the fibre. A jacket is a particular kind of plastic protective covering. A jacket's main purposes are to maintain fibre strength, absorb stress, and increase fibre protection.

Fibre optic cable uses include: Boundary Networks Several cable networks and local area networks.

Strapline cable: This kind of waveguide, sometimes referred to as a strapline cable, transmits high-frequency waves by employing a conducting material.

To provide EMI protection, this conductive material is sandwiched between two ground plane layers that are often short-circuited.

Microstripline cable: In a microstripline cable, the ground plane and the conducting material are separated by a layer of dielectric material.

Power Lines: Power line communication is a Layer-1 (Physical Layer) technique that sends data messages across power wires (PLC). In a PLC, modulated data is sent through the wires. The receiver on the other end demodulates and interprets the data.

Magnetic Media: Even before networking, moving data physically from one station to another via storage media was one of the most practical methods to move data from one computer to another. When there is a lot of data to convey, magnetic media might be helpful.

2. Unguided Transmission Media:

Transmitter and receiver are not physically connected. Although they are used across greater distances, these transmission media have become less safe than guided media. The features of the unguided media are that less secure, airborne signal transmission, and wide application range**.** They are also referred to as wireless or unrestricted transmission medium.

Unguided media have certain characteristics: Secure compared to directed media. It used across greater distances.

Different Forms of Unguided Transmission Media

Infrared: Infrared waves are employed when extremely close-range communication is required. However, they are unable to pass through any barriers or walls that are in the signal's path. The range of frequency is 300 GHz to 400 THz.

Infrared transmission characteristics: Because of its wide bandwidth, the data rate will be quite high. The walls are impermeable to infrared rays. Because of this, adjacent rooms cannot interfere with infrared communication taking place in one room. The transmission of information through infrared technology is safer and less disruptive. Infrared communication outside the building is unreliable due to interference from the sun's beams.

Advantages: inexpensive and economical. A lot of bandwidth. Simple to install. It can to be used without a licence.

Disadvantages: it cannot pass obstacles. There is no way to communicate across such distances.

Applications: Intermittent communication. Interaction between computers, keyboards, and mice.

Radio waves: extremely easily generated and widely utilised. These waves may readily travel past barriers. For the transmitting station and the receiving station, respectively, there are two antennas employed (these antennas need not be aligned). The range of frequency is 3 kHz to 1 GHz.

Radio transmission benefits: The main applications of radio transmission are mobile phones and wide area networks. Radio waves have the ability to cross obstacles and reach large areas. a quicker transfer rate.

Disadvantages: Because of radio spectrum regulation, it is costly to purchase. It cannot very effectively penetrate substance. The curvature of the planet prevents travel over the horizon.

Applications: both AM and FM radio. Cellular phones without cords

Microwaves: Since the transmission is line-of-sight, both the sending and receiving antennas must be positioned appropriately. The signal's range is proportional to the height of the antenna. These are mostly used for transmitting television and mobile phone communications. 1 GHz to 300 GHz is the frequency range.

Features of a microwave: Range of frequencies: 4 to 23 GHz. Broadband: It offers bandwidths between 1 and 10 Mbps.

Short-distance communication: Appropriate for short-distance communication.

Long range: It is expensive since a bigger tower is needed for a greater range.

Attenuation: Attenuation is the weakening of a signal. Attenuation may be altered by antenna size.

The benefit of microwave communication is: Compared to cable, microwave transmission is less expensive. Since the installation of cables does not require the purchase of land, it is not necessary to do so. In locations where running wires would be challenging, microwaves are more practical.

It is possible to communicate across oceans via microwave transmission.

Microwave transmission's drawbacks: Communications become risky when someone is listening in on them. The signal in the air is susceptible to capture by any rogue user using its own antenna.

Signal that is out of phase: The signal may change in phase. Weather: Any kind of environmental disruption might skew the signal. The amount of available bandwidth has decreased.

Applications; Cell phones Satellite Networks Cell phones

Light Transmission: The most potent electromagnetic spectrum that may be used for data transmission is light, or optical signaling. To achieve this, LASER is used. Light tends to go in a straight line because of its frequency of motion. The transmitter and receiver must thus be in a straight line of sight. The laser and photo detector must be placed at both ends of the link since laser transmission is unidirectional. Laser beams are generally 1mm wide, making it difficult to precisely align two distant receivers that are each pointing towards the laser's source.

Consider these variables while selecting your transmission medium:

1. Bandwidth: Assuming all other factors remain constant, a signal's data transmission rate increases with increasing medium bandwidth.

2. Transmission impairment: When there is a difference between the received signal and the sending signal as a result of transmission impairment. The signal quality will be compromised due to transmission issues.

3. Interference: The act of disrupting a signal as it passes across a communication channel due to the addition of an unwanted signal is known as interference.

4. Radiation: We must choose a medium with a low signal leakage rate.

5. Attenuation: In order to minimize signal loss over long distances, a transmission medium must also be used.

6. Noise Absorption: If the medium is not adequately insulated from such interference, external noise may have an influence on it.

Causes of Transmission Impairment:

1. Attenuation: Attenuation is the term for the energy loss that happens as a consequence of the signal's strength waning over longer distances.

2. Distortion: When the signal's shape changes, distortion results. We examine this kind of distortion using a variety of signals with different frequencies. Delay distortion occurs as a consequence of the fact that each frequency component has its own propagation speed and so arrives at different times.

3. Noise: Data is contaminated by an unwanted signal during transmission, creating noise.

Switching mode

A switching is networking equipment that functions at the OSI model's second layer (the data-link layer). Their primary function is to join various network nodes together and enable packet switching for data transmission. In a switch, all data is transferred across the local network. Because it has many ports through which PCs are connected to the network, it is also known as a multi-port network bridge. A switch's primary function is to execute essential checks, including looking up addresses for both destination and source computers and forwarding frames to the appropriate device**.**

Switching Technique

Switched communication networks convey data from a source to a destination through a number of intermediary nodes. The method through which node control or change data to send it between particular places on a network is known as switching.

Transmission Mode

The process by which information is sent by one device to the next is referred to as a transmission mode. Communication mode is another name for transmission mode. The transmission medium offers a direction for each communication channel called the transmission mode. Data transmission between two devices via a communication channel that comprises a copper wires, optical fiber, wireless channels, and other storage media is referred to as transmission mode or communication mode. Electromagnetic waves carry the data during transmission. There are several methods for transmitting data, using digital modulation to transfer the message as a series of pulses. In a computer networking system, the data transmission method was originally established in the 1940s with modems, followed by LANs, WANs, repeaters, and some other networking technologies.'

Types of Transmission Mode:

The phrase "transmission modes" refers to the exchange of information between two communication devices across a channel of interaction that specifies the direction of the information flow. There are primarily three types in a computer networking system.

1. Simplex
2. Half-Duplex
3. Full Duplex

1. Simplex

Simplex is a type of data transfer where communication is unidirectional and data can only go in one direction. A transmitter can only transmit information in this mode; they are unable to receive it. Similar to a sender, a receiver can only receive data no sending is allowed. Because we cannot do two-way communication between both the receiver and sender in this method, this transmission mode is not very common. It is primarily utilized in the business world for sales that don't need a response. It's like a one-way street, really. The transmission of radio and television, a keyboard and mouse, etc.

Example: A simplex transmission example where the keyboard operates as the inputs and the computer as the outputs is communication among a computer and a keyboard.

2. Half-Duplex

Half-duplex mode of transmission is used in computing networks where there is a two-way flow of data or a two-direction flow of data from the transmitter to the receiver, but just one at a time. In this type of transmission, communication can happen in both ways, but not concurrently between the connected devices. Due to the radio stations' ability to both send and receive data, and the simultaneous display of each communicated character on the screen, the channel of interaction can be reversed. Example: The ideal use of half-duplex communication is a walkie-talkie. When one person is speaking from one end of a walkie-talkie, another person is listening from the other end. Following a pause, the first individual but at the other end listening as the second person speaks. As a result of the sound distortion caused by simultaneous speech, neither the transmitter nor the receiver will be able to understand what is being said.

3. Full Duplex

In computing networks, the full duplex mode of communication is employed when there is continuous information flow from transmitter to receiver in both directions. Communication takes place in both directions through a communication link that necessitates two wires in this form of transmission, where the system capability is shared between the two devices. There are two simplex channels in the Full Duplex mode. While traffic is moving in one direction on one channel, it is moving in the opposite direction on the other. When two-way communication is required, the full duplex mode is employed. Example: The telephone is the most typical example of this kind of transmission. Both speakers and listeners are able to speak and listen at the same time when two people are speaking or communicating over the phone utilizing a telephone line (Table 5.1).

Table 5.1 Comparison between simplex, half duplex and full duplex.

S. No.	Features	Simplex	Half Duplex	Full Duplex
1.	Communication's Direction	Communication in simplex mode is unidirectional.	Half-duplex mode allows for interconnection, but only in one direction at the same time.	The communication is two-way when it is in full-duplex mode.

2.	Send/Receive	Depending on the device, it can either send data but not receive it or receive data but not send it.	Both devices have the ability to send and receive data, but only one at a time.	Data can be sent and received concurrently by both devices.
3.	Performance	Half-duplex mode operates more efficiently than simplex mode.	Full-duplex mode offers superior performance to half-duplex mode	Full-duplex mode performs better than simplex and half-duplex mode because it uses the communication channel's maximum capability.
4.	Benefits	To transmit data with a single control, the channel's entire range is used.	Therefore, it can be employed when the transmission requires the most bandwidth.	As only one communication channel is needed and is alternately shared by the two managements, it can sustain bandwidth. When a constant, uninterrupted connection between the two controls is required, it can be used.

Protocol:

One of the elements of a data communications system is a protocol. Protocol is necessary for communication to take place. Data cannot simply be sent from one device to another and expect the other to receive it and accurately understand it. When a sender transmits a message, it may include text, numbers, graphics, and other data that is broken down into bits and arranged into blocks to be conveyed.

Control information is often also included to aid the recipient in deciphering the data. The sender and the recipient must agree to a set of guidelines known as protocol for communication to be effective.

A protocol is described as a collection of guidelines for controlling data transmission. A protocol establishes the information that must be shared, how it must be shared, and when it must be shared.

Data Communications:

Data are the unprocessed facts that are gathered, while information are the processed facts that help us make judgments. Ex. Every student's data is included when the results of a test are released, so when you locate your score, you may determine if you passed or failed the exam. Any information that is displayed in a way that its authors and users have approved is referred to as data.

Data Transmission: The process of transmitting data or information is known as data communication. In computer networks, this exchange takes place across a transmission channel between two devices.

A hardware and software-based communication system is used in this procedure. The transmitter, receiver, and intermediary devices that the data flows through make up the hardware portion.

The software component includes rules that outline what must be conveyed, how it must be sent, and when it must be communicated. It also goes by the name of a protocol. The components of a data communications system are followed by sections that outline the essential qualities necessary for the efficient operation of the data communication process.

Data Communication Characteristics: Any data communications system must possess the four key essential qualities to function effectively:

1. Delivery: The data must be sent to the right user and destination.

2. Accuracy: The data should be sent precisely and without any mistakes being introduced by the communication technology. The correctness of the transmitted data may be impacted by data corruption that occurs during transmission.

3. Timeliness: Real-time data transmission refers to the need that audio and video data be transmitted promptly and without delay.

4. Jitter is a difference in packet arrival times. The timeliness of data transmission may be impacted by uneven Jitter.

Data Communication System Components

The components of a communication system are as follows:

Message: The message is the information or data that will be sent. Text, numbers, images, music, video, or any mix of these may all be included.

Sender: The sender of a communication is the machine or computer that creates and transmits it.

Receiver: The message is received by a computer or other device. The transmitter computer's location is often different from the recipient computer's location. The sort of network that is utilised in between will determine how far apart the transmitter and recipient are.

Medium: The physical road or channel used to transmit a message from one party to another. The medium may be wireless like a laser, radio waves, or microwaves or wired like twisted pair wire, coaxial cable, or fiber-optic cable.

Protocol: A protocol is a collection of guidelines that controls how devices communicate with one another. When communicating, the sender and recipient use the same protocols.

A protocol accomplishes the following tasks:

Sequencing of data. It means dividing a lengthy communication into discrete packets of a set size. Data sequencing rules provide the way of numbering packets in order to identify identical packets and detect packet loss or duplication.

Data movement. The most effective route between the source and the destination is defined by data routing.

Formatting of data. The bits or characters that make up a packet of data, control, addressing, or other information are determined by data formatting standards.

Flow management. Additionally, a protocol for communication prevents a quick transmitter from overwhelming a sluggish recipient. It controls the data flow on communication connections to provide resource sharing and protection against traffic congestion.

Control of errors. These guidelines are intended to identify message mistakes and guarantee that the right messages are sent. Retransmitting erroneous message blocks is the most used technique. A block with an error in this scenario is disregarded by the receiver and sent again by the sender.

Transmission sequence and precedence. These regulations make sure that every node has the opportunity to use the network's communication channels and other resources in accordance with the priority allocated to them.

Establishing and closing connections. When two nodes in a network desire to communicate with one another, these rules specify how connections are created, kept up, and ended.

Data protection. The majority of communication software packages also come with built-in data security and privacy features. Data access by unauthorized people is prevented.

Data from logs. Many communication programmes are designed to create log data, which records all jobs and data communications tasks that have been performed. Depending on how the users of the network utilise the network resources, this information could be used to charge them.

Four essential aspects of data communications determine its efficacy.

1. Delivery: The information has to go to the right place in the right sequence.
2. Accuracy: The data delivery must be precise.
3. Timeliness: The information must be delivered on time, delayed delivery Data not useful.
4. Jitter: The unequal packet arrival delays that result in inconsistent quality.

Signal

Expressions, noises, movements, and gestures all convey information to us, and they are the means by which people communicate with one another. Similar to signal, transmission of information from one system to another is communication. Or to put it another way, a signal is a function that expresses data or information. An electromagnetic wave known as a signal transports information via a physical medium. Here, the information is transformed into an electromagnetic signal, either analogue or digital, and sent from sender to receiver. Voltage and current are two examples of time-changing quantities that are used to represent data. Data may be transferred by modulating these quantities with regard to time. Similarly, signal is sometimes shown as a frequency-domain function rather than a time-domain function. A message signal is passed through an encoder and a modulator to be sent across a media, and it is passed through a decoder and a demodulator to be received at the other end. Based on the different types of signals, there are two kinds.

1. Analog signals are continuous and have a temporal component.
2. Digital signals are defined as discrete signals.

Analog signals:

An analogue signal is a kind of electrical energy (voltage, current, or electromagnetic power) in which the amount of electricity and the value it represents are linearly related. Analog signals are defined as those whose amplitudes may take on any value over a continuous range. Analog signals have a continuous nature and change over time. They may be regular or irregular. The physical variables that are measured in relation to their changes over time include voltage, current, frequency, pressure, sound, light, and temperature. When a graph of voltage against time is drawn, a curve with continuous values, such as sine waves, may be seen. As they move across the medium, these signals are more vulnerable to noise, which causes the signal's information to be lost. By using a technique known as sampling and quantization, analogue to digital converters transform analogue signals into digital signals. The method converts sound waves into a series of samples. Sampling

Analog signal examples include:

Transducers and conventional (vintage) transmitters send data in analogue mode. The signals include radio signals, wired audio transmissions, vintage video broadcasts, and analogue watch transmissions.

Digital signal

Digital signal refers to a signal whose amplitude may only take certain values. Digital signals only have unique values because they are discrete. Bits of binary data, or 0 or 1, are carried by digital signals; each bit may only hold one value at a time. Square waves or clock signals are used to represent digital signals. 0 volts is the lowest and 5 volts is the highest amount. Analog signals are more susceptible to noise than digital ones. Modulation is a procedure used to transmit digital data across an analogue channel. Digital data is transformed to analogue signals via amplitude modulation, which uses a single frequency carrier signal. Similar to this, FREQUENCY shift keying employs two frequencies and a constant amplitude carrier signal to distinguish between 1 and 0. Since digital signals have more productive uses and physical characteristics than analogue signals, their use for information transmission has risen quickly in all areas of application in the modern world.

Various types of digital signals

Data is sent via analogue and digital signals by smart transmitters that use a variety of protocols.

Digital timepieces: Signals for digital video, CD's, DVD's, Computer.

The differences between analogue and digital signals

The adaptability, continuity, representation, data type, signal type, transmission medium, type of values, security, bandwidth, hardware, data storage, portability, data transmission, impedance, power consumption, data recording, use, rate of data transmission, examples, and applications are the main characteristics of analogue and digital signals.

Adaptability: Digital signals may be adjusted more widely for a variety of uses than analogue signals, according to PCBWay.

Continuity: While digital signals only employ a small number of distinctive values at regularly spaced points in time, analogue signals use a continuous range of amplitude values.

Species of Waves

Digital signals have square waves, whereas analogue signals have sinusoidal waves.

A digital signal is sent over a wire, while an analogue signal uses a wire or wireless technology.

A digital signal is positive, but an analogue signal might have both positive and negative values.

A digital signal is encrypted, but an analogue transmission's security is not.

The digital signal has a higher bandwidth than the analogue signal, which is lower.

Hardware for analogue signals is not elastic, but software for digital signals is.

Analog signals store their data as waveforms, while digital signals store their data as binary bits. Digital signals are pricey and portable like computers, but analogue signals are portable like a thermometer. While being sent, an analogue signal may degrade as a result of noise, but a digital signal may remain noise-resistant without degrading. The analogue signal has a low impedance, whereas the digital signal has a high impedance. Digital equipment uses less electricity than analogue equipment does. In contrast to the digital signal, the analogue signal has a slower pace of data transfer. Example: Video, human speech over the air, radio waves, and TV transmission waves are the greatest examples of an analogue signal.

Applications: Digital signals are suitable for digital electronic devices such as computers, PDAs, and mobile phones, but analogue signals can only be used in analogue devices, such as thermometers.

Transmission impairment:

When the sent signal and the received signal vary, transmission degradation occurs. As is common knowledge, a signal may be sent as either an analogue or digital transmission. Due to transmission flaws, the received signal in analogue communications may have a different amplitude or form. We see changes in bits (0s or 1s) when digital signals are broadcast and received. The reasons of transmission impairments are many.

Noise

Noise is a key contributor to transmission distortion because any undesired signal that is introduced to the sent signal modifies the final transmitted signal, and it is challenging to eliminate the unwanted noise signal at the receiving end (Figure 5.1). There are many different types of sounds, including shot noise, impulse noise, thermal noise, etc.

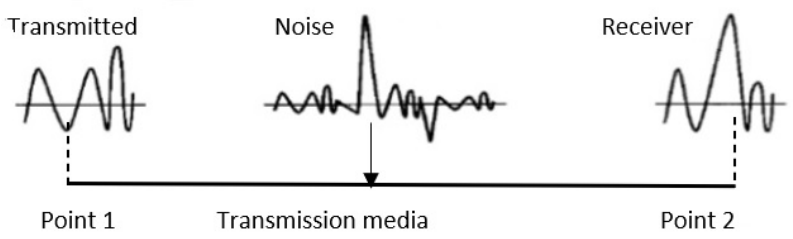


Figure 5.1: Noise.

Distortion

This kind of distortion is most often seen in composite signals, where each frequency component has a certain time limit and together they form a signal with a variety of frequency components. However, if there is a delay between the frequency components while this composite signal is being sent, there is a potential that each frequency component will arrive at the receiver end with a different delay constraint than when it left, changing the form of the signal. The delay is brought on by external factors, such as the separation between the transmitter and receiver, etc (Figure 5.2).

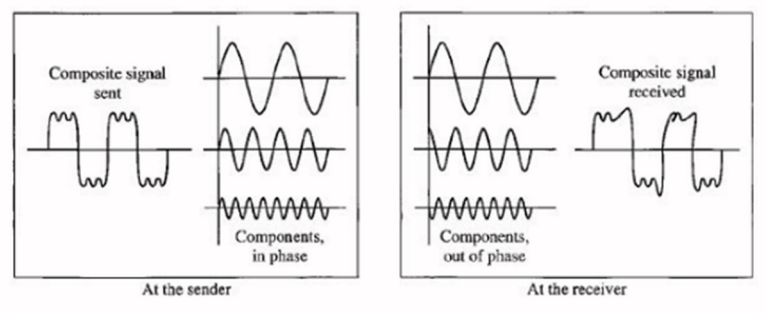


Figure 5.2: Distortion

Attenuation

Signal intensity is often reduced by attenuation, making it challenging for the receiver to pick up the incoming signal. The environment is the main cause of this attenuation since it places a lot of resistance on the signal, which causes it to weaken as it attempts to overcome that resistance (Figure 5.3).

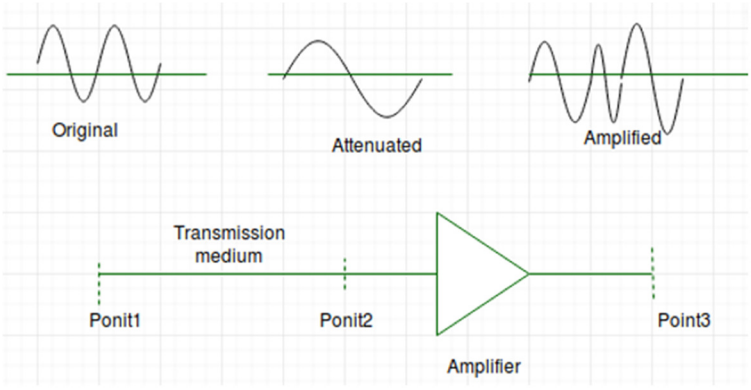


Figure 5.3: Attenuation

Chapter 6

DATA LINK LAYER

Ram Lal Yadav, Assistant Professor,
School of Computer & Systems Sciences, Jaipur National University, Jaipur, India,
Email Id-ramlal.yadav@jnujaipur.ac.in

The data link layer is a layer in the networking architecture that converts the unreliable transmission connection in charge of node-to-node or hop-to-hop communication that is given by the physical layer (Hub, Repeater, Cables, Modem, and Connectors). The data connection layer receives the network layer's bit stream and splits it into manageable data units known as frames. The data link layer now includes a header with the addresses of the frame's sender and recipient to each frame. To ensure dependable data flow through the physical media, the Data Link Layer offers Data Link Control. For instance, only one device can exchange data at once when using the half-duplex transmission option. Data loss will occur if the devices at the interconnections' ends broadcast information at the same time and collide. The devices are coordinated by the data link layer to prevent collisions. The data connection layer design considerations include, in addition to framing and addressing:

Flow control: The rate at which data is sent by the sender and received by the receiver varies. Therefore, the flow control mechanism must be managed by the data connection layer.

Error Control - The data connection layer also increases the physical layer's dependability. Yet how? It includes a system to find and send the broken or missing frames again.

Access Control for Media: The data link layer assists the frame in determining which device is in charge of the connection at any given moment if numerous devices are added to the same network link.

As a result, that the data link layer may transmit and receive data bits across the communication channel by employing the services of the physical layer. It gives the network layer a clear interface, handles transmission faults, and controls data flow to coordinate communication between sender and recipient.

Issues with Data Link Layer Design

Network Layer Framing Error Control and Flow Control Service

Providing Service to the Network Layer

The network layer receives services from the data connection layer. Data transmission from the network layer of the source computer to the network layer of the destination machine is one of the key services.

A few data bits (packets) are sent from the network layer at the source computer to the data link layer. These bits are now sent via the data link layer to the target machine's data link layer. The network layer at the destination computer receives the bits from the data link layer there. Here, it seems as if the source and destination machines' two data connection layers are in communication. But in reality, things are different. Instead, the data bits go from the physical layer of the source computer to the physical layer of the destination machine. These data bits are then sent from the

target machine's physical layer to the data link layer, where they are then transferred to the network layer. Because of the following factors, data connection layer design difficulties differ from protocol to protocol.

Connectionless Service Unacknowledged

This situation involves the source computer sending data frames to the destination machine without anticipating a response. Ethernet is the most prevalent instance of an unacknowledged connectionless service. In Ethernet, there is no logical link created between the sender and recipient. The received frames are not acknowledged by either recipient. The sender makes no attempt to find or recover any lost frames in the event that any are lost. Notably, this form of connection is suitable in situations when the channel's error rate is low.

Connectionless Service acknowledged

As the term implies, there is no logical relationship between the sender and the recipient. However, the receiver acknowledges the frames it has received. WiFi is the most well-known example of this sort of service. A frame is sent again if it is lost and the sender does not get acknowledgment within a certain amount of time.

Connection-Oriented Service with Acknowledgement

The sender and receiver first create a logical relationship while using this kind of service. Then, each frame that is sent out is given a sequential number, ensuring that each frame is sent out just once and in the correct sequence. The sender and receiver cut the connection after all the frames have been delivered. Long distance telephone lines are the most often used illustration of this kind of service.

Framing:

The streams of bits that are converted into manageable data units by frames come from the network layer. Data Link Layer divides the bit stream in this manner (Figure 6.1).

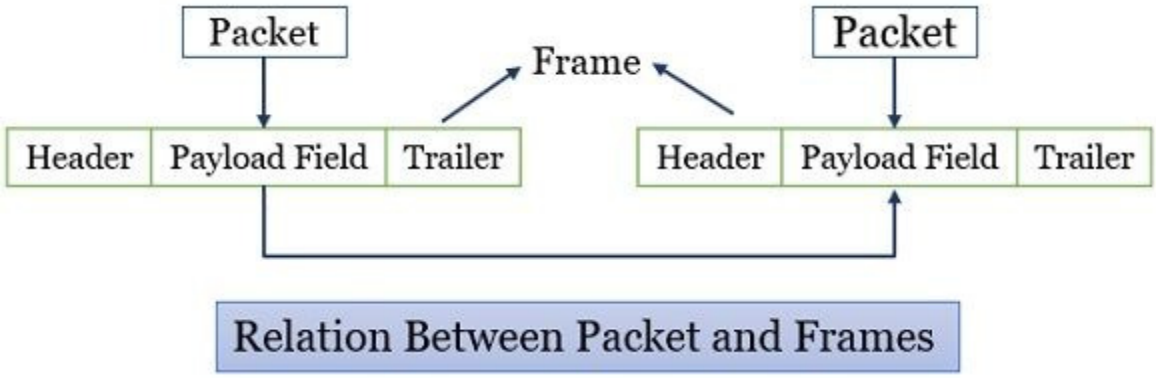


Figure 6.1: Framing

Requires framing

The physical layer provides services to the data connection layer. The destination is reached by the physical layer by simply accepting the raw bits stream. The physical layer, which includes any

utilized cable or wireless lines, May now be noisy, which eventually raises the bit error rate. The physical layer gives the signals more redundancy to lower the bit error rate. The bit of stream that is received at the destination data connection layer is not, however, guaranteed to be error-free. Consequently, it falls on the data link layer to find and fix the mistakes. The idea of framing is used to find and fix problems in the bit stream data connection layer. The data connection layer divides the bit stream into discrete frames during framing and computes the checksum for each frame. This checksum is part of the frame that is sent to the destination via the data link layer. The receiver recalculates this checksum when the frame reaches the destination, and if the results are different, it shows that the arriving frame had mistaken. These frames now come in fixed size and variable size varieties.

Frame types

Initial Fixed Length Frame

To provide any frame borders for fixed-size frames since the size of the frame itself serves as a delimiter.

Frame with Variable Length

Provide the frame boundaries, or the end of one frame and the start of the next frame, when dealing with variable-length frames. We have two ways for determining the bounds of a variable-length frame, which are explained below.

The Approach Is Character-Oriented

When text information was sent over the data link layer, the character-oriented strategy was widely used. The information that the header and trailer include should be multiples of 8, and the data sent in this method used to be 8 bits. The sender's data link layer adds an 8-bit flag to the start and end of the frame to indicate its beginning and finish. Any charter that isn't used in text communication might serve as this indicator.

Byte stuffing

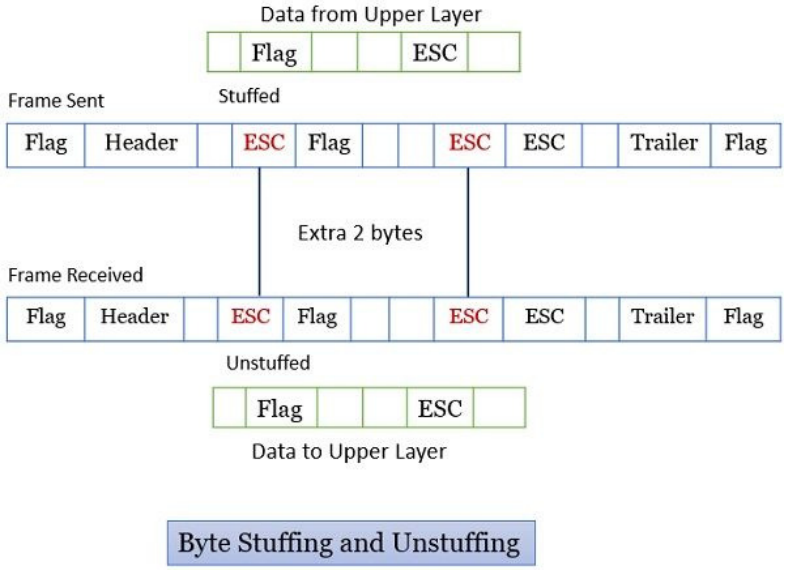


Figure 6.2: Byte stuffing

Character stuffing is another name for byte stuffing. If a character in the data section matches the flag's pattern in this case, the data link layer adds an additional byte to that portion of the data section. This additional byte is known as an escape character. The bit pattern for the escape character is predetermined. Now, if the receiver encounters this escape character, it will simply erase it and treat the following character as data alone. Until it comes across the last delimiter, which is the flag. The character with the escape pattern is thus indicated with another escape character to solve this issue (Figure 6.2).

However, since the current universal coding scheme uses 16-bit or 32-bit characters, the character-oriented approach is losing ground when it comes to framing notions. We must thus transition to a bit-oriented strategy.

Bit-Oriented Approach

In the character-oriented method, the start and end of the frame are identified by packing one complete byte (8-bit flag an escape character). The bit-oriented strategy, however, involves stuffing a single bit. In the bit-oriented technique, we insert a single bit 0 after five consecutive ones to avoid a data chunk from seeming like a flag. In this case, an additional bit 0 is inserted if the data link layer detects 0 and five consecutive 1s. The extra bit is taken out by the receiver when it gets the frame (Figure 6.3).

Figure 6.3: Bit-Oriented Approach

Error Prevention

The design challenges that we must deal with are how to guarantee that every frame has arrived at the destination in the right sequence and only once after marking the start and finish of the frame. Giving the sender input on the person on the other end of the communication line is a more broad technique to guarantee this. Feedback from the recipient to the sender may be either good or negative.

Positive feedback means that the frame arrived at its destination without incident, whereas negative feedback means that something went wrong and the frame has to be sent again. Even in this situation, because it hasn't received any frames, the receiver won't provide any good or negative feedback. Additionally, even if the frame is correctly received, the acknowledgment may not. The

sender will continue to wait in this case, whether the acknowledgment is positive or negative infinity. To fix this problem, we add a timer to the data connection layer.

Now a timer is started each time the sender delivers a frame. This timer is set to expire after a lengthy period of time so that there is enough time for the frame to arrive at the intended location, be processed there, and allow for the propagation of the acknowledgment back to the sender. The sender typically sends a frame and starts the timer. Before the timer runs out, the frame will reach its destination and the acknowledgment for it will go back to the sender.

Differentiate between retransmitted and original frames by giving the outgoing frames a sequence number. Thus, using the timer and sequence number ensures that each frame arrives at the target machine's network layer precisely once. Flow control is the following design concern for the data connection layer.

Flow Management

It is possible for a transmitter to send frames at a quicker pace than the receiver is capable of receiving them. This might happen if the transmitter is using a machine that is operating substantially quicker than the receiver. Even if the transmission is flawless in this case, it is possible that the receiver won't be able to digest the frames quickly enough and will lose part of them. There are two methods to stop this from happening:

1. Flow control based on feedback

The recipient agrees to receive more data from the sender or at the very least updates the sender on the recipient's progress.

2. Rate-based Flow Control

In order to prevent the receivers from being overloaded with frames, this method limits the pace at which the transmitter may deliver the data. These are the challenges that network designers must take into account while constructing the data connection layer. Framing, error control, and flow control are all functions of the data link layer, which also serves as a service to the network layer. The OSI (Open System Interconnection) system architecture model has two layers, the Data-link layer being the second from the bottom. It is in charge of data delivery from node to node. Its primary responsibility is to ensure accurate information delivery. Additionally, DLL is in charge of encoding, decoding, and organizing both incoming and exiting data. This layer of the OSI model is said to be the most complicated because it conceals from the layers above all the hardware's inner workings.

Elementary Data link Protocols

Framing, error control, and flow control are three essential tasks that the data connection layer must be able to do. Bit streams from the physical layer are split into data frames that vary in size from a few hundred to a few thousand bytes during the framing process. Transmission faults and the retransmission of damaged and missing frames are dealt with via error control techniques. Flow control controls delivery speed so that a quick sender won't overwhelm a sluggish recipient (Figure 6.4).

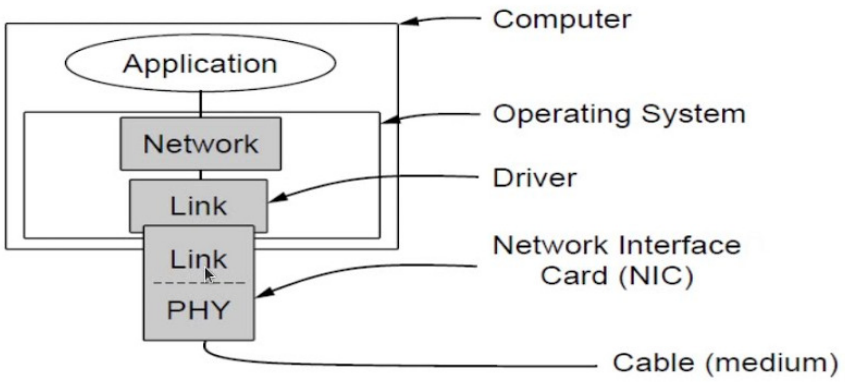


Figure 6.4: Elementary Data link Protocols

Types of Data Link Protocols

Depending on whether the transmission channel is noiseless or noisy, data connection protocols may be roughly categorised into two groups.

Simplex Protocol

A hypothetical protocol called Simplex is created for unidirectional data transmission across an ideal channel, or a channel where transmission is always successful. It has separate transmitter and receiver processes. As soon as data is accessible in its buffer, the transmitter simply broadcasts all available data over the channel. It is anticipated that the receiver will immediately digest all incoming data. Since it doesn't deal with flow control or error control, it is purely hypothetical.

The Stop-and-Wait Protocol

The Stop-and-Wait technique is also applicable to noiseless channels. It offers one-way data communication without any mistake correction tools. To prevent a quick transmitter from drowning a sluggish receiver, it does, however, provide flow control. The receiver's processing speed and buffer capacity are both limited. Only after receiving notification from the receiver that it is ready for further data processing may the sender transmit a frame.

Stop – and – Wait ARQ

Pause, then wait Automatic Repeat Request (Stop-and-Wait ARQ) is a variant of the aforementioned protocol that is suited for noisy channels and includes additional error control techniques. A copy of the transmitted frame is retained by the sender. It then waits for the recipient to respond positively for a certain amount of time. The frame is sent again if the timer runs out or there is no positive response. The next frame is transmitted if there is an affirmative acknowledgment.

Go – Back – N ARQ

Multiple frames may be sent using the Go-Back-N ARQ protocol before the first frame's acknowledgment is received. It is also known as sliding window protocol since it makes use of the sliding window idea. There are a limited amount of frames delivered, and they are consecutively numbered. If a frame's acknowledgment is not received within the allotted time, all frames after that frame are resent.

Selective Repeat ARQ

Additionally, this protocol enables transmitting additional frames before getting an acknowledgment for the first frame. The good frames are received and buffered, whereas only the incorrect or missing frames are retransmitted in this case.

Networking errors

Computer networks include the connection of devices that communicate data through a network. Due to the fact that data is provided as signals rather than bytes, it is possible for the sender's data to get garbled or lost during transmission. The interfaces have the ability to modify a signal's form, which may affect the interpretation of the data. An error occurs when data that was really delivered by the source computer but was not received by the destination machine.

Various Errors

In essence, there are two categories of faults that might happen during data transfer. The many error kinds are listed below.

Single Bit Error: When a data unit just has one bit that changes from 1 to 0 or 0 to 1, it is said to have a single bit error.

Burst Error: When two or more bits in a data unit shift from 1 to 0 or vice versa, it is said to have occurred.

Controlling Errors in Computer Networks

To make sure the target machine receives the precise data or message, the data connection layer employs error control methods. However, sometimes during transmission, data is lost or damaged. The two error control methods are used by the data connection layer. These methods are used to locate the mistake and rectify it. The methods for correcting errors are as follows:

Detecting Errors in Computer Networks

The technique of finding an error in the data or message is known as error detection in computer networks. For this, the data connection layer makes use of a variety of error detection mechanisms. The fundamental strategy is redundancy, where extra bits are introduced to make it easier to find and fix faults. The many sorts of error detection methods that we use for spotting errors in computer networks are listed below.

Easy parity check

Parity check in two dimensions

Cyclic redundancy check for checksum.

Simple Parity Check

The simplest method of error detection in computer networks is called parity check, and it uses a parity bit. Parity is only an extra bit, sometimes known as a superfluous bit. Before sending the data, a parity bit is added at the end of the data unit. Because we are tagging the data with an additional bit, this will make the data larger. For instance, if we transmit 8-bit data, the size of the data block will increase to 9 bits when the parity bit is added. For error detection, two different kinds of parity bits may be added:

Even Parity: Even parity involves adding a bit to the end of the data block to equalise the number of ones. The parity bit 0 is inserted if the number of ones in the data is already even. The parity bit 1 is inserted if the number of ones in the data block is odd.

Odd Parity: To make the number of ones odd, an extra bit is added. Parity bit 0 is inserted at the end of the data unit if the number of 1s in the data unit is already odd. Parity bit 1 is inserted if the number of ones is even.

Simple Parity Check Work

The two circuits used in a simple parity check are a parity generator and a parity checker. At the sender end, a parity bit is added to the data using the parity generator. Along with the data unit, the parity bits are sent. Another circuit a parity checker is utilized at the receiving end. Parity bits are verified. There is no mistake and the receiving computer accepts the data if the transmitted and received parity bits are identical. A simple parity check for computer networks. When transmitted and received parity bits do not match, a data mistake is revealed, and the data is discarded. The aforementioned illustrations demonstrate the fundamental role of parity checking fault detection. The fact that a basic parity check can only identify single-bit errors is a significant disadvantage. Multiple flaws in the data prevent it from detecting the faults.

Check for Two Dimensional Parity

The data in a two-dimensional parity check is organised in a table. The whole set of data is separated into rows using this procedure. Parities for rows and columns are computed. At the conclusion of the data block, parity bits are added, and the data is delivered with these parity bits. For a better understanding of the idea of a two-dimensional parity check, consider the data in the following example.

Checksum

Another method of fault detection in computer networks is a checksum. This approach for identifying faults uses the idea of redundancy. The checksum generator and checksum checker are the two main parts of the checksum. On the sender's end, a checksum generator separates the whole amount of data into k segments, each of which contains n bits. The total is determined by adding each section using the 1's complement. The checksum is created by complementing the sum after that. The checksum field and data segments are then sent from the sending machine to the receiving machine. Another circuit, known as a checksum checker, is used at the receiving end. The checksum checker's main job is to check the checksum and look for flaws in the received data.

The data is divided into k pieces, each with n bits. The complement of the total is determined by adding all the segments together. In the above graphic, the checksum's operation is shown. The receiver will get the data if the result is zero, which indicates that there was no mistake. If the outcome is not zero, it indicates that there is some kind of problem with the data, and it is rejected at the receiving end. In computer networks, there are primarily five kinds of checksums used for error detection.

1. Addition checksum for integers
2. Checksum using one's complement
3. Checksum for Fletcher
4. Checksum ATN
5. Checksum by Adler

Cyclic Redundancy Check (CRC)

Another crucial method for detecting errors in computer networks is the cyclic redundancy check (CRC). In this process, binary division is used. Cyclic redundancy check bits are the redundant bits that are inserted at the conclusion of the data. The CRC generator and CRC checker are the two circuits used in this method. The sender's side CRC generator generates the CRC bits, while the receiver's end CRC checker verifies the bits.

Computer networks CRC

CRC's Function in Computer Networks

The CRC method involves the following stages.

At the end of the data unit, N number of 0s are inserted. There should be one fewer zeros than bits in a predefined integer (Divisor). On the expanded data, the binary division operation is carried out. The residual, often known as the CRC remainder, is computed after binary division. The real data unit is completed by adding the CRC residual. The actual data unit and the remaining CRC information are transferred. The binary division is done on this using the same divisor after the receiver gets the real data plus the CRC remainder. The CRC bits are checked by a CRC checker. The receiver accepts the data if the division result is zero, which indicates that there are no errors in the data.

Switching

Messages are transmitted over the network of transmission media when a person uses the internet or another computer network from a place other than their local area. Switching is the term used to describe this method of moving data across computer networks.

1. Switches are used to perform switching in computer networks. A switch is a discrete piece of hardware that connects many computers to a single local area network (LAN).
2. In the OSI model, network switches function at layer 2 (Data link layer).
3. Switching is seamless to the user and doesn't need the home network to be configured.
4. On the basis of MAC addresses, switches are utilised to forward the packets.
5. Only the device that has been addressed receives the data thanks to a switch. It checks the destination address before properly routing the message.
6. Full duplex operation is used.
7. Since the source and destination are communicating directly, packet collision is minimal.
8. It does not transmit the message since its bandwidth is constrained.

Need of Switching Concept

The following factors lead to the development of the switching concept:

The highest possible transmission rate through a cable is referred to as bandwidth. It is a valuable but pricey resource. As a result, switching strategies are employed to efficiently use a network's capacity.

Collision: When many devices transmit data over the same physical medium and clash with one another, the impact of collision results. Switching technology is used to prevent packet collisions in order to solve this issue.

Benefits of Switching

1. The network's bandwidth is increased by the switch.
2. Since just the device that has been targeted receives the information, it lessens the stress on individual PCs.
3. By lowering network traffic, it improves the network's overall performance.
4. As the switch builds the collision domain for each connection, there will be fewer frame collisions.
5. Switching has the disadvantage
6. Switching has the disadvantage
7. Switches are unable to quickly identify network connection problems.
8. Multicast packet handling requires proper switch design and setup.

Error Correction:

When data is sent from the sender to the receiver, error correction codes are employed to identify and fix any problems. There are two methods for handling error correction:

Retransmission of the full data unit is requested by the receiver after the problem has been identified in backward error correction.

Forward error correction: In this scenario, the receiver makes advantage of the error-correcting code to instantly fix the mistakes.

The mistake may be found with only one more bit, but it cannot be fixed. One has to be aware of the precise location of the faults in order to rectify them. The error correction algorithm will identify which one of seven bits is incorrect, for instance, if we wish to compute a single-bit mistake. We must include some more unnecessary bits in order to do this. Assume that d represents the total amount of data bits and that r represents the number of superfluous bits. The following formula may be used to determine how many superfluous bits there are:2r>=d+r+1

Using the method above, one can determine the value of r. The least feasible number that meets the above relation, for instance, is 3 if d is equal to 4.

Hamming Code

Parity Bits: The bit that is added to the original binary data to determine if there are more even or more odd 1s in the total.

Even parity: If there are an equal amount of 1s overall, then the parity bit's value is 0. The parity bit has a value of 1 if the total number of occurrences of 1s is odd.

Odd Parity: If the total number of 1s is even, the parity bit's value is 1, indicating that the parity is odd. The parity bit has a value of 0 if the total number of 1s is odd.

Hamming coding algorithm: The superfluous bits "r" are combined with the information of "d" bits to generate "d+r."

Each of the (d+r) digits' locations is given a decimal value.

The placements of the "r" bits are 1, 2,..., 2k-1.

The parity bits are adjusted at the other end. The location of an error is determined by the decimal value of the parity bits.

Chapter 7

NETWORK LAYER

Ram Lal Yadav, Assistant Professor,
School of Computer & Systems Sciences, Jaipur National University, Jaipur, India,
Email Id-ramlal.yadav@jnujaipur.ac.in

Network layer is Layer 3 in the OSI paradigm. Managing sub-networks, internetworking, and host and network addressing are all responsibilities of the network layer. The network layer is in charge of routing packets to their destinations inside or outside of a subnet. It is conceivable for two separate subnets to have addressing types or schemes that are incompatible with one another. The same is true for protocols; two separate subnets may be utilizing unrelated ones. The network layer is in charge of routing packets from source to destination and mapping multiple addressing schemes and protocols (Figure 7.1).

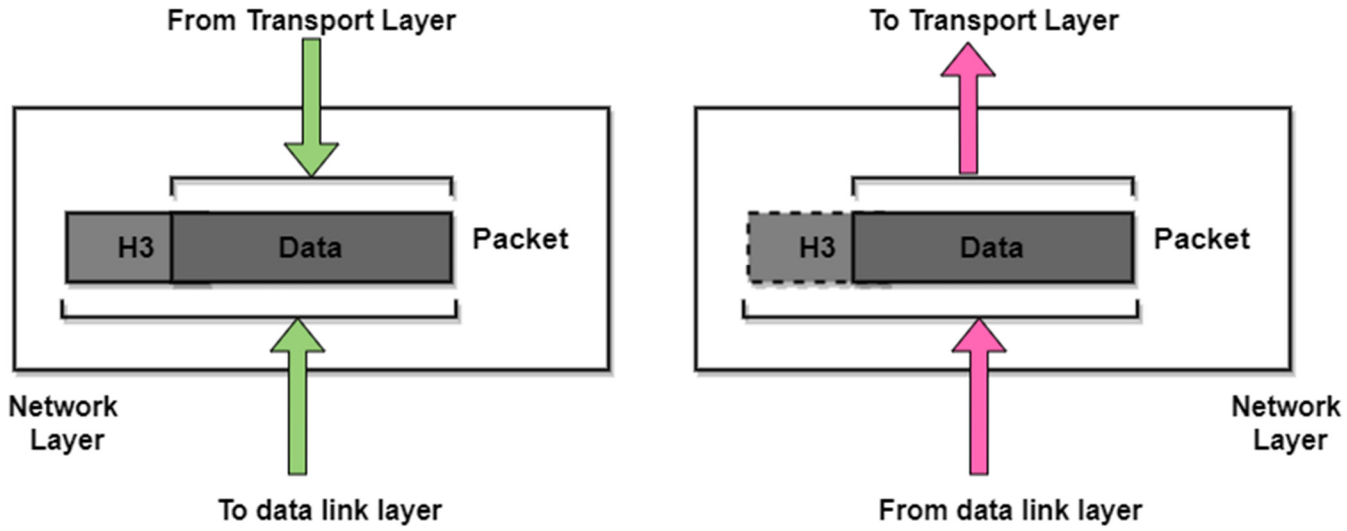


Figure 7.1: Illustrating the Network Layer.

- **Functions of Network Layer**

The network offers the aforementioned features.

- **Hosting-to-Hosting Data Transfer**

Data packets are delivered from source to destination by the network layer. This layer offers the guarantee that the packet will arrive at its designated location.

- **Reasonable Addressing**

To allow each network device to be exclusively identified, the network layer establish an addressing system. The network layer inserts the sender and receiver's IP addresses into the header. Each device can be identified individually and universally by such an address. The network ID and host ID of the network are contained in the header and identify which device on the system or network is the receiver.

- **Forwarding and Routing**

Routing determines the best route to the destination. To forward data packets, it selects the shortest path between the sender and the receiver. Path vector, link-state routing, and distance vector routing are some common routing protocols.

- **Fragmentation**

The network layer breaks up the large amount of data into smaller pieces before sending them from to the destination. Each reception node has a fixed ability to receive data, which is why it is done.

- **Congestion Mitigation**

Congestion is the aggregate of data packets into the networks caused when the router is unable to correctly route them due to the massive inflow of data packets into the network. The network layer is also in charge of managing network congestion and adjusting the flow of the network.

Network Addressing

Network addressing is one of the network layer's main responsibilities. Network addresses are always logical or software-based in nature. Hosts are end systems that have just one network connection. The line separating a host and a link is known as an interface. The host can only have one interface as a result. A router varies from a host in this sense since it has two or more links connected to it. When a gateway forwards the datagram, the packet is sent to one of the links. An interface is the physical separation among a router and a link. A router may have many interfaces, one for each of its connections. Subclasses of an IP address are further separated as follows:

1. **Class A:** Networks with a high number of hosts are given IP addresses.
2. **Class B:** Networks with sizes ranging from modest to large are given IP addresses.
3. **Class C:** Networks with a small size are given an IP address.
4. **Class D:** IP addresses are multicast-reserved and do not have sub netting.
5. **Class E:** An IP address that lacks sub netting is used for future use as well as for research and development.

Router

Network addressing is one of the network layer's main responsibilities. Network addresses are always logical or software-based in nature. Hosts are end systems that have just one network connection. The line separating a host and a link is known as an interface. The host can only have one interface as a result. A router varies from a host in this sense since it has two or more links connected to it. When a gateway forwards the datagram, the packet is sent to one of the links. An interface is the physical separation among a router and a link. A router may have many interfaces, one for each of its connections. The optimum route to the destination is determined by the routing algorithm using the statistic. Delay, hop count, bandwidth, current path load, etc. are a few examples of metrics. The routing algorithm initializes and maintains the routing table in order to determine a path.

- **Types of Routing**

a. Static Routing

Static routing is another term for non-adaptive routing. The administrator uses this technique to manually add routes to a routing table. A router can send the packets using the administrator-

specified route to the destination. This approach does not base routing decisions on the networks' topology or status.

b. Default Routing

When a router is configured to deliver all packets to a single hop device, irrespective of whether that device is a part of a specific network or not, this is known as default routing. The transmission is received by the device for which a packet is set up in default routing. Networks operate with a single exit point and use default routing. It is also useful when data must be sent to a single HP device over several transmission networks. When the specific route is shown in the routing table, the router will choose it rather than the default gateway. The default route is only used when a specific route is not included in the routing database.

4. Dynamic Routing

It is a technique where a router adds a new route for each packet to the routing table in response to changes in the state or topology of the network also known as adaptive routing. Using dynamic protocols, the new routes to the destination are discovered. The protocols used in dynamic routing to find new routes include RIP and OSPF. If any path is compromised, an automatic change will be made to reach the destination. Getting packets from the source to the destination is a concern of the network layer. It could take many hops at intermediate routers to get to the target. This purpose obviously differs from the data connection layer's, which only aims to transfer frames from one end of a cable to the other. So the lowest layer that deals with end-to-end transmission is the network layer. Even for huge networks, the network layer must pick acceptable pathways across it and be aware of the topology of the network (i.e., the set of all routers and connections) in order to accomplish its objectives. Additionally, it must be cautious while selecting routes to prevent overloading some of the routers and communication lines while leaving others inactive. Finally, additional issues arise when the source and destination are on separate networks.

Network Layer Design Issues

The network layer is responsible for handling them. We will examine all of these concerns in this chapter and provide illustrations, mostly utilizing the Internet and its network layer protocol, IP. Few of the problems that network layer designers have to deal with in the sections that follow. These problems involve the network's internal architecture and the service supplied to the transport layer.

Store-and-Forward Packet Switching

It is important to reiterate the context in which the network layer protocols function before delving into its specifics. Figure depicts the environment in question. The equipment of the ISP (routers linked by transmission lines), which is shown within the shaded oval, and the equipment of the customers, which is displayed outside the oval, are the two main components of the network. The host H1 is directly linked to router A of the ISP, maybe as a personal computer at home using a DSL modem. In contrast, H2 is connected to a LAN through a router, F, that is owned and managed by the client and may be an office Ethernet. A leased line connects this router to the ISP's hardware. F does not belong to the ISP, hence we have indicated that it is outside of the oval. However, since they employ the same algorithms as the ISP's routers, routers on customer premises are regarded as a component of the ISP network for the purposes of this chapter (and our main concern here is algorithms) (Figure 7.2).

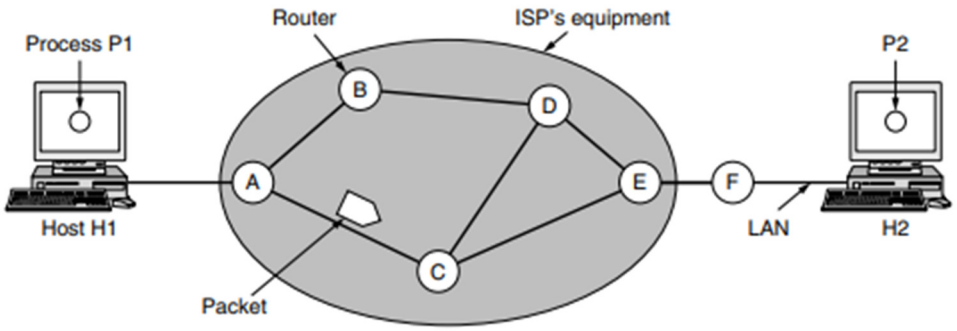


Figure 7.2: Store-and-Forward Packet Switching

The following is how this gear is utilized. A host that has a packet to send sends it across a point-to-point connection to the ISP or over its own LAN to the closest router.

The packet is kept there until the link has completed processing it by checking the checksum and the packet has completely arrived. When it reaches the target host, where it is delivered, it is then forwarded to the next router along the path. We have seen store-and-forward packet switching as this process in earlier chapters.

Services Offered to the Transport Layer

At the interface between the network and transport layers, the network layer offers services to the transport layer. What services the network layer specifically offers to the transport layer is a crucial topic. The following objectives need to be carefully considered while designing the services:

1. Services need to be unaffected by router technology.

2. The number, kind, and topology of the routers that are present should be hidden from the transport layer.

3. Even across LANs and WANs, the network addresses made accessible to the transport layer should follow a consistent numbering scheme.

Given these objectives, the network layer designers are given a great deal of latitude when creating comprehensive requirements for the services to be provided to the transport layer. This independence often turns into a bloody conflict between two opposing groups. The main point of contention is whether the network layer should provide connection- or connectionless-oriented services.

The Internet community represents one side that claims the only function of routers is to move packets from one place to another. This position holds that the network is intrinsically unstable, regardless of how it is constructed (based on 40 years of experience with a real computer network). As a result, the hosts should acknowledge this reality and handle their own flow control and error control (i.e., error detection and repair). According to this point of view, the network service should be connectionless and consist primarily of the primitives SEND PACKET and RECEIVE PACKET. In particular, there should be no packet ordering or flow control since hosts will often perform such things anyhow and there is seldom any benefit to doing them twice. The end-to-end argument, a design philosophy that has greatly influenced the development of the Internet, is an illustration of this line of thinking (Saltzer et al., 1984). Additionally, since each packet transmitted

is transported independently of its predecessors, if any, each packet sent must have the whole destination address.

The telephone corporations, who represent the other side, contend that the network ought to provide a dependable, connection-oriented service. They assert that the global telephone system's 100 years of successful operation serve as a good benchmark. According to this perspective, quality of service is the key aspect, and it is extremely challenging to create quality of service without network connections, especially for real-time traffic like phone and video.

This argument is still going strong even after many years. Early, extensively used data networks were connection-oriented, such as X.25 in the 1970s and Frame Relay in the 1980s. However, connectionless network layers have seen a huge increase in use since the ARPANET and the early Internet. The IP protocol is now a universally recognised sign of achievement. It remained unaffected by the connection-oriented ATM technology that was created in the 1980s to replace it; instead, IP is replacing telephone networks and ATM is now found in niche applications. However, behind the scenes, the Internet is developing connection-oriented characteristics as the importance of quality of service increases. MPLS (Multiprotocol Label Switching), which we shall discuss in this chapter, and VLANs, which we examined in Chapter 4, are two instances of connection-oriented technology. Both technologies have a large user base.

Connectionless Service Implementation

After examining the two types of services the network layer might provide to its consumers, it is time to examine this layer's internal operations. Depending on the kind of service provided, two distinct organizations may be viable. If connectionless service is made available, packets are sent into the network separately and routed separately from one another. No setup beforehand is required. In this context, the network is referred to as a datagram network, and the packets are commonly referred to as datagrams (to compare with telegrams). Data packets cannot be transmitted until a path from the source router to the destination router has been established if connection-oriented service is being utilized. In contrast to the actual circuits created by the telephone system, this link is known as a VC (virtual circuit), and the network is known as a virtual-circuit network (Figure 7.3).

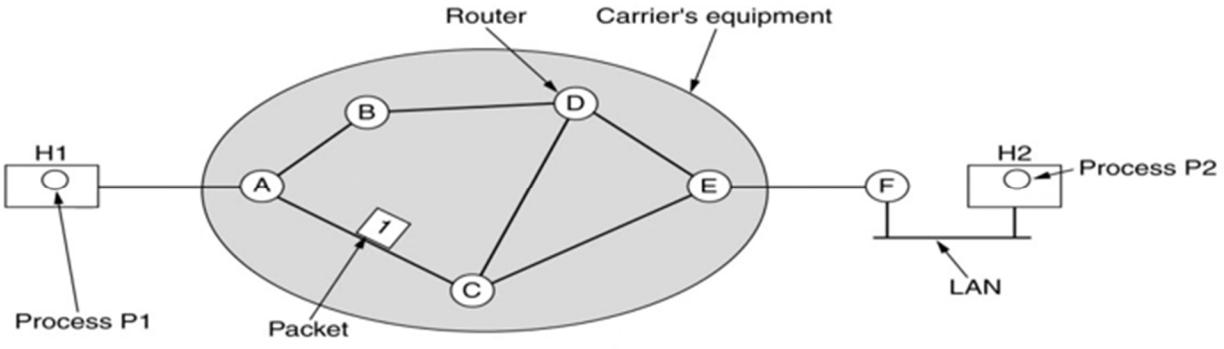


Figure 7.3: Connectionless Service Implementation

Connection-Oriented Service Implementation

A virtual-circuit network for connection-oriented service. Virtual circuits are designed to eliminate the need to choose a new route for each packet delivered, as seen in Figure. Instead, a route from

the source computer to the destination machine is selected as part of the connection setup and recorded in tables within the routers when a connection is made. Similar to how the telephone system operates, that route is used for all traffic moving across the connection. The virtual circuit is likewise ended when the connection is released. Each packet in a connection-oriented service has an identifier that indicates the virtual circuit to which it belongs (Figure 7.4).

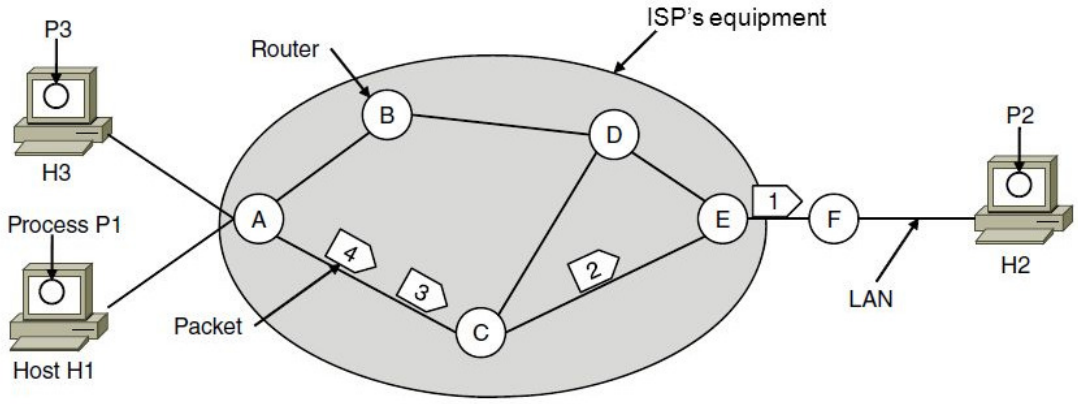


Figure 7.4: Connection-Oriented Service Implementation

Routing Methods

Routing packets from the source computer to the destination machine is the network layer's primary duty. The majority of networks need numerous hops for packets to complete their route. Broadcast networks are the sole prominent exception, however even in these cases routing problems might arise when the source and destination are on different network segments. One important aspect of network layer architecture is the algorithms used to choose routes and the data structures they employ.

The component of the network layer software known as the routing algorithm determines which output line an incoming packet should be sent on. The optimum path could have changed since the previous time, therefore if the network internally employs datagrams, this choice must be made every time a data packet arrives. Routing choices are only made when a new virtual circuit is being set up if the network internally employs virtual circuits. Data packets just continue along the established path after that. Because a route is still in effect for an entire session, the latter situation is frequently referred to as session routing. It might be helpful to distinguish between forwarding, which takes place after a packet arrives, and routing, which involves choosing which routes to utilise. A router may be thought of as having two processes running inside of it. Each packet that comes in is handled by one of them, who searches the routing tables for the appropriate outbound line to utilise. This procedure is moving forward. The other procedure is in charge of populating and maintaining the routing tables. The routing algorithm is used in this situation.

Certain qualities, including as accuracy, simplicity, resilience, stability, fairness, and efficiency, are desired in a routing algorithm, regardless of whether routes are selected individually for each packet delivered or just when new connections are made. Correctness and simplicity seldom ever need explanation, yet the need of robustness may not be immediately apparent. A significant network may be counted on to operate consistently for years after going live without experiencing any major breakdowns. There will be a variety of hardware and software problems throughout that time. Numerous hosts, routers, and lines will have failures, and the topology will often alter. The

routing algorithm need to be able to adapt to changes in traffic and topology without necessitating the termination of every task on every server. Imagine the chaos if every time a router failed, the network had to be restarted!

Another key objective of the routing method is stability. No matter how long they run, there are routing algorithms that never reach a definite set of pathways. An equilibrium is reached and maintained via a stable algorithm. Since communication could be hampered until the routing algorithm reaches equilibrium, it should converge swiftly as well.

Shortest Path Routing

This method finds the shortest path between two nodes and uses that information to choose a route. For measuring route length, it may make use of several hops, the geographic area in kilometres, or labelling of arcs. The labelling of arcs may be done using mean queuing, transmission delay for an hourly standard test packet, or determined as a function of bandwidth, average distance traffic, communication cost, mean queue length, observed latency, or other parameters. A directed weighted graph is used to design the topology of the communication network in shortest route routing. Switching components are represented in a graph by nodes, and their communication links are represented by directed arcs. The cost of splitting a packet between two nodes travelling in a certain path is determined by the weight of each arc. This cost, which is often positive, may represent a variety of things, including delay, throughput, mistake rate, financial charges, etc. There are many different intermediate nodes and arcs that may be used to connect two nodes. Finding the shortest way between two nodes with the lowest total cost is the aim of shortest path routing, where total cost of a path is the sum of arc costs in that path. Dijikstra, for instance, utilises the nodes along the more popular path that are labelled with their distance from the source node. All nodes are initially assigned the label "infinity," although this label may change as the algorithm moves on. In the illustration, the labelling graph is visible (Figure 7.5).

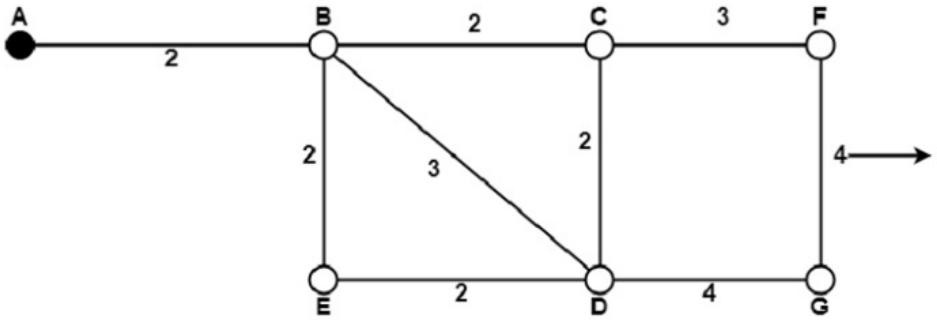


Figure 7.5: Shortest Path Routing

With source A, it may be completed in a variety of passes as shown below.

Pass 1. B (2, A), C(∞,–), F(∞,–), e(∞,–), d(∞,–), G 60

Pass 2. B (2, A), C(4, B), D(5, B), E(4, B), F(∞,–),G(∞,–)

Pass 3. B(2, A), C(4, B), D(5, B), E(4, B), F(7, C), G(9, D)

There are two possible routes connecting A and G. One continues through ABCFG, while the other via ABDG. The first one's path is eleven, whereas the second one's is nine. As a result, the second one, G (9, D), is chosen. Similar to Node A, Node D has three routes leading to it: ABD, ABCD,

and ABED. The first one and the other two each have a route length of five. The first one is thus chosen.

The routes with the shortest path lengths are made permanent, and the nodes of the path are utilised as a working node for the next pass after all nodes have been thoroughly inspected in previous runs.

DVR Protocol (Distance Vector Routing)

Distant vector routing protocol, commonly known as the Ford Fulkerson or Bellman-Ford algorithms, is used to determine a route. From the data gathered by the nearby router, a distance-vector protocol determines the distance and direction of the vector of the next hop. Monitoring the topology is crucial so that you can alert nearby devices if something changes. Information about the network: Each node in the system should have knowledge about the nodes next to it. Every node in the network is built to exchange data with every other node in the network.

Routing Pattern: In DVR, only nodes that are directly connected to one or more other nodes in the network get data shared by other nodes.

Data sharing: As the topology of the network changes, the nodes sometimes communicate information with their neighbours.

Distance Vector Routing Algorithm Definition

As it is used to determine the shortest path between two network nodes, the distance vector routing technique is also known as the Bellman-Ford algorithm or Ford Fulkerson algorithm. In order to create an ideal path, the routing protocol uses distance or the number of hops as its major metrics to determine the optimum route from source to destination. Whereas routing specifies the routes to the established node, the distance vector relates to the distance to the neighbouring nodes. The Distance Vector Routing Algorithm (DVR) chooses the best route from source to destination by exchanging routing table information with other routers in the network and keeping it current.

Understanding the Distance Vector Routing Algorithm's operation depends on three factors:

Understanding of the whole network: The whole network benefits from each router's knowledge sharing. The Router notifies its neighbours of the network information it has gathered. Solely directing to neighbours: Only those routers with direct connections get the router's network knowledge. Whatever information the router possesses about the network is sent via the ports. The router receives the information and utilises it to update its own routing table. Sharing information on a regular basis: The router transmits the data to the nearby routers in 30 seconds.

Link-State Routing

An intradomain protocol, link state routing is an internal protocol that updates the routers inside the autonomous system. To address the drawbacks of the distance vector routing protocol, link-state routing was developed. It would take too long to spread information about changes to the link's cost or if it became unavailable, which is why the distance vector routing protocol was replaced. Link State Routing: Building Routing Table and Link State Routing Operation

Link State Routing in Action

The first thing a new router does upon initialization inside an autonomous system's domain is calculate the cost of the connections on each of its interfaces. The router publishes the cost of the connection at each of its interfaces after it has established that cost, and it continues to track the

cost of the links after that. If the router notices a change in the link cost at any of its interfaces, it once again notifies all the other routers in the domain of the change. The topology of the whole domain is developed by each router in this protocol because each router has access to the set of link costs for every router in the domain. Now that each router has access to the domain's topology, they may use the Dijkstra algorithm to determine the shortest path and create a routing table. It is not possible to utilise the link-state routing protocol as an external or inter-domain routing mechanism. Below is a discussion of why link-state routing should not be used as an interdomain routing protocol. Various autonomous systems may employ different connection metrics in a vast network like the Internet. Link-state routing cannot be employed as a consistent routing technology since measurements differ from network to network. Link-state information is flooded to all of the routers in the domain during link state routing. Using it as an interdomain routing protocol might result in uncontrollable flooding across several autonomous systems.

Link-state routing may be explained in terms of four easy stages.

1. A router recognises its neighbours and their network address when it is started.
2. At each of its interfaces that connected it to its neighbour, it established the cost metric of the connection.
3. To all other routers in the domain, advertise the link-state packet (LSP) carrying its link-state information. Obtain data from other routers as well.
4. Create a routing table and determine the shortest path to each other router in the domain.
5. Link State Routing by Neha T on June 15, 2021 Submit a Comment
6. An intradomain protocol, link state routing is an internal protocol that updates the routers inside the autonomous system. To address the drawbacks of the distance vector routing protocol, link-state routing was developed.
7. It would take too long to spread information about changes to the link's cost or if it became unavailable, which is why the distance vector routing protocol was replaced.
8. Link State Routing: Building Routing Table and Link State Routing Operation
9. Link State Routing in Action

The first thing a new router does upon initialization inside an autonomous system's domain is calculate the cost of the connections on each of its interfaces. The router publishes the cost of the connection at each of its interfaces after it has established that cost, and it continues to track the cost of the links after that.

If the router notices a change in the link cost at any of its interfaces, it once again notifies all the other routers in the domain of the change. The topology of the whole domain is developed by each router in this protocol because each router has access to the set of link costs for every router in the domain. Now that each router has access to the domain's topology, they may use the Dijkstra algorithm to determine the shortest path and create a routing table.

It is not possible to utilise the link-state routing protocol as an external or inter-domain routing mechanism. Below is a discussion of why link-state routing should not be used as an interdomain routing protocol.

Various autonomous systems may employ different connection metrics in a vast network like the Internet. Link-state routing cannot be employed as a consistent routing technology since measurements differ from network to network.

Link-state information is flooded to all of the routers in the domain during link state routing. Using it as an interdomain routing protocol might result in uncontrollable flooding across several autonomous systems.

Link-state routing may be explained in terms of four easy stages. A router recognises its neighbours and their network address when it is started. At each of its interfaces that connected it to its neighbour, it established the cost metric of the connection. To all other routers in the domain, advertise the link-state packet (LSP) carrying its link-state information. Obtain data from other routers as well. Create a routing table and determine the shortest path to each other router in the domain. In order to briefly illustrate how link-state routing works, let's first briefly examine how each router in the domain builds its routing table.

Construction of Routing Tables

The routers must make sure they are displaying the shortest path to every other router in the domain while generating the routing table. The following are the stages involved in creating a routing table.

1. At each of its interfaces, a router must produce a link-state packet (LSP) containing a set of link charges.
2. Distribute this LSP to all domain-wide routers, not just the nearby ones.
3. Shortest-path trees are created for each router.
4. Creation of a routing table that includes the domain's shortest route to other routers.

Link State Packet Formation (LSP)

The link-state packet contains comprehensive information about the router. It contains details about the identity, list, age, and sequence number of the router. Another router in the AS may comprehend and create a topology of the whole domain with the aid of the router's identification information and list of connections from the router.

The receiving routers may compare the new LSP with the old LSP using the LSP's sequence number, and it also makes the flooding function of link-state routing more convenient. The domain's routers use the LSP's age to determine when it should be discarded. The routers in the domain produce the LSP twice: once when the domain's topology changes, and once on a regular basis. The LSPs distribute information to all the routers in the domain updating them whenever there is a little change in the topology of the domain. Every router in the domain won't have the outdated information if the LSPs are sent at regular intervals. A 60- to 2-hour timer has been established for the LSP's periodic distribution. The lengthy time avoids the flooding features from oversaturating the domain with traffic.

Flooding of LSPs

All other routers in the domain, not just those that are close by, get the newly formed LSPs. Flooding describes the distribution of LSPs to every router in the domain. The produced LSP is transmitted on the connection at each router interface in the first phase. The routers that are getting LSPs first compare them against LSPs they have already received. The freshly received LSP is deleted if it is older than the preceding LSP; otherwise, the router takes the following actions to guarantee flooding.

The previous LSP is first discarded by the router.

The router broadcasts a duplicate of the LSP across every interface save the one over which it originally got it.

Making the shortest possible path tree

The topology of the whole domain is created by each router since each router in the domain has information about every other router in the domain. The shortest-path tree has to be built for each router in order to identify the shortest route to every other router in the domain.

The router for which the shortest path tree is produced is the root node of the shortest-path tree, which contains a number of leaf nodes that represent the other routers in the domain. A single, shortest route to each other node in the tree is expressed by the shortest-path tree. Every router in the domain has a shortest-path tree generated for it, with the original router serving as the tree's root node. The Dijkstra algorithm, which uses the following stages, is used to find the shortest path for each router. Choose the root node during initialization. The cost between the root node and each associated node should be set to the shortest distance from the root node to that node. Zero is the smallest distance between root nodes. This process is continued until every router has been added to the root node. Two steps below this one

Unicast Routing Protocols

There are two types of routing tables: static and dynamic. An entry-by-hand table is referred to be static. On the other hand, a dynamic table automatically updates whenever there is a change on the internet. Dynamic routing tables are necessary for today's internet. As soon as there is an internet change, the tables need to be updated. For instance, they must be updated if a router goes down and whenever a better route is discovered.

Improvement

A packet is obtained from one network and forwarded to another via a router. Typically, a router connects to many networks. A strategy is to charge for moving across a network. We refer to this cost as a metric. However, the kind of protocol determines the metric given to each network. All networks are treated equally by certain simple protocols, such as the Routing Information Protocol (RIP). One hop via a network costs the same; it is one cost.

Count: The total cost is 10 hop counts if a packet travels across 10 networks to reach its destination.

Routing inside and across domains

One routing protocol may not be able to update all routers' routing tables due to the size of an internet. An internet is split into independent systems as a result. A collection of networks and routers operating under the control of a single administration is known as an autonomous system (AS). Intradomain routing is the term for routing inside an autonomous system. Interdomain routing is a term used to describe routing between autonomous systems. In use are a number of intradomain and interdomain routing protocols.

A. The intradomain routing protocols connect state and distance vector.
B. Path vector is a single interdomain routing mechanism.

The distance vector protocol is implemented by the Routing Information Protocol (RIP). The link state protocol is implemented using Open Shortest Path First (OSPF). Path vector protocol is implemented by Border Gateway Protocol (BGP).

Routeing Using Distance Vectors

The least-cost route between any two nodes is the path with the shortest distance in distance vector routing. According to the name of this protocol, each node keeps a vector (table) of the shortest

distances between each other. By displaying the next stop along the path, the table at each node also directs the packets to the target node (next-hop routing). How to go to any node from node A is shown in the table. For instance, it costs us six dollars to get to node E. C is a stop along the route.

Initialization

Each node in the stable tables in Figure 3.45 is aware of the cost and the best route to take to reach any other node. However, this is not the case at first. Only the distance between a node's direct neighbours, or those with whom it is directly linked, may be known to that node. In order to determine the distance between each node and its immediate neighbours, we will assume for the time being that each node may send messages to these neighbours. Any entry that isn't a neighbour is labelled as having an infinite distance (unreachable).

Sharing

The exchanging of information between neighbours is the foundation of distance vector routing. Node C is aware of node E, although node A is unaware of it. Node A may also know how to contact node E if node C shares its routing table with it. However, although node A knows how to connect to node D, node C does not. Node C will be able to connect to node D if node A shares its routing table with it. In other words, if nodes A and C cooperate with one another, they may both benefit from better routing tables.

Updating

A node must update its routing table after receiving a two-column table from a neighbour. Updates are done in three steps:

For each value in the second column, the receiving node must multiply it by the cost incurred by both it and the transmitting node. This makes sense. The distance between node A and node C, through C, is x + y mi if node C claims that its distance to a destination is x mi and the distance between A and C is y mi.

If the receiving node takes data from any row, it must include the name of the transmitting node as the third column to each row. The next node along the path is the transmitting node.

Each row of the receiving node's old table must be compared to its corresponding row in the changed version of the received table.

The receiving node selects the row with the lower cost if the next-node item is different. If a tie is present, the previous one is retained.

The receiving node selects the new row if the entry for the following node is the same. Assume, for instance, that node C had already advertised a route with a distance of 3 to node X.

Instability in a two-node loop

Instability is a drawback of distance vector routing, which indicates that a network utilising this protocol could have instability. Let's examine the shown example to better comprehend the issue. Infinity's Definition The most straightforward answer is to reinterpret infinity as a lower number, like 100. The system will reach stability in our earlier situation in fewer than 20 updates. In actuality, the majority of distance vector protocol implementations set the distance between each node to be I and the value of 16 to be infinite. However, this implies that huge systems cannot employ distance vector routing. The network cannot have more than 15 hops in each direction.

Divided Horizon Split horizon is a different approach. Each node distributes a portion of its table across each interface in this technique as opposed to flooding each interface with the whole table. If node B's table indicates that it believes the best way to go to X is via node A, then node B need not give A with this information since A already has it (A already knows). Confusion is produced when data is taken from node A, modified, and sent back to node A. In our example, node B trims the end of its routing table before sending it to node A. In this instance, node A maintains a distance to X of infinity.

Link State Routing

The approach of link state routing differs from that of distance vector routing. Each node in the domain may use Dijkstra's algorithm to create a routing table in link state routing if it is aware of the whole topology of the domain, including the list of nodes and links, how they are linked, and the type, cost (metric), and condition of the connections (up or down). Link state routing concept is shown in Figure. The basic domain in the illustration has five nodes. Although each node builds its routing table using the same topology, each routing table is distinct because it was calculated using a different interpretation of the topology. Similar to a city map, this. Despite having the same map, each individual must take a separate path to go to her own destination (Figure 7.6).

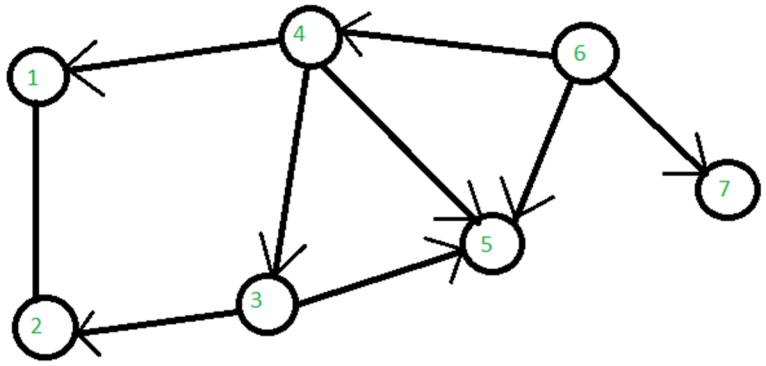


Figure 7.6: Link State Routing

Routing Table Construction:

To guarantee that each node has the routing table displaying the least-cost node to each other node in link state routing, four sets of activities are necessary.

a) Each node creates the link state packet, which contains the statuses of the connections (LSP).
b) Effective and dependable distribution of LSPs to every other router, also known as flooding.
c) Creation of a tree with the smallest distance between each node.
d) Shortest route tree-based routing table calculation.

Different Links

A connection is referred to as a link in OSPF. There are four different categories of links: point-to-point, temporary, stub, and virtual.

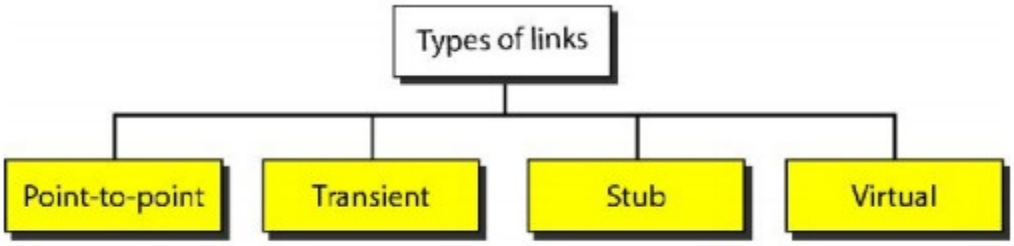


Figure 7.7: Different Links

Without any hosts or routers in between, a point-to-point connection links two routers. In other words, the network's only goal is to link the two routers together. Two routers linked together via a phone line or a T line are an example of this kind of connectivity. This kind of connection does not need a network address. On a graphic, the connection is represented by a bidirectional edge connecting the nodes, while the routers are represented by nodes. The metrics, one for each direction, which are often the same, are shown at the two ends. In other words, there is only one neighbour for each router on the other end of the network.

Path Vector Routing

Intradomain routing protocols include both link state routing and distance vector routing. They can be applied inside an autonomous system, but not across them. The fundamental reason why these two protocols are unsuitable for interdomain routing has to do with scalability. When the operational domain becomes big, both of these routing techniques become unworkable. If the operation domain contains more than a few hops, distance vector routing may become unstable. To generate routing tables, link state routing requires an enormous amount of resources. Flooding also contributes to excessive traffic. A third routing protocol, which we term path vector routing, is required. Interdomain routing has shown to benefit from path vector routing. The idea behind distance vector routing and path vector routing are similar. In route vector routing, we assume that each autonomous system consists of a single node that represents the whole autonomous system.

Initialization

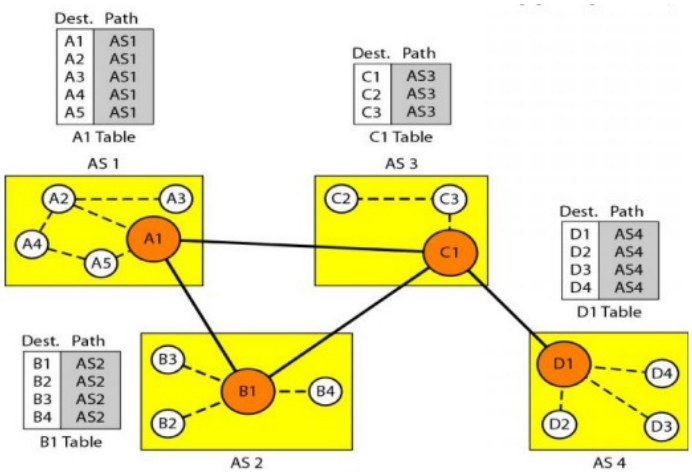


Figure 7.8: Initialization

For AS1, AS2, AS3, and AS4, the speaker nodes are Node Al, B1, C1, and Dl. Node Al provides a first table that lists the locations of Nodes Al through A5 in ASI and how to access them from there. Node B1 makes the claim that Bl to B4 are in AS2 and may be accessed through Bl. so on.

Each speaker node may initially just determine the reachability of the nodes in its autonomous system. Figure in route vector routing, the initial routing tables (Figure 7.8).

Chapter 8

TRANSPORT LAYER

Dr. Santosh S Chowhan, Assistant Professor
Department of Data Science & Analytics, School of Sciences, Jain (Deemed-to-be University), Bangalore-27, India
Email Id- santosh.sc@jainuniversity.ac.in

The primary goal of the transport layer is message delivery from destination to source. The transport layer guarantees that the entire message reaches intact and in the proper order, as well as flow control from the source to the destination. It chooses whether data transmission should take place on a single path or a parallel path. By dividing the message (data) into smaller units and checking for errors and flow control, the transport layer makes sure that the message arrives in the correct order and can be handled more effectively by the network layer.

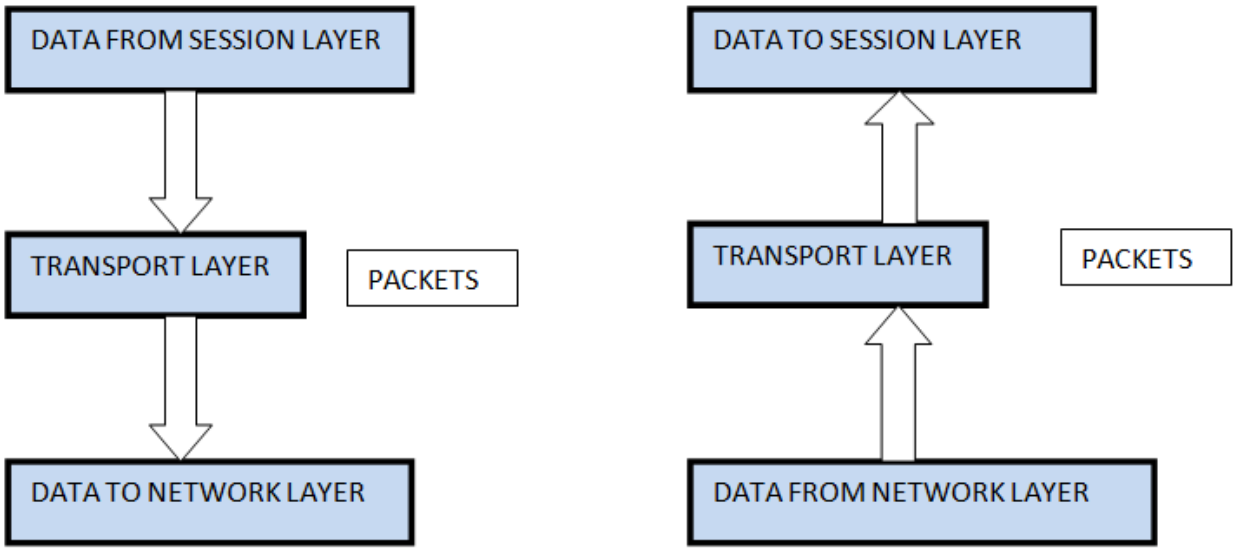


Figure 8.1: Transport Layer

The OSI Model's Transport Layer, which is the fourth layer from the top, offers communication services to application processes that are executing on various hosts. Transport Layer delivers the services to the session layer and it gets the services from network layer. Error correction, as well as segmenting and desegmenting data before and after it is delivered over the network, are among the functions offered by the transport layer. Additionally, the transport layer offers flow control capabilities and guarantees that segmented data is sent across the network in the proper order. The primary function of the transport layer is to enable communication between processes. The functions the Transport Layer provides

1. Communication between processes

Transport Layer is responsible for transmission of message to suitable procedure. To transmit segmented data to the appropriate process among the many processes operating on a given host, Transport Layer employs a port number. Any client-server software may be identified by its port number, which is a 16-bit address used by the transport layer.

2. Multiplication and division

Multiplexing is a function that the transport layer offers to increase the effectiveness of data transfer. DE multiplexing is necessary at the receiver side to gather the data from several procedures. Upward and Downward Multiplexing is provided via the Transport Layer: Multiple transport layer connections using the same network connection is known as upward multiplexing. Multiple transmissions with the same destination are sent over the same network route via the transport layer. Downward multiplexing is the use of several connections via a transport layer link. In order to increase network throughput, this multiplexing enables the transport layer to divide a network connection across numerous channels.

3. Flow management

By controlling data flow, flow control makes sure that the data is transferred at a pace that is acceptable to the sender and recipient. The TCP/IP model's transport layer offers a flow control function to the other levels above it. Sliding window protocol is a concept used by the Transport Layer to offer flow control.

4. Data reliability: Data integrity is provided by the Transport Layer by:

A. Spotting and throwing away corrupted packets.
B. Tracking and retransmission of dropped and lost packets.
C. Identifying duplicate packets and throwing them away.
D. Out of order packets are buffered until the missing packets show up.

5. Avoiding congestion

Congestion may happen in a network if the load on the network exceeds the load capacity of the network. Congestion control refers to the methods and procedures used to reduce congestion and maintain utilisation rates below capacity. The transport layer detects overloaded nodes and decreased traffic rates and responds appropriately to address these issues.

Each layer of the OSI model connects with the relevant layer of the recipient when an email is sent. Therefore, the email is divided into smaller portions when it arrives at the sender's transit layer. After that, the transport layer defines the source and destination ports and sends the broken segments to the network layer. When delivering data to the recipient, the transport layer reassembles every segment and uses the port number to identify the application.

The Transport Layer's Operation

The transport layer transfers services to the session layer after receiving them from the network layer. At the sender's end: The transport layer gathers data from the application layer, or the message, conducts segmentation to split the message into its component parts, adds the source and destination ports to the header, and finally sends the message to the network layer. At the receiver's end, the transport layer gathers data from the network layer, segments it, and then puts it back together. It then reads the message's header to determine the port number and sends the message to the proper port in the session layer.

The Transport Layer's Operation

Protocols for Transport Layers

UDP (User Datagram Protocol) (User Datagram Protocol)

TCP (Transmission Control Protocol) (Transmission Control Protocol)

SCTP (Stream Control Transmission Protocol) (Stream Control Transmission Protocol)

Protocol using UDP Connection Less

Ineffective protocol

One of the simplest transport layer protocols, UDP offers the capability of non-sequential data transfer. UDP is regarded as a transport layer protocol without connections. When speed and size are more crucial than dependability and security, this form of protocol is said to be employed. It is an end-to-end transport level protocol that augments the data received from the top layer with transport-level addresses, checksum error correction, and length information. The UDP protocol creates user datagrams as packets. Format of User Datagram.

User Datagram Format

I. User datagrams contain a fixed-size 8-byte header that is split into four sections:
II. The source port number It has 16 bits and specifies the source port number.
III. Destination port address: It has 16 bits and specifies the destination port number.
IV. Total length: This field is used to provide the user datagram's overall size, which is the sum of the header and data sizes in bytes. A 16-bit field is used.

Segment Format for TCP

1. A 16 bit column called the source port address specifies the application program's port number, which is used to deliver the segment.
2. A 16 bit column called the destination port address specifies the port number of the application software that is receiving the segment.
3. A field of 32 bits known as the sequence number will determine the number allocated to the segment's initial byte of data.
4. A 32-bit parameter called the acknowledgement number indicates which byte the recipient is expecting to receive next from the sender.
5. The 4 bit field known as Header Length (HLEN) is used to determine the number of 4 byte words in the TCP header. TCP headers may range in size from 20 to 60 bytes.
6. A field called "reserved" has six bits that will be used in the future.
7. In this field, there are six distinct independent control bits or flags.

Important pointer

1. ACK: Number of acknowledgements
2. Push Request (PSH)
3. Reset the connection (RST)
4. SYN: Number of sequences Synchronization
5. FIN: Connection closure
6. The 16-bit parameter known as Window Size specifies the window size in bytes for transmitting TCP.
7. A 16-bit parameter called the checksum is used to identify errors.
8. A 16 bit field is the urgent pointer.
9. When there is urgent data in the data segment, this flag is set.

10. For optional information in the TCP header, options and padding may use up to 40 bytes of space.

SCTP

Stream Control Transmission Protocol is its official name. SCTP is one of the protocols for the connection-oriented transport layer. It enables full duplex data transmission between the transmitter and the receiver. This protocol makes it easier to establish connections via wireless networks and to manage the delivery of multimedia data. SCTP Unicast features with many characteristics

Continuity of Transmission

Multi-homing with a focus on messages

Working of the Transport Layer:

The transport layer provides services to the application layer by requesting services from the network layer.

- **At the side of the sender:**

After receiving data (messages) from the application layer, the transport layer performs segmentation, separates the messages into their component parts, appends the source and destination ports to each segment's header, and then sends the message to the network layer.

- **On the side of the receiver:**

The message is forwarded to the proper port in the Application layer by the Transport layer after receiving data from the Network layer, reassembling the segmented data, reading its header, and determining the port number.

- **Transport Layer Services:**
- **Process to Process Communication**

The message delivery to the proper process is the responsibility of the transport layer. To transmit segmented data to the appropriate process among the many processes operating on a given host, Transport Layer uses a port number. Any client-server software can be identified by its port number, which is a 16-bit address used by the transport layer.

- **Multiplication and division**

Multiplexing is a function that the transport layer offers to increase the effectiveness of data transfer. Demultiplexing is necessary at the receiver side to gather the data from several procedures. Upward and Descending Multiplexing is offered by the Transport Layer. Multiple transport layer connections using the same network connection is known as upward multiplexing. Multiple transmissions with the same destination are sent over the same network path via the transport layer. Downward multiplexing is the use of several connections by a transport layer link. In order to increase network throughput, this multiplexing enables the transport layer to divide a network connection between numerous channels.

- **Flow management**

By controlling data flow, flow control ensures sure that the information is transferred at a speed that is acceptable to the sender and recipient.

The TCP/IP model's transport layer offers a flow control services to the other levels above it. Sliding window protocol is a concept used by the Transport Layer to offer flow control.

- **Data reliability**

Spotting and throwing away corrupted packets. Tracking and retransmission of dropped and lost packets. Identifying duplicate packets and throwing them away. Out of order packets are buffered until the missing packets show up.

- **Avoiding congestion**

Congestion may happen in a network if the load on the network exceeds the load capacity of the network. Congestion control refers to the methods and procedures used to reduce congestion and keep utilization rates below capacity. The transport layer detects overloaded nodes and decreased traffic rates and responds appropriately to address these issues.

The transport layer is characterized by two protocols:

- **UDP**

User Datagram Protocol is referred to as UDP. A straightforward protocol, UDP offers non sequential transport capabilities. A connectionless protocol is UDP. When speed and compactness are more important than dependability and security, this kind of protocol is utilized. UDP is an end-to-end transport level protocol that augments the data from the top layer with transport-level addresses, checksum error correction, and length information. The UDP protocol generates a packet known as a user datagram.

Datagram Protocol for Users (UDP)

A communications protocol called User Datagram Protocol (UDP) is largely used to provide low-latency, loss-tolerant connections between internet-based applications.

UDP allows data to be sent before the receiving side provides an agreement, which speeds up transfers. UDP is hence advantageous in time-sensitive communications, such as voice over IP (VoIP), DNS search, and video or audio playing.

A substitute for Transmission Control Protocol is UDP (TCP). Both UDP and TCP are commonly referred to as UDP/IP or TCP/IP since they both operate on top of IP. But there are significant variations between the two. For instance, TCP provides host-to-host communication whereas UDP offers process-to-process communication.

TCP is regarded as a trustworthy transport channel since it transmits discrete packets. On the other hand, UDP is regarded as a best-effort means of communication and transmits packets known as datagrams. This implies that UDP doesn't give any assurances about the delivery of the data or any unique capabilities to retransmit lost or damaged messages.

Two services that the IP layer does not provide are offered by UDP. It offers port numbers to make it easier to differentiate between various user requests. Additionally, a checksum capability is offered as an option to ensure that the data arrived undamaged.

Features of User Datagram Protocol

It is advantageous to utilise User Datagram Protocol with applications that can cope with missing data because of its characteristics. Here are a few instances:

It is appropriate for real-time applications where latency could be an issue since it enables packets to be lost and received in a different sequence than they were delivered.

Where a large number of clients are connected and real-time error correction is not required, such as gaming, audio or video conferencing, and streaming media. It may be used for transaction-based protocols, such as DNS or Network Time Protocol (NTP).

UDP header structure

When encapsulating message data for transmission across network connections, UDP employs headers. A group of parameters known as fields are included in UDP headers and are specified by the protocol's technical requirements. There are four fields with a total of 2 bytes each in the User Datagram Protocol header. Here are some of them:

The length of the datagram in bytes, the size of the UDP header and any encapsulated data, the source port number, the destination port number, the length, and the checksum, which is used for error checking and whose usage is essential.

How UDP operates

To transfer a datagram from one computer to another, UDP requires IP. UDP collects data in a UDP packet and adds its own header data to the packet to carry the data. The source and destination ports for communication, the packet length, and a checksum make up this data. UDP packets are despatched to their destinations after being enclosed in an IP packet.

UDP, unlike TCP, does not ensure that the packets reach their intended recipients. As opposed to TCP, UDP does not establish a direct connection with the receiving machine. Instead, it sends the information out and depends on the intermediary hardware to deliver it to the intended recipient computers.

The majority of programmes wait for any responses they anticipate getting in response to UDP packets. An application either transmits the packet again or gives up if it doesn't get a response within a certain amount of time.

Reliability, ordering, and data integrity are provided by UDP using a straightforward transmission paradigm without the requirement of handshaking conversations. As a result, the UDP service is unreliable. It's possible for packages to come out of sequence, seem like they contain duplicates, or vanish suddenly.

Although there is no assurance that the data being sent will arrive at its intended location, this transmission technique does offer a minimal overhead and is often used for services that don't have to function perfectly the first time.

UDP operation

The following list of UDP's many operations:

1. Connectivity-Free Services

Each user datagram delivered by UDP is an individual datagram since the User Datagram Protocol delivers Connectionless Services. Even if they originate from the same source process and are directed toward the same target programme, there is no link between various datagrams. There is no connection setup or termination, nor are user datagrams given a number. Each datagram mostly follows a separate route.

2. Flow regulation and error prevention

A very basic and unstable transport protocol is the user datagram. There is no window mechanism since it does not provide any flow control. As a result, the recipient can be overwhelmed with incoming communications. UDP only offers checksum as an error control method. Because of this, the sender is unable to determine if any messages have been lost or duplicated. Because there are no methods for flow control or error control, the process that utilises UDP should have these features.

3. Capsular and decapsular processes

The user datagram protocol wraps and decapsulates the message in the form of an IP datagram in order to transport it from one process to another.

UDP applications

Applications that call for lossless data communication may utilise UDP. UDP could be used, for instance, by an application that is set up to control the process of retransmitting missing packets and properly arranging incoming packets. Compared to TCP, this strategy may aid in enhancing the data transmission rate of huge files. UDP is in Layer 4, or transport, of the Open Systems Interconnection (OSI) communication paradigm. UDP collaborates with higher-level protocols like the trivial file transfer protocol (TFTP), real-time streaming protocol (RTSP), and simple network management protocol to assist manage data transmission services (SNMP). Video, voice, and gaming. For network applications where perceived latency is important, including in gaming, audio, and video communications, UDP is the best protocol. These illustrations may experience some data loss without degrading in apparent quality. Although there may be some loss, forward error correcting methods are sometimes employed in addition to UDP to enhance audio and video quality.

Services without a set packet transfer requirement

Applications that need the secure flow of information may also utilize UDP, but they should have their own ways of responding to packets. These services are useful since they are not constrained by predetermined patterns to ensure the accuracy and completeness of the delivered data packets. Users may choose how and when to react to inaccurate or poorly organized information.

Protocols for routing updates and multicasting

Due to its capability for packet switching, UDP may also be used for multicasting. Additionally, several routing update protocols, such Routing Information Protocol, employ UDP (RIP).

Speedy apps

UDP may be used in situations where dependability is not as important as speed. In a situation when it's acceptable to lose a few data points from a quick capture, it could be wise to utilize UDP.

- **TCP**

Transmission Control Protocol is known as TCP. Applications can access all transport layer services using it. Since the link between the two ends of the transmission must be established, it is a connection-oriented method. TCP creates a virtual circuit between both the sender and receiver for the period of a transmission in order to establish the connection. Protocol for Transmission Control (TCP). A server and a client are connected through the Internet protocol known as the Transmission Control Protocol (TCP). The set of networking protocols that allow computers to

connect over the Internet are TCP and Internet Protocol (IP). Internet traffic carries data in packets. They are broken down into packets for travel, and when they arrive at their destination, they are put back together. The dependability of the rails on which they move is managed by TCP to prevent packet loss, guarantee that they are sent in the right sequence, and prevent delays that might harm the quality or reassembly of the data. Data is addressed and sent to and from its correct destinations using IP. TCP/IP operate in tandem as a stack of protocols, one on top of the other. The Defense Data Network of the US Department of Defense invented TCP, and it is today's widespread usage that makes the Internet widely accessible for commercial purposes.

Characteristics of the Transmission Control Protocol

The TCP characteristics are listed below:

The Numerical System

TCP primarily uses the sequence number and acknowledgment number fields. Byte Number is the primary reference in these two TCP variables. Data Size: TCP assigns numbers to the bytes of data that are being sent throughout each connection. The majority of the numbering begins with a randomly generated number. All of the data bytes that are transferred via a connection are primarily numbered by TCP. For the first byte's number, it creates a random number between 0 and 2 raised to the power of 32. The bytes are numbered from 1056 to 7055 if the random number is 1056 and there are a total of 6000 bytes to be delivered. Numeral Order After allocating a numerical value to each byte, the TCP divides the data into "segments." Each segment being transmitted has a sequence assigned to it. Each segment's sequence number is determined by the first byte that is contained in that segment. As a result, the value in the segment's sequence number field mostly determines the number of the segment's initial data byte. Number of Acknowledgement A party's primary expectation for the following byte is determined by the value of the acknowledgement field in the segment.

Flow Management

The TCP offers the flow control feature. The quantity of data that is to be transferred by the sender is controlled by the recipient via TCP. The fundamental goal of the flow control is to keep the receiver from being overloaded with data. Additionally, the numbering scheme enables TCP to use byte-oriented flow control.

Error management

TCP includes an error control system since it offers dependable services, which is why it serves this function. However, the Error control uses the segment as the data unit for error detection. Byte-oriented error control is the norm nowadays.

Congestion management

Congestion control in the network is another important function of TCP. In addition to the receiver, network congestion also influences the amount of data that the sender delivers.

Full Duplex

Another capability offered by TCP is Full Duplex, which enables data to be transferred in both directions. Since it is primarily used to carry data from the sender to the receiver, TCP is a transport layer protocol.

Segment

The TCP packet is mostly referred to as a segment.

Format

The application software is followed by a 20–60 byte header, which makes up the majority of the segment. The header is typically 20 bytes, however if there are no choices, it may be up to 60 bytes if there are several options. Port Source Address: It is a 16-bit value that primarily specifies the host's application program's port number, which is used to transmit segments. The Source port address serves the same function as the Source port address in the UDP header. Port of Destination: Address This address is similarly 16 bits long and used to provide the port number of the host's primary application software for receiving segments. The Destination port address serves the same function as the Destination port address in the UDP header.

Numeral Order:

It is a 32-bit field that primarily specifies the number given to the segment's initial byte of data. Number of Acknowledgement: It is mostly used to provide the byte number that the receiver of the segment expects to receive from the other party and is similarly a 32-bit field. Title Length It is mostly used to identify the number of 4-byte words in the TCP header and is a 4-bit field. The header is anything from 20 to 60 bytes long.

Reserved: It is a 6-bit field that is mostly set aside for usage in the future.

Control Six separate control bits or flags are primarily defined by this field, and only one of them may be changed at any one moment. These bits primarily allow the TCP flow control, connection setup, connection termination, and data transport modes.

Window Size: The primary use of this parameter is to specify the window's size. This field has a 16-bit size. It mostly specifies how much data the receiver can handle in a given size. The receiver is primarily responsible for determining this field's value.

Checksum: The checksum is mostly included in the 16-bit field. In the case of TCP/IP, this field is required.

Quick Pointer This field's 16-bit size makes it only usable in situations when the urgent flag is set. Only when the segment includes urgent data is this field utilized.

Connection TCP

TCP creates a virtual route between the source and the destination since it is a connection-oriented protocol, as is well known. Then, this virtual route is used to send all of the message's parts.

Three stages are mostly needed for connection-oriented transmission in TCP, and they are as follows:

1. Phase of Connection Establishment
2. Phase of Data Transfer
3. Connection cut off.

Benefits of TCP

Several benefits of TCP are listed below:

1. TCP provides methods for data control and flow control.

2. TCP offers top-notch cross-platform support.
3. The data transmission of the TCP protocol is assured.
4. It sends the data in a certain sequence from the transmitter to the recipient.
5. It is a trustworthy and connection-oriented protocol.
6. It has a respectable throughput via a modem or LAN.
7. Offers a checksum-based error detection technique, and a go-back protocol or ARP-based error rectification mechanism.

The drawbacks of TCP

1. Neither broadcasting nor multicasting are permitted to utilise it.

2. The quantity of overhead has increased.

Providing services through the Transport Layer

The transport layer offers services that are comparable to those of the data link layer. While the transport layer offers services across an Ethernet network made up of numerous networks, the data link layer offers a service within a single network. While the transport layer is in charge of all the lower layers, the data link layer is in charge of the physical layer. There are five categories into which the services offered by transport layer protocols can be divided:

1. Complete delivery
2. Addressing
3. trustworthy delivery
4. Flow regulation
5. Multiplexing

UDP vs. TCP

The TCP/IP protocol suite, which contains a variety of protocols for conducting network communications, includes TCP and UDP. The key differences between TCP and UDP may be compared

Due to its capacity to divide enormous data sets into individual packets, check for and resend missing packets, and reassemble packets in the proper order, TCP has become the dominant protocol used for the majority of internet communication. However, the increased data overhead and delay associated with these extra services come at a price. UDP, on the other hand, is regarded as a connectionless protocol since no virtual circuit must be created prior to any data transmission. The communication protocol just delivers the packets, which results in much less delay and bandwidth overhead. When using UDP, packets may follow many routes from source to recipient. Some packages could therefore be misplaced or received out of sequence.

UDP features consist of the following:

The packets don't always arrive in the correct sequence, but it is a connectionless protocol that is used for VoIP, video streaming, gaming, and live broadcasting.

It is better suitable for applications that need quick, effective transmission, such as gaming. It enables missing packets the sender cannot tell if a packet has been received. TCP features consist of the following: It is the most extensively used protocol on the internet and is connection-oriented It ensures that all transmitted data reaches the appropriate receiver and that no packets are lost. It

delivers packets in the correct sequence to make putting them back together simple. It uses up more resources and is slower. It is best suited for applications that need high dependability, and transmission speed is comparatively less important; it has a larger header than UDP.

Congestion: a condition that happens at the network layer when there is so much message traffic that it slows down network response time.

Congestion's effects

Performance declines as delay rises.

Retransmission takes place as the delay grows, making the problem worse.

Congestion-controlling techniques

A system called congestion management regulates the flow of data packets into the network, allowing for more efficient use of a shared network infrastructure and preventing congestive collapse.

Congestive-Avoidance Algorithms (CAA) are used as a technique to prevent congestive collapse in a network at the TCP layer.

The following are two congestion control algorithms:

Leaky Bucket Method

The leaky bucket method finds applications for shaping or rate-limiting network traffic. For traffic shaping algorithms, a token bucket execution and a leaky bucket execution are often utilised. With the help of this method, the network's transmission rate may be managed, and bursty traffic can be turned into a constant stream. When compared to the leaky-bucket method, the drawbacks include the ineffective utilisation of available network resources. The bandwidth and other extensive network resources are not being utilised efficiently. Think of a bucket that has a little hole at the bottom. No matter how quickly water enters the bucket, the pace at which it exits remains constant. Water that is added after the bucket is full flows over the edges and is lost.

Vacant Bucket

Similar to this, each network interface has a leaky bucket, and the leaky bucket method involves the following steps:

1. Packets are dropped into the bucket when the host wishes to transmit them.
2. The network interface broadcasts packets at a consistent pace because the bucket leaks at a constant rate.
3. The leaking bucket converts chaotic traffic into regular flow.
4. The bucket really functions as a finite queue with a finite rate of output.

Bucket algorithm for tokens

The output architecture of the leaky bucket method is stiff at an average rate irrespective of the bursty traffic. When there are significant bursts, certain applications enable the output to accelerate. This need a more adaptable algorithm, ideally one that never loses data. A token bucket approach is therefore useful for rate-limiting or filtering network traffic. It is a control algorithm that suggests the best times to send traffic. Based on how many tokens are visible in the bucket, this ranking is generated.

Tokens are in the bucket. Each token designates a packet of a certain size. To allow sharing of a packet, tokens in the bucket are erased. If there is no token, no flow will transmit packets. As a result, a flow transfers traffic in good tokens in the bucket up to its max burst rate.

Token bucket algorithm needed

1. No matter how bursty the traffic is, the leaky bucket algorithm enforces output pattern at the average rate. So that the data is not lost, we need a flexible method to handle the bursty traffic. Token bucket algorithm is one of these algorithms.
2. The following steps of this method may be explained:
3. Tokens are dropped into the bucket at regular intervals.
4. The bucket can only hold so much.
5. A token is taken out of the bucket and the packet is transmitted if there is a ready packet.
6. The packet cannot be transmitted if there is no token in the bucket.

Five packets are ready to be transferred while a bucket containing three tokens. A packet must capture and destroy one token in order to send it. Three of the five packets have passed through, while the other two are blocked awaiting the generation of further tokens. Although it is fairly conservative in nature, the leaky bucket method regulates the pace at which packets are introduced into the network. The token bucket algorithm is given some latitude. Each tick of the algorithm generates a token for the token bucket (up to a certain limit). An incoming packet must capture a token before it can transmit, and transmission happens at the same pace for all incoming packets. As a result, if tokens are available, some of the busy packets are broadcast at the same pace, adding some system flexibility.

TCP Congestion Management

Let's first define what you mean by congestion in the TCP network before discussing TCP congestion management. An essential component of a packet switching network is congestion. It describes the condition of a network where message traffic is so high that the network's response time slows down, resulting in packet failure. Loss of packets results. As a result, network congestion must be managed, even if it cannot be prevented.The term "TCP congestion control" refers to the system that either stops congestion before it starts or clears it out after it does. TCP responds to network congestion by lowering the size of the sender's window. The following two elements define the sender's window size:

1. Receiver window dimensions
2. large congestion window
3. Receiver Window Dimensions
4. It demonstrates how many bytes of data a receiver can take in without responding.
5. Reminders about receiver window dimensions:
6. Data should not be sent that is larger than the receiver window size.
7. Because a TCP segment is dropped when the amount of data provided exceeds the capacity of the receiver's window, TCP must be retransmitted.
8. As a result, the sender should only ever communicate data that is less than or equal to the receiver's window.

Traffic Window

The sender's ability to transmit a certain quantity of data into the network even before getting acknowledgement is limited by TCP's state.

The following are important considerations for the congestion window:

Various TCP variations and techniques are used to determine the congestion window's size.

The congestion window's size is only known by the sender, and it is not communicated via the connection or network. The sender's window size is calculated using the following formula: Minimum Sender window size (Receiver window size, Congestion window size)

Congestion's root causes and costs

1. The reasons of network congestion are as follows:
2. Consumption of bandwidth that is excessive: Some devices may use more bandwidth than other devices do. This may sometimes place a burden on the network and its hardware, such as routers, and result in network congestion.
3. Improper subnet management: A bigger network is partitioned into many subnets in order to be managed more effectively. Ineffective scaling and management of these subnets results in network congestion.
4. Multicasting: Multicasting is the process through which a network enables simultaneous usage and communication by several computers. A collision may happen if two packets are transmitted at the same time; if this happens often, the network becomes crowded.
5. Outdated hardware: If communication is conducted using outmoded routers, switches, or servers, data transmission may be impeded.
6. Border gateway protocol (BGP): BGP uses the shortest path to route all traffic in a network. The volume of traffic on a route is not taken into account while routing. If a scenario like this arises, there is a chance that the packet will use the same path and generate network congestion.

Chapter 9

APPLICATION LAYER

Sampangirama Reddy B R, Assistant Professor
Department of Computer Science & IT, School of Sciences, Jain (Deemed-to-be University), Bangalore-27, India
Email Id- sampangi.reddy@jainuniversity.ac.in

Internet domain names are identified and converted into Internet Protocol (IP) addresses using the domain name system (DNS), a naming database. The IP address that a computer uses to find a website is mapped to that website's name via the domain name system. For instance, a server in the background transfers a user's typing of "example.com" into a web browser to the associated IP address. 203.0.113.72 is comparable to an IP address in structure. The majority of internet activities, including web surfing, depend on DNS to rapidly provide the information required to link users to distant servers. On the internet, DNS mapping is dispersed according to a hierarchy of authority. Governments, universities, and other institutions, as well as access providers and businesses, often have their own allotted IP address ranges and domain names. In most cases, they also control the DNS servers that translate those names to those addresses. The domain name of the web server that processes client requests serves as the foundation for the majority of Uniform Resource Locators (URLs).

How DNS operates

DNS servers translate URLs and domain names into computer-friendly IP addresses. They convert human input into something a computer can understand in order to locate a website. DNS resolution refers to the translation and lookup procedure.

The following phases make up the fundamental process of a DNS resolution:

1. The user types a domain name or web address into a browser.
2. To determine which IP or network address the domain points to, the browser sends a message to the network known as a recursive DNS query.
3. The request is sent to a recursive resolver, also known as a recursive DNS server, which is typically run by the internet service provider (ISP). The user will get the address back if the recursive resolver has it, and the website will load.
4. The DNS root name servers, top-level domain (TLD) name servers, and authoritative name servers will all be consulted if the recursive DNS server is unable to get a response.
5. The three server types cooperate and carry on rerouting until they locate a DNS record with the requested IP address. The users desired website loads once this information is sent to the recursive DNS server. DNS root name servers and TLD servers mostly redirect requests rather than solving problems directly.
6. The A record for the domain name, which includes the IP address, is stored or cached by the recursive server. The next time it gets a request for that domain name, it may answer to the user directly rather than asking other servers for information.
7. If the authoritative server receives the request but is unable to locate the data, it produces an error message.

It just takes a fraction of a second to query all the servers, and the user often isn't aware of it.

Both inquiries from inside and outside of their own domains are answered by DNS servers. A server responds with the authoritative response when a request for information about a name or address within the domain comes from outside the domain.

DNS architecture

A URL typically contains the domain name. A domain name is composed of several labels. Each part of the domain hierarchy represents a subdivision and should be read from right to left.

Following the period in the domain name is the TLD. There are several top-level domains, but some examples include .com, org, and.edu. Some domains, like.us for the United States or.ca for Canada, may indicate a country code or specific geographic area.

Each label next to the TLD on the left indicates a different subdomain of the domain on the right. For instance, "techtarget" is a subdomain of.com and "www." is a subdomain of techtarget.com in the URL www.techtarget.com.

Each label may have up to 63 characters, and there can be 127 levels of subdomains. Up to 253 characters may be used in the domain's total character count. A totally numeric TLD name is prohibited, and labels cannot begin or finish with hyphens.

Request for Comments (RFC) 1035, published by the Internet Engineering Task Force (IETF), contains standards for establishing domain names.

Kinds of DNS servers

A DNS resolution involves a number of different server types. The four name servers are shown below along with a description of how a query moves through them. They provide the desired domain name or pointers to other name servers. Recursive server is one. A web browser is one example of an application that sends DNS requests to the recursive server. It is the initial resource the user accesses, and depending on whether it has the answer to the query cached or not, either supplies it or visits the next-level server. Before responding to a client's query, this server may make numerous query iterations.

The root name server

If the recursive server doesn't have the response cached, it sends a query to this server first. An index of all the servers that will hold the requested information is kept on the root name server. The Internet Corporation for Assigned Names and Numbers (ICANN), more precisely a division of ICANN known as the Internet Assigned Numbers Authority, is in charge of monitoring these servers. The top-level domain in the URL—the.com,.edu, or.org—is used by the root server to determine where to send the request. This section of the search is more detailed.

A trustworthy name server.

The authoritative name server serves as the DNS query's last safeguard. These servers manage the subdomain portion of the domain name and are completely knowledgeable about a certain domain. These servers hold DNS resource entries, such as the A record, that provide detailed information about a domain. They provide the required record to the recursive server, which then sends it back to the client and caches it nearby for further lookups.

The recursive server mostly asks on behalf of the user, and the authoritative server primarily responds to the user's query, is a straightforward way to understand the process. As the request moves from the recursive server to the appropriate authority, the root and TLD servers process it.

Many DNS query types

The most common DNS requests that occur at various stages of DNS resolution are those listed below:

Recursive DNS requests are those that happen between the client and the recursive server. Either the complete name resolution or an error message stating that the name cannot be found is sent as the response. Recursive queries either provide the correct response or an error.

Recursive resolver, a local DNS server, and nonlocal name servers, such as the root, TLD, and authoritative name servers, exchange DNS requests iteratively. The name servers may provide a reference in response to iterative requests rather than a name resolution. The TLD directs the recursive server to an authoritative server after being referred by the root server to the TLD. If the authoritative server has the domain name, it gives it to the recursive server. Both a response and a referral are possible outcomes of iterative questions.

Nonrecursive queries are those for which the answer is already known to the recursive resolver. Either the recursive server has the response in its cache or it is aware to bypass the root and TLD servers and go straight to a certain authoritative server. There is no need for more queries, hence there is no request for them, making it nonrecursive. Nonrecursive queries have a solution. It is a nonrecursive query if a recursive resolver provides an IP address from a prior request that it has cached from a previous session.

In the fundamental DNS procedure, a client sends a recursive query to the recursive resolver, which sends a sequence of iterative questions that refer to the next iterative query. Once the authoritative server receives the query, it issues a nonrecursive query to get the response if the recursive resolver believes it will be present. The data is then saved on the recursive resolver (see "DNS caching" section) so that it may be retrieved in the future by a nonrecursive query.

Typical DNS records

A query looks for information in DNS records. Different information is needed depending on the query, client, or application. Some records, like the A record, must be kept.

There are several sorts of DNS records, each serving a specific function in indicating how a query should be handled. These common DNS records are available:

A document. This contains a domain's IP address and stands for "address." For IPv4 addresses only, A records are used. Instead, IPv6 addresses contain AAAA records, which make advantage of the lengthier format. The majority of websites have only one A record, however some bigger sites have numerous, which aids in load balancing by sending several A records to various visitors during periods of high traffic.

NS entry. These name server records identify the authoritative server in charge of maintaining all the data for a certain domain. To boost dependability, domains often have both primary and backup name servers, and several NS records are used to point queries at them.

A TXT entry. Administrators may insert text into DNS using TXT records. Although machine-readable annotations are now often added to DNS, human-readable remarks were the original intention. TXT records are used to safeguard email, prevent email spam, and verify domain ownership.

CNAME entry. When there is an alias, canonical name records are used rather than an A record. They are used to retry the same IP address's inquiry with two alternative domains. As an example, the CNAME would query techtarget.com in the URL searchsecurity.techtarget.com.

DNS boosts website performance

The A records, or IP addresses, that servers get from DNS queries may be cached for a predetermined period of time. By increasing efficiency, caching enables servers to react rapidly the following time a request for the same IP address is received.

For instance, the local DNS server would only need to resolve the name once if everyone in the workplace needed to watch the same training video on a certain website on the same day. After that, it could serve any subsequent requests from its cache. The time to live (TTL), often known as the duration of the record, is determined by administrators and is based on a number of variables. Shorter time intervals provide the most precise results, while longer ones lessen the pressure on servers.

Cache DNS

DNS caching seeks to shorten the time it takes to get a response to a DNS query. Caching allows DNS to provide the same information to clients quicker the next time they query it by storing prior replies to requests closer to the clients.

There are many areas where DNS data may be cached. Typical examples include the following:

Browser. Most browsers, including Apple Safari, Google Chrome, and Mozilla Firefox, automatically cache DNS information for a certain period of time. Before the request leaves the computer for a local DNS resolver server, the browser is the first cache that is examined when a DNS request is made.

Computer system (OS). Stub resolvers, which are incorporated into many OSes, cache DNS information and respond to requests before they are routed to an external server. Typically, the OS is questioned after the browser or other querying tool.

A resolver that recurses. On the DNS recursive resolver, the response to a DNS query may also be cached. DNS resolution stages may be skipped by resolvers if they already have part of the records required to respond. For instance, the resolver may bypass the root server and ping the TLD server directly if it only contains a records and no NS records.

DNS safety

There are a few flaws in DNS that have been found throughout time. One such vulnerability is DNS cache poisoning. Data is delivered to caching resolvers via DNS cache poisoning while acting as an authoritative origin server. The data may then include inaccurate information and have an impact on TTL. It is also possible for actual application requests to be diverted to a malicious host network.

With the goal of tricking consumers into thinking the website is legitimate, someone with bad intentions may develop a risky website and get access to their personal data. A user might be tricked into choosing a bogus link by changing a domain name's character with one that looks similar—for example, substituting the number 1 with the letter l. Phishing scams often use this as an opening.

DNS Security Extensions are available for personal usage and security. They accept replies that are cryptographically signed.

A quick overview of DNS

In the 1970s, Elizabeth Feinler from the Stanford Research Institute kept a single file named "HOSTS.TXT" that included all hostnames and their accompanying numerical addresses. Feinler manually assigned numerical numbers to domain names in this directory, which became known as the Advanced Research Projects Agency Network, or ARPANET. Calling Feinler was necessary to enter a new name in the directory. This method was too ineffective to continue by the 1980s. The domain name system was developed in 1983 to disperse what had previously been a single, centralised file containing each address among several servers and locations. One of the first internet standards, according to the IETF, was DNS in 1986. That group released two publications, RFC 1034 and RFC 1035, outlining the DNS protocol's specifications and the kinds of data it could convey. In order to suit the increasingly complicated internet since then, DNS has been regularly upgraded and extended. Large, all-encompassing information technology firms like Google and Microsoft now provide their own DNS hosting services.

Email

The Internet is used to transmit messages, which is referred to as email. It is a function that is utilised the most often across communication networks and might include text, files, photos, or other attachments. Typically, it involves sending data that is saved on a computer through a network to a specific person or group of people. Email communications are sent through email servers and employ a variety of TCP/IP protocols. For instance, the simple mail transfer protocol (SMTP) is a protocol that is used to transmit messages, while IMAP or POP are used to receive messages from a mail server. You only need to input a valid email address, a password, and the mail servers used to send and receive messages in order to log into your mail account. You simply need to provide your email address and password since the majority of webmail services establish your mail account automatically. However, if you use an email programme like Microsoft Outlook or Apple Mail, you may have to manually setup each account. You may also need to input the incoming and outgoing mail servers as well as the appropriate port numbers for each one, in addition to the email address and password.

- Three parts are included in email messages, and they are as follows:
- The message envelope represents the electronic format of the email.
- Email subject line and sender/recipient information are included in the message header.
- Body of message: It includes text, graphics, and other file attachments.

The original email standard could only accept plain text communications, thus the email was designed to provide rich text with customised formatting. Email can now support the same layout as webpages since it is capable of supporting HTML (Hypertext Markup Language). Links, photos, CSS layouts, and files, or "email attachments," may all be included in emails that support HTML. Users may send several attachments with each message on most mail servers. In the early days of email, attachments were often restricted to one megabyte. Even yet, many mail servers in use today can accommodate email attachments that are 20 megabytes or more in size. Ray Tomlinson sent the first email to himself in 1971 as a test message. The wording of this email was "something like QWERTYUIOP." Nevertheless, even though he sent the email to himself, it was still sent across the ARPANET. Up until 1996, electronic mail predominated over postal mail in terms of volume transmitted.

A comparison between email and webmail

Today, both browser-based and non-browser-based electronic mail are widely referred to as emails. AOL and Gmail are web-based email services, whereas Outlook for Office 365 is a non-web-based email service. Email was formerly distinguished as a non-browser application that required a specific client and email server. The benefits of non-browser emails include improved security, interaction with business software systems, and a lack of ads.

Email's purposes

Email may be used for a variety of purposes, including personal communication between two individuals, a small group of people, or an entire company. The majority of people find email communication with coworkers, friends, individuals, or small groups to be beneficial. It enables you to share and receive photographs, documents, links, and other things while communicating with people all over the globe. It also allows users to interact on their own terms and at their own convenience.

Another advantage of email communication is that it may be used to send professional follow-up emails after meetings and to remind participants of upcoming deadlines and time-sensitive tasks. Email communication is best for two-person or small group conversations. Additionally, users may instantly notify everyone about all planned activities or update the group on a schedule change via email. Additionally, it may be utilised by businesses or organisations to instruct a sizable workforce or clientele. Email is mostly utilised for newsletters, which are used to send email marketing campaigns and promoted content from businesses to mailing list members. Email may also be used to convert leads into paying clients or drive a latent transaction toward completion. For instance, a business may develop an email that is used to automatically send emails to online shoppers who have items in their shopping carts. This email may encourage customers to buy the products in their basket before they run out of stock by reminding them that they have them there. Additionally, emails are utilised to solicit feedback from clients after they make a purchase. By incorporating a question on service quality, they may conduct a survey.

Evolution of email

Email is significantly older than ARPANet or the Internet. Early email was just a little improvement over what is today referred to as a file directory. It was used to just place a message in another user's directory, where they could access it by signing in. Like placing a letter on someone's desk, as an illustration. It's possible that Massachusetts Institute of Technology utilised MAILBOX, the earliest email system of its kind, which dates back to 1965. Another pioneering software was SNDMSG, which was used to transfer messages between computers.

Email messages could only be sent to many users of the same machine while internetworking was not yet active. When computers started communicating with one another across networks, the issue grew somewhat more complicated, necessitating the use of envelopes with proper addresses for each recipient.

Ray Tomlinson created email later that year to help with certain issues. Tomlinson served as an ARPANET contractor for Newman and Bolt Beranek, like many other Internet pioneers. He selected the @ symbol from the keyboard to signify transmitting messages from one machine to another. Then, with the use of Internet protocols, it was simple to send a message to someone else; all they had to do was suggest name-of-the-user@name-of-the-computer. Internet pioneer Jon

Postel was one of the new system's initial users. Also ascribed to Jon Postel, who described it as a "great hack."

Despite the fact that the World Broad Web provides a wide range of services, email is still the most popular and crucial Internet application. Email is used by more than 600 million individuals worldwide. By 1974, hundreds of people were using email, thanks in part to ARPANET. A major change in Arpa's mission was also brought about by email, which emerged as Arpanet's rescuer.

The email system underwent fast growth beginning in. Sorting emails was a significant improvement, and Larry Roberts even created some email folders for his employer. In 1976, John Vittal created some software to structure an email. By 1976, email had really taken off and commercial packages had started to emerge. People were now on the Internet instead of Arpanet after receiving the email. There were several intriguing things here that common folks everywhere wished they could utilise.

A few years later, Ray Tomlinson made a comment about email. Every new development moves quickly and is almost always followed by the one before it. I believe a major revolution would be necessary to address all the changes.

The offline reader was one of the first innovations when personal computers first appeared. Once offline readers became available, email users could view and save their email on their own computers. Additionally, they were able to create responses without really being connected to the network, much as Microsoft Outlook can now. This was especially helpful for those in regions of the globe where phone service was more costly than email.

It was possible to create a response without a phone connection, connect to the network to transmit it, and pay significant connection fees every minute. Additionally, the offline mode made for more straightforward user interfaces, which was helpful. The ability for text to wrap around on the user's computer screen was often lost in the present era with relatively few standards connecting directly to the host email system, along with additional annoyances as the possibility that the backspace and delete keys wouldn't function. More assistance was provided by offline readers in overcoming these types of obstacles.

The first significant email standard was the SMTP (simple mail transfer protocol). It was an outdated protocol that was very naive. And no effort was taken to track down the sender of the communication, whether it was accurate or not, as alleged. Fraudulent in the email addresses was relatively simple and is still possible. Later, security frauds, worms and viruses, and spammers using forged identities utilised these fundamental protocol weaknesses. Some of these issues from 2004 are still being investigated for a solution.

However, a more advanced email system included certain crucial characteristics that made it easier for consumers to interpret email. One of the first effective commercial systems, Eudora, was created by Steve Dorner in 1988. However, it took a while for it to show up once Pegasus mail arrived. When POP (Post office protocol) for email on the Internet started to develop as a standard, servers started to become commonplace. Before there existed a uniform post office protocol, each server was a bit unique (POP). POP was a crucial standard that made it possible for users to collaborate.

In those days, each individual dialup user had to pay a minute-by-minute fee for an email. Additionally, email and email discussion groups were the most popular applications of the Internet for most users. Numerous problems covering a broad range of topics eventually came to be known

as USENET as a collection of newsgroups. Email became accessible over the World Wide Web (WWW), and service providers like Hotmail and Yahoo provided it with a straightforward user interface. Additionally, there were no fees for customers to pay on these services. Given that email is so easy to use and so reasonably priced, everyone now wants at least one email account.

By the 1980s, Internet Service Providers (ISPs) were establishing connections between individuals all over the globe. Additionally, by 1993, Internet use was becoming more popular, and email took the position of electronic mail. Email is becoming the preferred method of communication with individuals throughout the globe. Since so many individuals communicate by email, the system is always being updated. Even though email has certain security vulnerabilities, throughout the years rules have been established to stop the proliferation of spam email.

Benefits of Email

Email has a variety of benefits, including the following:

Cost-effective: Due to the abundance of free email services accessible to both people and businesses, email is a relatively affordable method of communication. Once a user is online, there are no more fees for the services. If a person has an Internet connection, they may access their email at any time and from any place. Email gives you a permanent method of contact that lets you respond whenever it's convenient for you. Additionally, it gives users a better way to converse effortlessly despite having various schedules.

Speed and ease: With the right connections and information, email may be written extremely quickly. There is very little lag time, so it may be swiftly traded.

Mass messaging: Email makes it simple to communicate with a lot of people at once.

Users may preserve significant discussions or confirmations in their records and search for and quickly recover them when required by saving email exchanges for later retrieval.

Users of email may classify and filter their communications using a straightforward user interface. This might assist you in identifying undesired communications, such as spam and junk mail. Additionally, users may quickly locate certain messages when they are required.

Emails are delivered very quickly when compared to conventional mail.

Email is good for the environment since it uses no paper. By using less paper, it lowers the cost of paper and contributes to environmental protection.

When you respond to an email, it also has the advantage of allowing you to attach the original message. When the receiver is knowledgeable about the subject and you get hundreds of emails every day, this is advantageous.

Email marketing is also useful for selling things. Organizations or businesses may communicate with many individuals and inform them quickly since email is a mode of communication.

Email disadvantages include impersonality and lack of intimacy compared to other modes of communication. For instance, speaking on the phone or meeting in person is preferable over email when talking with someone.

Misunderstandings: Since emails just include text, there is no context provided by speech or body language. Therefore, email makes it simple for misunderstandings to happen. Email jokes may be taken seriously if they are sent by someone. Additionally, well-intended information might be

hastily transcribed as unpleasant or confrontational, which can have an incorrect impression. Additionally, it is simple for material to be misunderstood if it is written in emails using brief abbreviations and explanations.

Malicious Use: Anyone with a single email account is able to send emails. You could sometimes get mail from an uninvited source, which might be dangerous in terms of identity theft. They may thus use email to propagate rumours or inaccurate information.

Accidents Will Occur: When using email, rushing to press the incorrect button might result in disastrous errors. For instance, you may unintentionally email private material to a broad group of individuals rather than a single recipient. As a result, if you click the incorrect name in an address list, the information may be shown. As a result, it may be damaging and cause significant difficulties at work.

Spam: Although email's functions have recently improved, there are still significant problems with spam and unwanted advertising reaching inboxes. It requires time and effort to manage and is often overpowering.

Information overload might occur since it is so simple to send emails to numerous recipients at once. It is a significant issue in many contemporary organisations where it is necessary to transmit a lot of information but hard to determine whether an email is vital. Email also requires structure and maintenance. One of the major issues with email is the uneasy feeling you get after returning from vacation to see hundreds of unread emails in your inbox.

Viruses: Email is one of the most popular ways for viruses to infiltrate systems and spread across them, despite the fact that there are other methods as well. Sometimes when you receive email, a virus may be attached to a document. Additionally, when you click the email's link or open the attachment, the virus may enter your computer. Infected emails may also be sent by an anonymous sender, a friend, or another trustworthy contact.

Pressure to React: If you get emails and do not reply, the sender may become irritated and believe that you are ignoring them. As a result, you may want to put pressure on yourself to continue reading emails and then responding in some manner.

Time-consuming: Reading, writing, and responding to emails when you get them may take up a significant amount of time and effort. Email is where many contemporary professionals spend the majority of their time, which may make it take longer to finish tasks.

Overlong Communications: Email is often used as a form of communication when quick messages are intended. Some individuals tend to compose notes that are much longer than necessary, which might take a lot of time.

Insecure: There are several hackers out there that want to get your sensitive information, making email a popular place to look for such information as political, financial, or personal emails. Numerous high-profile incidents in recent years have shown how vulnerable email is to information theft.

Different Email Formats

There are several varieties of email, including the following:

According to a Clutch survey, the newsletter—which may be delivered daily, weekly, or monthly is the most popular kind of email sent to mailing list members. These emails often include

information from the company's blog or website, links carefully chosen from other sources, and carefully chosen current content. Email newsletters are often issued on a regular basis and provide companies the chance to educate customers of crucial information from a single source. Additionally, future events, brand-new information, business webinars, or other updates may be included in newsletters.

Lead Nurturing: Marketers employ lead-nurturing emails to guide consumers through a journey that might affect their purchasing behaviour. Usually, these emails are sent over a few days or weeks. Trigger campaigns, often referred to as lead-nurturing emails, are used for solutions in an effort to convert any possible transaction into a completed purchase and inform potential customers about the services. These emails promote interaction in addition to helping convert emails. A prospective customer's first action, such as clicking links in a promotional email or downloading a free sample, initiates lead-nurturing emails.

The most typical B2B (Business to Business) email kind is a promotional email, which is designed to tell your email list about your new or current goods and services. These emails aim to attract new or existing clients, hasten the purchasing process, or motivate recipients to take some kind of action. Buyers get a number of important advantages from it, like a free month of service, lower or waived costs for managed services, or a discount on the purchase price.

Standalone Emails: Similar to newsletter emails, these emails are popular, but they have a drawback. Your primary call-to-action may become less compelling if you wish to send an email that has many links or blurbs. Your subscriber could delete your email and go on, just as they might click the first one or two links in it before moving on.

Onboarding emails, commonly referred to as post-sale emails, are messages sent to customers to increase their loyalty. Users start receiving these emails as soon as they subscribe. The purpose of the onboarding emails is to acquaint and instruct customers on how to utilise a product successfully. Additionally, these emails assist companies in facilitating user acceptance during large-scale service launches.

Transactional: These emails are sent from one sender to one recipient and are about account activity or a business transaction. Purchase confirmation emails, password reminder emails, and customised product alerts are a few instances of transactional email. When your firm has any kind of e-commerce component, you utilise these emails. Transactional email messages get 8x more opens and clicks than any other kind of email.

Emails that are merely text and have no pictures, graphics, or formatting are known as plain-text emails. If you strive to only only send beautiful designed emails, text-only communications, these kinds of emails could be worthwhile. Despite the fact that consumers prefer fully designed emails with a variety of graphics, every A/B test showed that plain text emails with less HTML were more effective. In actuality, HTML emails have lower open and click-through rates, and plain text emails are ideal for sending blog posts, invitations to events, and requests for surveys or feedback. Even if you don't send any plainer emails, making your emails simpler and using less pictures can increase the open and click through rates.

Greeting emails: It is a form of business-to-business email that contains typical elements of welcome emails that introduce recipients to the company. These emails may increase subscriber consistency since they include extra information that benefits the new subscriber in terms of achieving a business goal. Buyers who signed up for a company's opt-in initiatives, such as a blog,

mailing list, or webinar, are often given welcome emails. Additionally, these emails might aid companies in improving consumer interactions.

Illustrations of email attacks

Email is one of the most popular vectors for cyberattacks, despite the fact that there are other methods for viruses to spread inside systems. Spear-phishing, spamming, phishing, ransomware, and corporate email intrusion are some of the techniques (BEC).

Every month, a BEC assault affects a large number of firms (about 7710) since one in every 412 emails includes malware. The most common infection vector, according to the Symantec Internet Threat Security Report, is spear-phishing. A detailed explanation of various assaults is provided below:

Phishing: A kind of fraud in which the assaults consist of sending phoney emails or other forms of contact that look to be from a reliable organisation or individual. Phishing emails are often used by attackers to steal personal information like credit card numbers and login credentials or to infect victims' computers with malware. Additionally, as phishing is a widespread kind of cyberattack, everyone should become familiar with it in order to defend themselves. Sense of urgency, Hyperlinks, Too Good to Be True, Unusual sender, and Attachments are frequent characteristics of phishing emails.

Spamming: Also referred to as junk email, spam email is any unsolicited mass communication that is sent without the recipient's express permission. Spam has been a concern for most email users since the 1990s and has grown in popularity. Spam mail receivers' email addresses have been obtained by spambots, automated programmes that search the Internet for email addresses. This is the unethical side of email marketing, when spammers build email distribution lists using spambots. A spammer would often send an email to millions of email addresses with the assumption that just a small portion of those addresses will engage with the message.

Email spoofing is the process of sending an email message that seems to have come from a different source than it really did. Since the fundamental email protocols do not have an internal mechanism for authentication, it is a common tactic employed in spam and phishing operations. Additionally, individuals are more inclined to open an email if they believe it has come from a reliable or well-known source. As a result, it is a strategy often utilised in spam and phishing emails. To encourage receivers of mail to open emails and maybe react to a solicitation, email spoofing is used.

Compromise of business email (BEC): A business email compromise (BEC) is an exploit in which an authorised user or attacker gains access to a business email account and assumes the identity of the owner to steal money from the organisation, its clients, and partners. Frequently, an attacker just sets up an account with an email address that is almost similar to one on the company network, gaining the victim's confidence and their email account in the process. A BEC may also sometimes be referred to as a man-in-the-email assault. Examples of BEC email communications using words like "urgent," "transfer," "request," "payment," and more in the subject line. According to the FBI, there are five different forms of BEC scams: false invoice schemes, CEO fraud, data theft, attorney impersonation, and account compromise.

Email spoofing, often known as spear-phishing, is an attack when hackers target a particular person or company in order to get private data via unauthorised access. Spear phishing attempts are made by culprits seeking financial gain or access to sensitive information rather than by random hackers.

Attackers pose as reputable senders and send emails to predetermined, well-researched targets in this kind of assault. The primary goals of spear phishing are to infect devices with malware and persuade victims to provide information or money.

Ransomware is a kind of malware that is used to encrypt the data of its victims. Usually, it encrypts data and locks it on the victim's computer. On the victim's machine, the data is often encrypted and locked, and the attackers demand money before the data can be released. Unlike other attack types, ransomware assaults almost invariably have financial gain as their main objective. The victim is often informed of the attack and provided information on how to recover from it when the exploit happens.

Common email addresses

The following are some examples of free email websites: AOL \sZoho \sGmail \sProtonMail \sCom

Office Outlook

A platform called Yahoo Mail Email enables users to connect with individuals or groups of individuals all around the globe. Email security is increasingly crucial, yet it lacks intrinsic security as a result. There are several strategies that people, businesses, and service providers may employ. These methods describe ways to prevent unauthorised access, loss, or destruction of sensitive information while using email communication and accounts.

By using secure passwords and updating them often, users can safeguard their accounts. They are able to create a strong password that helps to safeguard your account by using alphabetical, numerical, and special symbols. Users may also establish spam filters and folders to distinguish potentially harmful emails from junk mail, as well as instal and run antivirus and antimalware software on their computer.

Implementing an email security gateway, teaching staff on using automatic email encryption solutions, and correct email use are further approaches that assist firms in securing email. Email gateways examine and scan every email that is received, looking for dangers and determining whether or not to let it into the system. Since attacks are become more frequent, intricate, and intelligent, a multilayered gateway is a strong strategy. The greatest method for preventing people from receiving dangerous emails is to teach staff on how to distinguish between legitimate and malicious emails and correctly utilise email.

The automatic email encryption systems are used to analyse all outgoing messages for potentially sensitive information; they encrypt the data before it is transmitted to the intended recipient. Even if hackers manage to halt it, this procedure aids in securing email transmission and guards against hackers getting access to the confidential data. The original information may only be seen with permission by the one intended recipient.

Email service providers may also contribute to increased security by gaining access to control guidelines and procedures and creating a strong password. In order to safeguard emails while they are in use and while they are in transit, providers should also provide digital signatures and encryption tools. Finally, service providers should employ firewalls and spam-filtering software to safeguard consumers against dangerous, unknown, and unreliable communications.

Address breakdown by email

The department of an organisation, alias, user, or group is included in the email address before the section that begins with the @ sign. Help in our firm, javatpoint, is the support division, as seen in the aforementioned example.

Since Ray Tomlinson delivered the initial message, all SMTP (Simple Mail Transfer Protocol) email addresses that include a divider must also include the @ (at symbol).

Last but not least, users are a part of the javatpoint.com domain. The top-level domain for the domain is.com (TLD).

Communicated using email

A platform that allows people to connect with one another is an email. Users may send text messages, along with a file or other data, through email to anybody in the globe. A photo, word processing document, PDF, application, video, or any other material saved on your computer may also be attached to an email. Certain file formats, however, may not be able to be sent by email owing to security concerns; they need some further measures. For instance, many businesses may forbid the sending of.exe files over email, thus you will need to compress the file into a.zip file type. Additionally, since most email carriers have file size constraints, you may not be able to transmit any huge files or applications by email.

Type in an email

According to the style manual you are using, you may use either the term email or the phrase e-mail since they are both acceptable and have the same meaning. E-mail, on the other hand, is a compound noun that combines the words "electronic" and "mail" and has a hyphen in it.

Methods for sending and receiving email

Email application

An email application may be used to send and receive emails. Email clients are another name for email programmes. Mozilla Thunderbird and Microsoft Outlook are only two of the numerous email clients available for sending and receiving emails. While you use an email client, a server is utilised to store and distribute your messages. This server is often hosted by your ISP (Internet service provider), but it may also be hosted by another Internet provider. Email clients must connect to a server in order to download fresh emails, but Internet-connected devices always have access to online storage of emails.

Internet email

For the majority of people, webmail, an online e-mail service, is a popular alternate method for sending and receiving e-mail. Yahoo Mail, Gmail, and Hotmail are a few examples of online emails (now Outlook.com).

Several of the well-liked email programs

Users may now access a variety of software-based email applications, but they are not online. There is a list of the most well-liked customers below.

- DreamMail Microsoft Outlook for Windows 10 Mozilla Thunderbird eM Client Mailbird
- characteristics distinguish a legitimate email address
- Users must abide by the numerous guidelines below to create legitimate email addresses:

The most crucial part of an email address is a username followed by @ (the at symbol), which is then followed by the domain name with a domain suffix. Therefore, a username is required for an email. The username cannot exceed 64 characters, and the domain name cannot exceed 254 characters. There may be only one @ symbol per email. Space and special characters like [] (),: ; > shouldn't be used in emails. Some symbols, including the backslash, space, and quote mark, need a forward slash to be placed before them. However, some email service providers do not support these characters. The username and email address cannot begin or stop with a period in the email. The email cannot include two or more subsequent periods.

FTP Protocol

File transfer protocol, or FTP, is the common method made available by TCP/IP for copying files from one host to another. A protocol included in the OSI Model's Application layer is the File Transfer Protocol. One of the simplest, safest, and easiest methods for exchanging data online is FTP. Since FTP creates two connections between the hosts, it differs from conventional client/server programmes. when just one connection—known as a data connection—is used for data transport. The other connection, known as a control connection, is used to control information such as instructions and answers. FTP is more effective since commands are separated. Two protocols are employed by the File Transfer Protocol; port 21 is used for control connections while port 20 is used for data connections. A single line of instruction or a single line of answer must be sent at a time when using the control connection in FTP. On the other hand, since there are several different kinds of data that must be exchanged, the data connection requires more sophisticated regulations. The word "uploading" refers to the transfer of files from the client computer to the server, while the term "downloading" refers to the transmission of data from the server to the client computer. ASCII files, EBCDIC files, or picture files may all be sent using FTP.

Utilizing FTP

The user interface, client control process, and client data transfer process are the three components that make up the client in the file transfer protocol's basic model, which is shown in the image below. The server, on the other hand, is made up of two parts, namely the server control process and the server data transmission process. Additionally, while the data connection is created between the data transfer processes, the control connection is made between the control processes.

While the data connection is created and then closed for each file transmitted, the control Connection stays open for the whole of an interactive FTP session. In plain English, the control connection opens when a user initiates an FTP connection, and the data connection may be started and closed several times if multiple files need to be sent.

Data Organization

Three data structures that FTP supports are listed below:

- File Structure a file is essentially a never-ending stream of bytes in the File data structure.
- Record Structure The file is simply partitioned into records in the Record data structure.
- Page Structure The file is split into pages in the Page data structure, and each page contains a page number and a page header. Both randomly and sequentially may be used to store and retrieve these pages.

FTP Clients.

In essence, it is software created to facilitate file transfers between a computer and a server via the Internet. An active Internet connection is required in order to utilise the FTP client, which must be installed on your computer. Dreamweaver, FireFTP, and Filezilla are three examples of frequently used FTP clients.

Qualities of FTP

- The File Transfer Protocol provides the characteristics listed below:
- One file at a time transfers are the core purpose of FTP.
- FTP can also list files, create and delete directories, delete files, rename files, and conduct many more operations.
- FTP also conceals information about certain computer systems.
- FTP permits files with ownership and access limitations.
- It is a protocol that is connection-oriented.
- As the client creates a control connection for the length of an FTP session, which often includes numerous data transfers, FTP is a stateful protocol.

Modes of Transmission

One of the three available modes may be used by FTP to transport a file over the data connection:

1. Streaming Mode

The standard transmission method for FTP is called Stream Mode. In this mode, the File is sent to TCP as an unbroken stream of bytes. End-of-File is not required if the data is merely a stream of bytes; rather, the sender's closing of the data connection is regarded as EOF or end-of-file. Each record contains an I-byte of EOR if the data is separated into records, which is the record structure (end-of-record).

2. Block Mode

Block mode is used to transfer data in the form of blocks from FTP to TCP. Each block of data is preceded by a header of 3 bytes, the first of which contains the block descriptor and the second and third of which include the block size.

3. Comprehended Mode

If the file being transferred is particularly large, data compression is an option in this mode. Run-length encoding often use this technique. Text files often have blanks and spaces deleted. While null characters are not compressed in a binary file.

Benefits of FTP

Some advantages of utilising the File Transfer Protocol include the following:

- FTP implementation is easy.
- FTP is one of the quickest methods for transferring data between computers.
- FTP is a commonly used, standardised protocol.
- The File Transfer Protocol is more effective since not all actions are required to get the whole file.
- The drawbacks of FTP
- The File Transport Protocol is not a secure method of data transfer.
- FTP does not provide removal actions for recursive directories or server-to-server copying.
- Using the FTP protocol to script the tasks is challenging.

Any unauthorised machine may be used to transmit data to a random, unknown port by impersonating the server.

Application Layer

The highest level of the OSI model, known as the application layer, is the only one that directly engages with end users and defines the common protocols and interface techniques employed by hosts in a communications network. It serves as a conduit between the users and the real software application. It offers complete end-user access to a number of shared network services, including file transfers, directory services, and mail services. Its duties include addressing errors and recovering from them (Figure 9.1).

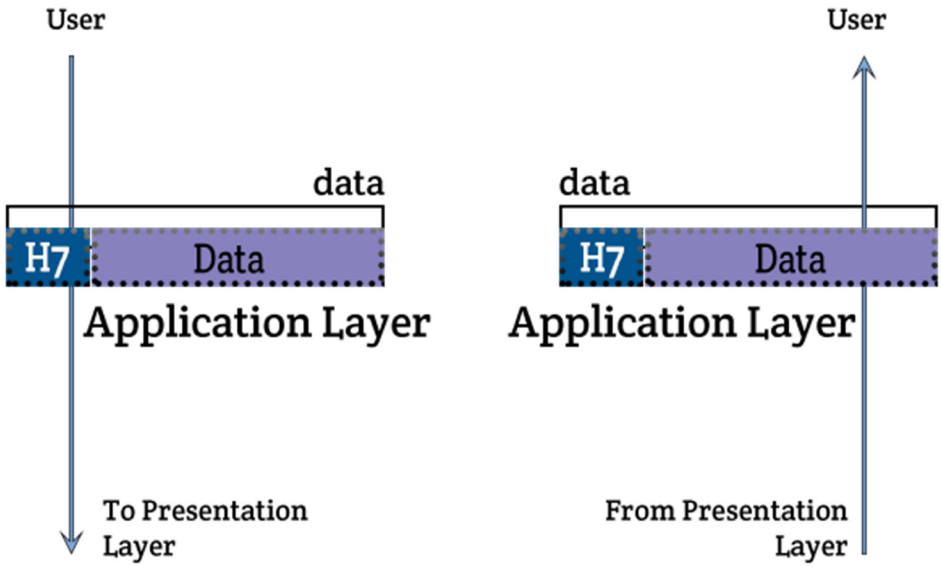


Figure 9.1: Illustrating the Application Layer [2].

The application layer confirms resource availability, synchronizes communication, and decides the identity and availability of communicating parties for an application with information to transmit. The application layer protocols that are implemented on the source and the destination hosts must be compatible in order for the communications to be successful. The protocols and essential services by network-aware programs to connect to the network are provided by this layer. Applications that are aware of networks can interact with lower tiers of the protocol stack directly by implementing protocols at the application layer. Examples of these kinds of apps include web browsers and email clients. The application layer does not include application programs. Just a few examples of standards and protocols used in this layer include TFTP, HTTP, POP3, FTP and SMTP.

- **Network Application Architecture**

The network architecture is distinct from the application architecture. A collection of services are offered to apps by the fixed network architecture. On the other hand, the application developer creates the application architecture, which specifies how the application should be organised among the various end systems.

➢ Two Types of Application Architecture

- **Client Server Architecture:**

In a client-server computing model, the server hosts, provides, and manages the majority of the services and resources that the client requests. Due to the fact that all requests and services are supplied across a network, it is also referred to as the networking computing paradigm or client server network. The client-server architecture or model makes use of additional systems that are networked together and exchange resources among numerous computers. Client-server architecture is typically set up so that clients are frequently located at desktops or on personal computers, while servers are placed somewhere else on the network, typically on more powerful machines. A model like this is very useful when clients and servers carry out routine operations [3].

- **Peer-To-Peer:**

A popular form of computer networking called peer-to-peer (P2P) architecture gives every workstation, or node, the same capabilities and obligations. It is frequently contrasted with the traditional client/server architecture, where some computers are set aside to serve other computers, and compared to it. P2P can also be defined as a single piece of software that is built to allow each instance to perform the same duties and functions as both clients and servers. Although P2P networks have various uses, content distribution is the most popular. On-demand content delivery is made possible via peer casting for multicasting streams, content delivery networks, streaming media, and software publication and distribution. Science, networking, search, and communication networks are further applications [4].

➢ Client and Server model

Any process can function as a server or client in a client-server architecture. The ability to fulfil requests is what distinguishes a machine as a server, not just the type of hardware, size, or computational capability of the system (Figure 9.2).

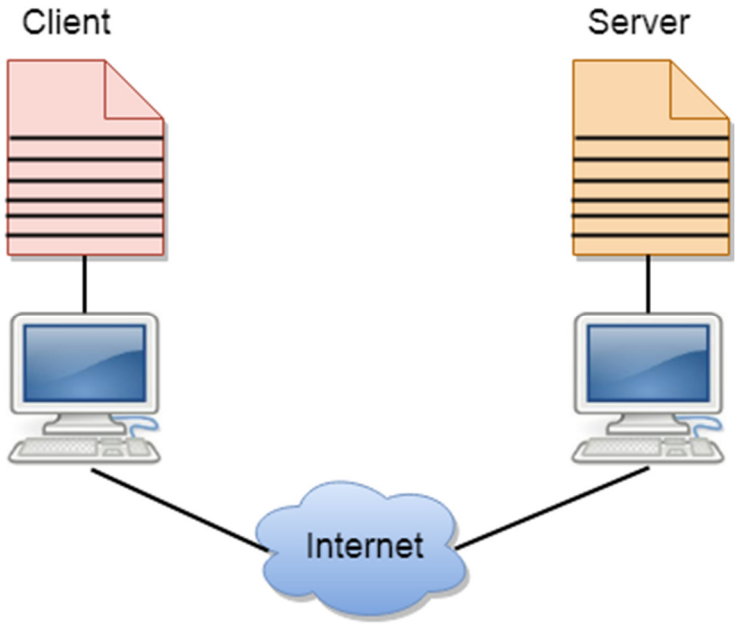


Figure 9.2: Illustrating the Client and Server Models [5].

The client-server application programs should adhere to the following tactics:

- An application program known as a server program, running on a remote machine, responds to a service request from a client program, running on a local machine.
- A client program only runs when it asks the server for a service, whereas a server software runs always because it is unaware of when its service is needed.
- A server doesn't just serve one client; it serves other clients as well. Thus, we may state that client-server architecture adheres to the many-to-one connection. One server can serve a large number of clients.
- Many users have a specialized client-server application software, and services are commonly needed. For instance, the client-server application program enables users to access files, send emails, and perform other tasks. The user should be able to access the services on the distant computer using a single, generic application program if the capabilities are more customized.

Clients:

Thin, thick, and hybrid clients are the three categories used by IT professionals to describe clients or server requesters. For many of a device's fundamental operations, thin clients require the resources and computing power of a server. Devices known as thick clients are capable of doing numerous jobs and processing vast volumes of data without the assistance of a server. Devices known as hybrid clients are those that have the ability to analyze data on their own but depend on a server to retain the data for more involved or repetitive processing operations.

Server:

Computer hardware or software that offers functioning to its users or customers is referred to as a server. Six different servers are available for usage by IT professionals to set up client-server connections.

Client-Server Model Benefits:

1. Centralized database containing all of the data.
2. Cost-effective maintenance costs are lower, and data recovery is an option.
3. Separate adjustments can be made to the Client and Server capacities.

Client-Server Model Drawbacks:

1. If viruses, Trojan horses, and worms are uploaded to or present on the server, clients are vulnerable to them.
2. The Denial of Service (DOS) assault is a common one on servers.
3. Data packets may be altered or spoofed while being transmitted.
4. Deception and MITM (Man in the Middle) assaults are frequent, as are attempts to capture login passwords or other crucial user information.

Chapter 10

APPLICATION PROTOCOLS

Jayaprakash B, Assistant Professor
Department of Computer Science & IT, School of Sciences, Jain (Deemed-to-be University), Bangalore-27, India
Email Id- b.jayaprakash@jainuniversity.ac.in

The communication between application processes operating on various end systems is governed by application layer protocols. An application layer, in particular, is an abstraction layer that manages the TCP/IP and OSI model's sharing protocol. Application layer protocols are designed to enable workers to communicate over networks and send and access data. Additionally, the application layer facilitates communication and occasionally permits operators to use software applications.

Simple Mail Transfer Protocol

1. Simple Mail Transfer Protocol is known as SMTP.
2. The Simple Mail Transfer Protocol (SMTP) is a set of rules for communication that enables applications to send electronic mail over the internet.
3. Based on email addresses, it is an application used to deliver messages to other computer users.
4. Between users using the same or other computers, it offers mail exchange, and it also supports:
5. One message may be sent to one or many recipients.
6. Messages may be sent using text, audio, video, or graphics.
7. The communications may also be sent through networks other than the Internet.

Setting up communication rules between servers is the major usage of SMTP. The servers may identify themselves and state the kind of communication they are attempting to carry out. They also provide a method for dealing with issues like a wrong email address (Figure 10.1). For instance, if the destination address is incorrect, the receiving server will respond with some kind of error message.

SMTP components

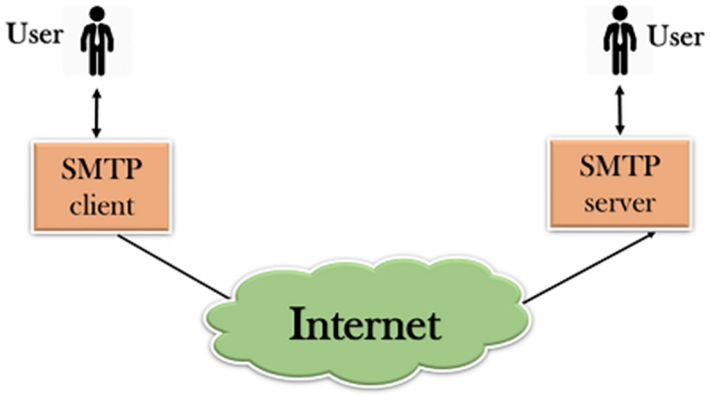


Figure 10.1: SMTP components

SMTP on a computer network

We will first separate the SMTP client and SMTP server into two parts, such as the user agent (UA) and mail transfer agent (MTA). The message is prepared by the user agent (UA), who also makes the envelope and inserts the message. This letter is sent over the internet via the mail transfer agent (MTA) (Figure 10.2).

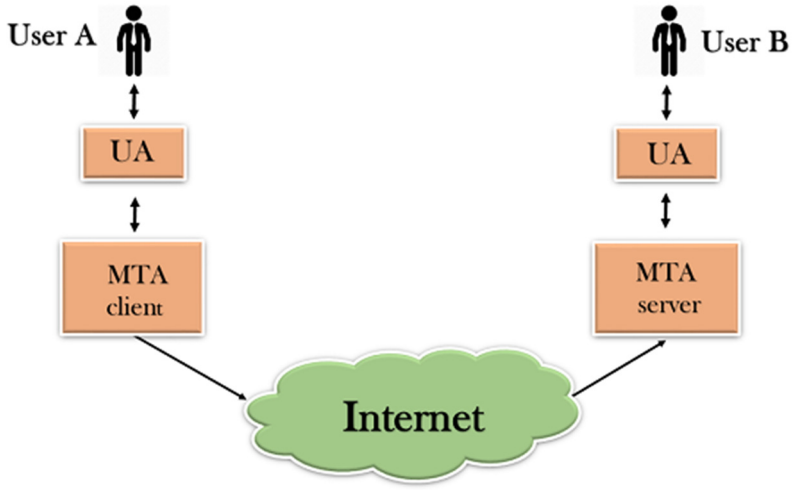


Figure 10.2: SMTP on a computer network

Network of Computers SMTP By including a relaying mechanism, SMTP enables a more complicated system. More MTAs may be added, operating either as a client or server to relay the email, rather to only having one MTA at the sending side and one at the receiving side (Figure 10.3).

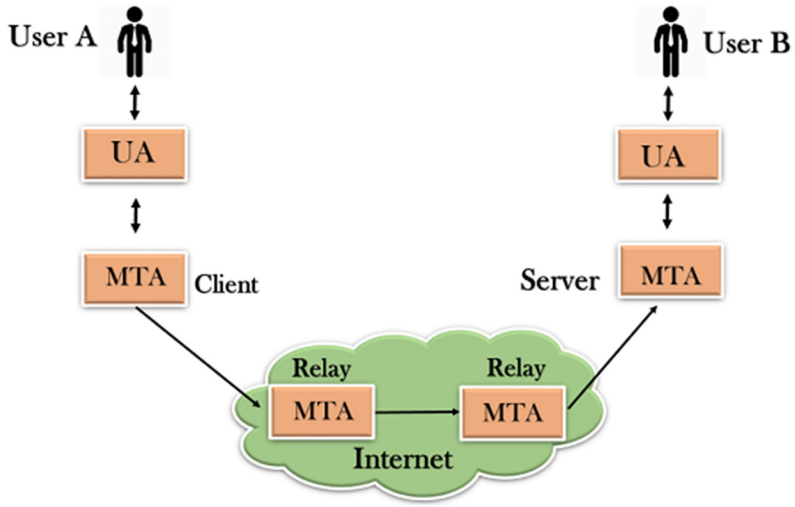


Figure 10.3: Network of Computers SMTP

SMTP on a computer network

The usage of the mail gateway makes it possible to send emails to people using a relaying system without the TCP/IP protocol. A relay MTA that may be used to receive emails is the mail gateway (Figure 10.4).

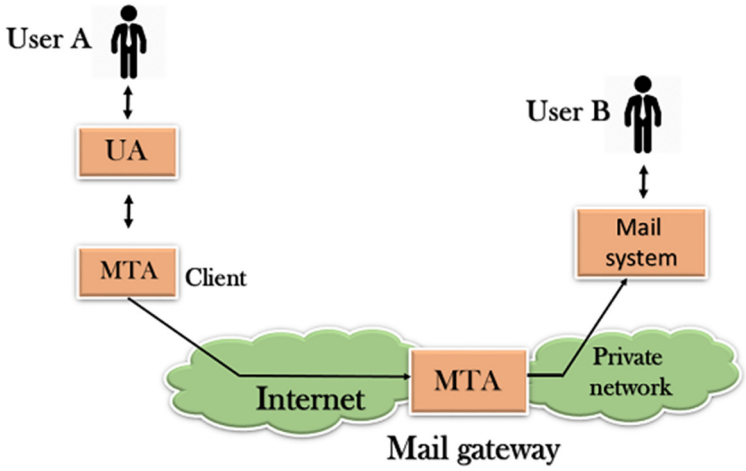


Figure 10.4: SMTP on a computer network

Computer network SMTP functionality

Composition of Mail: A user composes an electronic mail message using a Mail User Agent before sending it (MUA). An application called Mail User Agent is used to send and receive mail. Body and header are the two components of the communication. The message's primary component is its body, while the header contains details like the sender and recipient addresses. Additionally, the header contains descriptive details like the message's topic. In this instance, the message content resembles a letter, and the header resembles an envelope with the address of the receiver.

Submission of Mail: The mail client uses SMTP on TCP port 25 to send the finished email to the SMTP server once it has been composed.

Delivery of Mail: An email address consists of the recipient's username and the domain name. For instance, vivek@gmail.com, where the recipient's login is "vivek" and the domain name is "gmail.com."

Mail will be sent to the Mail Transfer Agent if the recipient's email address's domain name differs from the sender's domain name (MTA). The MTA will locate the destination domain and transmit the email there. To retrieve the target domain, it looks for the MX record from the Domain Name System. The IP address and domain name of the recipient's domain are included in the MX record. MTA establishes a connection with the exchange server to transport the message after locating the record.

Mail processing and receipt: When an incoming message is received, the exchange server sends it to the mail delivery agent (incoming server), who holds it until the user retrieves it. Access and Mail Retrieval: MUA may be used to retrieve the emails that were saved in MDA (Mail User Agent). MUA is accessible with a login and password.

Telnet

The primary function of the internet is to offer users services. Users might, for instance, desire to run various application programs at the remote site while sending the results back to the local site. A client-server application, such as FTP or SMTP, is needed for this. However, this would prevent us from developing a unique program for each demand. The preferable option is to give users

access to any application program on a distant computer using a general client-server program. Consequently, a program that enables logging on to a remote computer. To address these needs, the well-known client-server application Telnet is employed. Terminal Network is referred to as telnet. A local interface appear to be at the distant side thanks to the connection provided by Telnet to the distant machine. Telnet is a network protocol that allows for two-way, collaborative, text-based communication between two computers as well as remote computer access.

It uses the Transmission Control Protocol/Internet Protocol (TCP/IP) networking protocol to create remote sessions in response to user commands. While Telnet allows users to log in as normal users with the access credentials they are permitted to the particular apps and data on that computer, HTTP and FTP on the web only allow users to request specific files from faraway computers.

In response to this request, the user would get a login invitation and a password prompt from the application. The user is given access to the remote host if it is approved.

Programmers and anybody else who needs to access certain apps or data that are on a distant system are most likely to use Telnet.

Telnet's workings

A distant computer, usually a server, may have its command line opened via the client-server protocol called Telnet. This utility allows users to ping a port and determine if it is open. Telnet emulates a physical terminal connected to a machine by employing what is known as a virtual terminal connection emulator, or an abstract instance of a connection to a computer. For users sending data files, FTP may be utilised in addition to Telnet.

Telnet, sometimes referred to as Telnetting into the system, allows users to connect remotely to a computer. To access the distant computer, they are required to provide their login and password combination, which permits the execution of command lines as if they were physically there in front of the computer. Users' IP addresses will always match the computer they are currently signed into, not the one they used to physically connect, regardless of where they are physically located.

Using Telnet

On a server, Telnet may be used for a number of tasks, such as file editing, running different applications, and checking email.

Some servers allow remote connections through Telnet so users may access open data to access basic games or check the weather. Many of these functions are still functional in older systems that need access to certain data or are there for nostalgic enjoyment. Telnet allows users to connect to any programme, including web servers and ports that uses text-based, unencrypted protocols. The telnet connection will ping the port to determine if it is open or not when users open a command prompt on the remote system, enter the word telnet, and the name or IP address of the remote machine. A blank screen indicates that a port is open, whereas an error message indicating that a port is connecting indicates that a port is closed.

Security

Telnet is an insecure, unencrypted protocol. Anyone who keeps an eye on a user's connection may see their plaintext username, password, and other secret information entered during a Telnet session. With this knowledge, access to the user's device is possible.

Protocols associated to SSH

Some contemporary systems only permit command-line access over a virtual private network (VPN) or utilising Secure Shell (SSH), an encrypted tool comparable to Telnet (VPN). Many professional groups demand the usage of SSH, PuTTy, or other solutions instead than Telnet due to security concerns. The main reason SSH is preferred over other alternatives is because it encrypts all data travelling across the communication connection.

Additionally, unlike more recent protocols, Telnet does not allow graphical user interfaces (GUIs), rendering it incompatible with a wide range of contemporary applications, including word processors, spreadsheets, and web browsers. Large quantities of data, particularly visual data, would be lost over a Telnet session connection since such systems operate intricate graphical interfaces.

Telnet's past

Initially, Network Control Program (NCP) protocols were used by Telnet. Later, it was referred known as TONP, or Teletype Over Network Protocol. Although it has been used indiscriminately for some time, it was formally formed on March 5, 1973, in papers that were published.

Early versions of Telnet allowed distant computers to connect with simple text by using American Standard Code for Information Interchange (ASCII) sent over an 8-bit channel.

Numerous Telnet extensions have been developed throughout time. Telnet has been a resource for programmers for many years. For the Advanced Research Projects Agency Network (ARPANET), the forerunner to the current internet, the first Telnet version was developed in the 1960s. It was one of the first devices made to remotely connect computers across vast distances. Researchers and experts created the Telnet protocol in 1971, and the Telnet system followed in 1983.

Simple Network Management Protocol:

In Internet Protocol networks, devices linked to the network are maintained and tracked using a networking protocol called Simple Network Management Protocol (SNMP). The SNMP protocol is supported by a large number of local devices, including routers, switches, servers, firewalls, and wireless access points. These devices can all be reached via their IP addresses. SNMP can be used by network devices to relay management data in single- and multi-vendor LAN or WAN environments. It is an application-layer protocol in the OSI model architecture. The SNMP protocol is commonly implemented using User Datagram Protocol (UDP). UDP is a connectionless protocol that operates similarly to the Transmission Control Protocol (TCP) on the premise that error-checking and recovery services are not required. Instead, UDP continuously transmits datagrams to the destination, regardless of whether they are received.

As its name suggests, SNMP is utilised at the application layer of the TCP/IP architecture to manage and monitor networks and network failures. It is sometimes also used to change the configuration of the network's remote endpoint devices.

Modems, routers, switches, printers, servers, and other devices are among those that support the Simple Network Management Protocol.

Components of SNMP

SNMP has three parts that work together to carry out its fundamental functions. These are listed below:

SNMP Manager

It is also known as a Network Management System and is a centralised GUI-based node system that is used to monitor the network (NMS). It facilitates the two-way information transfer between the network components and the NMS node. Switches, routers, servers, modems, computer hosts, IP-based phones, video cameras, and other network components are included here.

SNMP Agent

On a network device, such as a host PC, server, router, etc., the agent is a module of network administration software. When the NMS asks any information, the agent responds by providing the data that was saved in the database to the NMS. The agent maintains the database on the controlled network components. The agent delivers the SNMP trap message to the SNMP manager indicating the live status whenever it encounters any trap or error on a managed device.

Database for Management Information (MIB)

Each SNMP agent keeps the information database for the controlled devices up to date, which explains the devices' parameters. This database is used by the SNMP manager to query the agent for details about a specific device for NMS. Consequently, a management information database is the term used to describe the information that the agent and manager communicated (MIB).

The MIB's structure

It is a collection of data made up by variables, each of which contains values pertinent to the network element's parameter stores. These variables are referred to as managed objects and are given an Object Identifier to identify them (OID).

Each object identifier in the hierarchical MIB collection may indicate a variable that the SNMP can set or read. Scalar and tabular OIDs are available. The scalar one report just one incidence of an event denotes that there is only one outcome. Text or number, for instance.

The Tabular object is a table that collects all associated OIDs, providing several results for a single object value. For instance: There will be two values as a consequence for the dual processor of the CPU. Components flow diagram for SNMP

Network Management Protocol Operates Clearly

All SNMP messages will be sent through the UDP protocol since it uses the application layer of the TCP/IP protocol stack (User Datagram Protocol). The SNMP agent receives the request from the management using UDP port 161. The NMS will handle all of the administration and monitoring tasks for the network components and devices and will provide the bulk data required for network management.

Each network managed element has an associated SNMP agent, which converts local MIB data including performance statistics, error information, and the occurrence of any event into a readable form for the NMS. The agent utilises Get-Requests to provide the data to the NMS programme for this purpose.

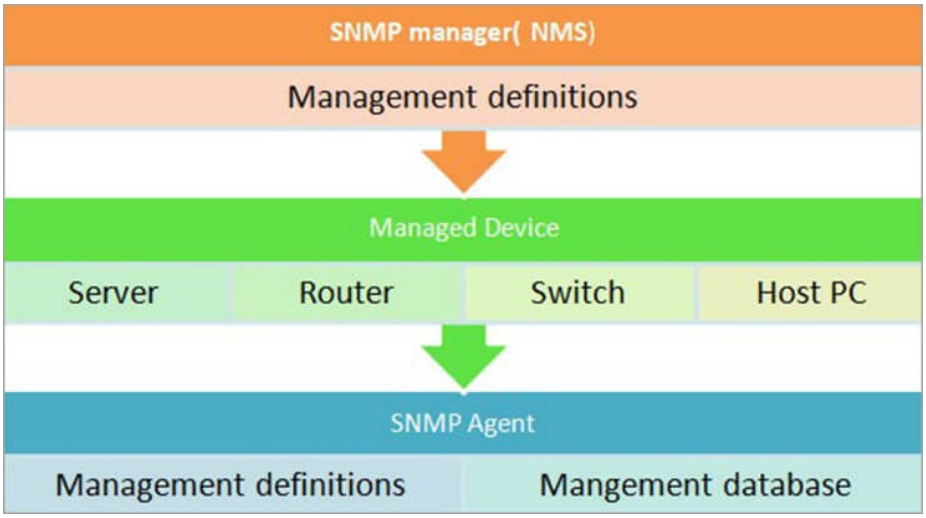


Figure 10.5: MIB's structure

Network Management Protocol Operates Clearly

All SNMP messages will be sent through the UDP protocol since it uses the application layer of the TCP/IP protocol stack (User Datagram Protocol). The SNMP agent receives the request from the management using UDP port 161. The NMS will handle all of the administration and monitoring tasks for the network components and devices and will provide the bulk data required for network management.

Each network managed element has an associated SNMP agent, which converts local MIB data including performance statistics, error information, and the occurrence of any event into a readable form for the NMS. The agent utilises Get-Requests to provide the data to the NMS programme for this purpose.

The MIB data is gathered and stored by network components such routers, switches, PCs, and modems, and is then made accessible to management systems that are compatible with them through the SNMP agent. The following illustration can help you understand this: Figure of the SNMP architecture (Figure 10.6)

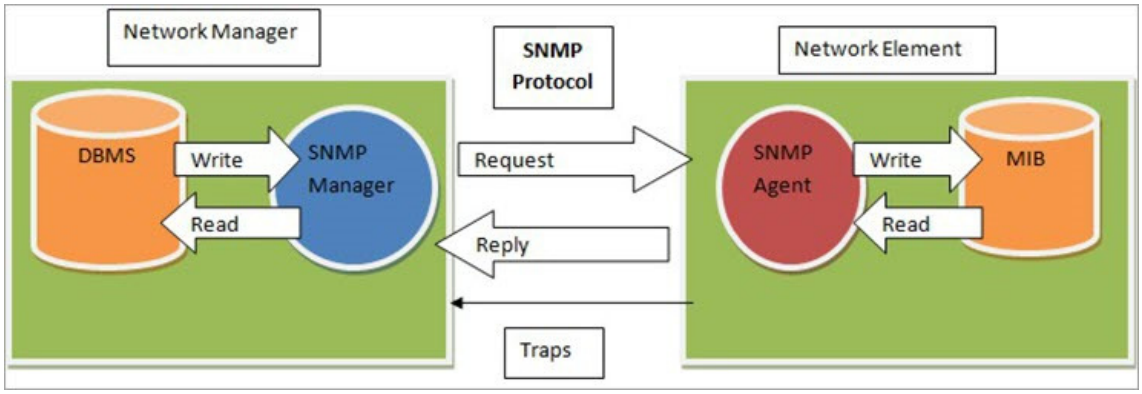


Figure 10.6: SNMP architecture

Similar to Solar winds and Cisco IOS, Network Manager is an open-source application. The network manager has to instal this programme on the server in order to execute SNMP. The role of the Simple Network Management Protocol manager is to request and receive data from the

agent in order to administer and monitor the network components, as shown in the above image. Additionally, to modify the configuration as necessary to meet network requirements. Receiving messages from Trap and Inform on network issues and event occurrence is another crucial duty.

Commands for SNMP

Three commands Read, Write, and Trap—are used to manage the network components by installing SNMP. The NMS uses the read command to keep an eye on the controlled network components, such as switches and routers. NMS carries out this process by looking at the many variables supported by the network components. The NMS uses write commands to manage the network components. The NMS may change the values of the variables that are stored in the managed network components using this command. The managed network nodes use the trap command to inform the NMS of incidents and mistakes.

PDUs used in SNMP request messages include the operations "Get," "GetNext," and "GetBulk."

Get: The NMS requests to obtain many variables from the SNMP agent using this message.

GetNext: With this command, the NMS is able to retrieve one or more subsequent variables from the SNMP agent.

GetBulk: This procedure corresponds to the subsequent GetNext procedure. We are able to bulk get the database from the agent using this combination of request messages.

In response to the Get and Set request PDUs, the agent sends the variable data unit back to the NMS.

Trap: The SNMP agents are the ones that start this command. When an event happens, the agent sends a signal to the SNMP manager in the form of this PDU to acknowledge the occurrence.

Inform Request: This command does the same task as the Trap command. It contains the acknowledgement that the packet was received by the SNMP management (Figure 10.7).

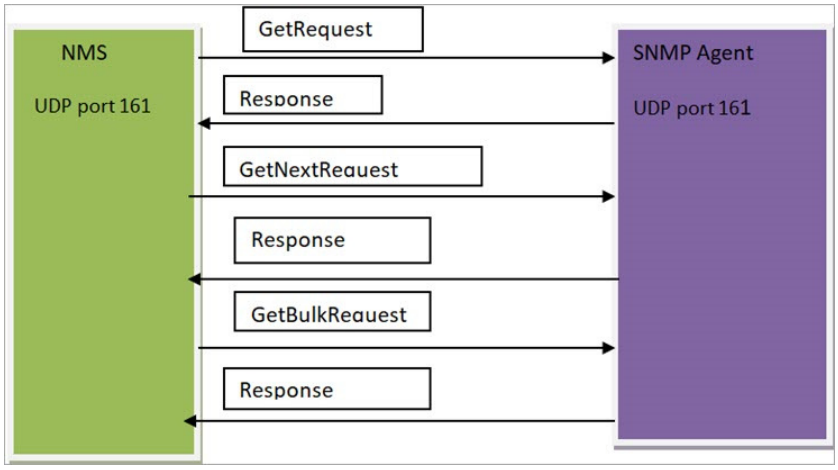


Figure 10.7: Inform Request

RequestInformant 1

NMS and controlled devices employ UDP ports and instructions that SNMP traps:

SNMP snare

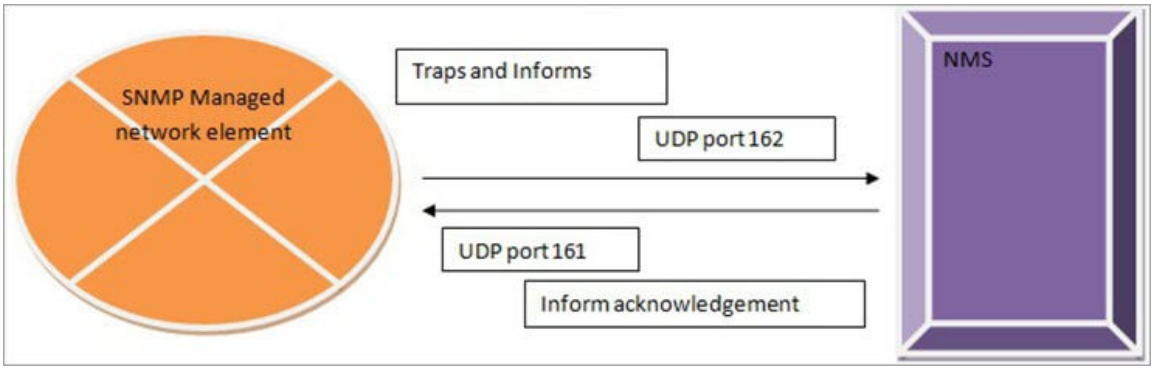


Figure 10.8: SNMP snare

The SNMP Manager will get a report from the SNMP Traps whenever an event happens in the network. Changing a port in a router from the DOWN state to the UP state is one example. In addition to being SNMP traps, SNMP informs are the manager's acknowledgement receipts. The communication between the SNMP-managed network components and the Manager for issuing Traps and Informs is shown in the above image. Trap and Inform both have distinct functions. The SNMP trap message is only sent once and is also deleted when it is sent. They are not stored in memory so that the Manager can respond to them. Until it receives a response from the NMS or the request times out, the Inform is sent again (Figure 10.8).

If the host device doesn't obtain a response from the NMS, it will submit the Inform request again until it does, using up additional memory and resources on the network and network devices in the process.

Versions of the Simple Network Management Protocol are mentioned below:

Version 1 of the SNMP protocol is known as SNMPv1. It offers the fewest network control features. Since its authentication is based on community names, it also provides a very low degree of security and gives fewer error control codes.

Security, network management, and performance management have all been improved upon in SNMPv2, which is the updated version of SNMPv1. This created a new PDP message called "GetBulkRequest," which is used to request a large amount of data from the agent at once. The security architecture of earlier versions is compatible with SNMPv2c, often known as a community-based simple network management version 2.

SNMPv3 (version 3): This version is more effective than earlier versions since it adds the functionality of cryptographic security. Additionally, it provides the capability of remote network administration and configuration for the network components and is based on the View-based Access Control Model and the User-based Security Module (USM) (VACM).

HTTP:

Hyper Text Transfer Protocol is known as HTTP. It is an access protocol for data on the World Wide Web (www). Information in the form of plain text, audio, hypertext, video, and other formats can all be transferred using the HTTP protocol. Because of its effectiveness in a hypertext context where there are quick jumps through one document to another, this protocol is also known as the "Hyper Text Transfer Protocol." Since it also moves files from one site to another, HTTP is

comparable to FTP in this regard. However, HTTP is easier to use than FTP because it simply makes one connection and doesn't utilize a control connection to move files. Since information is being shared between the client and server using HTTP, it is comparable to SMTP. The method that messages are sent from the client to the server and from the server to the client differs between HTTP and SMTP. While HTTP messages are delivered instantly, SMTP messages are saved and forwarded. HyperText Transfer Protocol is known as HTTP. It is an access protocol for data on the World Wide Web (www).

HTTP protocol.

Because of its effectiveness in a hypertext context where there are quick hops from one page to another, this protocol is also known as the "HyperText Transfer Protocol." Since it also moves files from one site to another, HTTP is comparable to FTP in this regard. However, HTTP is easier to use than FTP since it simply makes one connection and doesn't utilise a control connection to move data. Data in a MIME-like format is sent through HTTP. Since data is exchanged between the client and server through HTTP, it is comparable to SMTP. The method that messages are transferred from the client to the server and from the server to the client varies between HTTP and SMTP. While HTTP communications are sent instantly, SMTP messages are saved and forwarded.

Properties of HTTP:

Connectivity-free protocol a connectionless protocol is HTTP. A request is made by the HTTP client, who then waits for a response from the server. When the HTTP client delivers the request to the server, the server processes it and sends back the response before the client cuts off the connection. Only during the period between a request and a response does a connection between the client and server exist.

Media independence: The HTTP protocol is media independent, allowing data to be transferred between clients and servers as long as they are both aware of how to handle the data's content. The MIME-type header's content type must be specified by both the client and the server.

Stateless: Since only the current request is known to the client and server, HTTP is a stateless protocol. Because of the nature of the protocol, neither the client nor the server stores the information across requests for different web pages.

Transactions over HTTP

Network of Computers HTTP

The HTTP interaction between the client and server is shown in the previous illustration. A transaction is started by the client submitting a request message to the server. The server sends a response message in response to the request message.

Messages

Request and response messages are the two forms of HTTP communications. The message format is the same for both message kinds.

Computer Network HTTP:

Request Message: The client sends the HTTP request message, which is made up of a request line, headers, and sometimes a content.

Computer Network HTTP

Response Message: The response message, which includes a status line, headers, and sometimes a content, is delivered by the server to the client.

Network of Computers Uniform Resource Locator for HTTP (URL)

A client that wants to view a document via the internet requires an address, and the HTTP protocol makes use of the idea of a uniform resource locator to make document access easier (URL).

Any kind of information on the internet may be specified using the Uniform Resource Locator (URL).

Method, host computer, port, and path are the four components of the URL.

Network of Computers HTTP \sMethod: The protocol used to get the document from a server is the method. for instance, HTTP.

The machine that stores the data is referred to as the host and is given an alias name. The majority of web pages are saved on computers, which have been given an alias name that starts with the letters "www". This field is optional.

Port: Although it is an optional parameter, the URL may additionally include the server's port number. If the port number is present, it must appear between the host and the route and be followed by a colon.

Path: The pathname of the file containing the information is called "Path." Slashes in the route itself divide directories from their subdirectories and files.

Characteristics of HTTP:

1. HTTP is an IP-based communication protocol used to send data from server to client or the other way around.
2. Client makes a request, which the server responds to. The server and client only interact during the current request and response cycle.
3. As long as the server and client can share the desired kind of material, it can be done.
4. Servers and clients are no longer linked to one another after data has been transmitted.
5. It is a client- and server-based request and response protocol.
6. It is a connection-less protocol because, when a connection is broken, neither the server nor the client retain any information about the other.
7. Because the client and server have no expectations of one another yet are still able to interact, it is a stateless protocol.

Advantages:

1. There are fewer simultaneous connections, which results in reduced memory and CPU utilisation.
2. The amount of network congestion is lower since there are fewer TCP connections.
3. Since handshaking is completed at the beginning of the connection, latency is decreased since no more handshaking is required for future requests.
4. You may report the mistake without cutting off the connection.
5. HTTP permits request or response pipelining.

Disadvantages:

1. To establish communication and transport data, HTTP needs a lot of electricity.

2. Because HTTP does not employ TLS to encrypt its standard requests and responses, it is less secure than https.
3. HTTP is overly gabby and not designed for mobile devices.
4. Because HTTP is less secure than other protocols, it cannot provide true data sharing.
5. Clients do not cut off connections until they have received all of the data they requested from the server, thus the server must wait until this is done in order to serve future clients.

Chapter 11

NETWORK MANAGEMENT

Ghouse Basha M A, Assistant Professor
Department of Computer Science & IT, School of Sciences, Jain (Deemed-to-be University), Bangalore-27, India
Email Id- ghouse.basha@jainuniversity.ac.in

Let's first take a look at a few interesting "real-world" non-networking instances where a complex system with numerous interconnected components has to be monitored, managed, and controlled by an administrator before getting into network administration itself. Electrical power generating facilities contain a control room where dials, gauges, and lights monitor the condition of distant valves, pipelines, vessels, and other plant parts (temperature, pressure, and flow). These tools enable the plant's operator to keep an eye on its many components and may warn them of impending problems via the well-known flashing red warning light. The plant operator takes action to manage these components. The numerous parts that make up an aircraft are instrumented similarly to enable a pilot to keep an eye on them and operate them. In these two instances, the "administrator" keeps an eye on remote devices and examines their data to make sure they are operational and operating within set parameters (for example, that a nuclear power plant's core meltdown is not about to occur or that a plane is not about to run out of fuel), reactively controls the system by making adjustments in response to changes within the system or its environment, and proactively manages the system (for example, by detecting potential threats before they arise). Similar to this, the network administrator actively oversees, controls, and manages the system with which they are entrusted.

"Network management" was unheard of in the early days of networking, when computer networks were research artefacts rather than a vital infrastructure utilised by hundreds of millions of people every day. A few pings might be used to identify the cause of a network issue before changing system settings, restarting hardware or software, or making a call to a distant coworker. ([RFC 789] provides a fairly accessible explanation of the first significant "crash" of the ARPAnet, which occurred on October 27, 1980, long before network management tools were widely used, as well as the actions taken to remedy and comprehend the disaster.) The necessity to manage the enormous number of hardware and software components inside these networks more methodically has become increasingly crucial as the public Internet and private intranets have expanded from tiny networks into a vast global infrastructure. Let's start with a basic example to encourage our study of network administration. A modest network with three routers, several hosts, and servers is shown in Figure 11.1. There are several situations, even in such a basic network, when a network administrator might greatly benefit from having the right network management tools:

Spotting an interface card failure on a host or router. A network entity (such as router A, for instance) may notify the network administrator that one of its interfaces has failed using the proper network management tools. A network manager who consistently keeps an eye and examines by anticipating interface issues and replacing the interface card before it breaks, network traffic may be able to genuinely wow the potential furious user. This may be done, for instance, if the administrator saw a rise in checksum problems in the frames being delivered by the interface that would soon stop working.

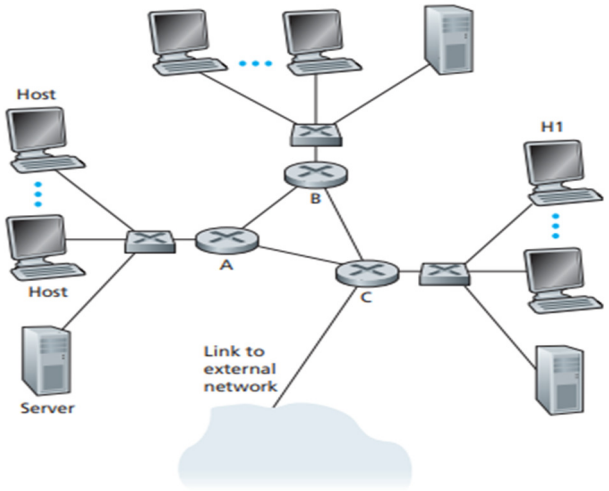


Figure 11.1: A modest network with three routers, several hosts, and servers

Host surveillance. In this case, the network administrator may recheck the status of each network host on a regular basis. Once again, the network administrator may be able to genuinely dazzle a network user by promptly addressing an issue (host down) before a user reports it.

Traffic monitoring to assist in resource distribution. By keeping an eye on source-to-destination traffic patterns, a network administrator may discover, for instance, that by moving servers across LAN segments, the volume of traffic that spans numerous LANs may be greatly reduced. Imagine how happy everyone would be when improved performance is accomplished without the need for new equipment. Similar to this, a network administrator may find via link usage monitoring that a LAN segment or external connection to the outside world is overloaded and that, as a result, a higher-bandwidth link should be provided (alas, at a greater cost). In order to provide a higher-bandwidth connection before congestion becomes a severe problem, the network administrator may also wish to be automatically warned when congestion levels on a link surpass a specified threshold value.

Spotting sudden modifications to routing tables. Routing instability or a poorly designed router may be indicated by route flapping, which is a pattern of frequent changes in the routing tables.

If a router has been set incorrectly, the network administrator would undoubtedly like to find the mistake before the network falls down.

Monitoring for Service Level Agreements (SLAs): According to contracts [Huston 1999a], SLAs specify precise performance metrics and the acceptable levels of network provider performance with regard to these metrics. Among the various network operators that provide their clients SLAs, Verizon and Sprint are only two. These SLAs specify the throughput, latency, service availability (outage), and outage notification standards.

Measuring and monitoring performance will undoubtedly be of utmost significance to the network administrator if performance requirements are to be a component of a service agreement between a network provider and its users.

Detection of intrusions. When network traffic originates from or is directed toward a suspect source (for instance, a host or port number), a network administrator may wish to be warned.

Similar to this, a network administrator might want to look for (and, in many cases, filter out) specific traffic patterns that are known to be indicative of the kinds of security attacks we discussed in Chapter 8 (such as sourcerouted packets or a high volume of SYN packets directed at a specific host).

The anecdotal instances above may be usefully placed in a more organised framework using a network management model developed by the International Organization for Standardization (ISO). There are five categories of network management:

Performance administration. Performance management is to quantify, measure, report, evaluate, and regulate various network component performance (such as utilization and throughput). These elements include specific gadgets (such connections, routers, and hosts) as well as end-to-end abstractions like a network path. We'll see in a moment how important protocol standards like the Simple Network Management Protocol (SNMP) [RFC 3410] are to managing Internet performance.

Management of faults. Problem management aims to record, identify, and react to network fault situations. It might be difficult to distinguish between performance management and defect management. In contrast to performance management, which takes a longer-term approach to maintaining acceptable levels of performance in the face of fluctuating traffic demands and sporadic network device failures, fault management can be thought of as the immediate handling of transient network failures (for instance, link, host, or router hardware or software outages). The SNMP protocol is essential to fault management, just as it is to performance management.

Management of configuration. A network manager can keep track of the hardware and software settings of the devices that are connected to the managed network thanks to configuration management provides an overview of configuration management and IP-based network needs.

Management of accounting. The network manager may define, record, and manage user and device access to network resources via accounting management. Accounting management include utilisation limits, usage-based billing, and the distribution of resource access rights.

Security administration. Controlling access to network resources in accordance with a clearly defined policy is the aim of security management. Security management includes the important distribution centres.

We'll merely touch on the basics of network administration in this chapter. We'll explore solely the network management infrastructure—the general architecture, network management protocols, and knowledge base—through which a network administrator maintains the network's uptime. This restrictive emphasis is on purpose. We won't go into the network administrator's decision-making procedures, which include planning, analysing, and responding to management data sent to the NOC. This field takes into account issues like anomaly detection , fault identification and management which deals with the supply of resources like bandwidth, server capacity, and other computational/communication resources required to satisfy an enterprise's mission-specific service needs.

Security and Management

"SNMPv3 may be regarded of as SNMPv2 with added security and management features," according to the SNMPv3 authors [RFC 3410]. It's true that SNMPv3 differs from SNMPv2 in several ways, but administration and security are the two areas where these differences are the most noticeable. Since SNMP was mostly used for monitoring rather than control due to

inadequate security (SNMPv1 seldom uses SetRequest, for example), the fundamental role of security in SNMPv3 was especially crucial.

Sadly, as SNMP has evolved through three versions, the quantity of standards papers pertaining to it has increased along with its capability. The existence of an RFC that "describes an architecture for specifying SNMP Management Frameworks" is proof of this. While it may be difficult to comprehend the idea of an "architecture" for "defining a framework," RFC 3411's objective to provide a uniform vocabulary for describing the functions and activities conducted by a SNMPv3 agent or management entity is an ideal one. A tour of the architecture of a SNMPv3 entity will help us better grasp SNMP since it is a simple structure.

A controlling entity's command generator, notification receiver, and proxy forwarder are all examples of so-called SNMP applications. An agent's command responder and notification originator are all examples of so-called SNMP applications. The GetRequest, GetNextRequest, GetBulkRequest, and SetRequest PDUs that we looked at in Section 9.3.3 are generated by the command generator, and it also manages the answers that are sent in response to these PDUs. The GetRequest, GetNextRequest, GetBulkRequest, and SetRequest PDUs are received, processed, and responded to by the command responder, which runs in an agent. Trap PDUs are produced by the notification originator application in an agent; the notification receiver application at a management entity finally receives and processes the Trap PDUs. Request, notification, and answer PDUs are sent via the proxy forwarder programme. After passing through the SNMP "engine," a PDU sent by an SNMP application is then transmitted via the appropriate transport protocol. Figure 11.2 depicts the first entry of a PDU produced by the command generator application into the dispatch module.

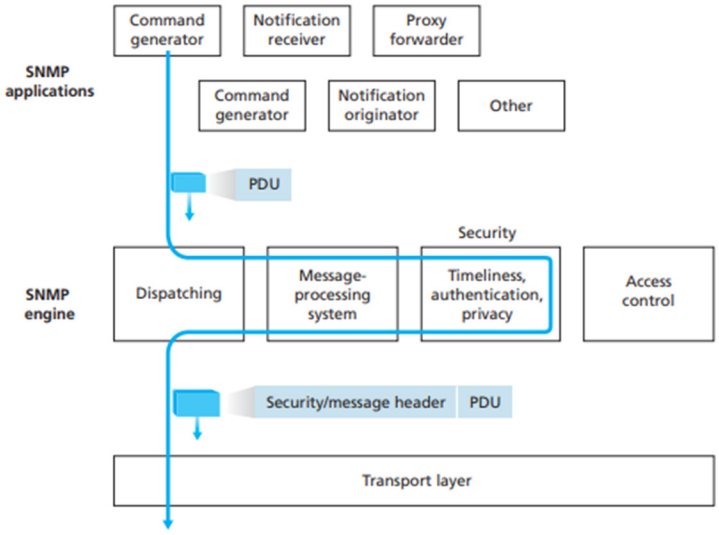


Figure 11.2: SNMP

where the version of SNMP is identified. The PDU is subsequently processed in the messaging system, where it is enclosed in a message header that includes the SNMP version, a message ID, and information about the message size. The necessary header elements are also supplied if encryption or authentication are required; see [RFC 3411] for further information. The appropriate transport protocol receives the SNMP message (the application-generated PDU plus the message header data). The chosen port number for SNMP is port 161, and UDP is the preferred transport

protocol for SNMP messages (i.e., SNMP messages are transmitted as the payload of a UDP datagram). For trap messages, port 162 is utilised. As we saw above, SNMP messages are used to not only monitor network objects but also to manage them (for instance, using the SetRequest command).

It is obvious that a hacker who gained access to the management infrastructure and was able to intercept SNMP messages or create its own SNMP packets might cause havoc in the network. Consequently, it is essential that SNMP messages be sent securely. Surprisingly, security hasn't been given the attention it merits until the most current iteration of SNMP. According to RFC 3414, SNMPv3 security is referred to as "user-based security" because it uses the conventional idea of a user who is recognised by a username and to whom security data like a password, key value, or access rights are attached. Access control, encryption, authentication, and defence against playback attacks are all features of SNMPv3.

Cryptography

The Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode may be used to encrypt SNMP PDUs. The receiving entity that must decode the data must be aware of the user's secret key since DES is a shared-key scheme.

Defense against replay

The receiver demands that the sender provide a value in each message that is based on a counter in the receiver in order to guarantee that a received message is not a replay of some previous message. The time since the receiver's network management software was last restarted and the total number of reboots since the receiver's network management software was last configured are both reflected in this counter, which serves as a nonce. The message is accepted as a no replay communication and may then be authenticated and/or decrypted as long as the counter in the received message is within a certain margin of error of the receiver's real value.

Access management.

SNMPv3 offers a view-based access control that regulates which users may query and/or set which network management data. In a Local Configuration Data store, an SNMP entity stores data about rules and access privileges (LCD). As managed objects described in the View-Based Access Control Model Configuration MIB, some LCD components may be maintained and controlled remotely using SNMP.

Chapter 12

NETWORK SECURITY

Dr. Gokul Thanigaivasan, Assistant Professor
Department of Computer Science & IT, School of Sciences, Jain (Deemed-to-be University), Bangalore-27, India
Email Id- t.gokul@jainuniversity.ac.in

Computer network security refers to the steps that companies and other organizations take to monitor and stop unwanted access from outside intruders. Depending on the scale of the computer network, different ways to managing network security have varied requirements. A home office, for instance, needs only the most basic network security, whereas major organizations need intensive maintenance to shield their networks from hostile attacks. Access to the information and software on the network is managed by the network administrator. The user ID and password are given to the authorized person by the network administrator.

- **Features of Network Security:**

Privacy: By maintaining secrecy, both the sender and the recipient are maintaining privacy. Only the intended recipient should get the transmitted message, and it should be opaque to all other users. The message being broadcast should only be understood by the sender and receiver because it could be intercepted by eavesdroppers. Therefore, it is necessary to encrypt the message in order to prevent message interception. Secure communication is frequently achieved by utilizing this characteristic of confidentiality.

End-point authentication: Authentication ensures that the message was sent by the intended party and that it wasn't delivered by an impostor.

Message Integrity: Data integrity refers to the requirement that the message be received exactly as it was transmitted. There cannot be any intentional or unintentional changes made to the data's content while it is being transmitted. Data integrity is becoming important as there are more and more financial transactions taking place online. Secure communication necessitates the preservation of data integrity.

Non-Repudiation: In order for a message to be considered non-reputable, the sender's identity must be established by the recipient. A message's sender cannot claim they never sent it. The recipient is responsible for establishing their identification. For instance, if a consumer requests that money be transferred from one account to another, the bank needs verification that the customer actually requested the transaction.

- **Privacy:**

The idea of how to obtain privacy has not changed: the communication cannot be encrypted. To all uninvited parties, the message must appear opaque. To some extent, privacy can be achieved using effective encryption and decryption methods. By using this method, the message's contents are rendered incomprehensible to the listener. Privacy is the capacity of a person or organisation to distance themselves or information about themselves and therefore express themselves judiciously. The idea of achieving privacy has not changed much throughout time: the communication cannot be encrypted. The message must be kept secret from all uninvited parties.

A strong encryption/decryption method may help you achieve privacy to some degree. This method makes sure that the message's contents are hidden from the intrusive party.

Encryption

The process of encryption transforms the original data into a false representation. Because the senders used an encryption mechanism to prevent the hacker from reading the contents, this new version of the message is wholly different from the original. Key algorithms are often used to master encryption. Sender carries out this.

Decryption

The opposite of encryption is decryption. In this procedure, the encrypted or disguised data is returned to its original state, or you could say it is formatted in a readable manner. The data must be manually decrypted using these instructions or the keys that were used to encode the original data. The recipient executes it. At the sender's end, the data that will be encrypted (the original data) is known as unencrypted, and the encrypted data is known as cipher text. The information is decrypted at the receiving end. The opposite of encryption is decryption. In this procedure, the encrypted or disguised data is returned to its original state, or you might say it is formatted in a readable manner. The data must be manually decrypted using these instructions or the keys that were used to encrypt the original data. The recipient executes it. At the sender's end, the data that will be encrypted (the original data) is known as plaintext, and the encrypted data is known as ciphertext. The data is decrypted at the receiving end.

The Decryption/Encryption Need

It protects our sensitive information, including documents, bank account information, passwords, and login information.

1. Our data is secure because of it.
2. It guarantees that our materials have not been altered.
3. It also helps in defending our intellectual property (IP) from infringement.
4. The definition of a "Key" and the many sorts of keys used in cryptography before reviewing the various encryption methods.

Keys

In the field of cryptography, a "key" is a numeric piece of data that is used with an algorithm (a "cypher") to transform plaintext into ciphertext and vice versa (decryption).

Different Keys:

Synchronized Key

The same cryptographic keys are used by symmetric-key encryption techniques for both the original and encrypted material.

Key Asymmetry

Two key pairs are used for asymmetric encryption. While only the message's receiver has access to the secret key, anybody can access the public key. It guarantees boot security.

Private Key

Two key pairs are used in public key cryptography, a kind of encryption. Data for a receiver is encrypted using these.

Secure Key

A public key and a private key may form an asymmetric key pair. Because the same key is used to encrypt and decrypt data, it may be utilised in asymmetric encryption.

Shared Before

Before being utilised in cryptography, a pre-shared key (PSK) is a shared secret that is first communicated between the two parties over a secure channel.

Encryption and decryption techniques are categorised.

Two categories of encryption and decryption methods are recognised:

- Discretion with a hidden key Method for encryption and decryption
- Using a public key for privacy Method for encryption and decryption

Discretion with a hidden key Encryption/Decryption

Both the sender and the receiver utilise the same key in both encryption and decryption operations. The same key is used to encrypt the data by the sender and to decode it by the recipient. Due to the fact that it employs the same secret key for communication on both sides, it is sometimes referred to as a symmetric encryption algorithm. To instal the key on each computer, we must be aware of which machines are communicating with one another.

Advantages:

1. These are more effective than public key encryption algorithms since they encrypt the data in a materially shorter amount of time.
2. The key is quite tiny.
3. The primary functions of these keys are encryption and decryption.

Disadvantages:

1. The key must be shared by each pair of parties.
2. It might be challenging for multiple parties to share keys.
3. Using a public key for privacy Encryption/Decryption
4. Public-key encryption uses both a public key and a private key.
5. While the public key is made available to the general public, the private key is given to the recipient. RSA is the most used public-key algorithm.

Digital Signature:

A personal signature on a written document is the same as a digital signature for an electronic message, which is produced using a type of cryptography. The electronic tying of the signer's identity to the communication's origin is made possible by the digital signature on a message. A digital signature offers evidence of the message's origin and a way to check the message's consistency. The owner of a digital certificate combines the data to be signed with their private key before subjecting the data to an algorithmic transformation. The signature is decrypted by the message's recipient using the accompanying certificate's public key. The signed message's integrity and the sender's identity are both confirmed by the public key decryption. The only entity that can generate a digital signature is the one holding the private key. The digital signature can be validated by anybody who has access to the accompanying public key, though. A digital signature is exactly what it sounds like—a more contemporary option to writing your signature by hand on

paper. To verify the integrity and validity of digital communications and documents, it employs a cutting-edge mathematical approach. It helps us combat the issue of impersonation and tampering in digital communications and ensures that the contents of a message are not changed while in transit. Additionally, digital signatures include details about the message's origin, status, and signer's agreement.

The stages involved in creating a digital signature are as follows:

A. The digital signature is created when the sender uses their private key to encrypt the message digest after computing it (using an algorithm like RSA or SHA1) to create the message digest. A message may have several signatures and signature formats attached, each referencing various (or even overlapping) elements of the message.
B. The sender sends the message together with the digital signature.
C. The message digest is generated once the receiver decrypts the digital signature using the sender's public key.
D. The receiver generates a message digest from the received message data and confirms that the two digests are identical. The text is both intact and legitimate if these digests agree.

Digital signatures' function

Digital signatures are regarded as legally binding and have equal weight as conventional document signatures in many jurisdictions, including sections of North America, the European Union, and APAC. They are used for financial transactions, email service providers, and software distribution in addition to digital document signing, all of which need the authenticity and integrity of digital communications.

Data authenticity and integrity are guaranteed via a public key infrastructure, an industry-standard technique.

Digital Signatures Work

Digital signature service providers like Zoho Sign will produce two keys using a mathematical algorithm: a public key and a private key. A cryptographic hash of the document is produced when a signer digitally authenticates it.

The sender's private key, which is kept in a safe HSM box, is subsequently used to encrypt that cryptographic hash. The document is then transmitted to the recipients with the attachment attached and the sender's public key included.

With the help of the sender's public key certificate, the receiver may decode the encrypted hash. The recipient's end again creates a cryptographic hash.

Its legitimacy is verified by comparing the two cryptographic hashes. They must match in order for the document to be regarded genuine and unaltered.

PGP

A security program called Pretty Good Privacy (PGP) is used to encrypt and decrypt email as well as to authenticate email communications using digital signatures and file encryption. Cybercriminals often launch attacks using email because it's simple for them to create forged messages using the name or identity of a victim. By encrypting the data to increase the privacy of the communication method, PGP strives to address this issue and improve email security. One of

the earliest public-key cryptography programs that was freely accessible was PGP. It was initially employed to allow private user communication on bulletin board system computer servers. Later, it became standardized and supported by additional programs like email. It is currently a widely accepted fundamental standard for email security and has been utilized to safeguard both people and businesses. For data used in online communication, the data encryption program offers cryptographic authentication and privacy. As a result, PGP can be used to encrypt and decrypt files, emails, and text communications.

The steps PGP takes to establish secure email at the sender site are as follows:

A. To construct a digest, the email message is hashed using a hashing function.
B. Using the sender's private key, the digest is then encrypted to create a signed digest, which is then appended to the original email message.
C. A one-time secret key generated by the sender is used to encrypt both the initial letter and the signed digest.
D. The public key of a receiver is used to encrypt the secret key.
E. The message and digest combination are sent encrypted, together with the secret key that is also sent encrypted.

A well-known tool called PGP (Pretty Good Privacy) is used to provide secrecy and authentication services for storage of electronic messages and files. Phil Zimmermann created it way back in 1991. RSA, Diffie-Hellman key exchange, and DSS are used for public-key encryption (or asymmetric encryption), CAST-128, 3DES, and IDEA are used for symmetric encryption, and SHA-1 is used for hashing. These are all the greatest cryptographic algorithms, according to the way he built it. The open source PGP programme is independent of the OS (Operating System) and the CPU. The programme is built around a handful of simple instructions.

PGP provides the following services:

A. Verification
B. Remaining discreet
C. Constriction
D. Support for Email
E. Segmenting

Authentication: Authentication is the process of confirming the truth or reality of something. We sometimes provide our account name and password when logging onto various websites; this is a method of authentication and verification.

In the realm of email, the only way to determine whether an email is legitimate is to see if the sender is who they claim they are. Email authenticity must be verified since spammers and individuals who spoof emails exist, and they may sometimes be very inconvenient. The following is how the PGP authentication service is offered:

The Hash Function (H) determines the message's hash value, as shown in the image above. SHA-1 is used for hashing and generates an output hash value of 160 bits. Then, it is encrypted and is referred to as a digital signature using the sender's private key (KPa). The signature is then followed by the Message. The whole procedure up to this point has been referred to as signing the message. The message is then delivered to the recipient after being compressed to lower the transmission overhead.

The data is decompressed and the message and signature are retrieved at the receiver's end. Using the sender's public key (PUa), the signature is then decrypted, and the hash value is then acquired. The message is once again processed through the hash function to get the hash value.

If the two values—one from the signature and the other from the most recent output of the hash function—are the same, the email was sent from a recognised source and is legitimate; otherwise, it wasn't.

Confidentiality: On sometimes, we come across packets marked "Confidential," which denotes that only a restricted group of individuals should have access to them. The secrecy of emails also applies in this case. Only the sender and the recipient should be allowed to view this email, which implies that everyone else must be kept in the dark about the message's contents.

The following is how PGP delivers that Confidentiality service:

The message is initially compressed before being symmetrically encrypted using a 128 bit session key (Ks) produced by PGP. The receiver's public key (KUb) is then used to encrypt the session key (Ks) using public key encryption (EP). The recipient will now get a concatenated version of both encrypted elements. the first message was compressed and then encrypted, so even if someone managed to intercept the traffic, they would not be able to read the contents since they are not in readable form. Instead, they could only do so if they had access to the session key (Ks). Even if the session key is sent to the recipient and therefore included in the traffic, it is encrypted and can only be unlocked with the private key (KPb) of the recipient, guaranteeing the entire security of our communication.

The encrypted session key is decrypted at the receiving end using the receiver's private key (KPb), and the message is then decrypted using the acquired session key. The message is then uncompressed in order to get the original message (M).

For symmetric key encryption, CAST-128 (or IDEA or 3DES) is utilised, while for public-key encryption, the RSA method is employed.

Cryptography

The military, the diplomatic community, diarists, and lovers have all utilised and contributed to the art of cryptography throughout history. The military has played the most significant part in shaping this sector throughout the ages. Within military organisations, the task of encrypting and transmitting communications has usually fallen to low-level, poorly paid code clerks. This job couldn't be completed by a small group of top experts because to the enormous amount of communications. The capacity of the code clerk to carry out the required transformations, often on a battlefield with limited equipment, had been one of the primary limitations on cryptography prior to the invention of computers. Another obstacle has been the difficulty of swiftly moving from one cryptographic approach to another, since this necessitates retraining a large number of individuals. However, it is crucial to be able to alter the cryptographic technique immediately if necessary due to the risk of an enemy code clerk being caught. The model was created in response to these competing needs. The plaintext of the communications to be encrypted is changed by a function that is parameterized by a key. The ciphertext, the result of the encryption operation, is subsequently sent by radio or messenger. We presumptively assume that the adversary or intruder hears and properly records the whole ciphertext. He cannot simply decipher the ciphertext because, unlike the intended receiver, he is unaware of the decryption key. In certain cases, the intruder (passive intruder) is able to do more than just listen in on the communication channel. He may also

record communications and replay them later, insert his own messages, or alter valid messages before they reach the recipient (active intruder). Cryptology is the study of creating and cracking cyphers. Cryptanalysis is the practise of cracking cyphers. By using codes, cryptography is a technique for encrypting data and communications so that only the intended audience can read and comprehend it.

In computer science, the term "cryptography" refers to safe information and communication methods that use mathematical principles and a system of computations based on rules, or "algorithms," to change messages in ways that are challenging to read. These deterministic algorithms are used in the creation of cryptographic keys, digital signature, online surfing on the internet, and private communications like email and credit card transactions.

Cryptanalysis Methods

The fields of cryptology and cryptanalysis are closely connected to those of cryptography. It comprises methods for concealing data while it is being stored or transported, including microdots, word-image fusion, and other approaches. But in today's computer-centered society, cryptography is most often linked with changing plaintext (regular text, also known as cleartext) into ciphertext and back again (known as decryption). Those who work in this area are referred to as cryptographers.

The following four goals are of particular relevance to modern cryptography:

A. Confidentiality. Anyone for whom the information was not meant cannot understand it.
B. Integrity.
C. The information cannot be changed while being stored or being transported between the sender and the intended recipient without the change being noticed.
D. Non-repudiation. The person who created or sent the material cannot afterwards deny that they had any motivation for doing so.
E. Authentication. Both the sender and the recipient are able to verify each other's identities and the information's source and destination.

Cryptosystems are procedures and protocols that satisfy any or all of the aforementioned requirements. However, they also include the control of human behaviour, such as selecting difficult-to-guess passwords, logging off unused systems, and refraining from discussing sensitive procedures with outsiders. Cryptosystems are frequently thought to only refer to mathematical procedures and computer programmes.

Cryptographic procedures

Cryptosystems encrypt and decode information using a collection of techniques called cryptographic algorithms, or cyphers, to secure communications between computer systems, devices, and applications.

A cypher suite employs three different algorithms: one for encryption, one for message authentication, and one for key exchange. On operating systems (OSes) and networked computer systems, this procedure, which is entrenched in protocols and implemented in software, entails: public and private key creation for data encryption and decryption; digital signature and verification for message authentication; and key exchange.

Cryptography Types

Single-key or symmetric-key encryption methods produce a block cypher, which is a fixed-length of bits, with a secret key that is used by the creator/sender to encrypt data and by the recipient to decrypt it. The Advanced Encryption Standard is a kind of symmetric-key encryption (AES). The National Institute of Standards and Technology (NIST) created the AES standard in November 2001 as a Federal Information Processing Standard (FIPS 197) to safeguard sensitive data. The standard is extensively used in the business sector and is required by the American government.

The U.S. government granted AES permission to use secret material in June 2003. It is a standard that is used without charge in hardware and software all around the globe. The Data Encryption Standard (DES) and DES3 were replaced by AES. To thwart brute force and other assaults, it employs greater key lengths (128-bit, 192-bit, and 256-bit).

Public-key or asymmetric-key encryption methods employ two keys: a public key connected to the creator or sender for encrypting communications and a private key that the originator only knows for decrypting messages (until it is revealed or they want to share it).

Public-key cryptography examples include:

A. RSA, which is commonly used on the internet.
B. Bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA)
C. In FIPS 186-4, NIST approved the Digital Signature Algorithm (DSA) as a Federal Information Processing Standard for digital signatures.

Exchange of Diffie-Hellman keys

In order to preserve data integrity in cryptography, data is mapped to a defined data size using hash functions, which provide a predictable output from an input value. SHA-1 (Secure Hash Algorithm 1), SHA-2, and SHA-3 are examples of cryptographic hash algorithms.

Encryption Issues

Attackers are able to defeat cryptography, get access to the computers in charge of data encryption and decryption, and take advantage of shoddy implementations such the usage of default keys. Cryptography, on the other hand, makes it more difficult for attackers to access communications and data that are encrypted. NIST issued a call for papers among the mathematical and scientific community in 2016 for new public key cryptography standards in response to growing worries that quantum computing's processing capacity may be used to crack existing encryption standards.

Quantum computing, in contrast to conventional computing, employs quantum bits (qubits), which may simultaneously execute two computations and represent both 0s and 1s. NIST claims that even if a large-scale quantum computer may not be constructed in the next decade, the current infrastructure needs the standardisation of publicly known and understood algorithms that provide a safe method. The submission deadline was in November 2017, and it would take three to five years to analyse the plans.

The evolution of encryption

Greek kryptos, which means concealed, is where the name "cryptography" originates. "Writing" is denoted by the suffix "-graphy," which follows the word "crypt-," which meaning "hidden" or "vault." Most historians place the invention of cryptography about 2000 B.C., with the Egyptian usage of hieroglyphics. These were made up of intricate pictograms, the meaning of which was

only fully understood by a select group of people. Julius Caesar (who ruled from 100 to 44 B.C.) is credited with using a sophisticated cypher for the first time because he didn't trust his messengers when he spoke with his governors and commanders. He devised a mechanism wherein each letter in his communications was substituted with a character that was three places higher in the Roman alphabet.

Some of the brightest mathematicians and computer scientists in the world are now engaged in a war over cryptography. Success in business and combat has been shown to depend heavily on one's capacity to convey and preserve sensitive information safely.

Cryptography has been subject to a variety of restrictions in many countries, ranging from limitations on the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems, because governments do not want certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests. However, the internet has made it possible for the dissemination of strong software and, more crucially, the fundamental principles of cryptography, such that many of the most cutting-edge cryptosystems and concepts are now available to the general public.

TRANSMISSION SECURITY

The remainder of the chapter describes how these methods are used in the real world to offer network security, and it concludes with some reflections on the social elements of security. Communication security in the following four parts, namely how to transmit bits from source to destination covertly and unaltered as well as how to prevent undesired bits outside the door. While not the only security concerns in networking, they are unquestionably some of the more significant ones.

1 IPsec

Since years, IETF has been aware that the Internet lacked adequate security. Its addition was challenging since there was disagreement about where to place it. The majority of security professionals think that end-to-end encryption and integrity checks are necessary for really secure systems (i.e., in the application layer). That is, the data are encrypted and/or integrity protected at the source process before being sent to the destination process for decryption and/or verification. Then, every alteration made between these two procedures, even modifications made inside either operating system, may be discovered. The issue with this strategy is that it calls for updating all programmes to include security awareness. According to this viewpoint, the next best strategy is to include encryption into the transport layer or into a new layer between the application layer and the transport layer, maintaining end-to-end functionality without changing the applications.

According to the opposing viewpoint, users cannot or will not properly utilise security because they do not understand it, and no one wants to alter any current applications. As a result, the network layer should authenticate and/or encrypt packets without the users' involvement. This viewpoint gained enough support after years of heated debates that a network layer security standard was developed. Part of the argument was that network layer encryption helps security-unaware users to some level while not impeding security-aware users from doing it correctly.

This conflict gave rise to the IPsec (IP security) architecture, which is discussed among other places in RFCs 2401, 2402, and 2406. Not every user wants encryption (because it is computationally expensive). Instead of making encryption optional, it was chosen to always

enforce it while allowing the use of a null algorithm. In RFC 2410, the null method is discussed and lauded for its clarity, simplicity, and speed. A foundation for various services, algorithms, and granularities is provided by the whole IPsec architecture. The availability of a la carte services stems from the fact that not everyone wants to pay the fee for having all the services accessible all the time. Secrecy, data integrity, and protection against replay attacks are the three main services (where the intruder replays a conversation). Due to the need of high performance, all of them are based on symmetric-key cryptography.

The existence of many algorithms is necessary since an algorithm that is now believed to be safe might become vulnerable in the future. Making IPsec algorithm-independent allows the framework to continue to function even if a certain algorithm is subsequently shown to be flawed.

To protect a single TCP connection, all communication between a pair of hosts, all traffic between a pair of secure routers, among other possibilities, it is necessary to have several granularities. The fact that IPsec is connection-oriented while being at the IP layer is a little unexpected. Actually, it shouldn't come as a big surprise since in order to have any security, a key has to be created and used for a while basically, a connection by another name. Connections also spread out the setup (Security Association). A security identification is attached to a SA, which is a simplex connection between two endpoints. Two security associations are needed if secure traffic is required in both directions. On these secure connections, packets carrying security identifiers are utilised to search up keys and other pertinent data when a secure packet arrives.

Technically, IPsec consists of two main components. The security identification, integrity control data, and other information may be carried by packets by means of two additional headers that are described in the first section. The establishment of keys is covered by the other section, ISAKMP (Internet Security Association and Key Management Protocol). A framework is ISAKMP. IKE is the primary protocol used to carry out the task (Internet Key Exchange). It is recommended to utilise IKE version 2, as stated in RFC 4306, since the previous version had serious flaws, as noted by Perlman and Kaufman (2000). You may use IPsec in one of two ways. The IPsec header is added immediately after the IP header in transport mode. The IP header's Protocol field is modified to note that an IPsec header comes after the regular IP header and before the TCP header. The SA identification, a new sequence number, and perhaps an integrity check of the payload are the security-related items in the IPsec header.

The whole IP packet, header and all, is encased in a new IP packet with a brand-new IP header while in tunnel mode. When the tunnel terminates somewhere other than the intended site, tunnel mode might be helpful. Sometimes the tunnel's exit is a security gateway device, such a corporate firewall. For a VPN, this is often the case (Virtual Private Network). As packets move through it in this mode, the security gateway encapsulates and decapsulates them. The computers on the corporate LAN do not need to be aware of IPsec as the tunnel is terminated at this secure workstation. All that needs to be aware of it is the security gateway.

Due to the fact that it prevents an intrusive party from knowing who is transmitting how many packets to whom, tunnel mode is especially advantageous when a collection of TCP connections is aggregated and processed as one encrypted stream. Sometimes useful information is as simple as understanding where and how much traffic is moving. An intruder might be able to infer some useful information from these data, for instance, if during a military crisis, traffic between the Pentagon and the White House were to sharply decline while traffic between the Pentagon and some military installation buried deep in the Colorado Rocky Mountains were to increase by the

same amount. Traffic analysis is the study of packet flow patterns, including encrypted packets. It can be somewhat thwarted using tunnel mode.

The drawback of tunnel mode is that it significantly increases packet size by adding an additional IP header. Transport method, however, has less of an impact on packet size.

AH is the first new header (Authentication Header). It offers antireplay security and integrity checks but not confidentiality (i.e., no data encryption).

Firewalls

It's a mixed blessing to be able to link any computer, anytime, to any other computer, everywhere. Online exploration is a lot of fun for those who are at home. It is a nightmare for corporate security managers. The majority of businesses publish a lot of sensitive material online, including trade secrets, plans for new products, marketing tactics, financial analysis, etc. If this knowledge were to be made available to a rival, terrible things may happen.

Information leakage into the system is also a risk in addition to information leakage out. Viruses, worms, and other digital pests in particular may compromise security, damage important data, and take a lot of administrators' work to clean up after themselves. They are often brought in by reckless workers who want to play a cool new game. Therefore, there is a need for systems to keep "good" bits in and "bad" bits out. Utilizing IPsec is one approach. Using this strategy, data between secure locations is protected. IPsec, however, has little effect on preventing digital invaders and pests from connecting to the corporate LAN. A deep moat surrounding your castle was the traditional mediaeval security measure; firewalls are only its contemporary equivalent. Because of this layout, each person entering or departing the castle had to cross a separate drawbridge so that they could be checked by the I/O police. The similar method may be used with networks: a business may have several LANs linked in any order, but all traffic to or from the business must pass through an electrical drawbridge (firewall). There is no other option. Packet filtering is done by the firewall. Every every incoming and outgoing packet is examined. Packets that comply with a requirement outlined in rules created by the network administrator are generally forwarded. Those who don't pass the exam are mercilessly dismissed.

A rule or table that lists allowed sources and destinations, forbidden sources and destinations, and default rules for what to do with packets arriving from or going to other computers often serves as the filtering criteria.

The area of the enterprise network that is not inside the security perimeter is known as the DMZ. Here, everything goes. Computers on the Internet can connect to a device, such as a Web server, in the DMZ to browse the business website. So that computers on the Internet cannot utilise port 80 to attack machines on the local network, the firewall may now be set up to block incoming TCP traffic to this port. The firewall may contain a rule allowing connections between internal computers and the Web server so that the Web server can be controlled. Firewalls have advanced significantly over time as a result of an arms race with attackers. Initially, firewalls implemented a rule set separately for each packet, but it was challenging to create rules that permitted needed functionality while blocking all undesired traffic. Stateful firewalls employ TCP/IP header fields to monitor connections and map packets to connections. As an example, this enables rules that let packets to be sent from an external Web server to an internal host, but only after the internal host first establishes a connection with the external Web server. Stateless architectures that must either pass or drop all packets from the external Web server are unable to implement such a rule.

Application-level gateway implementation by the firewall represents a further advancement in sophistication over stateful processing. In order to determine what the application is doing, this step entails the firewall examining within packets, beyond even the TCP header. This makes it easy to discriminate between HTTP traffic used for peer-to-peer file sharing and HTTP traffic used for surfing the web. Administrators may create policies to prevent peer-to-peer file sharing while still allowing business-critical Web surfing. To stop critical papers from being sent outside of the firm, for all of these approaches, both incoming and outgoing traffic may be scrutinized.

Virtual Private Networks (VPNs)

Numerous businesses have facilities dispersed throughout numerous cities, and even over several nations. Before public data networks, it was typical for these businesses to lease telephone lines from the telephone company to connect some or all of their sites. This is still done by certain businesses. A private network is one created using leased phone lines and business computers.

Private networks function well and provide high security. If the only lines accessible are the leased lines, no traffic can escape from business facilities, and anybody trying to break in would have to physically wiretap the lines, which is difficult. Private networks have the drawback that renting a dedicated T1 line costs thousands of dollars per month between two places, and T3 lines are far more costly. Many businesses desired to shift their data (and maybe voice) traffic to the public network when public data networks and subsequently the Internet first arose, but they didn't want to give up the security of the private network.

Virtual Private Networks (VPNs), which are overlay networks on top of public networks but with most of the characteristics of private networks, were quickly developed in response to this need. They are only an illusion, just as virtual circuits are not genuine circuits, and virtual memory is not real memory, which is why they are termed "virtual" in the first place.

The construction of VPNs straight over the Internet is one well-liked method. As shown in Fig. 8-30, a typical architecture involves installing firewalls in each office and building Internet tunnels between each pair of offices (a). Another benefit of utilising the Internet for connectivity is that, if the user has an Internet connection, tunnels may be built up at any time to include, for instance, a worker's computer when they are travelling or at home. However, from the viewpoint of the computers connected to the VPN, the topology seems exactly like the private network. This flexibility is far larger than that offered by leased lines (b). The parameters of each firewall pair's SA, including the services, modes, algorithms, and keys, must be negotiated when the system is started.

Any communication between any two pairs of offices may be combined onto a single authenticated, encrypted SA when IPsec is used for the tunnelling, enabling integrity control, confidentiality, and even significant immunity to traffic analysis. Many firewalls provide VPN functionality by default. Some regular routers can do this as well, but because firewalls are largely in the security industry, it makes sense for the tunnels to start and stop there, creating a distinct barrier between the company's network and the Internet. As a result, IPsec in tunnel mode with ESP and firewalls, VPNs, and other security measures make sense and are often used in reality. Traffic may start moving once the SAs are in place. A packet going across a VPN tunnel appears to an Internet router as an ordinary packet. The only oddity is the IPsec header after the IP header, but because these additional headers have no effect on the forwarding process, the routers are unconcerned with this extra header.

The process of having the ISP set up the VPN is another one that is gaining popularity.

Paths for the VPN traffic may be established through the ISP network between the corporate offices using MPLS. These routes maintain the confidentiality of VPN communication while guaranteeing a particular level of bandwidth or other service quality.

A VPN's total transparency to all user software is a significant benefit. The SAs are created and managed by the firewalls. Only the system administrator, who must manage and configure the security gateways, or the ISP administrator, who must manage and configure the MPLS pathways, is even aware of this configuration. Everyone else sees it as though they are back in a leased-line private network. Read more about VPNs here.

Mobile Security

It is surprisingly simple to create a system utilising firewalls and VPNs that is logically totally safe yet leaks like a sieve in reality. This scenario may arise if some of the devices are wireless and communicate using radio waves, which pass directly through the firewall in both ways. A person who wants to spy on a business may easily pull into the employee parking lot in the morning, leave an 802.11-capable notebook computer in the vehicle to record all it hears, then drive off for the day since 802.11 networks often have a range of a few hundred metres. The hard drive will be loaded with priceless treasures by late afternoon. This leakage is not meant to occur, in theory. Theoretically, it is also forbidden for anyone to loot banks.

The attempt by makers of wireless base stations (access points) to make their products user-friendly has led to a significant portion of the security issue. When a user removes a gadget from its packaging and plugs it into an electrical outlet, it often starts working right away with almost no security at all, broadcasting information to everyone within radio range. If it is connected to an Ethernet after that, all Ethernet traffic will then show unexpectedly in the parking lot as well. Wireless is a snooper's paradise since it offers free data without requiring any effort. So it should come as no surprise that security is much more crucial for wireless systems than for wired ones.

Security

A data linklevel security mechanism is outlined in the 802.11 standard, which was originally known as 802.11i, which prevents a wireless node from reading or interfering with messages carried between two other wireless nodes. WPA2 is another trademark for it (WiFi Protected Access 2). Plain WPA is a temporary protocol that carries out a portion of 802.11i. WPA2 should be used instead to prevent it. The original generation of 802.11 security protocols, WEP (Wired Equivalent Privacy), is being replaced by 802.11i, which we shall discuss in more detail later. A networking standards group created WEP, which is an entirely different approach than, say, how NIST chose the architecture of AES. The outcomes were disastrous. What was incorrect with it? It turns out that from a security standpoint, pretty much everything. As an example, WEP encrypts data for secrecy by XORing it with a stream cipher's output. Unfortunately, poor keying arrangements led to frequent reuse of the output. This resulted in easy solutions to overcome it. Another example is the integrity check, which used a 32-bit CRC. Although such code is effective at spotting transmission faults, it is not a robust enough cryptographic defence against intruders.

Because of these and other design faults, WEP was particularly vulnerable to attack. When Adam Stubblefield was an intern at AT&T, he provided the first concrete evidence that WEP was flawed. In one week, he was able to write and test an attack described by much of which was spent persuading management to purchase a WiFi card for him to utilise in his experiments. Wep

passwords can now be cracked in under a minute using free software, hence using WEP is highly discouraged. While it does limit unauthorised access, no actual security is offered. When it became apparent that WEP was fundamentally flawed, the 802.11i group was quickly formed. By June 2004, a formal standard had been created.

We will now discuss 802.11i, which, when configured and utilised correctly, does provide true security. There are two typical situations when WPA2 is used. The first situation is a corporate one, where a business maintains a separate authentication server with a username and password database that can be used to check if a wireless client is authorised to access the network. In this situation, clients authenticate themselves to the network using industry-standard protocols. The two primary standards are EAP (Extensible Authentication Protocol) (RFC 3748), which describes how the client and the authentication server communicate, and 802.1X (which allows the access point to let the client carry on a conversation with the authentication server and monitors the outcome). The messages of the protocol are defined by other standards, while EAP is only a framework. We won't go into all the specifics of this conversation, however, since a summary does not really need them.

The second scenario takes place at home without an authentication server. Instead, customers log in to the wireless network using a single common password. This configuration is used at home and in small enterprises since it is less complicated than having an authentication server, but it is also less secure. The primary distinction is that each client using an authentication server receives a key for encrypting communication that is private to all other clients. Different keys are generated for each client using a single common password, but because everyone uses the same password, they may all generate each other's keys if they so want.

In the course of an authentication handshake, the keys that are used to encrypt communication are calculated. The handshake takes place immediately after the client connects to a wireless network and, if necessary, authenticates with an authentication server. The client has either the shared network password or its password for the authentication server at the beginning of the handshake. The master key is obtained with this password. However, packet encryption is not carried out directly using the master key. Standard cryptographic procedure calls for generating a session key for each time a system is used, changing the key between sessions, and exposing the master key to as little scrutiny as feasible.

The access point (AP) delivers a random identification number first. Nonces, which is essentially an abbreviation of "number used once," are random numbers used just once in security procedures like this one. The nonce is also chosen by the customer. It generates a session key, KS, by computing the nonces, its MAC address, the MAC address of the AP, and the master key. We have overlooked the fact that the session key is divided into parts, each of which is utilised for a separate function. Now, only the client and AP have access to the session keys. As a result, the client provides the AP its nonce, and the AP does the same calculation to produce the identical session keys. The keys cannot be determined from the nonces without additional, secret information, therefore the nonces may be communicated in the open. A MIC (Message Integrity Check), which is based on the session key, is used to secure the message from the client. After computing the session keys, the AP may verify that the MIC is accurate, proving that the message did, in fact, originate from the client. A message authentication code, such as an HMAC, is sometimes known as a MIC. Because MAC (Medium Access Control) addresses may be confused with networking protocols, the term MIC is often used instead.

Safety using Bluetooth

Security is still a concern since Bluetooth has a far lower range than 802.11, making it more difficult to attack from the parking lot. Imagine, for instance, that Alice's PC has a wireless Bluetooth keyboard. Without protection, Trudy could see anything Alice wrote, even all of her outgoing email, if she happened to be in the neighbouring office. Additionally, she had the ability to record whatever Alice's computer communicated to the Bluetooth printer next to it (e.g., incoming email and confidential reports). Fortunately, Bluetooth has a sophisticated security system in place to attempt to thwart global Trudies. Now, let's review its primary attributes.

Four security settings are available in Bluetooth versions 2.1 and beyond, ranging from no protection at all to complete data encryption and integrity control. Similar to 802.11, there is no security if security is turned off, which is the default for older devices. Security is often deactivated until a significant breach occurs, at which point it is switched on. This strategy is known in the agricultural community as locking the barn door after the horse has bolted.

Multiple levels of protection are offered by Bluetooth. Frequency hopping offers a modest measure of security at the physical layer, but because each Bluetooth device moving into a piconet must be informed of the frequency hopping sequence, it is clear that this sequence is not secret. When the freshly arriving slave requests a channel with the master, the actual security begins. Prior to Bluetooth 2.1, it was thought that two devices would share an advance-set secret key. In certain instances, the manufacturer will hardwire both (such as when a headset and mobile phone are supplied together). In other situations, the user must input the hardwired key from one device (such as the headset) as a decimal number into the other device (such as the mobile phone). Passkeys are the name for these shared keys. Unfortunately, the passkeys are sometimes hardcoded to "1234" or similar predictable figure. They are also always four decimal digits long, giving users just 104 options. Devices choose a code from a six-digit range when using basic secure pairing in Bluetooth 2.1, making the passkey significantly less predictable but still far from secure. The master and slave both verify that the other is aware of the passkey before opening a channel. If so, they discuss the channel's encryption, integrity control, or combination of the two. They then choose a random 128-bit session key, some of which bits could be accessible to the public. Allowing this key weakening serves the purpose of adhering to government prohibitions in different nations intended to prevent the export or use of keys that are more durable than those that the government can destroy.

Integrity control makes use of SAFER+ while encryption makes use of the stream cypher E0.

Both are conventional block cyphers with symmetric keys. The AES bake-off contender SAFER+ was entered, but due to its poorer performance than the others, it was disqualified in the first round. AES was selected before Bluetooth was finished; otherwise, Rijndael would have been used.

Figure 8-14 illustrates the real stream cypher encryption process, which involves XORing the plaintext and keystream to create the ciphertext. Unfortunately, RC4 and E0 may also contain catastrophic flaws.

Although it had not yet been cracked as of this writing, its resemblance to the A5/1 encryption, whose dramatic failure jeopardises all GSM telephone communications, should raise suspicions. People are sometimes surprised—including the authors of this book—by how often cryptanalysts prevail in the ongoing cat-and-mouse game between cryptographers and them.

Another security concern is that Bluetooth only authenticates devices, not individuals, thus if a device is stolen, the criminal may get access to the user's bank accounts and other accounts. Even if link-level security is compromised, Bluetooth implements security at the higher levels, thus some protection may still be present, particularly for apps that need a PIN number to be manually input from a keyboard to complete the transaction.

Web security

Just now, we looked at two crucial areas where security is required: email and communications. These might be regarded as the soup and the appetiser. The main entrée, web security, is now ready. Nowadays, the majority of Trudies hang around on the Internet and do their illicit business. We'll look at some of the challenges and concerns pertaining to web security in the parts that follow.

Web security may be categorised broadly into three categories. How are resources and objects named safely, first? Second, how can authorised, secure connections be created? Third, what happens when a client receives executable code from a website? We will look at all these issues after looking at some threats.

Threat

The circumstances are really rather dire. Let's examine a few instances of what has already occurred. First, various organisations' home sites have been attacked and changed with new ones of the crackers' choice. (While many programmers reserve the word "hacker" for exceptional coders, the public press refers to persons who breach into systems as "hackers." These folks are most often referred to as "crackers." Yahoo!, the U.S. Army, the CIA, NASA, and the New York Times are just a few of the websites that have had their security breached. Most of the time, the crackers just posted some humorous text, and the websites were fixed within a few hours.

Let's examine some considerably more severe instances right now. Denial-of-service attacks, when the cracker loads the site with traffic and prevents it from responding to genuine requests, have taken down several websites. The assault is often launched from several computers that the cracker has previously gained access to (DDoS attacks). These assaults are so frequent that they no longer even make the headlines, yet they may cause the sites to be targeted to lose thousands of dollars in revenue. When a Swedish hacker gained access to Microsoft's Hotmail website in 1999, he set up a mirror site where anybody could enter in a user's name and view all of their recent and old emails.

Another instance included a 19-year-old Russian hacker called Maxim who obtained 300,000 credit card details from an e-commerce website. Then he went up to the site's proprietors and threatened to publish all the credit card data online unless they paid him $100,000. They refused to cave in to his threats, and he did publish the credit card data, causing significant harm to a large number of innocent people.

In a separate vein, a 23-year-old California student sent a news organisation an email with a press release that falsely claimed that the Emulex Corporation would report a substantial quarterly deficit and that the CEO would be stepping down right away. The company's price fell by 60% within hours, costing owners more than $2 billion. Just before making the notification, the criminal earned a quarter million dollars by selling the stock short. Even though this incident did not involve a website hack, it is obvious that posting such a notice on the homepage of any significant company would have a comparable impact. Unfortunately, we could continue in this manner for many more pages. But it's time to look at some of the technological problems with web security right now.

A Web page appears shortly after she puts Bob's URL into her browser. Do you mean Bob's? Possibly, both yes and no. Trudy could be pulling one of her old ruses. She may, as an example, be checking all of Alice's outgoing packets. She may visit Bob's website herself to retrieve the page when she intercepts an HTTP GET request that is going to his website, change it as she pleases, and send Alice the fictitious page back. Alice would remain in the dark.

Even worse, Trudy may lower the pricing at Bob's online shop to make his products seem extremely appealing, deceiving Alice into giving "Bob" her credit card information to make a purchase. This traditional man-in-the-middle attack has the drawback that Trudy has to be in a position to fake Alice's incoming traffic and intercept Alice's outgoing communication. She must really touch Alice's or Bob's phone connection since it is quite hard to tap the fibre backbone. It is possible to actively wiretap someone, but it takes some effort, and although Trudy is shrewd, she is also lazy.

In addition, there are simpler methods to deceive Alice.

Spoofing DNS

One method would be for Trudy to get into Alice's ISP's DNS cache or DNS system and swap out Bob's IP address (for example, 36.1.2.3) with her own IP address (say, 42.9.9.9). This results in the subsequent assault. Figure 8-46 depicts how it is intended to operate (a). Here, Alice requests Bob's IP address through DNS, receives it, asks Bob for his home page, and receives both of those requests from Bob. Following Trudy's modification of Bob's DNS record to substitute her own IP address for Bob's, we get the scenario shown in Fig. 8-46. (b). Here, Alice's search for Bob's IP address returns Trudy's, causing all of her traffic meant for Bob to flow to Trudy. Trudy no longer has to bother with phone line tapping in order to launch a man-in-the-middle assault. Instead, she must hack into a DNS server and modify a single record, which is a far simpler task.

It ends up being really simple. In a nutshell, Trudy can deceive Alice's ISP's DNS server into issuing a request to check for Bob's IP. Unfortunately, since DNS utilises UDP, there is no meaningful mechanism for the DNS server to verify who sent the response. By altering the anticipated response and inserting a fake IP address into the DNS server's cache, Trudy may take advantage of this characteristic. For the sake of simplicity, let's suppose that Bob's website, bob.com, does not already have a listing with Alice's ISP. If so, Trudy may wait until it expires and try again later (or use other tricks).

SSL -The Secure Sockets Layer

Although secure naming is an excellent place to start, web security involves much more. Secure connections are the next stage. We'll now examine methods for establishing secure connections. Security is never straightforward, and this is no exception. The Web was originally only used for disseminating static pages when it first came into the public eye. However, soon after, several businesses came up with the concept of utilising it for financial operations like internet banking, stock trading, and credit card purchases of goods. There is now a need for secure communications because of these applications. In order to satisfy this need, Netscape Communications Corp., the major browser provider at the time, introduced a security package known as SSL (Secure Sockets Layer) in 1995. Since Firefox, Safari, and Internet Explorer all now make extensive use of this programme and its protocol, it is important to look at it in more depth.

Using

A. Parameter negotiation between the client and server, SSL creates a secure connection between two sockets.
B. The client authenticating the server.
C. Silent correspondence.
D. Protection of data integrity.

Mobile Security Code

In terms of web security, naming and connections are two areas of concern. However, there are more. Early Web pages were just static HTML files and did not include executable code. These days, they often include little programmes like Java applets, ActiveX controls, and JavaScripts. Numerous strategies have been developed to reduce the security risks associated with downloading and running such mobile programmes. Now, let's quickly review some of the problems that mobile code raises as well as possible solutions.

Social Concerns

An area where social concerns, public policy, and technology collide head-on, often with significant implications, is the Internet and its security technologies. Below, we'll only quickly look at three topics: copyright, freedom of expression, and privacy. The Internet is also a wealth of information. Simply enter terms like "privacy," "censorship," and "copyright" into any search engine to get started. For further connections, see the website for this book. You may find it at tanenbaum.pearsonhighered.com. A good query. The U.S. Constitution's Fourth Amendment forbids the government from examining people's homes, documents, and possessions without a warrant and further limits the conditions in which search warrants may be given. As a result, at least in the United States, privacy has been a hot topic for more than 200 years.

The ease with which governments may eavesdrop on their residents and the simplicity with which the people can stop such espionage have altered during the last ten years. In order for the government to examine a citizen's papers in the 18th century, it had to send a policeman riding a horse to the citizen's farm and demand to view certain documents. It was a laborious process. When given search warrants, telephone and internet service companies now routinely offer wiretaps. The police officer's job is made considerably simpler, and there is no risk of falling off a horse. Cryptography alters everything. Anyone who bothers to download and instal PGP and who use a carefully preserved alien-strength key may be reasonably certain that no one in the known universe can read his email, search warrant or no search warrant. Governments are aware of this and disapprove of it. Real privacy makes it far more difficult for them to spy on criminals of all colours, as well as on journalists and political adversaries. As a result, several countries impose restrictions on or outright ban the use of encryption. Prior to 1999, for instance, all forms of encryption were prohibited in France unless the government was provided the keys.

Questions for Revision

1. Why is the computer network so important?
2. Which is the shortest network covering network?
3. Which topology uses a single cable which connects all the including nodes?
4. What are the layers in OSI Reference Models?
5. What is analogue signal and digital signal in computer network?
6. What are the properties of data link layer?
7. Which is main function of transport layer?
8. What is the purpose of Domain Name System?
9. What is network management?
10. What is the purpose of the public key?

References books for Further Reading

1. McGraw Hill CompTIA Network+ Certification All-in-One Exam Guide Mike Meyers 7th edition
2. ′Reilly Network Programmability and Automation Jason Edelman, 1st edition
3. Computer Networking: A Top-Down Approach James Kurose 7th edition Pearson
4. "Data and Computer Communication" by William Stallings
5. "Data Communication and Networking" by Behrouz A Forouzan
6. "Computer Networks" by Andrew S Tanenbaum
7. "Internetworking with TCP/IP, Volume 1" by Douglas Comer
8. "TCP/IP Illustrated" by W Richard Stevens
9. "Computer Networks 5th Edition" by Tanenbaum