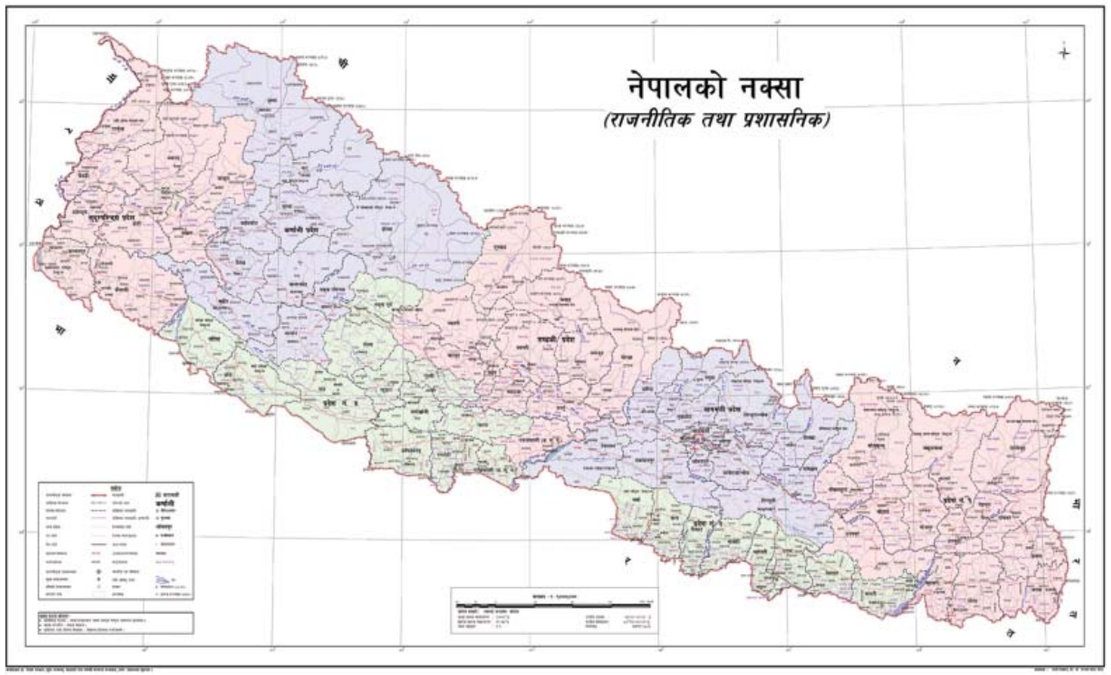


Computer Networks

Government of Nepal
Ministry of Education, Science and Technology
Curriculum Development Centre
Sanothimi, Bhaktapur
Phone : 5639122/6634373/6635046/6630088
Website : www.moecdc.gov.np

Feedback Copy

Technical and Vocational Stream
Learning Resource Material

Computer Networks
(Grade 10)

Secondary Level
Computer Engineering

Government of Nepal
Ministry of Education, Science and Technology
Curriculum Development Centre
Sanothimi, Bhaktapur

Publisher : Government of Nepal
Ministry of Education, Science and Technology
Curriculum Development Centre
Sanothimi, Bhaktapur

Layout by Khados Sunuwar

Preface

The curriculum and curricular materials have been developed and revised on a regular basis with the aim of making education objective-oriented, practical, relevant and job oriented. It is necessary to instill the feelings of nationalism, national integrity and democratic spirit in students and equip them with morality, discipline and self-reliance, creativity and thoughtfulness. It is essential to develop in them the linguistic and mathematical skills, knowledge of science, information and communication technology, environment, health and population and life skills. it is also necessary to bring in them the feeling of preserving and promoting arts and aesthetics, humanistic norms, values and ideals. It has become the need of the present time to make them aware of respect for ethnicity, gender, disabilities, languages, religions, cultures, regional diversity, human rights and social values so as to make them capable of playing the role of responsible citizens with applied technical and vocational knowledge and skills. This Learning Resource Material for Computer Engineering has been developed in line with the Secondary Level Computer Engineering Curriculum with an aim to facilitate the students in their study and learning on the subject by incorporating the recommendations and feedback obtained from various schools, workshops and seminars, interaction programs attended by teachers, students and parents.

In bringing out the learning resource material in this form, the contribution of the Director General of CDC Dr. Lekhnath Poudel, Pro, Dr. Subarna Shakya, Bibha Sthapit, Anil Barma, Bimal Thapa, Yogesh Parajuli, Bhuwan Panta, Asharam Suwal, Shankar Yadav is highly acknowledged. The book is written by Rajendra Rokaya and the subject matter of the book was edited by Badrinath Timalsina and Khilanath Dhamala. CDC extends sincere thanks to all those who have contributed in developing this book in this form.

This book is a supplimentary learning resource material for students and teachrs. In addition they have to make use of other relevnt materials to ensure all the learning outcomes set in the curriculum. The teachers, students and all other stakeholders are expected to make constructive comments and suggestions to make it a more useful learning resource material.

2076 BS

Ministry of Education, Science and Technology
Curriculum Development Centre

Table of Contents

UNIT-1

Introduction to Computer Network

Objectives:

At the end of this unit students will be able to:

- Define computer network and its components.
- Distinguish advantages and disadvantages of computer network.
- List the application fields of computer network.

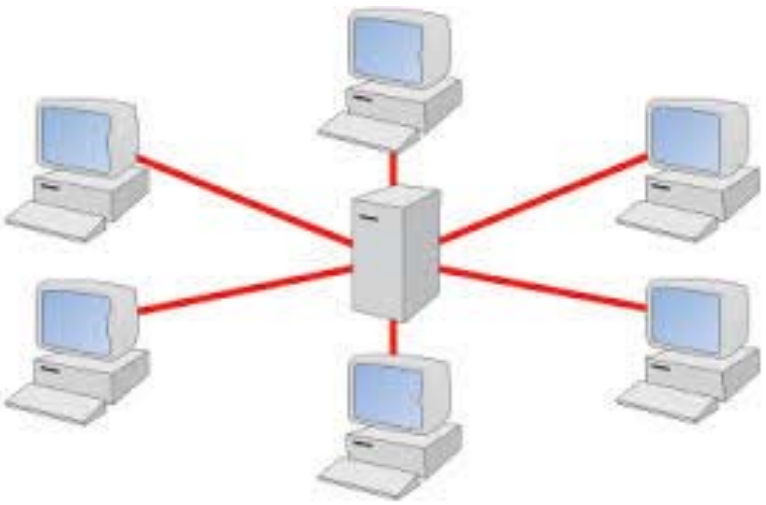
Learning Process and support material: Support Materials:

i. Two Computer systems or computing devices, any guided media or unguided media.

ii. **Learning Process:** The basic ideas about computer network i.e. what is computer network? why it is needed? and what are its basic component? are generated and delivered to the students by using above support materials.

Content's Elaboration

Computer Network



Computer networks have become integral part of our everyday lives. It's difficult to perform our simple daily routine tasks in the absence of computer network. We use them to take cash from the bank local ATM. Whenever we send mail or browse the web, we rely on the world's largest computer network, the Internet.

In simple term computer network is the interconnection between two or more computing devices for the purpose of resource sharing.

A group of computers and peripheral devices connected together by communication channel to enable users to share and exchange information.

Application of computer networks

A network is a collection or set of computing devices connected to one another to establish communication and also share available resources. A network will comprise of software and hardware devices. They help us to transfer data from one point to another within the network. Computer networks plays an important roles in the all of the area of human life. They have great impact on the activities and the work do. The development of computer networks have changed the way of work we do. Some of the applications of the computer network are mentioned below:

Business Applications

Most of the business organizations have large numbers of computers to do different types of works. In earlier days these computers were stand alone, isolated from others, but at some point, management may have decided to connect these computers to correlate information about entire company.

A business organization can easily share its resources with the help of computer network and make all programs, equipment and data available to anyone on the network without regard to the physical location of the resource and the user. A group of office workers can share the single printer. Along with the hardware resources such as printer, CD, scanner most of the business organizations can share data and information. Such information may include customer records, inventories, financial statements and others. So all small to large business organization needs computer network computer network for the remote access of data and information by stakeholders. Almost every business uses computers to complete daily tasks. From making contact with clients to input data for reports, computers allow businesses a more efficient way to manage affairs when compared to traditional paper and heap of files.

Apart from sharing the hardware and information the computer network provides strong communication medium among employee and customers. Most of the business personnel use the email for their communication. Computers give businesses access to email, instant messaging and custom customer contact systems. Computerized phone systems allow for automated support during off hours and a virtual operator can quickly direct callers to the correct department for faster support.

For promoting their business several business organization are keen in using the computer network. They advertise their products as well as their company using several ads in the internet.

The uses of computer network can be listed as

- Communication
- Marketing
- Budgeting and forecasting
- Storage
- Documents and Reports
- Education
- Research
- Data mining
- Customer relation

Home Application

In earlier days the use of computer at home was just for playing games, watching videos or word processing works. But due to the development of internet technology the use of computer at home has been rapidly changed. The probable main reason for having computer at home is for Internet access. Nowadays there are several computing devices in home along with the computer such as smartphones, smart TV, printers etc. people needs to connect these devices with each other for communicating and sharing information. Computer network provides helps them to communicate with each other. A home user can use computer network for

- Accessing the remote information: People can have access to the information on any subject either news, business, politics and many others by surfing the

internet. Educational and informative websites are available to download books, tutorials etc. to improve their knowledge and learn new things.

- Person to person communication: People can communicate with friends and family on the internet using different software like Skype etc. One can interact with friends over social media websites like Facebook, Twitter. They can also share photos and videos with friends. Video calls, group chat, group call are based on computer network which are the most modern ways of communicating among people.
- Interactive entertainment: People can find entertainment on the internet using computer. They can watch movies, hear songs and download different stuff. They can also watch live matches on internet.
- Electronic commerce: E-commerce or Electronic Commerce is the process of buying or selling goods online. Due to the busy life people don't get time to go for shopping, moreover that different online shopping sites provide varieties of goods and deliver to our doorsteps. It has make shopping easier. By sitting in the room, using their computer network people can buy their needed goods.

Mobile Application

Mobile application is one of the growing concern of the computer network. People are mostly using the mobile devices such as tablet, smart phones, PDAs (Personal Digital Assistants), notebooks for computing. Many of these people have desktop or laptop computer in their home still using these mobile devices because these devices are easier to use and can be carried with ease with the feature of wireless connection.

(Tanenbaum, 2003)

Basic Terms used in Computer Network:

Client: Those less powerful computers on which the user runs the applications are client. They have less processing speed and storage capacity in comparison to server computers and they further request to the server computers for information.

Server: The more powerful computers than client computers and responsible for providing services to those client computers are called server.

Node: Any active electronic device connected in a network that can receive, generate or forward any piece of information over network. E.g. Printer, switch, hub…etc.

Protocol: Set or rules followed by computers to communicate over the computer network.

Bandwidth: The amount of data transferred through the communication channel during fixed period of time is called bandwidth. It is also referred to the data holding capacity of computer network. It is measured in bps (bits per seconds) in digital devices and in cycles per second (hertz) in analog devices.

Communication Channel: Communication channel is the path or medium from which data is transmitted from source to destination. The communication channels can be classified as:

a) Bounded/Wired/Guided: The communication channel in which different types of wires are used to transfer data are wired medium. The communication devices are directly linked together by using cables or physical media for data transmission. Types of guided media: Twisted pair cable, Coaxial cable and Fiber optic cable.
b) Unbounded/Wireless/Unguided: The communication channel in which data are transmitted through waves instead of wire are called wireless medium. The signals are not bound in particular path or wire so they are called unbounded medium. Its types are Microwave, Satellite, Radio waves, infrared communication, and satellite communication.

Advantages and Disadvantages of Computer Network

Advantages:

- Provides convenient resource sharing
- Reduces the operational cost
- Provides hardware and software sharing facility
- It boosts storage capacity
- Ease data backup and recovery
- It enhance communication and information availability.

Disadvantage

- Computer network provides route for virus to spread.
- Initial setup cost is very high.
- Cybercrime may occur.
- Technical manpower in needed.

Key Points

- A computer network is a set of autonomous computers connected together for the purpose of sharing resources.
- Computer networks are used for business applications, home applications and mobile applications.
- Computer networks can share hardware such as printer, scanner, storage location etc.
- Software are also shared on the computer network.
- Server computer are the powerful computers which provides services to the client computers.
- Client computer are less powerful computer on which user run applications.
- Protocols are the set of rules that define the communication between two or more devices over a network.

Students' Assessment

Answer the following questions

Very Short-Answer Questions

a) Name any one application of computer network.
b) On which computer does user run applications?
c) Write a peripheral device that is connected to a computer in your lab.
d) Does computer network share software only?

Short-Answer Questions

a) Define protocol. Give some examples.
b) What is bandwidth?
c) How the bandwidth is measured in analog and digital devices?
d) List the types of communication channel?

Long Answer Questions

1) What is computer network?
2) List any five advantages and disadvantages of computer network?
3) Explain the application fields of computer network.
4) What are the components of computer network? Illustrate them.
5) How server differs from client computers? Explain.

Glossary

- Ads: Advertisement
- ATM: Automated Teller Machine
- Autonomous: Independent, Self- Sufficient
- CD: Compact Disk
- Correlate: Connect, Link
- Integral: Essential
- Probable: Possible
- Virtual: Simulated/ Not Real

Reference

Computer Network

- https://www.techopedia.com/definition/25597/computer-network
- Concept Draw Pro 11: http://www.conceptdraw.com/How-To-Guide/metropolitan-area-networks
- http://ecomputernotes.com/computernetworkingnotes/computer-network/what-is-a-computer-network
- https://www.techopedia.com/definition/5537/network
- http://vfu.bg/en/e-Learning/Computer-Networks--Networking.pdf

UNIT-2

Types of Networks

Objectives:

At the end of this unit students will be able to:

- Arrange the different type's network on the basis of size.
- Explain the types of networks.
- Compare and contrast different types of computer network.
- Sketch the figures of LAN, MAN and WAN.
- Explain the characteristics of different types of network.

Learning Process and support material:

- **Support Materials:** At least two computer systems or computing devices, network devices (router or switch) guided media (straight or cross cables), Unguided media (Bluetooth, microwave).
- **Learning Process:** The concept of networks on the basis of geographical region i.e. LAN, MAN, WAN is explained and made well realized to student by displaying above support materials.

Content's Elaboration:

There are several types of computer networks. The classification of computer networks is done on the basis of the geographical location and the numbers of computer they have i.e. their size. The categories of computer network are:

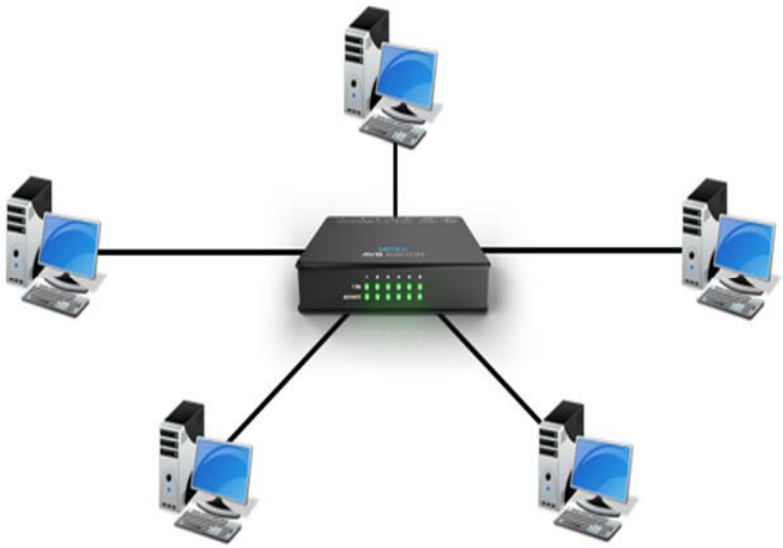
a) Local Area Network (LAN)
b) Metropolitan Area Network(MAN)
c) Wide Area Network (WAN)
d) Wireless Network
e) Home networks
f) Internetworks

Local Area Network (LAN)

LAN is the computer network which relatively occupies small geographical area such as a single room or a building. The numbers of computers in LAN may vary from just two or three computers to hundreds of different kinds of computers. Computers in LAN are nearer to each other and are connected in a way that enables them to communicate by cables or wireless devices.

Along with the limited space or area, LANs are also typically owned, managed, controlled by the single organization or person. Networking done in computer lab is example of LAN.

Features of LAN



- It covers limited geographical area.
- It offers bandwidth of 10 to 100 Mbps (Megabits per second)
- It is owned and controlled by single organization.

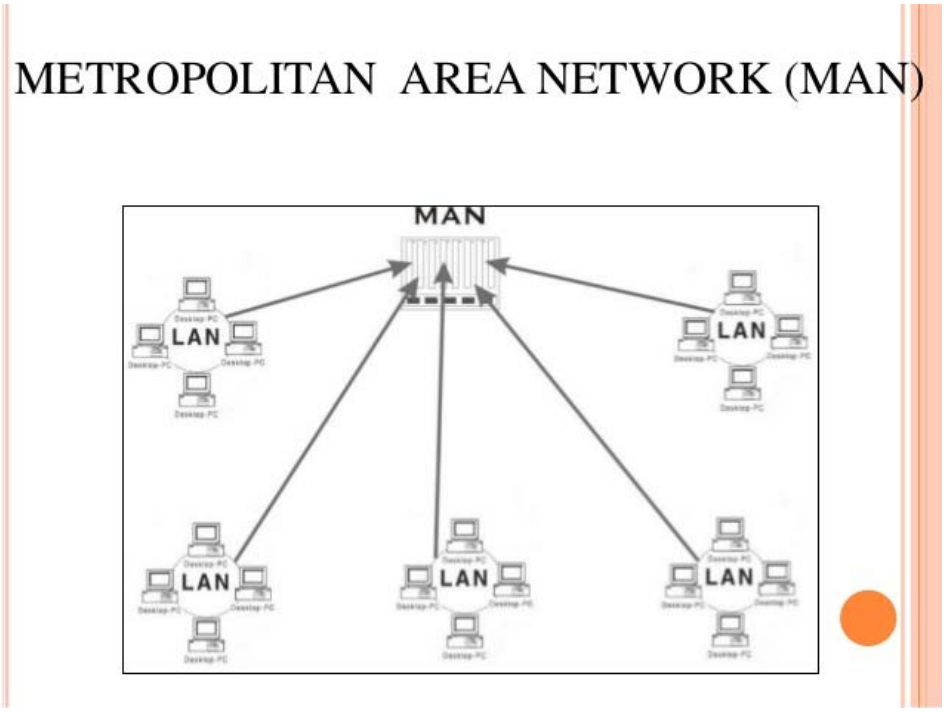
Advantages of LAN

- It has higher bandwidth.
- Low cost
- Easy configuration
- Easy to manage

Disadvantages of LAN

- It covers small geographical region.
- Limitation in exchanging information.
- Difficult to set up the network.

Metropolitan Area Network(MAN): The computer network which is speeded over the metropolitan area or city is called metropolitan area network. It is the medium sized network larger than LAN and smaller than WAN. Several LANs are connected together to form a MAN using different wires or wireless technologies. A MAN is typically owned and operated by a single entity such as a government body or large cooperation.



Features of MAN

- It covers larger geographical area than LAN.
- The number of computers connected are also more than LAN.
- Multiple LANs are connected to form a MAN
- It is owned by single or multiple organizations.

Advantages of MAN

- It covers wider area than LAN.
- MAN requires fewer resources in comparison to WAN.
- Higher security.
- Increases the efficiency of handling data.

Disadvantages of MAN

- The large the network becomes difficult to manage.
- Difficult to make system secure from hackers.

Wide Area Network(WAN): The computer network which is spreads all over the world connecting hundreds thousands of computers. It is the largest network in the world where several LANs and MANs are connected through satellite links or microwave system. This network connects two or more computers generally across a wide geographical area such as cities, districts and countries. Internet is the example of WAN.

Features of WAN:

- It is not restricted to a geographical locating; it is spreads all over the world.
- Satellites links and microwave system is used for connectivity.
- The technology is high speed and expensive.
- Data transmission is slower in comparison to LANs.

Advantages of WAN:

- It covers large geographical area.
- Ease update to the data and information.
- Scope of activities are not limited.

Disadvantages of WAN:

- The cost is higher.
- More associated errors occurs.
- Need to invest on good firewall system.

- High security challenges from hackers.

Wireless Networks: A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networks are the alternative of traditional wired networks that relies on cables to connect the device with each other. The network where the digital devices are connected together without wires through wireless technology such as Wi-Fi is called wireless network. Several wireless networks are Wi-Fi, Bluetooth, 3G,4G networks, wireless hotspots.

Features of wireless networks

- Easy to use around the wireless networks.
- It increases the mobility.
- Public hotspots can be created.
- It saves time setting up wired Ethernet hook up and cost.
- It provides convenience.

Home Networks: A home network or Home Area Network (HAN) is the computer network that connects devices with in the vicinity of a home. It is also a type of LAN. A home network is a group of devices such as computers, game systems, printers and mobile devices that connect to the internet and each other.

Features of Home Networks

- Devices such as CD-ROMs, printers, mobile devices and can be connected.
- Contents can be easily shared.
- Files and documents can be shared
- Stereos, TVs and game system can be shared.

Internetworks: Internetworking is the practice of connecting a computer network with other networks through the use of gateways that provide a common method of routing information packets between the networks. It is the process of connecting different networks using devices such as routers, gateway etc. Internet is the example of internetwork. The internetworks can be classified as:

Intranet: An intranet is a private network owned by single organization and accessed to that organization's staffs. It is based on internet concept and use TCP/IP, HTTP protocol but accessed to limited people only. The main purpose of an intranet is to share company information and computing resources among employees. An intranet can also be used to facilitate working in groups and for teleconferences.

Extranet: An extranet is a private network that uses Internet technology and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An

extranet can be viewed as part of a company's internet that is extended to users outside the company.

Internet: It is the largest global computer network that connects billions of computers around the world. It is also called network of networks.

Features of Interworks:

- Two or more different networks are connected.
- Data communication is ensured among networks owned by different entity.
- Devices such as router, gateway having capability to connect different networks are needed for internetworking.

KEY POINTS

- LAN is the smallest form of network.
- MAN is larger than LAN and smaller than WAN.
- WAN is the largest computer network.
- Several homely used devices can be connected in home network.
- Router, gateway devices are needed to connect internetworks.

Students' Assessment:

Answer the following questions:

A. Very Short-Answer Questions.

a) What does LAN stand for?
b) What does MAN stand for?
c) What does WAN stand for?
d) Name the largest computer network?
e) Which computer network is limited with in the room?

B. Short-Answer Questions:

a) Arrange the computer networks on the basis of their size.
b) Define LAN with its characteristics.
c) What is MAN? Mention any 3 characteristics.
d) What is internetworks?

e) What is home networks?

C. Long Answer-Questions:

a) Compare and contrast between LAN and MAN?
b) Explain the LAN, MAN and WAN with figures.
c) Mention the characteristics of all types of networks.

Glossary

- Bandwidth: number bits transferred through channel over period of time.
- Convenience: easy/ suitable
- Restricted: limited/ constrained
- Stereos: sound systems, CD players.
- Vicinity: locality, area, neighborhood

Reference

- https://www.lifewire.com/lans-wans-and-other-area-networks-817376 By Bradely Mitchell
- www.webopedia.com
- Computer Operator Google
- https://www.webopedia.com/TERM/L/local_area_network_LAN.html
- http://vfu.bg/en/e-Learning/Computer-Networks--Networking.pdf
- http://www.eazynotes.com/notes/computer-networks/slides/types-of-networks.pdf

UNIT-3

Network Topologies

Objectives:

At the end of the lesson students will be able to:

- Define network topology with types.
- Compare peer to peer and client server topologies.
- Say the advantages and disadvantages of each topology.
- Sketch the architecture of network topologies

Learning Process and Support Materials:

a) Support Materials: At least two or more computing devices, Network devices (switch/hub) Guided media (straight or cross cables).
b) Learning Process: The physical and logical arrangements of network is elaborated by showing above support materials.

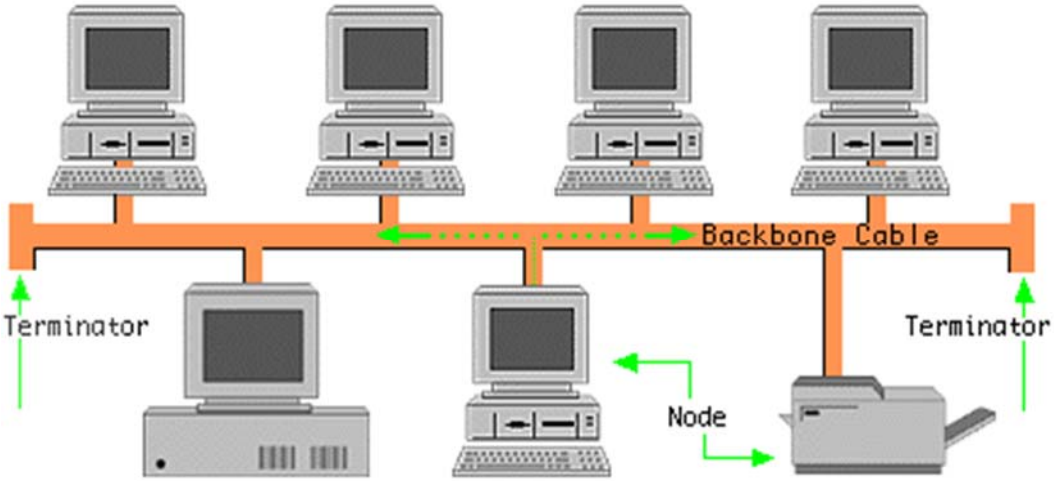
Content's Elaboration:

Each device connected in the computer is called node. And the physical arrangement or the connection pattern of each device connected in the network is called network topology. It also refers to the cabling structure or geographical structure of the LAN. The basic network topologies are:

a) Bus or linear topology
b) Star topology
c) Ring topology

Bus or linear topology: It is the simplest of all network topology where all computers are arranged in linear format. In this topology all nodes of network are connected to the single cable by the help of connectors. The cable is backbone of the network and called bus. Data are transmitted on network through bus using the address of destination computers. The bus contains the terminator in each end and these terminator are responsible for stopping the flow of data out of the bus. This topology

has maximum chance of data collision and if the backbone cable breaks then whole network gets jammed.



Features of Bus Topology:

- Data is transmitted in single direction.
- Every device is connected to a single cable.

Advantages of linear bus topology:

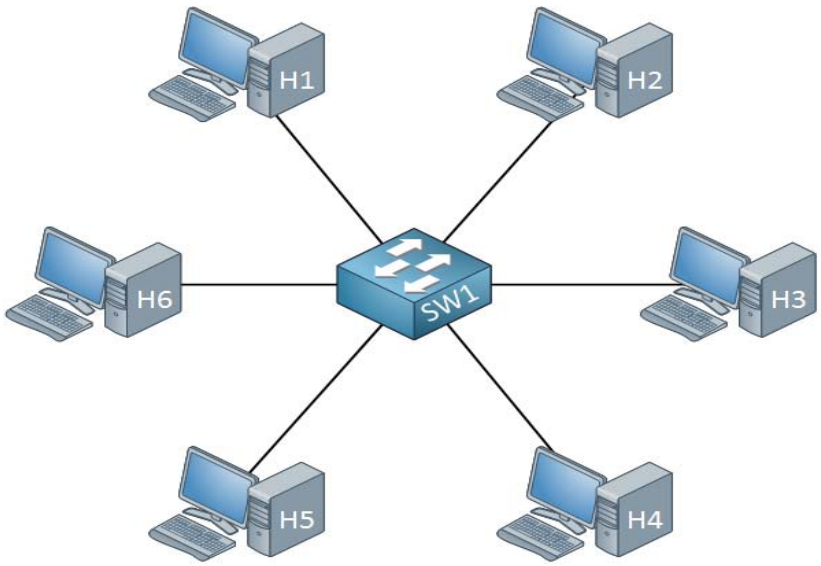
- It is easier to set up and extend.
- It requires fewer cables, so it is cheaper.
- New nodes can be easily added.
- It is mostly used in small networks

Disadvantages of linear bus technology

- Whole network stops functioning if backbone cable is damaged.
- Network slows down if additional computers or nodes are added.
- There is maximum chance of data collision.
- Cable has limited length.
- It is difficult to detect and troubleshoot the errors.

Star Topology: This is the most commonly used and popular network topology. In star topology all nodes or computers are connected through a central device called hub or switch. This is the most popular topology to connect nodes in the LAN. All

devices are connected indirectly with each other with the help of hub or switch. If a device needs to communicate with another it needs to pass form the switch or hub before reaching to destination. Hub acts as a junction to connect different nodes, manages and controls entire network. Unshielded Twisted Pair (UTP), Ethernet cable is used to connect nodes to hub in star topology. If the central server or hub fails the whole network stops functioning but failure of single computer don't affect the whole network.



Features of Star Topology:

- Every node has its own connection to the hub.
- Hub acts as a repeater for data flow.
- Can be used with twisted pair, coaxial or fiber optical cable.

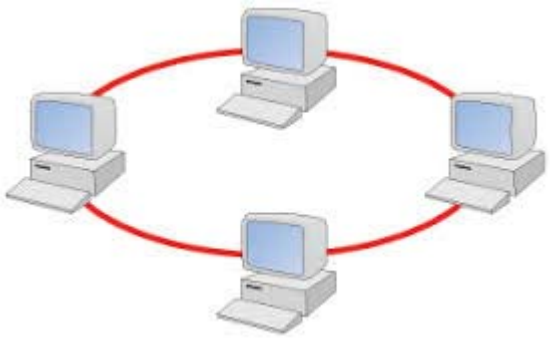
Advantages of star topology:

- It is easy to setup and configure.
- It provides better performance than bus topology.
- Easy to add and remove new nodes.
- Centralized management helps in monitoring the network.
- Failure of a single node doesn't affect functioning of the network.
- It is easy to detect the errors in this topology.

Disadvantages of star topology:

- It requires more cables in comparison to bus so, it is costlier.
- Failure of central switch/hub breaks down the whole network.
- Capacity of central device determine the numbers of nodes and performance of star topology.

Ring Topology: In ring topology all nodes are connected to each other in the shape of circle without the end point forming a closed circular loop. In this topology one computer is connected to other and so on to form a ring pattern. Each computer has two neighbors either side of it. There is no central controller in this type of topology and data are from one computer to another in circle passing through each computer on the network until destination computer is met.



The TOKEN passing method is used to pass data from one computer to another in ring topology. Source computer generates the token containing data and destination address. Then the token is passed to the next node, which checks if the data is for it or not. If yes, it receives the data otherwise it passes the token to next node, the process continues until the destination computer is met.

Advantages of ring topology:

- Ring topology is easy to set up and configure.
- Each computer get equal opportunity to access the network resources.
- This topology helps to reduce chances of data collision.

Disadvantages of ring topology:

- Data packet needs to pass through all nodes between source and destination.
- If one node or port goes down, the entire network gets affected.
- It is difficult to detect errors in this type of network.
- Adding or removing the devices affects the entire network.

Key Points

- Cabling structure of LAN is called network topology.
- Bus, Star and Ring are the three main network topologies.
- All nodes are connected through central cable called bus in bus topology.
- Star topology use hub or switch to connect nodes.
- All nodes are connected in circular loop in ring topology.
- Token passing is done in ring topology to send data.

Students' Assessment

Answer the following questions

A. Very Short-Answer Questions

a) How many types of network topologies are there?
b) In which topology token passing is done?
c) Name the topology where hub or switch is used?
d) Which topology has infinite loop?
e) What is the name of backbone in bus topology?
f) In which topology a node have two adjacent nodes?

B. Short Answers:

a) What is network topology? List its types.
b) Sketch the figure of star topology.
c) Write advantages and disadvantages of BUS topology?
d) Write advantages and disadvantages of token ring topology?

C. Long Answer-Questions:

a) What is star topology? Write its advantages and disadvantages.
b) Compare and contrast between star and ring topology?
c) Explain bus topology with figure.
d) Define Ring topology with figure.
e) How data is transmitted in it?

Glossary

Collision: crash

Detect: find, identify

Errors: bugs, mistakes

Linear: line

Troubleshoot:

Reference

https://www.webopedia.com/quick_ref/topologies.asp

https://www.techopedia.com/definition/5538/network-topology

http://www.eazynotes.com/notes/computer-networks/slides/network-topologies-handouts.pdf

https://www.studytonight.com/computer-networks/network-topology-types.php

CHAPTER 4
IP Address

Objectives:

At the end of the lesson students will be able to:

- Define IP Address.
- Classify the different classes of IPv4.
- Define IPV4 and IPV6.
- State the key features of IPv4 and IPv6
- Differentiate between IPV4 and IPV6.

Learning Process and support materials:

Support Materials: Network device (router), computing device (Smart phone).

Learning Process: How any host is connected with client with internet is explained by using above support materials.

Content's Elaboration:

An IP (Internet Protocol) address is a logical numeric address that is assigned to every single node in a TCP/IP based network. It is a unique identifier of a node connected in TCP/IP network. The networks using TCP/IP protocol routes messages based on the IP address of the destination. Generally a node have static or dynamic IP address. Static refers to the IP address which remains permanent and a dynamic IP address is a temporary address that is assigned each time a computer or device accessed the internet.

IP (Internet Protocol) address is a numerical identification assigned to each of the computers in a network. Although the actual IP address is stored in binary (0,1) form, they are normally seen as "human-readable" numeric form.

There are two types of IP addresses: IPv4 and IPv6. An IPv4 address, for example, 192.168.1.153, has 4 octets separated by decimals. Which represents 8 bits (in binary) of the address. The first octet represents the network address and the last

three octets are to identify the host. Each of the octets can take any number from 0 to 255 as that is the largest number possible in an 8-bit binary. This limits the number of unique possible combinations of IPv4 addresses to 232.

IPv6 on the other hand uses hexadecimal system where each address is assigned a space of 16 bytes unlike 4 bytes in IPv4. This increases the number of possibilities to 2128 or 3.408 X 1038, the number which looks vast enough to accommodate the need of all networks in the foreseeable future. A typical IPv6 address looks like this: 2001:0db8:85a3:08d3:1319:8a2e:0370:7334.

IPV4: IPV4 stands for Internet Protocol Version 4. It is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. It provides the logical connection between network devices by providing identification for each device. IPv4 uses 32-bit addresses for Ethernet *communication in five classes: A, B, C, D and E. Classes A, B and C have a different bit length for addressing the network host. Class D addresses are reserved for multicasting, while class E addresses are reserved for future use.

Whenever a device access the Internet (whether it's a PC, Mac, smartphone or other device), it is assigned a unique, numerical IP address such as 192.168.1.1 To send data from one computer to another through the web, a data packet must be transferred across the network containing the IP addresses of both devices.

Without IP addresses, computers would not be able to communicate and send data to each other. It's essential to the infrastructure of the web.

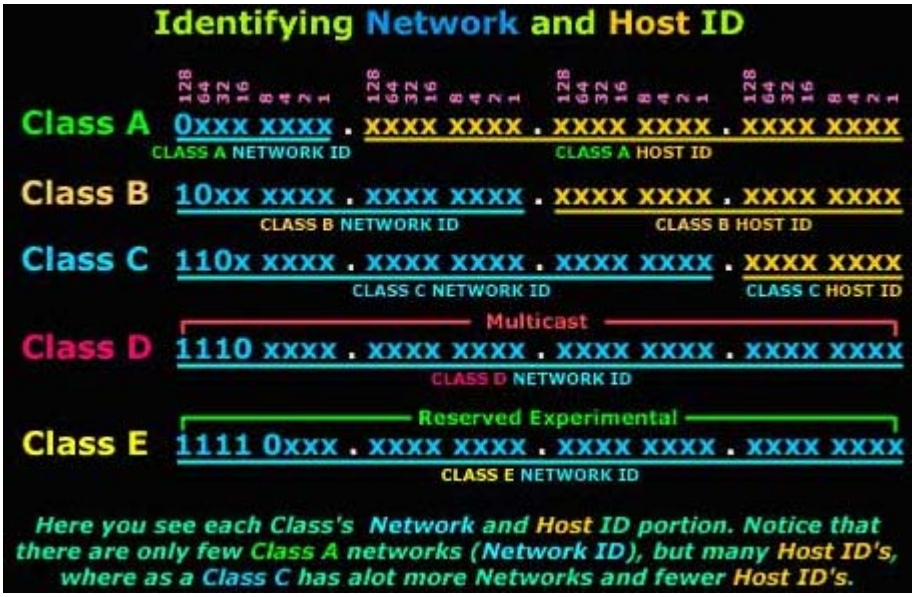
Key Features:

- The packet sizes are limited to 64KB.
- The address size of IP is limited to 32 bit addressing.
- The IP header includes checksum.
- IPsec support is optional.
- It doesn’t supports multicasting.

Classes of IPv4

A simple IP address is a lot more than just a number. It tells about the network of workstation along with the node ID. When the IEEE committee divide five different ranges IPv4, as we call them, "classes" of IP addresses. When someone applies for IP addresses they are given a certain range within a specific class depending on the size of their network. The class A IP address were designed for large networks, class B for medium sized networks and class C for smaller networks. Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. IPv4 is broadly classified into 5 classes of IP address as:

- Class A: 1.0.0.0 to 127.255.255.255
- Class B: 128.0.0.0 to 191.255.255.255
- Class C: 192.0.0.0 To 223.255.255.255
- Class D: 224.0.0.0 to 239.255.255.255
- Class E: 240.0.0.0 to 255.255.255.255

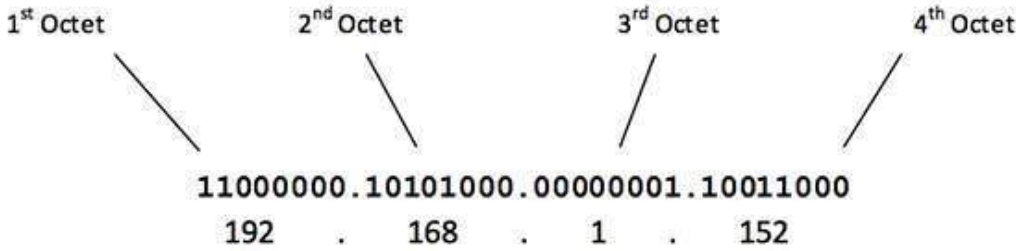


In the above list, there are five classes. The first class is A and last is E. The first three classes (A, B and C) are used to identify nodes such as workstations, routers,

switches and other devices, whereas the last two classes (D and E) are reserved for special use.

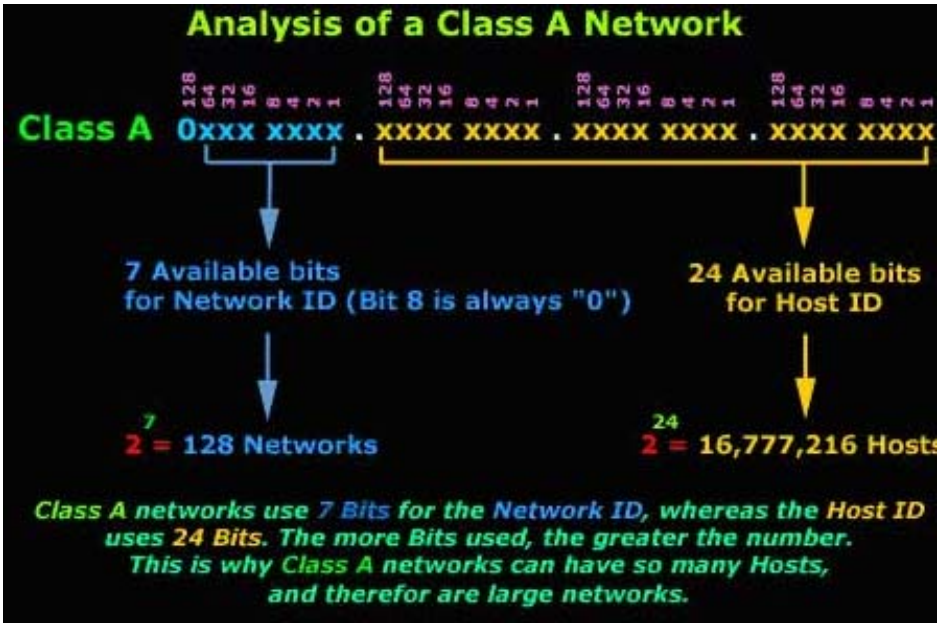
An IP address consists of 32 Bits, which means its four bytes long. The first octet i.e. first byte of an IP address is enough for us to determine the class to which it belongs. For example, if first octet of an IP address is 169 then from above list we can say that it falls within the range 128-191 i.e. it is B class IP address.

IPv4 contains 4 octet separated by dots (.). The first octet is left most and so on as shown below.



The classes of the network are assigned on the basis of the size of network of any organization. For instance, if a company required 1000 IP address, it would probably assigned a range that falls within a class B network rather than A or C. The different classes of IPv4 are discussed below:

Class A:



The Class A network have largest numbers of host in it and used by larger organizations. Class A network has total 7 bits for the network ID (8th bit is always set to 0) and 24 bits for the Host ID i.e. the first bit of the first octet is always set to 0 (zero). Thus the first octet ranges form 1-27 i.e. 00000001-01111111 (1-127). Class A addresses only include IP starting form 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reversed for loopback IP address. Class A addressing can have 126 networks (27-2) and 16777214 hosts (224-2). This is why when the valid hosts are to be calculated subtract 2. So the valid hosts on class A networks are 16777216-2=16777214. The default subnet mask for class A IP address is 255.0.0.0.

Thus Class A addressing format is as:

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B: An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 – 10111111
128 – 191

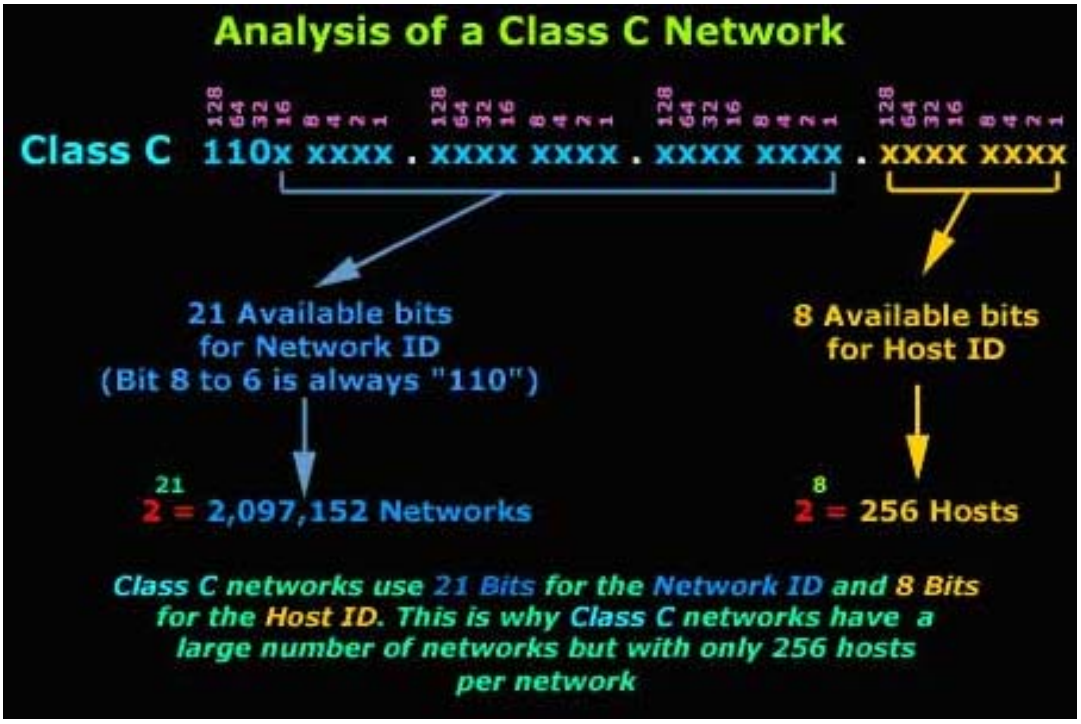
These networks have 14 bit for the network ID (bit 15 and 16 are set and can't be changed) and 16 bits for host ID i.e. there are 214=16384 network address and 216=65536 hosts address in each network among 65536 two because one is the network address and other is broadcast address of class B network has 216 -2 = 35534 valid hosts. The default subnet mask for class B IP address is 255.255.x.x

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. and its IP address format is:

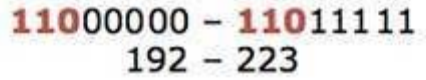
10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

Where N=Network ID and H= Host ID

Class C:



The first octet or class C IP address has its first 3 bits set to 110 and cannot be changed, that is:



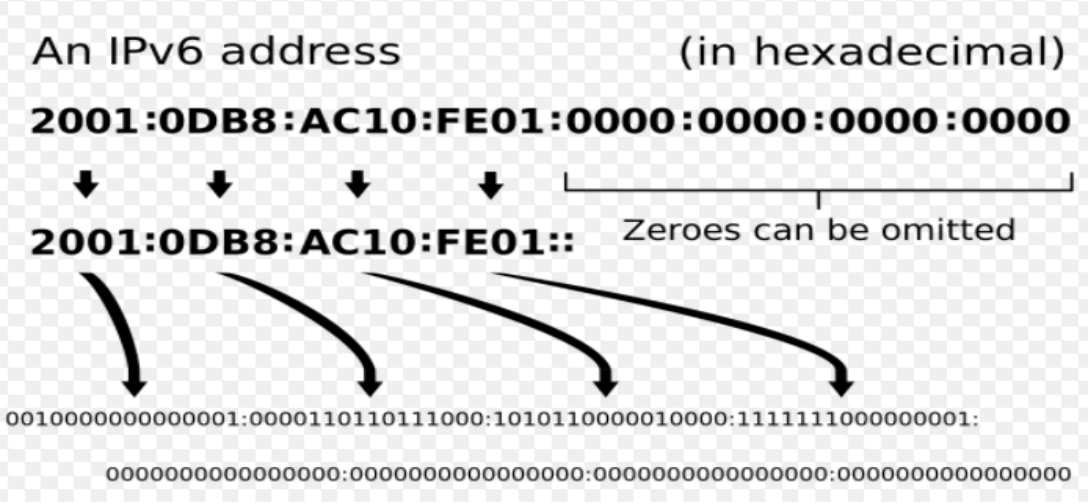
The class C networks have 21 bits for network ID and bits (22,23 and 24 are set and can't be changed) and eight bits for the host ID. This means there can be 221=2,097,152 networks and 28=256 hosts in each network. Among 256 two cannot be used because one is network address and another is network broadcast address so there are 28-2=254 valid hosts in class C networks. The default subnet mask for class C is 255.255.255.x. Its IP address format is:

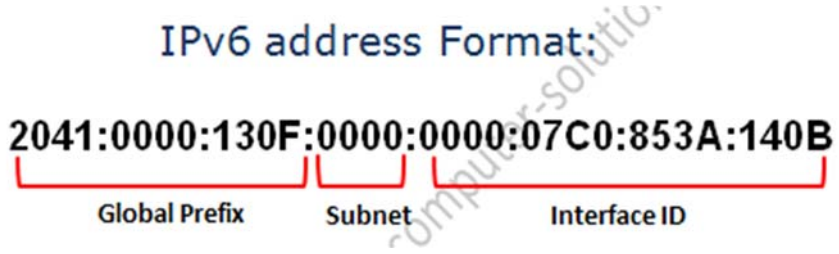
110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

Class D: The Class D IP addresses range from 224.0.0.0 to 239.255.255.255. It is reserved for multicasting. In multicasting data is not destined for a particular host, that is why there is no need to determine the host address. It doesn't have any subnet mask.

Class E: The Class E IP addresses range from240.0.0.0 to 255.255.255.254 and this class IP is reserved for experimental purpose only. This class also don't need subnet mask.

IPV6: IPv6 is short for "Internet Protocol Version 6". IPv6 is the Internet's next-generation protocol, designed to replace the current Internet Protocol, IP Version 4. It is also known as Internet Protocol Next Generation (IPng). IPv6 is the enhanced version of IPv4 and can support very large numbers of nodes as compared to IPv4. The most obvious improvement in IPv6 over IPv4 is that IP addresses are lengthened from 32 bits to 128 bits. This extension anticipates considerable future growth of the Internet and provides relief for what was perceived as a forthcoming shortage of network addresses. The 128 bits IP address is separated in 8 groups of four hexadecimal digits, each group contains 16 bits or 2 octet. And these groups are separated by colons as given below.





Key Features:

- It supports 128 bit long source and destination addresses.
- It has larger address space
- It provides faster routing.
- IPv6 provides Auto configuration feature.
- No more private address collisions.
- The header format is simpler.
- More security for applications and networks.

Difference between IPv4 and IPv6

IPv4	IPv6
Source and destination address are of 32 bits (4 bytes) long.	Source and destination address are of 128 bits (16 bytes) long.
Broadcast address are used to send traffic to all nodes.	Multicast scoped addresses are used.
IP header includes checksum	IP header doesn't include checksum
IPv4 uses octal system separated by decimal to represent IP address.	IPv6 uses hexadecimal system separated by colons to represent IP address.
Chances of private address collision	No chances of private address collision

Sub netting: "Subnetting" is dividing a default address space into separate networks. Sub netting enables the network administrator to further divide the host part of the address into two or more subnets. In this case, a part of the host address is reserved to identify the particular subnet. An IP address includes a network ID and a host ID. Subnets are designed by accepting bits from the IP address's host part and using these bits to assign a number of smaller sub-networks inside the original network.

Sub netting allows an organization to add sub-networks without the need to acquire a new network number via the Internet service provider (ISP).

Sub netting helps to reduce the network traffic and conceals network complexity. Sub netting is essential when a single network number has to be allocated over numerous segments of a local area network (LAN).

Key Points

- IPv4 address classes can be listed as:
- IP address is a unique numeric address assigned to each node in network.
- IPv4 is the fourth version of Internet Protocol which uses 4 octet separated by dots (.).
- Those each octet contains 8 bits so IPv4 address length is 32bits.
- IPv6 is also called Internet Protocol Next Generation (IPng).
- It uses 128 bit hexadecimal system for addressing unlike 32 bit octet addressing of IPv4.
- An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets, a group sometimes also called a hextet).
- Sub net divide default address space into several sub networks.
- Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets).

Ipv4 Address Classes

Class	Theoretical Address Range	Binary Start	Used for
A	0.0.0.0 to 127.255.255.255	0	Very large networks
B	128.0.0.0 to 191.255.255.255	10	Medium networks
C	192.0.0.0 to 223.255.255.255	110	Small networks
D	224.0.0.0 to 239.255.255.255	1110	Multicast
E	240.0.0.0 to 247.255.255.255	1111	Experimental

Students' Assessment

Answer the following questions

A. Very short answer Questions

a) How many classes of IPv4 are there?

b) List the names of IPv4 classes.

c) How many bits does IPv4 contains?

d) In which number system does IPv6 represented?
e) Is octal system used in IPv4?
f) Which IP class has largest numbers of hosts?
g) Which IP class 254 hosts per network?
h) What is the full form of IPv4 and IPv6?
i) Which IP is called IPng?
j) How many bits does IPv6 have?
k) Which class is reserved for multicasting?
l) What is the range of class A address?

Short Answer-Questions:

a) What an IP address?
b) Define static and dynamic IP?
c) Define subnetting?
d) List the characteristics of IPv4.
e) List the characteristics of IPv6.

Long Answer Questions

a) Explain the different classes of IPv4.
b) Differentiate between IPv4 and IPv6.
c) Write short notes on each classes of IPv4.

Glossary:

- Unique: Distinctive, single
- Static: stable, unchangeable
- Dynamic: unstable, changeable
- Octet: Combination of 8 bits.
- Forthcoming: upcoming
- Anticipate: Antedate, Do in advance

Reference:

https://www.techopedia.com/definition/5367/internet-protocol-version-4-ipv4

- https://www.webopedia.com/DidYouKnow/Internet/ipv6_ipv4_difference.html
- https://www.techopedia.com/definition/5367/internet-protocol-version-4-ipv4
- https://www.tutorialspoint.com/ipv4/ipv4_address_classes.htm
- http://whatis.techtarget.com/definition/IPv4-address-class

CHAPTER 5

Network architecture and Devices

Objectives:

At the end of the lesson students will be able to:

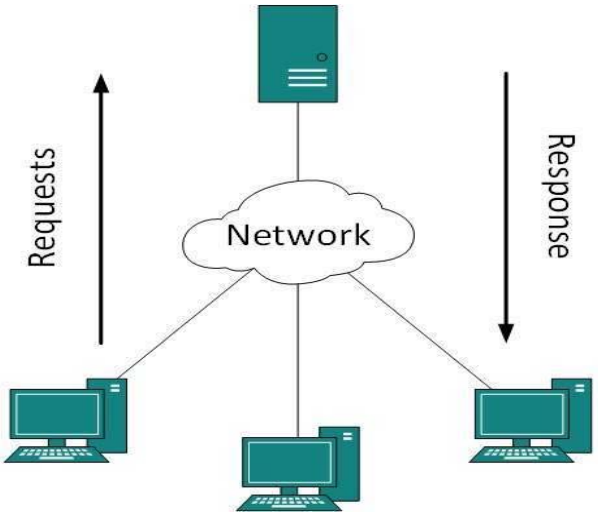
- Define network architecture.
- Describe client server and peer to peer network architecture.
- Sketch the types of network architecture.
- Say the advantages and disadvantages of client server and peer to peer architecture.
- Differentiate between client server and peer to peer architecture.
- Describe different hardware component used in networking.

Learning Process and support materials:

a) Support materials: At least two computer system or computing devices, repeater, hub, NIC, bridge, switch, router.

b) Learning Process: How any host is connected with client with internet is explained by using above support materials.

Content Elaboration:



Network architecture describes how network is organized and the computers on the network interact and communicate with each other. The major types of network architecture are: Client server and peer to peer

Client server network architecture: The client server network architecture consists at least one server and one or more client computers

connected in the network. The server is a powerful computer with high processing, large memory and storage responsible for providing services to the workstation connected to the network. It provides easier network administration with secure and manageable access to the company data.

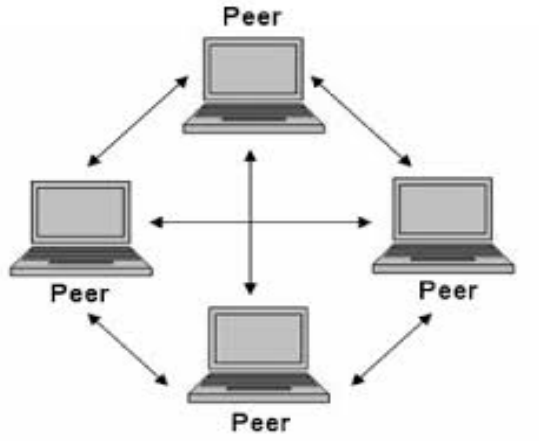
Advantages

- It covers larger geographical area.
- Its cabling structure may vary from simplex to complicated one.
- The network traffic is reduced in client server mode.
- The security management is centralized to the server.
- Backup of data is centralized.

Disadvantages:

- Too many requests from the client may hang/breakdown the server.
- In this system if the server fails the whole network goes down.
- Initial setup of client server model is expensive.
- Professional technical IT person are needed to maintain the servers and other technical detail of networks.

Peer to peer network architecture: The peer to peer network architecture consists of several computers connected together which functions both as server and client. In this architecture each computers has equal roles, responsibility, privileges and capabilities. Here the need of central server is removed and each computers interact and share resources. This model is best fitted for small offices and home usages where data and other securities are not of big concern.



This architecture is suitable for the networking environment where all nodes has the same capabilities and responsibilities.

Advantages:

- All resources are easily shared by all client computers.
- It is easy to install and configure.
- It's more reliable because central dependency is reduced.
- Failure of one client doesn't affect he network.
- Overall building and maintenance of this type of network is less than client server.
- No need of full time system administrator because each peer can control their resources.

Disadvantages:

- As whole system is decentralized, it is difficult to administrate.
- The network architecture is less secure.
- Data recovery and backup is very difficult since each client need its own backup.

Components of Computer Network

Hardware: Mechanical parts used in the computer network refers to the hardware components which are listed below:

- Computer: A well-functioning set of computer is a main element of the network. There may be just two or hundreds of computer connected in a single network.

- Hub: The networking device used to connect the multiple computers in LAN. It broadcasts the information to all the ports and send to all connected computers because it can't identify the destination computers.
- Switch: An intelligent device that joins multiple computers together in the local area network (LAN) is switch. Unlike hub hey identify the destination computer and forward the information to destination computer only.

- Network Interface Card (NIC): It is the Ethernet card or Network adapter that enables a computer to connect to a network.

Repeater: The signals transmitted become weak when they need to travel longer distance. Repeater is a device that increases the length of network by amplifying the weak signals. It receives the weak signals, regenerates them and send them to the destination. So, it enables signals transfer the longer distance.

Bridge: The networking device used to connect two similar types of network is known as Bridge. It is used to connect two LANs or different segments of the same network.

Router: It is the device connecting two different networks having similar protocols. Along with this it is used to determine the best path for sending the data packets from source to destination. That means, routers are responsible for traffic management in computer network.

Gateway: Gateway are hardware or software responsible for connecting two different networks having dissimilar protocols. They make communication possible between different architecture and environment. They repackage and convert data going from one environment to another so that each environment can understand the other environment's data.

Software:

Network Operating System (NOS): The collection of program responsible for managing all the hardware and software resources in computer network is called network operating system Eg. Linux, Windows server 2012.

Protocols: Set or rules followed by computers to communicate over the computer network.

Key Points:

- Network architecture describes how the computer on the network interact and communicate.
- The client server network architecture consists at least one server and one or more client computers connected in the network.
- In peer to peer architecture each computers has equal roles and responsibility.
- Hub is a device which connects nodes in LAN and broadcast message to all connected nodes.
- Switch is intelligent hub which sends message to destination node only instead of broadcasting to all nodes.
- Router is a device which determines best path for forwarding data packets.
- Router is also responsible for connecting two different networks having similar protocols.
- Gateway is the device which connects networks having dissimilar protocols.

Students' Assessment

Answer the following questions

A. Very short answers Questions

a) Name the device used to connect different segments of same network.
b) How many types of network architecture are there?
c) List the types of network architecture?
d) Which device is used to connect nodes in the LAN?
e) Name the networking device used to connect networks having different architecture and environment.
f) Which architecture is more secure client server or peer to peer?

B. Short Answers Questions:

a) Define network architecture?
b) Sketch and describe the peer to peer network architecture.

c) List the advantages and disadvantages of peer to peer network architecture.

C. Long Question Answers:

a) Explain the advantages and disadvantages of client server architecture.
b) Differentiate between client server and peer to peer network architecture.
c) Draw the diagram of client server network architecture and explain in detail.
d) Write short notes on:
    i. Hub
    ii. Switch
    iii. Router
    iv. Gateway
    v. Bridge
    vi. Repeater

Glossary:

- Consist: contain
- Expensive: costly
- Dissimilar: different

Reference:

http://ccm.net/faq/2761-what-is-network-architecture
https://www.techopedia.com/definition/454/peer-to-peer-architecture-p2p-architecture
https://www.webopedia.com/TERM/C/client_server_architecture.html
https://www.britannica.com/technology/client-server-architecture

CHAPTER 6

Introduction to OSI reference model

Objectives:

At the end of this unit students will be able to:

- Define OSI reference model.
- List the different layers of OSI reference model.
- Explain the function of each layers of OSI model.

Learning Process and support materials:

a) Support Materials: At least two computing devices (smart phones), sender and receivers, browsers.
b) Learning Process: How data is transmitted from one computing device to another is explained using devices.

Content Elaboration:

The Open Systems Interconnection (OSI) Model is a conceptual and logical layout that defines network communication used by systems open to interconnection and communication with other systems.

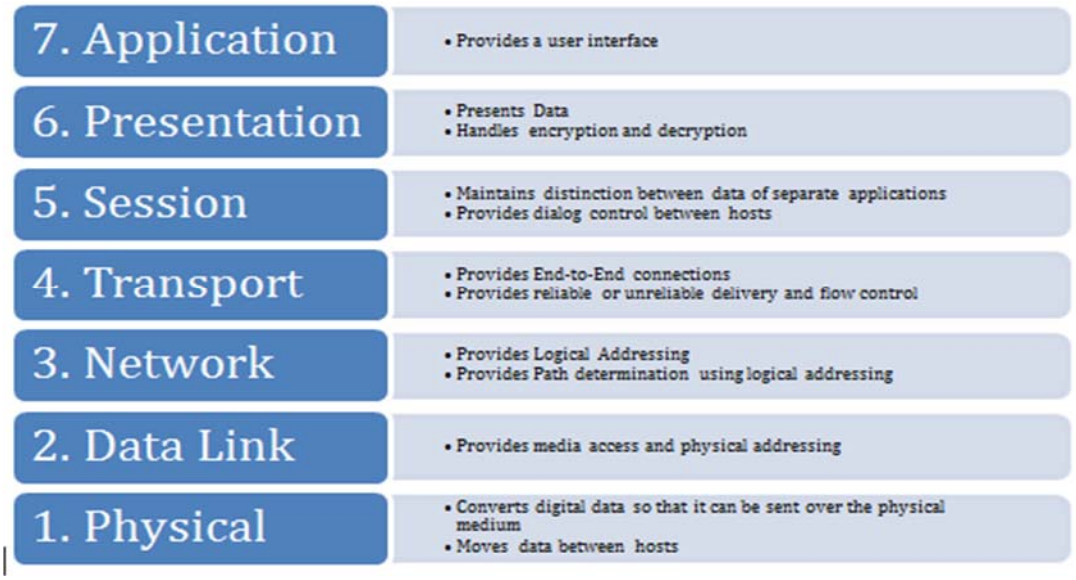
The model is broken into seven subcomponents, or layers, each of which represents a conceptual collection of services provided to the layers above and below it. The OSI Model defines a logical network and effectively describes computer packet transfer by using different layer protocols also referred to as the seven-layer OSI Model or the seven-layer model.

The OSI Model was developed by the International Organization for Standardization (ISO) in 1978. While working on a network framework, ISO decided to develop the seven-layer model.

The OSI Model works in a hierarchy, assigning tasks to all seven layers. Each layer is responsible for performing assigned tasks and transferring completed tasks to the

next layer for further processing. Today, many protocols are developed based on the OSI Model working mechanism.

The seven layers of OSI model are:



(source: www.freecnnstudyguide.com)

PHYSICAL LAYER

The physical layer, the lowest layer or first layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It activates, maintains and deactivates the physical link between systems (host and switch for example). Essentially this layer puts the data on the physical media as bits and receives it in the same way. Hubs work at this layer.

Characteristics:

- Responsible for electrical, light or radio signals.
- This is the hardware layer of OSI layer.
- Device like repeaters, hub, cables, Ethernet work on this layer.
- Protocols like RS232, ATM, FDDI, Ethernet work on this layer.

Functions:

- Data encoding.
- Physical medium attachment, accommodating various possibilities in the medium.
- Determine transmission technique i.e. baseband or broadband.
- Transmits bits as electrical or optical signals appropriate for physical medium.

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. Data Link layer deals with data moving within a local network using physical addresses. Each host has a logical address and a physical address. The physical address is only locally significant and is not used beyond the network boundaries (across a router). This layer also defines protocols that are used to send and receive data across the media. The Data Link layer determines when the media is ready for the host to send the data and also detects collisions and other errors in received data. Switches function at this layer.

Characteristics:

- Data link layer is divided into two layers: Media Access Control (MAC) layer and Logical Link Control (LLC).
- MAC (Media Access Control) address is the part of layer 2 (data link layer)
- Devices like switch work at this layer.

Functions:

- It convert electrical signals into frames.
- Manages data errors form the physical layer.
- Responsible for establishing and terminating logical link between two nodes.
- Encodes and decodes electrical signals into bits.
- Converts electronic signals into frames.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. To best understand what the Network layer does, consider what happens when you write a letter and use the postal service to send the letter. You put the letter in an envelope and write the destination address as well as your own address so that an undelivered letter can be returned back to you. In network terms, this address is called a logical address and is unique in the network. Each host has a logical address. When the post office receives this letter, it has to ascertain the best path for this letter to reach the destination. Similarly in a network, a router needs to determine the best path to a destination address. This is called path determination. Finally the post office sends the letter out the best path and it moves from post office to post office before finally being delivered to the destination address. Similarly data is moved across network mainly by routers before being finally delivered to the destination.

All these three functions – logical addressing, path determination and forwarding – are done at the Network Layer. Two types of protocols are used for these functions – routed protocols are used for logical addressing and forwarding while routing protocols are used for path determinations. There are many routed protocols and routing protocols available. Some of the common ones are discussed in great detail later the book. Routers function at this layer. Remember that routers only care about the destination network. They do not care about the destination host itself. The task of delivery to the destination host lies on the Data Link Layer.

Characteristics:

- Switching and routing technologies work in this layer.
- It creates logical paths between two hosts across WWW.
- Routers work in this layer.
- Network protocols like TCP/IP, IPX, and AppleTalk work at this layer.

Functions:

- Responsible for routing and forwarding data packets.
- Routes the data packets to the destination.
- Logical-physical address mapping occurs in this layer.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers. Where the upper layers are related to applications and data within the host, the transport layer is concerned with the actual end-to-end transfer of the data across the network. This layer establishes a logical connection between the two communicating hosts and provides reliable or unreliable data delivery and can provide flow control and error recovery.

Characteristics:

- Message segmentation occurs in this layer.
- Message acknowledgement i.e. provide reliable end to end message delivery with acknowledgements.
- Message traffic control occurs in this layer.
- Multiplexes several message streams or sessions onto one logical link.
- Protocols like SPX, TCP and UDP work here.

Functions:

- Responsible for the transparent transfer of data between end systems.
- Responsible for end to end error recovery and flow control.
- Responsible for complete data transfer.

SESSION LAYER

The session layer allows session establishment between processes running on different stations. In a host, different applications or even different instances of the same application might request data from across the network. It is the Sessions layer's responsibility to keep the data from each session separate. It is responsible for setting up, managing and tearing down sessions. It also provides dialog control and coordinates communication between the systems.

Characteristics:

- It establish, maintain and terminate the session.
- Protocols like NFS, NetBios names, RPC, SQL work at this layer.

Functions:

- It is responsible for establishment, management and termination of connection between applications.
- It sets up, coordinates and terminates conversation, exchanges and dialogues between the applications at each end.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

As the name suggest, this layer presents data to the Application layer. The Presentation Layer is responsible for data translation and encoding. It will take the data from the Application layer and translate it into a generic format for transfer across the network. At the receiving end the Presentation layer takes in generically formatted data and translates into the format recognized by the Application layer. An example of this is an EBCDIC to ASCII translation. The OSI model has protocol standards that define how data should be formatted. This layer is also involved in data compression, decompression, encryption, and decryption.

Characteristics:

- Character code translation for example, ASCII to EBCDIC
- Presents data in specific format to application layer.
- Data encryption and decryption for security purpose is done in this layer.

Functions:

- Responsible for data representation on screen.
- Responsible for compression, decompression, encryption and decryption of data.
- Data semantics and syntax.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. The Application Layer provides the interface between the software application on a system and the network. This layer does not include the application itself, but provides services that an application requires.

Characteristics:

- It supports applications, apps and end use processes.
- This layer works on protocols like Telnet, FTP, HTTP.

Functions:

- Responsible for resource sharing and device redirection.
- Remoter file access.
- Network management.
- Responsible for application services for file transfers, e-mail and other network software services.

KEY POINTS

- OSI reference model is a seven layer conceptual model developed by ISO in 1984.
- OSI model describes standards for inter computer communication.
- In Application layer network applications such mail web, etc. works.
- Datagrams are called Upper layer data in application, presentation and session layer.
- Presentation layer prepares the data to be presented in application layer from lower layer.
- Session layer controls the dialogs between the computers. It
- Transport layer provides transparent transfer of data.
- TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocol are operated in transport layer.
- Datagrams are called segments in transport layer.
- Routers are operated in network layer.
- Network layer provides connection between hosts on different networks.

- Datagram are called packets in network layer,
- Routing of packets is done in Network layer.
- IP addresses are operated at layer 3.
- Data link layer provides connection between hosts on same network.
- MAC addresses are operated at layer 2.
- Datagrams are called frames in layer 2.
- Data at layer one are called bits.
- When troubleshooting is started it starts at layer 1.
- Physical layer describes electrical and physical specifications for devices.

Students' Evaluation

Answer the following questions:

1. Very Short Answer-Questions.

a) What does OSI stands for?
b) How many layers are there in OSI reference model?
c) What are datagrams called in layer 7?
d) What are datagrams called in layer 4?
e) Routers work at which layer of OSI mode?
f) In which layer does switch work?
g) Who developed OSI reference model?

2. Short Answer-Questions:

a) What is OSI reference model?
b) List the layers of OSI reference model.
c) Which layer is responsible for encryption and decryption?
d) What is the function of Network Layer?
e) Describe the function of Presentation layer?
f) At which layer of OSI model is a path decision made based upon IP address?

3. Long Answer-Questions

- Describe all the layers of OSI reference model?
- Explain the function of each layers of OSI reference model?
- What is the job of transport layer under OSI reference model?

Glossary:

Framework: basic structure of something.

Hierarchy: Order, rank,

Reference:

https://www.techopedia.com/2/27094/networks/an-introduction-to-the-osi-model

http://searchnetworking.techtarget.com/definition/OSI

https://www.techopedia.com/definition/24961/osi-protocols

https://www.webopedia.com/quick_ref/OSI_Layers.asp

CHAPTER 7

Network Security

Objectives

At the end of the unit students will be able to:

- Define network security.
- List 4 network security mechanisms.
- Define cryptography.
- Describe application of digital signature.
- Say importance of firewall.
- Define web security and virtual private network.

Learning Process and support materials:

- Support Materials: Firewall, Digital Smart Cards.
- Learning Process: The explanation firewall and other security mechanism will be given by using above support materials.

Content Elaboration

Network is one of the sensible and important aspects of human life, in the absence of which the simple routine task is difficult to complete. Now the world cannot be imagined without the networks. Different types are used by different organizations

to facilitate their personnel, customers. The valuable information of person, organization are stored and communicated through the network in this 21stcentury. The discloser or theft of those data and information may cause great damage to the individual or an organization. So, network and computer system needs better security mechanism.

In general sense, security refers to the protection from risk or danger. In context of computer or network security refers to the protection of data, information, hardware and software form intentional or accidental harm, theft or unauthorized access.

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network kand network-accessible resources.

A security mechanism is any process that is designed to detect, prevent, or recover from a security attack. Some of the security mechanisms:

Cryptography concept

The word cryptography is derived from Greek work Kryptos which means “secret” and graphein, means "writing”. If the data and information are transmitted as they are over the network, the intruders or hackers may access and misuse it. So the data and information should be converted into the secret writing which is called cryptography. ". Cryptography is the process of conversion of data into a secret code for transmission over the public network. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text.

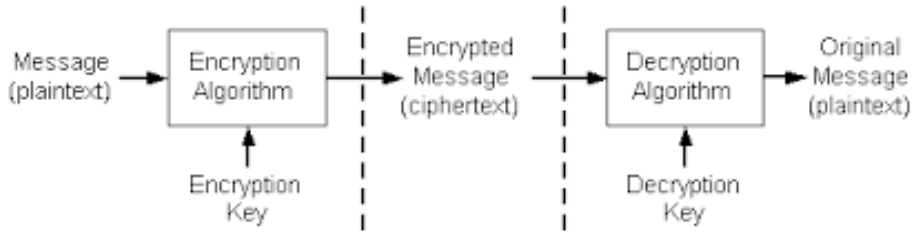


Fig. The encryption model.

The above figure shows the conversion of original message (plain text) into the secret encrypted message (chipper text) by the sender using encryption key. And the message is transmitted and the intruders can't read it on way. Then the receiver decrypts the chipper text into the plain text using decryption key.

Digital signature concept

Digital signature is a security mechanism in a cyber space. It is a digital identity of a sender which electronically uniquely identifies the sender. In cyber space digital signature are used for secure transactions.

A digital signature guarantees the authenticity of an electronic document or message in digital communication and uses encryption techniques to provide proof of original and unmodified documentation. Digital signatures are mostly used in online transactions, e commerce etc. Digital signature is also known as electronic signature. The creation of a digital signature is a complex mathematical process that can only be created by a computer.

Application of Digital Signature:

- Authentication: The digital signature are responsible for authenticating the source of message. For example, if a bank's branch office sends a message to central office, requesting for withdrawing balance from an account. If the central office could not authenticate that message is sent from an authorized source, acting of such request could be a great mistake.
- Integrity: Once the message is signed and sent any modification to that message would be unacceptable because its integrity is lost. If such change is made that would invalidate the signature.

- Non-repudiation: By this property, any entity that has signed some information cannot at a later time deny having signed it.

Firewalls

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls can be implemented as both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Advantages:

- It monitors incoming and outgoing data from the network.
- It blocks the harmful packets from being entering the network.
- It maintains the security of private network.
- It protects computer from unauthorized remote access.
- Firewall make online gaming safer.
- Firewall can be hardware or software.

Web Security

Today's most of the work is web based. Either that is communication or transportation, medicine, shopping, etc we need to access different websites in order to complete them. Web sites are unfortunately prone to security risks. And so are any networks to which web servers are connected. Setting aside risks created by employee use or misuse of network resources, the web server and the site it hosts present most serious sources of security risk. Web security is the process of securing confidential data stored online from unauthorized access and modification.

Web security commonly known as cyber security includes the mechanism of protecting the information by preventing, detecting and responding to attacks.

Virtual Private Network

A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. VPN technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources.

With a VPN, all your traffic is held inside a private, encrypted tunnel as it makes its way through the public internet. You don't access the destination until after you've reached the end of the VPN tunnel.

The benefit of using a secure VPN is it ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it.

Advantages:

- Enhanced security: when the network is connected to through VPN the data is kept secured and encrypted which provides security.
- Remote control: The information can be accessed remotely even from home or from any other place.
- Unlock websites and bypass filters: VPNs are great for accessing blocked websites or for bypassing internet filters.
- Better performance: The bandwidth and efficiency of the network can be generally increased once VPN is implemented.
- Reduce Cost: The maintenance cost is very low when VPN is created.

Key Points

- Network security refers to protection of computer network and network resources and information from unauthorized access, misuse, modification.
- Cryptography is the process of converting the plain text into chipper text for transmission over public network.
- Digital signature is a digital identity of a sender which electronically uniquely identifies the sender.
- A firewall is a network security device that monitors incoming and outgoing network traffic.

- Web security is the mechanism of protecting the information by preventing, detecting and responding to attacks.

Students' Assessment

Answer the following questions

A. Very Short Answers-Questions

1) What does VPN stand for?
2) Write any 3 security measures.
3) From which word does the word cryptography derived?

B. Short Answers-Questions

1) What is network security?
2) Write any four advantages of VPN?
3) Define firewall.
4) Write the advantages of firewall.

C. Long Answers-Questions

a) What is network security?
b) Define cryptography.
c) What is digital signature? Explain about its implication.
d) Write short notes on web security and virtual private network.
e) Define web security with its importance.

Glossary

Disclose: To open up
Integrity: the quality of being fair.
Prone: suffer from something

Reference

https://www.techopedia.com/definition/24783/network-security
https://www.webopedia.com/TERM/C/cryptography.html
https://www.techopedia.com/definition/5426/digital-signature
https://www.techopedia.com/definition/5426/digital-signature