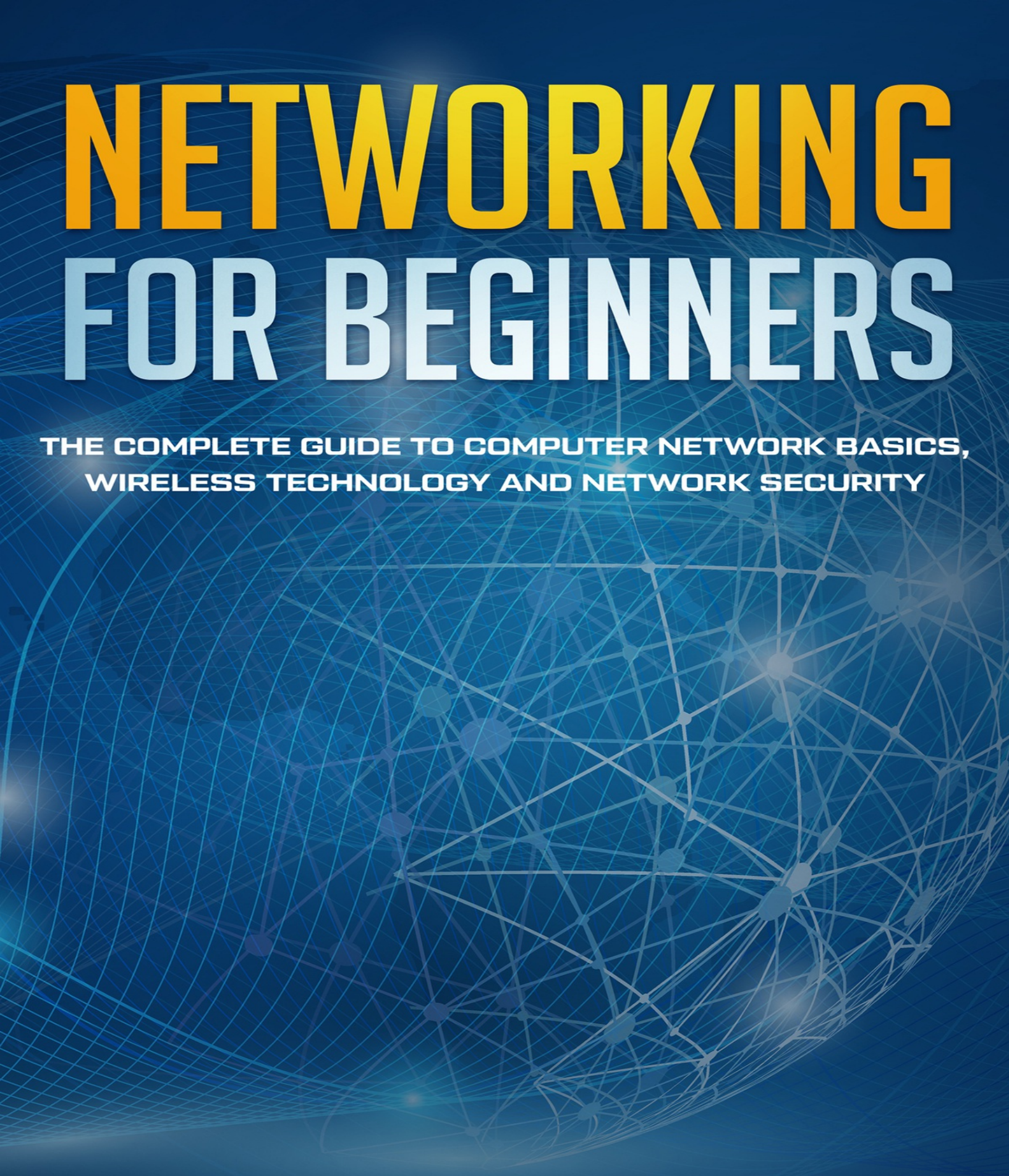
NETWORKING FOR BEGINNERS

THE COMPLETE GUIDE TO COMPUTER NETWORK BASICS, WIRELESS TECHNOLOGY AND NETWORK SECURITY



JOHN MEDICINE

Networking for Beginners:

The Complete Guide to Computer Network Basics, Wireless Technology and Network Security

John Medicine

Download the Audio Book Version of This Book for FREE

If you love listening to audio books on-the-go, I have great news for you. You can download the audio book version of this book for **FREE** just by signing up for a **FREE** 30-day audible trial! See below for more details!

Audible Trial Benefits

As an audible customer, you will receive the below benefits with your 30-day free trial:

- FREE audible book copy of this book
- After the trial, you will get 1 credit each month to use on any audiobook
- Your credits automatically roll over to the next month if you don't use them
- Choose from Audible's 200,000 + titles
- Listen anywhere with the Audible app across multiple devices
- Make easy, no-hassle exchanges of any audiobook you don't love
- Keep your audiobooks forever, even if you cancel your membership
- And much more

Click the links below to get started!

For Audible US

For Audible UK

For Audible FR

For Audible DE

Table of Contents

Introduction

Congratulations on downloading your eBook copy of the *Networking for Beginners*. I am very much delighted that you all have shown so much interest in learning about the basics of networking and the functioning of each and every component of the same. Networking can also be regarded as the main component of every organization as without proper networking it is not possible to set up a proper business.

Networking is the technique which is used for transferring various forms of data from one end to another with the use of intermediary systems. Networking is not only about the design, use or construction of its structure. It also comes with management, operation and maintenance of each and every component that builds up the network. It can also be said that a properly structured network can help in transferring data and information in lightning speed from one system to another. Networking allows various devices and systems to be connected with each other via various networking systems that you will learn more about in this eBook. The various components of networking make it possible for the human world to send uninterrupted messages from any corner of the world. Not only that but with the various types of networking, the organizations can server their function in a better way.

There are various other eBooks available in the market on Networking. Thank you for choosing this eBook on Networking for Beginners. Every effort has been made for making this book as much interesting as possible. Enjoy!

Chapter 1: Logic of Computer Networking

In this world of today, where nothing is possible without the touch of technology in it, computer networking is also such a thing without which setting up an organization or business cannot be imagined at all. It helps in connecting various related devices to the endpoints with the help of various networking systems. Networking serves a very essential function for all the service providers, consumers and businesses all over the world for the purpose of sharing, using and offering various services and also for communicating at the same time. Networking comes with everything, from text messages to telephone calling and ending with video streaming and IoT. Network operation requires some serious skills that depend completely on the network complexity. For instance, in a very large enterprise, it might have millions of nodes along with several other requirements of network security like encryption, administrator functioning and many more.

On the other side, a normal person who uses internet and networking daily at his home can easily set up along with troubleshooting of various basic problems in the wireless network at their home. Both the examples given

require the basics of networking to some extent.

Computer Network Basics

For understanding the prime functioning and components of networking, you need to learn about the basics first. A computer network is made up of various components that help in its overall functioning. Let’s have a look at the basics of networking.

Networking and its types

Computer networking can be divided into two different types: wired network and wireless network. In the case of a wired network, it needs a physical medium for the purpose of transporting information between the nodes. For the purpose of digital communication in homes and in businesses, Ethernet cables are used for its durability and low cost as well. Optical fiber is also being now for data transportation to great distances and also at a much faster speed. However, whenever it comes to costing, Ethernet cables are much more cheaper than optical fibers.

In wireless networking, the radio waves are used for transporting data around the air in which the devices in the network are connected with each other without any form of cables in between. WLAN or wireless LAN is the most widely used and well-known version which is used for wireless networking. There are also several alternatives in the market today such as satellite, Bluetooth, microwave, cellular any many more.

It has been found that when it comes to networking, wired networking provides better speed, security along with reliability when it is compared with wireless form of networking. However, wireless networking provides much more mobility, scalability and flexibility that wired networking.

Wired and wireless networking is classified according to the networking physical layer. However, networking can also be differentiated in accordance with the design and built of the network, approaches of encompassing like SDN or overlay network. It can also be classified according to the scale, environment like campus, LAN, WAN, storage area network, data center network and many more.

Types of networking systems

There are two types of networking system: open and closed. In an open system, the system is connected with the network and is also ready for communication. However, in the case of a closed system, the system is not linked with the network and it is not possible to connect with the same.

Networking components

Computer networking comes with the requirement of the infrastructure of physical network. It includes various components such as routers, switches, access points along with the basic firmware which will help in operating the other components. When it comes to the other components, it includes the necessary software for the purpose of monitoring, securing and managing the network. All forms of networking rely largely on the standards of protocols for performing uniformly various discrete jobs or for communicating with various types of data. Protocol is nothing but a set of algorithms or rules which helps in defining the various ways in which two different entities communicate with each other across a network. There are various types of protocols that can be found within a network such as IP, ARP, DHCP, TCP, FTP and many more.

VoIP or voice over IP is used for the transportation of IP telephonic traffic to the endpoint which also supports the protocol. TCP/IP is known as the internet protocol suite which is responsible for data transportation over a network based on IP.

An IP address is the logical address which acts as the network address for the systems in a network. It helps in creating a unique identification for all the devices across the network. The IP addresses are in 32 bits. IANA or Internet Assigned Numbers Authority assigns a unique IPV4 for each and every system or device in a network.

MAC address is regarded as the physical address for every host in a network. It is linked with the NIC or network interface card. The MAC addresses can be found in 48 bits or 6 bytes or 12 nibble. Each MAC address is assigned to the system NIC while manufacturing of the system or device.

Chapter 2: Internet Communication

The world today has completely changed from which it was a few years back. It is changing every day. With the advancement of digital technology, the pace of change has also become very fast. There were times when a simple message used to take a few months to deliver and now it takes just a few seconds. Internet communication has evolved so much that it can now connect people seamlessly from every corner of the world.

Internet Communication

Internet communication is a very simple thing. It is the sharing of ideas, information or just mere words over the internet or World Wide Web. Internet is composed of a huge string of worldwide connected networks which helps in exchanging information and data with the help of packet switching by using the TCP/IP.

Internet communication comes with a bunch of advantages that can help us in a lot of ways.

Internet communication and its advantages

Communication system on the internet comes with more number of advantages than disadvantages. For a business person, he/she can be at the comfort their home, drinking tea or coffee and having a conference call with the clients as well at the same time. It can help in saving a lot of time, money along with growth in business.

- **Versatility:** Internet communication is versatile in nature. It is available 24*7. Internet communication will keep on working as long as you are connected with the web. Internet communication can also be regarded as a boon for the businesses, especially at the time of emergency incidents such as in the sector of social media advertising, bad publicity of even one second can lead to a disaster. In such case, internet communication helps in mending it all up.
- **Leveling:** It is a fact that everyone cannot in front of everybody at once. Also, there are many people around us who do not like to talk that much. Such people always love to express their feeling by writing. Some people feel more comfortable while talking from behind the keyboards. In that case, internet communication helps in building up a communication line for such people.
- **Well documented:** Face to face communication is not much documented whereas, internet communication is well documented. It helps in various situations especially when people need to be accounted for the words they speak. Thus, internet communication helps in establishing a very responsible environment.
- **Fast communication:** Internet communication is fast. It transfers messages in blazing fast speed that makes it possible to send out messages at the time of emergency.

Tools for internet communication

Internet communication has provided the human world with a wide range of tools for the purpose 0f communication. Let’s have a look at them.

Email

Email is regarded as one of the fundamental tools for internet communication. Today, email addresses are required in almost all forms of services today and it is also believed that everyone who is active on the internet has at least one single email address. Email addresses can be taken from various free services such as Google and Microsoft. Email is most widely used for the purpose of sending out official or confidential information. However, in this world of today, it is also being used for various harmful activities such as spreading malware or scams with the use of phishing emails. In the case of phishing, a third party tricks the victim into sharing his/her sensitive data such as bank or credit card details, account numbers etc. So, it is always better to be a little cautious while fetching any form of email from unrecognized sources.

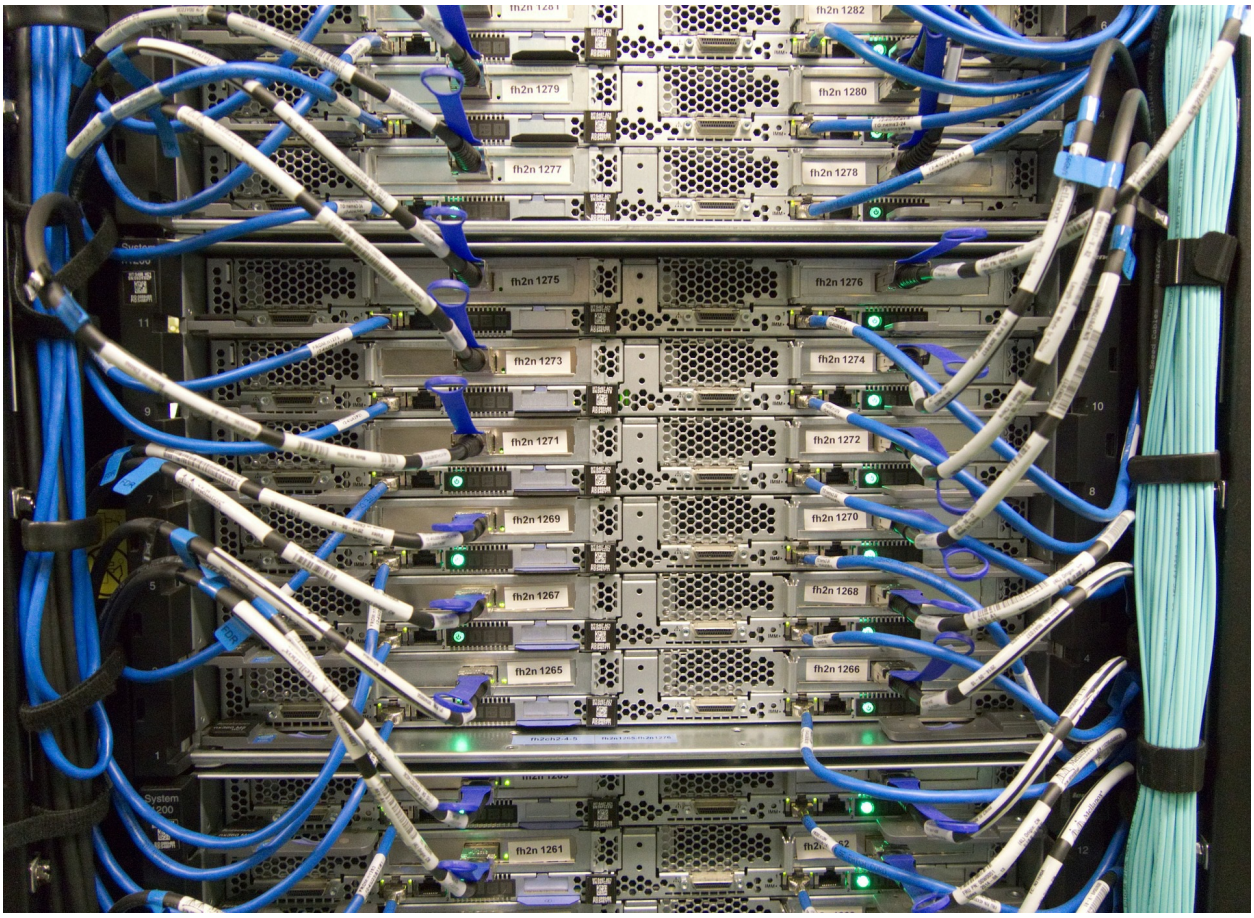
Social media

One of the trending tools of today, it is being used for seamlessly connecting millions of people from all over the world without any kind of delay in transmitting the messages. It is also being used for spreading awareness or alert in case of any emergency situation, share important information with anyone you want and many more. But, the case of fraudsters in social media today is increasing day by day. Also, social media is used for spreading various information which is being used by the fraudsters at times for spreading hoax.

World Wide Web

World Wide Web is the most dominant form for internet communication. It is being used for everything, starting from online shopping to checking out the weather. It also helps in communicating online such as using digital messaging board or email. The users need to have a web browser in order to

access the web. There are various types of browsers available today both for computers and smart devices. Each website is built with the use of HTML which is the website language, CSS which defines each and every element on the screen and JavaScript which is used for processing of data and also provides logic for programming. Every other form of internet communication such as VoIP or voice over internet protocol also relies on the web. VoIP helps in internet-based systems of calling. Using VoIP systems is regarded to be much cheaper as well as faster than traditional mobile phones. It also allows international calls with no form of delay in transmission.



Chapter 3: Client-Server Approach

The client-server approach is the architecture of computer networking in which various clients or the remote processors requests for a service and receives the same from the host or server computer. The computers of the clients come with an interface for the purpose of allowing the user of a computer for requesting various services from a server and then display the requested result which is returned by the server. All the servers in a network wait for the arrival of the requests from the clients and then only respond to each of the requests. Generally, a network server comes with a transparent standardized interface for the clients so that all the clients are aware of the system specifications such as software and hardware which is responsible for providing the services.

The clients typically are on their PCs or at their workstations and the servers are located right on the network i.e. on much powerful systems than the clients. The client-server approach is the most effective when both the server

and the clients have some specific job to perform regularly. For example, in data processing of hospitals, the computer which acts as the client system runs a program for entering all the patient information and the server system helps in managing the patient database in which all form of information is stored permanently. All the clients on the network can access the information which is given out by the server and the client system can also perform various other jobs like sending out emails.

Both the client and the server in the networking approach are regarded as intelligent devices. So, the client-server model is also completely different and much more advanced than the old model of mainframe in which the central server computer used to perform all jobs for all the terminals in a network.

Components of the client-server model

The client-server model works with three components: servers, network devices and workstations. Workstations in a network are those computers which are subordinate to the servers. Workstation sends out various requests to the servers for accessing the shared files, programs, databases and files. It is governed by the server policies. The server in a network serves all the requests that come from the workstations and can also perform several other functions like management of the programs, files, databases along with the policies of management. Network devices in a network help in establishing communication between the servers and the workstations. In simple words, the network devices act as the connectors and also routes the data in and out from the network.

Workstations

Workstations, also known as client computers, are the ones which send out requests to the servers. They are differentiated by the OS which runs their systems. In a network of client-server, Windows XP, Windows 7, Windows 10, Linux etc. are the OS of the workstations. As these OS are cheaper than the OS of servers, the processes and functions of such OS are intended for the client computers or workstations only. Shared programs, policies of security and management and centralized databases are not part of the OS. They come

with a localized version of policies programs and databases. The workstations come with a lower level of technical specifications when compared with the servers in respect to processor speed, memory and space of hard drive as the client systems are not required to record any form of data or process any request like the server system.

Servers

Servers are differentiated from each other by their individual sets of OS such as Windows 2003, Windows 2008 or Windows 2000 server. When it comes to the servers, they come with faster speed of processing, higher hard drive space along with more memory. It is mainly because the servers stores up various forms of data and also services multiple workstation requests simultaneously. A server can perform any type of role within a client-server network. It can act as the mail server, file server, domain controller and database server at the same time. However, for a network which is well-setup always divides all these roles among all the available servers for optimizing the network performance. But, no matter what role a server performs, it acts as the centralized repository for databases, programs, network files and policies.

Servers are very easy to manage and also take backup as the servers in a network are not all dependent on the configuration of the individual user and it can be implemented seamlessly across the network.

Network devices

Network devices act as the intermediary between the server and the workstation and help in establishing a connection between the two. Network devices make sure that the requests going from and to the workstations are properly routed with the concerned server. There are various types of network devices available today and each performs different functions of connectivity. In a basic client-server network, the hub helps in connecting a server with the various workstations. It also functions as a repeater and passes on information and data from one device in the network to another. Network devices such as bridges help in separating the various segments of a network.

Chapter 4: Peer to Peer Connection

In the world of networking, there are various types of connection that can be found and created easily. Each of the connections comes with a particular purpose and structure of its own. A P2P or peer to peer network is created when two or more than two computers are connected with each other and share resources and data with each other without the presence of any separate server system. In this form of connection, all the computers within the network share an equal amount of responsibility for the purpose of data processing. Peer to peer network is completely different from client-server networking. In a client-server network, the server acts as the master system and processes data which is consumed or used by the other client systems within the network. However, this is not the case with peer to peer connection.

A peer to peer network can act like an ad hoc connection in which several computer systems are connected with each other via Universal Serial Bus for the purpose of transferring files and data. It can also perform as a permanent infrastructure which links up several computers within a small office network

with the use of copper wires. A P2P connection can also be a larger network of much bigger scale which uses up special protocols along with applications for the purpose of setting up a direct relationship with all the users over the internet. In simple words, a peer to peer network can assume various at times and as required.

Peer to Peer connection and its characteristics

Peer to peer connection can be found on all forms of small-sized LAN or local area network. It is most commonly found in home networks. Both the wired and wireless form of home network can be set up as peer to peer network. All the computers which are involved in a peer to peer network run the same protocols of networking and software. The network devices of peer are most often located near another peer generally in small businesses, homes, schools and smaller organizations. There are also other types of peer to peer connection that utilizes the internet and are dispersed at long distances geographically all over the world.

The home networks which use routers of broadband are a hybrid form of peer to peer and client-server network. The broadband router provides a centralized sharing connection of internet but the printer, files and all other sharing of resources are directly managed between all the involved local computers.

Peer to peer along with Ad Hoc network

The Wi-Fi or wireless networks support ad hoc connection in between the devices. Ad Hoc networks are a form of pure peer to peer connection which can be compared with those networks that use wireless routers as the intermediary device. The devices that build up ad hoc networks require no form of infrastructure for the purpose of communication.

Benefits of Peer to Peer connection

Peer to peer network is robust in nature. In case one of the attached devices fails to perform, the network continues to function with the use of other devices. You can easily configure the computers in a peer to peer network workgroups for allowing file sharing, printers along with other resources across all the connected devices. Peer to peer connection allows both way

sharing of data, whether for the purpose of downloading to the computer or for uploading from the computer.

While on the internet, peer to peer networks can easily handle huge volumes of traffic of file sharing. It handles huge traffic by distributing all the load across all the computers in the network. As P2P connections are not dependent on any form of central server, this network is better in scalability and is also more functional when compared to client-server network at the time of any kind of emergency or heavy traffic.

You can easily expand a peer to peer network. As you keep on increasing the total number of devices in the network, the power of peer to peer network also keeps on increasing. This is because in peer to peer connection, all the devices are responsible for data processing and with the increase in the number of devices within the network, the processing power and speed of the network also increases.

Peer to Peer connection and the security concerns

In this world of today, none of the network systems is safe from external attacks. Just like client-server network, peer to peer connection is also a vulnerable network form to security attacks. In peer to peer connection, all the devices in the network participate in traffic routing across the network. So, it becomes easier for the attackers to launch attacks such as denial of service by the use of one such device on the network. The software for peer to peer connection acts both as the client and the server. This makes P2P network much more prone to remote attacks when compared with a client-server network.

The corrupted data can still be shared on the peer to peer network simply by modifying the files which are on the network for the purpose of introducing malware or malicious codes.

Chapter 5: Basic Components of Computer Networking

Computer networking functions with various components. All the components work together and make data transfer possible from one system to another and help in establishing a smooth connection between the sender and the receiver. A computer network works with one or more than one servers, network interface cards or NIC, workstations, passive and active hub, gateways, bridges, modem, routers, hub, software like OS for networking and many more.

Server

It is regarded as the mother of a network. It is the most powerful system within a network. In the case of LAN, a powerful computer is generally used as the server. In computer networking, two types of servers are used: dedicated and non-dedicated. A dedicated server performs all the services and functions in a network. It helps in running the user applications and also helps in improving the overall cost of the system. However, in a dedicated

server, the users cannot directly run their applications. A dedicated server provides the users with sharing of various hard disks, service regarding email along with sharing of several other data and resources. It comes with a very fast time of response. For all those networks where it is required to handle heavy loads, dedicated servers are employed usually.

In the case of the non-dedicated server, it also functions as a workstation besides functioning as the controller of network. It comes equipped with a prodigious form of memory. The network in which this server is used uses up only a portion of the memory of the server. The rest of the server memory is used up for applications of the users. It is useful for light traffic load condition.

Networking hardware

Network hardware is those devices which are used for interconnecting the various components of a network like the network cards, connection between the servers and the workstations and the cables that connect the peripherals to the network.

Resource sharing

These are the resources of both hardware and software devices. The most commonly found hardware devices are drives, printers, hard disks, CD drives etc. The software resources include programs, applications, files etc.

File Server

The main goal of computer networking is to share information and data among various users. The users also make their printers, modems, disk drives and other links of communication with other client stations as well. The client systems can raise a request to access the shared facility from the server. The file server runs on a special software and is generally served by a powerful system of computer. It helps in sharing files and other resources to all the users within a network. File server also provides other facilities such as authentication of user, program and data security and many more. It generally operates via NOS. All the file server activities are controlled and monitored from the console. The prodigious memory of the file server is used for caching of files and directories.

Workstation

Workstation is regarded as a critical component of a network system. It is also known as the client system. It comes with the capability of connecting and communicating with all other machines in a network. However, for a workstation to function properly, it is required to comply with the software and hardware of the LAN. A workstation is capable of communicating with the server for getting data and other resources. The hardware which is required by the workstation depends completely on the size and application of the network.

NIC

Also known as network interface card, it serves as an add-on card for the computers in a network. It is also called network interface adapter or Ethernet adapter. NIC performs the function of moving the signals across the cables of the network into a parallel stream of data directly inside the systems of the computers. You can also use more than one NIC for splitting the load in the network.

Hub

It is a centralized point of distribution which is required for transmission of data in the network. The hub is generally used for receiving the data packets and then rebroadcast them to all the other computer systems which are connected with it. It is a passive device in nature. The destination of the received data packet is unknown to the hub. Hubs can be easily classified into three categories:

- **Stackable and non-stackable**: The stackable hubs are those hubs which can be interconnected for making a single hub. The non-stackable hubs cannot be connected.
- **Active and passive:** Active hubs are those which connect to the backbone of the network. The hubs which only connect with the active hubs are the passive hubs.
- **Intelligent and non-intelligent:** Intelligent hubs come with a special type of firmware which can also be accessed by the workstations which are remote in nature. The non-intelligent

hubs come without any form of firmware.

Bridge

It is used for interconnecting two different networks by the use of the same technology like Ethernet. It reads the address of the destination of the received packet and also makes sure that the destination address is also on the similar network segment as the origin. In LAN, local bridges are being used for connecting two different segments.

Gateway

Two networks which are different in nature can be connected with the use of a gateway. It converts the data format which is sent in between the networks.

Modem

It helps in facilitating two-way communication in between a telephone network and a computer network.

Chapter 6: OSI Model

OSI model or Open System Interconnection model is a model which has been created for enabling diverse systems of communication for communicating with the use of various standard protocols. In simple words, OSI provides a network standard for the different systems of computer for communicating with each other. The OSI model is also regarded as the universal language for networking. It is based on a concept in which a communication system is split into seven different layers each of the layers are stacked upon one another. Each layer of the model performs a specific function and also communicates with the layers above it and below that layer.

Importance of the OSI model

The modern internet structure does not follow the structure of OSI model strictly but it is still useful for the purpose of network problems troubleshooting. Whether it is just one single person who is unable to connect his PC with the internet or a huge website which is down that serves thousands of users, OSI model helps in breaking down the main problem in layers and also isolates the trouble source.

Seven layers of the OSI model

The seven layers of the OSI model are stacked in inverted order which means that the 7th layer at the top and the 1st layer at the bottom.

Application Layer

This layer is the one which interacts directly with the user data. Various software applications like email clients and web browsers depend on this layer of the OSI model for initiation of communication. However, it needs to be cleared that the software applications of the clients are not a part of this layer. The application layer is liable for manipulation of data and protocols on which the software relies on for presenting data which is meaningful for the user. This layer includes both HTTP and SMTP.

Presentation Layer

The presentation layer is liable for data preparation which can be used by the application layer on top of it. In simple words, this layer transforms data in presentable form so that it can be consumed by the applications. This layer is liable for encryption, translation and also data compression. The 6th layer is responsible for the translation of incoming data into a simpler syntax so that it can be understood by the application layer on top of it. In case the devices are communicating with each other over a connection which is encrypted in nature, this layer applies encryption to the sender's end and also decodes the data on the end of the receiver so that the data can be presented to the application layer in a readable and unencrypted format. It also helps in data compression before delivering data to the 5th layer.

Session Layer

The session layer is responsible for the closing and opening of the system of communication between two devices in a network. Session is the time in between the opening and closing of the communication. This layer makes sure that the communication stays in the open state till the time before the data exchange has been done.

Transport Layer

This layer is liable for communication between two devices as an end to end communication. This whole process involves data collection from the session layer and then breaking them into segments just before sending them out to the 3rd layer. This layer on the recipient device is liable for segment reassembling into complete data so that it can be consumed by the session layer. This layer also takes care of flow and error control. Flow control helps in determining a normal speed for transmission so that a sender who is having a fast connection does not deluge the receiver who is having a slow connection.

Network Layer

This layer is liable for allowing transfer of data in between two different forms of networks. In case both the devices in the communication are functioning on the similar network, this layer becomes unnecessary in such case. This layer breaks up the segments from the transport layer just above it into various smaller units known as packets on the device of the sender and the reassembles the packets on the device of the receiver.

Data Link Layer

This layer is very much similar to that of the network layer. The only difference is that this layer allows transfer of data between two devices which are on the same network. This layer takes in packets from the network layer and then breaks them into frames.

Physical Layer

This layer involves all the physical form of equipments which are used in the transfer of data like switches and cables. This layer also converts data into bit stream in which the string is of 0s and 1s. The physical layer present in both the devices needs to agree on the convention of the signal so that it is possible to distinguish 1s from 0s in both the devices.

Chapter 7: Wired Network VS. Wireless Network

There are two types of networks systems that can be found in most of the organizations and homes: wired network and wireless network. Wired form of network in which Ethernet is used is the most common choice in most of the homes but Wi-Fi along with other forms of wireless networking are also gaining its momentum. Both forms of networking come with pros and cons over each other where both can be used for homes and for office purpose.

Wired LANs

In this form of network, Ethernet cables are used along with the network adapters. Two devices can be easily connected with each other by using Ethernet cables but sometimes intermediary components such as hubs, routers and switches are also used.

Installation

The Ethernet cables run from one computer to the other or directly to the server or central system. The installation process is time-consuming especially when the computers are at a distance from each other or at different rooms. However, CAT5 cables are also used today which helps in simplifying the process of cabling and also minimizes the cable runs which are unsightly. The configuration of cabling depends greatly on the mixture of devices which will be used on the network, the internet connection type and

also on various factors such as whether internal or external modems will be used or not. The configuration of the network relies on the standard IP and on other options of network OS.

Costing

The whole setup of wired LAN is cheap. The cables, switches and hubs are inexpensive. The software required for connection sharing such as ICS comes free. In general, the wired LAN is really cheap in nature however, it might turn out to be costly when other features such as security devices and broadband routers are used in the network.

Reliability

The hubs, Ethernet cables and switches are reliable in nature as the developers of such items have been improving the technology with time. The only drawback of a wired network is loose cables. It might hamper the entire network if one of the cables is not connected properly. However, this form of network allows fast transfer of data across the computer systems with no lags in performance.

Performance

The wired LANs come with superior quality of performance. It can offer a bandwidth of 10 Mbps to 100 Mbps. It makes file sharing among the systems a very easy job and can transfer them within no time. It also allows high-speed access to the internet.

Security

Firewalls are the main consideration for security in wired LANs. The various components do not support firewall but it can be installed on the computer.

Wireless Network

This form of network uses Wi-Fi for setting up a connection with the other devices on the network. It does not involve any type of wired connection with the systems.

Installation

The wireless networks or Wi-Fi networks can be easily configured and it can be done in two different ways:

- Infrastructure mode which allows the devices to communicate to a prime node that can, in turn, communicate with the wired form of nodes on the LAN.
- Ad-hoc mode allows the devices to connect with each other using peer to peer mode.

Ad hoc mode allows only the basic form of file sharing between the devices. Both the configuration types need network adapters which are also known as WLAN cards.

Costing

Wireless networking is much more expensive when compared to wired LANs. The wireless adapters are costlier than the Ethernet adapters, switches, hubs etc.

Reliability

Wireless LANs also suffers from reliability problems just like wired LANs. The main problem that comes with wireless LAN is the concern about signal strength. It is subject to various interferences such as microwave ovens, garage door openers and cordless phones. It requires to be installed carefully for minimizing the interference in signal strength.

Performance

The wireless LANs which uses 802.11b can provide a maximum bandwidth of 11 Mbps. It can support a maximum of 54 Mbps which is half when compared with the bandwidth of wired LANs. The performance of Wi-Fi connection depends on the distance between the access point and the device. The larger the distance the slower the connection. However, it removes the use of long Ethernet cables for setting up a network and is thus mobile in nature.

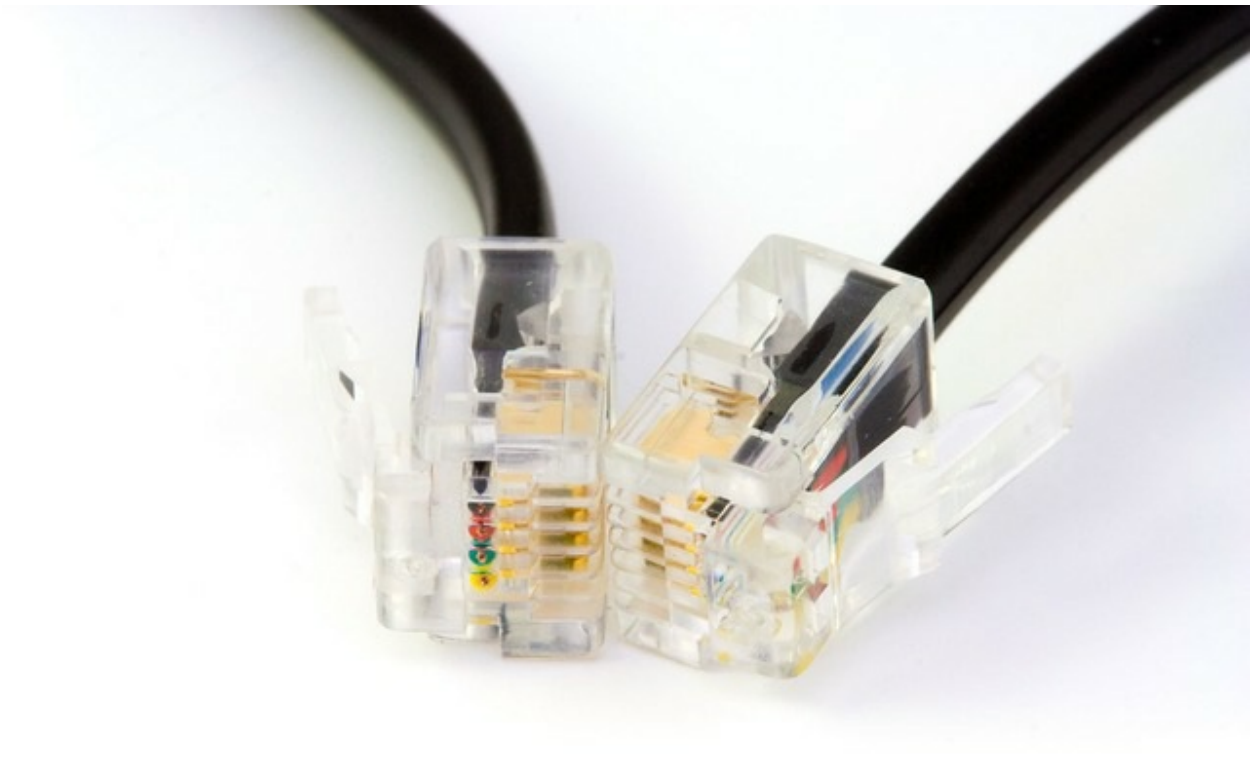
Security

The wireless LANs are less secure in nature when compared with the wired

LANs. This is mainly because of the fact that the signals of wireless communication travel through the air and it can be intercepted very easily. For making the connection more secure some measures need to be taken such as the internet firewall needs to be configured properly. Any inappropriate access to the network should also be avoided.

Bottom line

In case you are looking out for a networking system which is cost-effective, fast and you are not concerned about mobility, then wires LAN is the best option. If you are willing to speed up with the technology with the mobility of network, then wireless LAN is the option for you. Both come with pros and cons and you need to analyze them according to your need.



Chapter 8: Hardware Involved in Computer Networking

Computer networking is mostly about hardware. There are various types of hardware components used in setting up a network and for its functioning. You can set up a network with the minimal hardware requirements but as you keep on adding more elements one by one, the performance and reliability of the network also increase.

Networking cables and wires

In spite of so much advancement in wireless networking technologies, many of the computer systems in this 21st century still rely on wires and cables as the physical medium for transferring information data across the network. There are various standards of cables in the world of networking and each of them is designed for some particular purpose. The most common types of

networking cables and wires that can be found today are Ethernet cables and fiber optic cable.

Ethernet Cable

Ethernet cable is the most common form of cable that is used for wired networking. It helps in connecting various devices such as computers, switches and routers within a network of local nature. However, Ethernet cables are very much limited when it comes to durability and length. If the cable is kept too long or is of not good quality, the cable won't be able to carry good signal. That is the reason why different types of Ethernet cables are used for different functions.

Types of Ethernet cable

The Ethernet cables which are used today support many of the industry standards that also includes category 5 and 6. The technicians who are experts in computer networking refer to these Ethernet cable standards as CAT5 and CAT6. Ethernet cables are developed in two forms:

- **Solid Ethernet cables:** This form of Ethernet cable offer a bit better performance along with improved security against all forms of electrical interference. Such cables are also being used in the business networks, office wall wiring and under-floor wiring.
- **Stranded Ethernet cables:** This form of Ethernet cable is less vulnerable in nature are also less prone to breaks or cracks. This type of Ethernet cable is suitable for the home-based network.

Ethernet cables and limitation

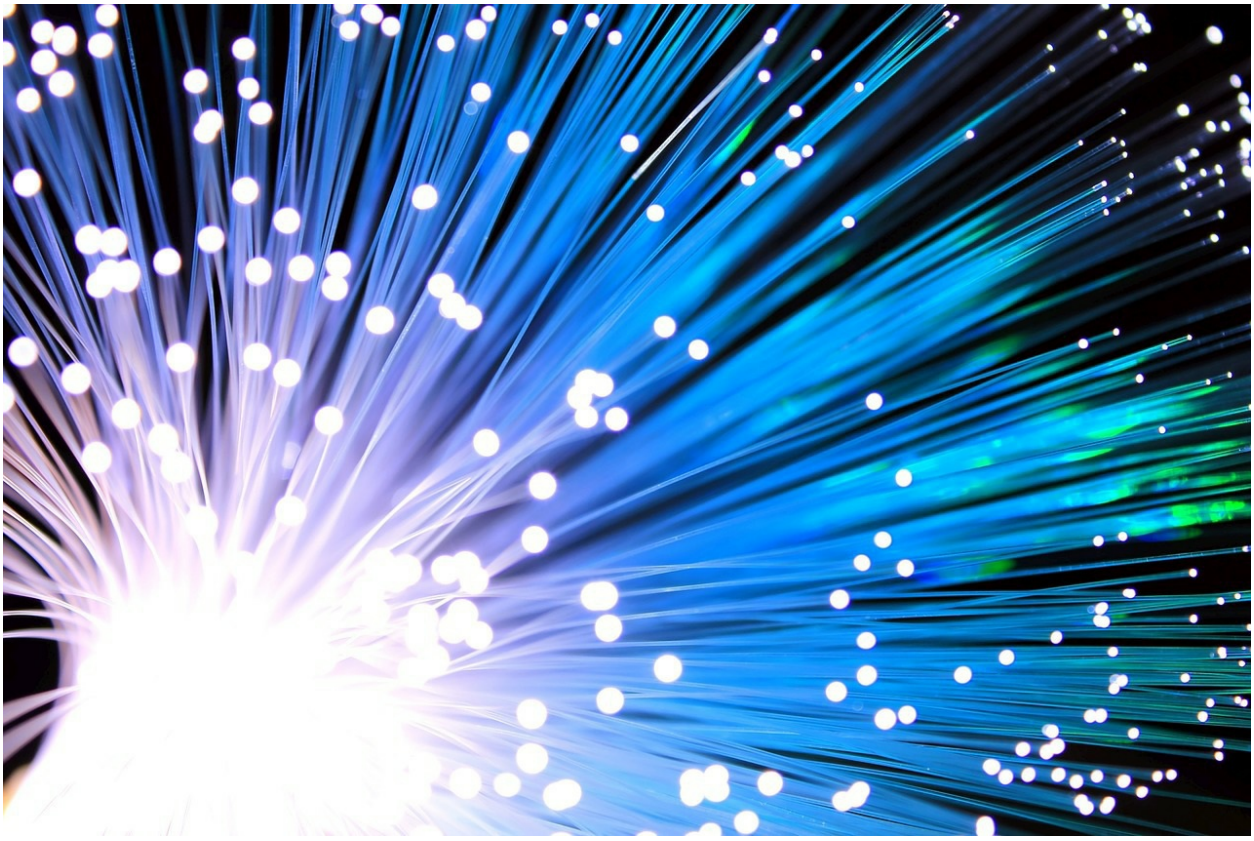
Ethernet cables come with distance limitation. It comes with a distance capacity where the cable comes with a maximum upper limit for how long it can run before there is any form of loss in network signal. This is also known as attenuation. This is mainly because long cables come with an electrical form of resistance that prohibits signal flow and thus affects the overall performance of the network. Both the ends of the Ethernet cable needs to be close enough for receiving signals fast and also at a distance from any form of external interference for avoiding interruptions in the connection. This

practice does not interfere with the network size as various hardware components such as routers and hubs can be used joining various Ethernet cables on the same wired network. The distance between the two devices is known as network diameter.

The length of CAT5 cable just before attenuation takes place is 324 feet. However, CAT6 can extend up to a distance of 700 feet. If you want you can also keep the Ethernet cables longer than the standard lengths but the only problem that you will be facing is loss in signal, especially in cases when the cables need to pass across large appliances.

Alternative option for Ethernet cable

There are various alternatives that can be found today for Ethernet cables such as Bluetooth and Wi-Fi. It is mainly because the devices and systems of today are not having a network port and come with Wi-Fi only. But, still the security and performance which is provided by Ethernet cables are really outstanding and many of the big organizations and various home networks still use Ethernet cables for a wired network.



Fiber Optic Cable

Fiber optic cable is a form of network cable that comes with glass fiber strands inside the insulated casing of the cable. It has been designed for long-distance transmission of data, telecommunications and for high performance of the network. When compared with Ethernet cables, fiber optic provides larger bandwidth and it is capable of transmitting data to long distances without any loss in signal. It supports most of the world's cable television, internet and telephonic systems.

How does fiber optic cable function?

Fiber optic cable is composed of several strands of glass which are slightly thicker when compared with human hair. The center of each of the glass strand is known as the core which provides the travelling pathway for light. The core of the glass strands is surrounded by a glass layer which is known as cladding which helps in reflecting all the light inwards and thus helps in preventing signal loss. It also allows the light to travel through cable bends easily. Fiber optic cables are of two types: single-mode and multi-mode. The single-mode cable uses super thin strands of glass along with a laser for the purpose of generating light. The multi-mode cable uses LEDs for generating light.

The single-mode fiber optic cable uses a technique known as Wave Division Multiplexing for the purpose of increasing data amount traffic which can be carried by the glass strands. This technique allows light to travel at various wavelengths for combining and then separating later for transmitting various streams of communication via a single pulse of light.

Fiber optic cable and its advantages

Fiber optic cables offer various advantages for long distance transmission. Fiber optics can easily support higher capacity of transmission. The bandwidth of fiber optic cables is 10 Gbps, 40 Gbps and 100 Gbps as standards. Fiber optics do not need any form of signal booster this is because light travels for longer distances without any form of loss in its strength.

The cable of fiber optics is less vulnerable to any form of interference. The Ethernet cables require shielding for its protection from electromagnetic

interference. However, this shielding is not enough for the ultimate protection. However, the physical properties of fiber optics cable can easily avoid all these problems.

Fiber optics to the home

In most of the cases, fiber optic cables are being used for long distance communication in between the cities and countries. However, some of the local internet providers are also extending their network by installing fiber optics which can be accessed directly by the households. One of the prominent fiber to home service which is available in the market today is Google fiber. Such fiber optics services can easily provide gigabits of internet speeds to the households. There are various versions of fiber to the home network such as:

- **Fiber to the premises or FTTP:** In this, the fiber optic cables are laid to the buildings directly.
- **Fiber to the building or FTTB:** It is similar to that of FTTP.
- **Fiber to the curb of node or FTTC/N:** In this, fiber optic cables are laid till the node and then copper wires are used for completing the overall connection inside the household building.
- **Direct fiber:** In this, the fiber optic cable is taken from the central office and is connected to the system of the customer directly. This form of connection provides the best bandwidth but is expensive as well.
- **Shared fiber:** It is similar to direct fiber but as the fiber optic cable reaches the premises of the users, it is distributed into several fiber optic cables for the users.

Other Required Forms of Hardware

Wireless Hardware

For setting up a wireless network, you need certain components of hardware. When it comes to a wireless network, there are two types of network: ad hoc and infrastructure. The infrastructure mode of network is the kind of wireless network that can be found in offices and homes. It is somewhat similar to the

wired network but it is done without wires.

The basic form of wireless network which is peer to peer network requires these hardware components.

- **Router:** Wireless router can be regarded as the heart of a wireless network. Just like a wired network, it is the central location with which all the computers connects to for accessing the network. The wireless routers are also called as access points. It helps in managing the connections in a wireless network and also helps in establishing a connection with the network.
- **NIC:** Every computer which wants to connect with the network requires a NIC or network information card. It allows the system to communicate with the router. Laptops come with in-built NIC but in the case of PCs, you are required to install NIC for getting a wireless connection in the system. It can be installed either internally or it can also be used as a plug-in USB device. This is the standard which is used for infrastructure mode of wireless network.

In the ad hoc mode of wireless network, all the computers in the network are connected with one another. It functions without any form of router or central hub. Instead of sharing one common server, all the computers in the ad hoc mode can access directly the files and resources in the other computers.

Wireless network comes with various advantages when it comes to hardware components. You can easily mix up wired network components like switches to a wireless network in case you require more number of Ethernet ports. In spite of the wireless structure, you are still required to use an Ethernet cable for the purpose of connecting the router of a wireless network with the modem of broadband.

Chapter 9: Network Mode Security

The algorithms of network security have gone through various changes along with upgrades since the year 1990. It has turned out to be more effective and secure in nature. Today, various types of protocols have been developed for the protection of home wireless networks. The most common protocols are WPA, WEP and WPA2. All of these serve a similar purpose but each differs from one another in some aspects. Wireless protocols for security not only helps in preventing unwanted people from connecting to the network but it also helps in encrypting the data which is sent via the airwaves.

WEP

Also known as wired equivalent privacy, it was developed for the security of wireless networks and was accepted as a standard in the year 1999. WEP was expected to offer the same kind of security level just like wired networks but there are various issues in security in this protocol. It is very easy to break the security and is also very hard to configure the same. Despite all the upgrades which have been applied to WEP, it is still a very vulnerable form of security protocol.

WPA

It is also known as Wi-Fi protected access. It was adopted one year back just before WEP was abandoned. Most of the WPA applications of modern-day use a PSK or pre-shared key which is often referred to as WPA personal and TKIP or temporal key integrity protocol for the purpose of encryption. It uses a server for the purpose of authentication for the generation of certificate and for the keys.

Just like WEP, WPA was also found out to be vulnerable to external intrusions. The attacks which were posed as most dangerous for the protocol were not direct in nature but the ones which were set up on WPS or Wi-Fi protected setup developed for simplifying the linkage between the devices for the modern-day access points.

WPA2

WPA was improved and was made into WPA2. It is also known as Wi-Fi protected access version 2. The major upgrade that this protocol received was the usage of AES or access encryption standard. AES has been approved by the government in the U.S. for the purpose of encrypting data and information.

The main form of vulnerability to a system with WPA2 is when the attacker has complete access to the secured network of Wi-Fi and can also access some of the keys which are required for carrying out the attack on the devices in a network. In WPA2 systems, the security threats are mainly at enterprise levels and are not at all relevant to the home networks. However, attacks via WPS are still there in the WPA2 systems just like WPA.

Which method of security to opt for?

When all the security methods are arranged in order of best to worst it goes on like:

WPA2+AES

WPA+TKIP/AES
WPA+AES
WPA+TKIP
WEP
Completely open network

The best method is to deactivate WPS and then set the wireless router for WPA2+AES. Both WPA2 and WPA are used for securing networks from any form of unauthorized access. In case you leave the system with no form of security, any third party can easily steal bandwidth of the network, perform various illegal jobs with the help of the network, monitor your activity on the web and can easily install malware on the system.

WPA2 is regarded as the best out of all. The only downside that comes with WPA2 is determining the power of processing that the protocol needs for protecting the network. So, it means that super-powerful hardware is required for avoiding lower performance of the network. You should always opt for WPA2 or otherwise WPA in case you have no other option. Using WPA can help in handling heavy loads but when there is heavy load in WPA2 system, it might also affect the network speed.

When it comes to encryption, it will depend on the type of protocol that you are using. WPA2 comes with the fastest speed of encryption and WEP provides the slowest speed of encryption.

Protecting the Wi-Fi network

While it is evident that WPA2 provides more advanced protection than WPA and WEP, the router security depends completely on the password that the user sets. WPA2 and WPA allow a maximum password length of 63 characters. Try to use as many characters as you can for your Wi-Fi password. Hackers always lookout for easy targets. If they are unable to crack the password within minutes they will move on to the next target.

WPA3

WPA3 or Wi-Fi protected access version 3 is the next-gen security protocol for Wi-Fi. It helps in safeguarding the Wi-Fi networks completely and also

saves the users from their own shortcomings in security. WPA3 protects the Wi-Fi network password from dictionary attacks by the implementation of a new key exchange protocol. WPA3 also supports the function of forwards secrecy in which any form of traffic that has crossed the system just before an attacker gained access to the network, remains encrypted which is not the case with WPA2. WPA3 also provides extended security to the public networks that keep the users safe from any form of vulnerability that they cannot realize.

Chapter 10: Circuit and Packet Switching

Circuit Switching

In the process of circuit switching, the network bandwidth or resources are divided into small pieces and a little bit of delay is permanent at the time of establishing a connection. The circuit or path which is dedicated between the sender and the receiver gives out a proper data rate. All forms of data can be transported via the circuit without any form of delay once the dedicated circuit has been established. The system of a telephone network is the best example of circuit switching. Time division multiplexing or TDM and frequency division multiplexing or FDM are the two different methods which are used for multiplexing various signals into one single carrier.

- **FDM:** It divides the network bandwidth into various frames. It is mainly used when various data signals are connected for transmission through a shared medium of communication. It is used for dividing the bandwidth into a number of non-overlapping sub-bands frequencies. Each of the sub-band

frequency carries various forms of signals. It is used in optical fiber along with radio spectrum for sharing various signals of independent nature.

- **TDM:** It divides the network bandwidth into frames. It is used for transmission and receiving of independent signals across a common path of signal with the help of switches in a synchronized manner at every end of the line of transmission. It is used for communication for long-distance links and it can also bear huge data traffic load from the end-user.

Phases of circuit switching

In circuit switching, everything is done in various phases.

- **Establishment of the circuit:** During this phase, a circuit is established directly from the end of the source to the receiver across various intermediary centers of switching. The sender and the receiver both transmit signals of communication for requesting and acknowledging the establishment of the circuits.
- **Data transfer:** After the circuit has been created, voice and data are transferred from the sender to the receiver. The connection stays as long as both the parties want to communicate.
- **Disconnection of the circuit:** Once the transfer of data is finished, the connection is abandoned. The disconnection request rises from either of both the parties. The process of disconnection includes removal of all forms of intermediary links between the sender and the receiver.

Advantages of circuit switching

Circuit switching comes with a wide range of advantages:

- It is best suited for transmission of longer duration. It is possible because a continuous route of transmission is created which remains in place as long as the conversation goes on.
- The dedicated communication path makes sure that there is a steady communication rate.

- There are no forms of intermediary delays after the circuit has been established. So, it is a great option for real-time communication for both data and voice transmission.

Disadvantages of circuit switching

- In circuit switching, a connection is established between two parties. This connection cannot be utilized for transmission of any other form of data, no matter what is the load of data.
- The bandwidth is required to be very high even if the data volume is low.
- The total time which is required for establishing a connection is high.
- The system resources are underutilized. After the resources have been allocated for one particular connection, the resources cannot be utilized for any other connection.

Packet Switching

It is a method which is used for transferring the required data to the network in the form of packets. The data which is meant for transmission is broken down into smaller pieces called packets. This is done for ensuring that the file is transferred fast and in an efficient manner directly across the network and also for minimizing and latency in transmission. All the small data packets are reassembled after reaching the destination. A packet is composed of payloads along with several information of control. For this, there is no need for reservation or pre-setup of the resources.

The whole process of packet switching uses the technique of store and forward at the time of packet switching. While the packets are forwarded, each of the packets is stored first and is then forwarded. This whole technique is very important as the data packets might get discarded at any of the hops due to any form of reason. There can be more than one single path in between the source and the destination. Each of the data packets comes with the addresses of both the source and the destination and thus the packets can travel independently across the network. In simple words, data packets of the

same file might or might not travel along the same path. In case of any form of congestion at any of the paths, the packets can choose some different path over the existing network.

For overcoming the all over weaknesses of the circuit-switched network, packet-switched network was developed. This is mainly because the circuit-switched networks are at all effective for messages of smaller size.

Advantages of packet switching

Packet switching comes with various advantages over circuit switching.

- It is more efficient when it comes to the bandwidth of a network. It is because there is no concept of circuit reservation in packet switching.
- There is very less latency in transmission.
- It is of more reliable nature as the destination is capable of tracing out the missing packet.
- It is more tolerant of faults as the packets can choose any other path if there is any congestion in the path.
- It is very cost-effective and is also cheaper when implemented.

Disadvantages of packet switching

- The packets are not delivered in proper order but in circuit switching the packets are delivered in an orderly manner as all the data packets travel through the same circuit.
- As the packets travel unordered, each of the packets needs to be provided with a sequence number which is time-consuming.
- The complexity arises at the nodes as the packets can follow several paths.
- There is delay in transmission because of rerouting of the packages.

- It is not at all suitable for heavy load and is best for small messages.

Packet switching and its modes

- **Connection oriented:** Before the transmission starts, it helps in establishing a virtual connection or logical path with the use of signaling protocol. The path is established in between the sender and the receiver and all of the packets which are part of this flow will follow this established path. Virtual circuit ID is given out by the routers or switches for unique identification of the virtual connection. All of the available data is divided into various smaller units and the units are affixed with a sequence number. In this, three phases work together: setting up, transferring of data and tear down phase. The information regarding address is transferred only during the phase of setup. After the destination route has been figured out, entry is added up to the table of switching for each of the intermediate nodes. At the time of data transfer, the local header or packet header might contain other information like timestamp, length, sequence number and many others. It is of great use in switched WAN.
- **Connectionless switching of packet:** In connectionless packet switching, each of the data packets contains all the relevant and important information like destination address, source address, port number etc. which is not the case with connection-oriented packet switching. In this form of packet switching, all the data packets are treated in independent form. All the packets which belong to one flow might also take up different paths as the decision of routing is completely dynamic in nature. So, the data packets after arrival might not be in proper order.

Types of delay in packet switching

- **Transmission delay:** It is the time which is taken for putting a

data packet into the link. It completely depends on the packet length along with the network bandwidth.

- **Propagation delay:** It is the time which is required by the bits for reaching the destination from the origin. It depends on propagation speed and distance.
- **Queuing delay:** It is the time that one job waits in the queue for getting executed. It is dependent on network congestion. It is the difference in time when the destination received the packet and when the data packet was executed.
- **Processing delay:** It is the time which is taken by the routers for processing the packet headers. The packet processing helps in the detection of bit-level faults that takes place at the time of packet transmission to the destination.

Chapter 11: Connection Between the Network Devices

For the purpose of connecting to a network, the computer systems need to have certain components for a seamless connection. Without such components which include IP address, subnet mask, DHCP and many others, it will not be possible for the system to connect with a network. Each system comes with its unique set of components that helps in establishing a new connection.

IP Address

The IP address or Internet Protocol Address is the number of identification for the network hardware which is connected with the network. When your system has an IP address, it can communicate with all the other devices across a network based on IP address such as the internet. Most of the IP addresses look like 123.121.52.141.

What is the use of an IP address?

The IP address helps in providing a unique identity to the devices in a networked structure like the internet. It is somewhat similar in nature to your home or business addresses which helps in the delivery of supplies to a particular location that comes with an address which is identifiable. All the devices on a network can be differentiated from each other with the help of IP addresses. When you want to send a gift or package to one of your friends who live in a foreign country, you need to know the exact location of your friend. This same process is being sued for sending data across the internet. However, in place of using a physical form of mailing address, the computer systems use DNS servers for looking up at a hostname in order to find out the IP address.

For example, when you want to browse a website by entering the URL of the respective website such as www.google.com, your request for loading the page is sent over directly to the DNS servers which find out for the hostname for google.com for finding out the related IP address. Without the presence of a proper IP address, your computer will be having no clue that what are you up to.

IP address and its versions

IP address comes in two different versions: IPv4 or internet protocol version 4 and IPv6 or internet protocol version 6. IPv4 is the older version of IP address whereas IPv6 is the latest and the upgraded version.

- **IPv4:** IPv4 addresses are constructed in such a way so that it capable of providing about 4 billion IP addresses which are all unique in nature. Although it comes with a huge number of addresses, it is still not enough for the modern world of today with various types of devices being used on the web or internet.
- **IPv6:** IPv6 can support 340 trillion, trillion and trillion addresses which come out like 340 along with 12 zeros by its side. It means that each and every person on the Earth will be able to connect a billion numbers of devices with the internet.

One of the reasons why IPv4 is being replaced by IPv6 is that the latter one

provides more number of IP addresses when compared to the former. When various devices are all connected on the similar network, it is very important for each of the devices on the network to have a unique address of its own. IPv6 also comes with a wide number of added benefits over IPv4:

- There is no collision of IP addresses which is caused by the private addresses
- It comes with auto-configuration feature.
- There is no need for NAT or network address translation.
- It comes with an efficient feature of routing.
- The administration of the IP addresses is very easy.
- It comes with in-built privacy for the IP addresses.

In IPv4, the IP address is displayed as a 32-bit number which is written in the format of decimal such as 210.251.165.40 or also 192.251.1.1. As in IPv6, there can be trillions of possible IP addresses, it is written in a hexadecimal format such as 3gge:1500:6565:4:100:f7ff:fe31:97cf.

IP addresses and its types

There are various types of IP addresses that can be found. While all forms of IP addresses are constructed of letters or numbers, not all of them are being used for the same function. The types of IP addresses are private IP address, public IP address, static IP address and dynamic IP address.

- **Private IP address:** This form of IP address is generally used inside one network such as any form of a home-based network which is used by Wi-Fi cameras, mobile devices, desktop PCs and wireless printers. This type of IP address allows the devices to communicate with the central router along with other devices which are based on the similar home network which is private in nature. This type of IP address can be configured manually or it can also be assigned automatically by the network router.
- **Public IP address:** This type of IP address is used for the outside area of a network and it is assigned by the internet service provider or ISP. It is the prime address which is used by

the business or home networks for communicating with the other networked devices all over the world. It helps by providing a path for the home-based devices to reach the ISP and therefore with the world outside as well. It allows the devices in a network to access various websites and also to communicate with the rest of the computers directly along with other servers all over the world.

Both these types of IP addresses are either static or dynamic in nature which means that they change either or not. The IP address which has been assigned by the DHCP server is known as a dynamic IP address. In case a device is not having DHCP server enabled or if it does not support DHCP, the IP address needs to be manually assigned and in such case, the IP address is called static IP address.

Dynamic IP Address

A dynamic IP address is the one which is assigned automatically to every node in the network like desktop PC, smartphone or tablet. This automatic assigning of the IP address is done by the DHCP server. An IP address which has been assigned by a DHCP server is known as dynamic as it will be changing in the future depending on the future connections with the network.

Where to find dynamic IP addresses?

The public IP address which is assigned for the router for most of the business and home network users by the internet service providers or ISPs is dynamic in nature. Bigger organizations and companies try not to connect with the internet with the use of IP addresses which are dynamic in nature and prefer using static IP addresses which are assigned specifically for them.

In any form of a local network like the one in your business place or home, where private IP addresses are used, most of the devices are pre-configured for DHCP. This means that all such devices use a dynamic IP address. In case the devices do not have DHCP enabled, each of the devices is required to manually set up the network information.

Dynamic IP address and its advantages

One of the prime advantages that come with assigning of IP addresses dynamically is that it is more flexible in nature. It is very easy to set up and the administration part is also easier when compared to static IP addresses. For instance, when one of your devices connects with the network, it is assigned with one specific IP address. Once the device disconnects from the network, the same IP address becomes free and it can be used for another device that can connect afterwards, even if it is not the same device again.

Dynamic IP addresses come with little limitation to the total number of devices which can connect with the network as the devices which do not require to stay connected can easily disconnect from the network and thus freeing up the available pool of IP addresses for the other devices. There is an alternative in which the DHCP server can pre-configure some specific IP addresses for each of the devices in a network in case all of the devices want to get connected with the network at the same time. In such case, hundreds of networked devices, whether they were being used by the users or not can have their own specific IP address which can easily limit network access for all the new devices in a network.

The implementation process of dynamic IP addresses is easier when compared with the static IP addresses. There’s no need to set up anything manually for the new devices which want to connect with the network. All that you need to do is to be sure that the DHCP has been enabled on the network router. As all the networked devices are by default configured to have a specific IP address for each from the huge pool of available IP addresses, each and every step turns out to be automatic in nature.

Dynamic IP address and its disadvantages

It is a very common thing which is acceptable technically as well for any form of a home network to use a dynamic IP address which has been assigned by the DHCP server for the router, problem comes up when the user tries to access the same home network from any other outside network.

Static IP Address

A static IP address is the one which has been manually configured for a

networked device in place of the one which was assigned by DHCP server. The name static IP address means that the IP does not change and is static in nature. It can be regarded as the complete opposite of a dynamic IP address which changes. Phones, tablets, laptops, routers and other forms of network devices which uses IP address can be easily configured for having a static form of IP address. This can be done by the device which gives out the IP addresses such as a router or also manually by typing the device IP address into the device only.

Why does static IP address needs to be used?

You can think of static IP addresses just like your physical home address or your email address. Such addresses do not change and they are static in nature. It helps in contacting with people or finding someone. Similarly, IP addresses of static nature are very beneficial when you are hosting a website from your home, having a file server in the network, forwarding network ports to some particular device, using networked printers, using any form of remote access program or running a printing server. As static IP addresses never change, all the other devices in a network will know how to connect with a device which uses IP address of static nature.

For example, when IP address which is static in nature is set up for a PC within a home network, once the device gets a particular IP address for itself, the network router can be configured in a particular way for forwarding all the inbound requests to that device directly, like requests for FTP in case the device can share files over FTP.

If you are hosting a website and not using a static IP address for the same, it might turn out to be a hassle. This is mainly because when the computer gets some new IP addresses, you need to change the settings of the router every time for the purpose of forwarding the requests to the new IP addresses. When you neglect to do so, anyone can get inside your website as the router will be having no idea about which device within the network is serving solely for the website.
Another great example of an IP address of static nature at work is the DNS server. The DNS servers always use static IP addresses for making sure that the devices in the network know exactly how to connect with the servers. If they were regularly changed, you would also have to reconfigure the DNS

servers regularly on the router for using the internet.

The static form of IP addresses is also very useful when the domain name of the device is not accessible. Those computers which connect with the file server within a workplace network could also be set up for instance with the server by using the static IP address of the server in place of the name of the host. Even if there is malfunctioning of the DNS server, the computers in the network can still access and connect with the file server as they communicate with the server by using the IP address. With applications which support remote access like the Windows Remote Desktop, using an IP address of static nature means that the user can access the computer always by using the same address. When you use an IP address which changes frequently, you need to know what it has changed to so that the new address can be used by you for establishing the remote connection.

Disadvantages of static IP address

One of the major disadvantages that come with static IP address when compared with a dynamic IP address is that all of the devices in a network are required to be manually configured. All forms of home-based web servers along with programs of remote access requires setting up the devices with a particular IP address and also configure the same properly with the router in order to communicate with a particular address. This comes with more amount of work than just plugging in the router and then allowing it to give the dynamic IP address via the DHCP servers.

In case a device has been assigned with an IP address like 192.168.1.10, and you are going to a completely new and different network which gives out the address as 10.x.x.x, you will not be able to connect with your static IP address. The device will require to be configured again for the purpose of using a DHCP server or for using an IP address of static nature that will work well with the new network.

Security can also be regarded as another downfall when a static IP address is being used for a device. When an IP address is used which is never changed, it will give the attackers much time for finding out various vulnerabilities

within the network of the device. The only alternative would be to use an IP address of dynamic nature which changes and thus it will also make the attackers to change the way in which they communicate with that device.

Static IP address vs. Dynamic IP address

A dynamic IP address is exactly the opposite type of IP address than the IP address that never changes. Dynamic form of IP address is like any regular IP address just like static IP, but the dynamic IP is not tied with the device permanently. Instead of using one IP address for a lifetime, the dynamic IP addresses are used only for a particular time frame and then it returned to the pool of IP addresses so that the same can be used by the other devices in the network.

Dynamic IP addresses can outnumber in case of benefits when compared to static IP address. In case if an ISP kept on using static IP address from all its customers, there will be shortly a limited IP address supply for all the new customers. Dynamic IP addresses provide with the solution in which one IP address can be reused by some other device when it is not being used by any other device. Thus, providing access to the internet for more number of devices than it would have been possible with static IP address.

The static form of IP addresses come with limited downtime. While the dynamic form of addresses obtains a new IP, the user who is connected with the existing IP address is removed out of the connection and else has to wait for finding any new address. This will not be a recommended setup while you are going to a website, service of file sharing or online game, all of these will be requiring active connections constantly.

In case of any local network such as in place of business or in home, where you generally use an IP address of private nature, most of the devices in such network are configured for DHCP. Thus, all the devices use dynamic form of IP address. The public form of IP address which is assigned to the routers of the business or home-based network is dynamic in nature. Large-sized companies do not use the dynamic address for connecting with the internet. Instead of dynamic addresses, they use static IP address which is assigned to them.

How can you get a static IP address?

Some of the routers of today already reserves and IP address for the devices which are connected with the network. This process is generally done with the help of DHCP reservation and it performs by linking a specific IP address with the MAC address so that every time that device requests the router for IP address, the router can assign it the one which has been already chosen by the user with that particular MAC address. When you want to get a static IP address for your business or home network, you can do it by contacting your ISP but this option varies depending on the company that provides you with the internet. Having a static IP address for home-based and other local network is quite expensive when compared with getting a dynamic IP address.

Faking static IP address by using dynamic IP address

As getting a static IP address for your home or business network might turn out to be very expensive than a regular dynamic address, the best option is to opt for both forms of IP addresses by using dynamic DNS service or DDNS. The service of DDNS associates a changing form of a dynamic IP address with the hostname that does not change as well. It is exactly like having your very own static form of IP address without even paying anything extra than a dynamic IP address.

No-IP is an example of a free DDNS service. You can use this for redirecting your required hostname for associating with the present IP address. In simple words, if you are having a dynamic IP address, you can access the network by using the exact same hostname. DDNS service is very helpful when you are required to access the home-based network remotely but you do not want to pay more for static IP. You can also host your personal website from your home and use up DDNS for ensuring that the visitors of your website can have access to the network any time they want.

DHCP Server

A DHCP server is nothing but a server of the network which provides and assigns the IP addresses automatically along with default gateway and various other parameters of a network for the devices of the clients. It is dependent on the standard protocol which is called DHCP or Dynamic Host

Configuration Protocol for responding to the queries of the clients regarding broadcasting. The DHCP servers send out necessary parameters of the network automatically for the clients for establishing proper communication with the network. Without the presence of a DHCP server, the administrators of a network need to set up manually each and every client who joins with the network. This might turn out to be a cumbersome process, especially when large networks are involved. The DHCP servers assign each of the clients with one unique IP address of dynamic nature.

Benefits of DHCP server

A better option than using DHCP on the switch or router is to have a centralized server of DHCP. This is true in case of network environments which requires support from both DHCP for IPv4 and DHCO for IPv6, both at the same time. DHCPv6 comes with various benefits.

- When you have DHCPv6 server which is also integrated into the system of IPAM for IPv6, it will provide you with the visibility of all the client nodes of IPv6.
- The DHCP servers also provide management and logging of interfaces which aids in managing the scopes of the IP addresses by the administrators.
- DHCP servers also provide high availability along with redundancy. In case one of the DHCP servers fails to perform, the clients in the network will be preserving their present IP addresses and will not lead to any form interruption for the nodes at the end.

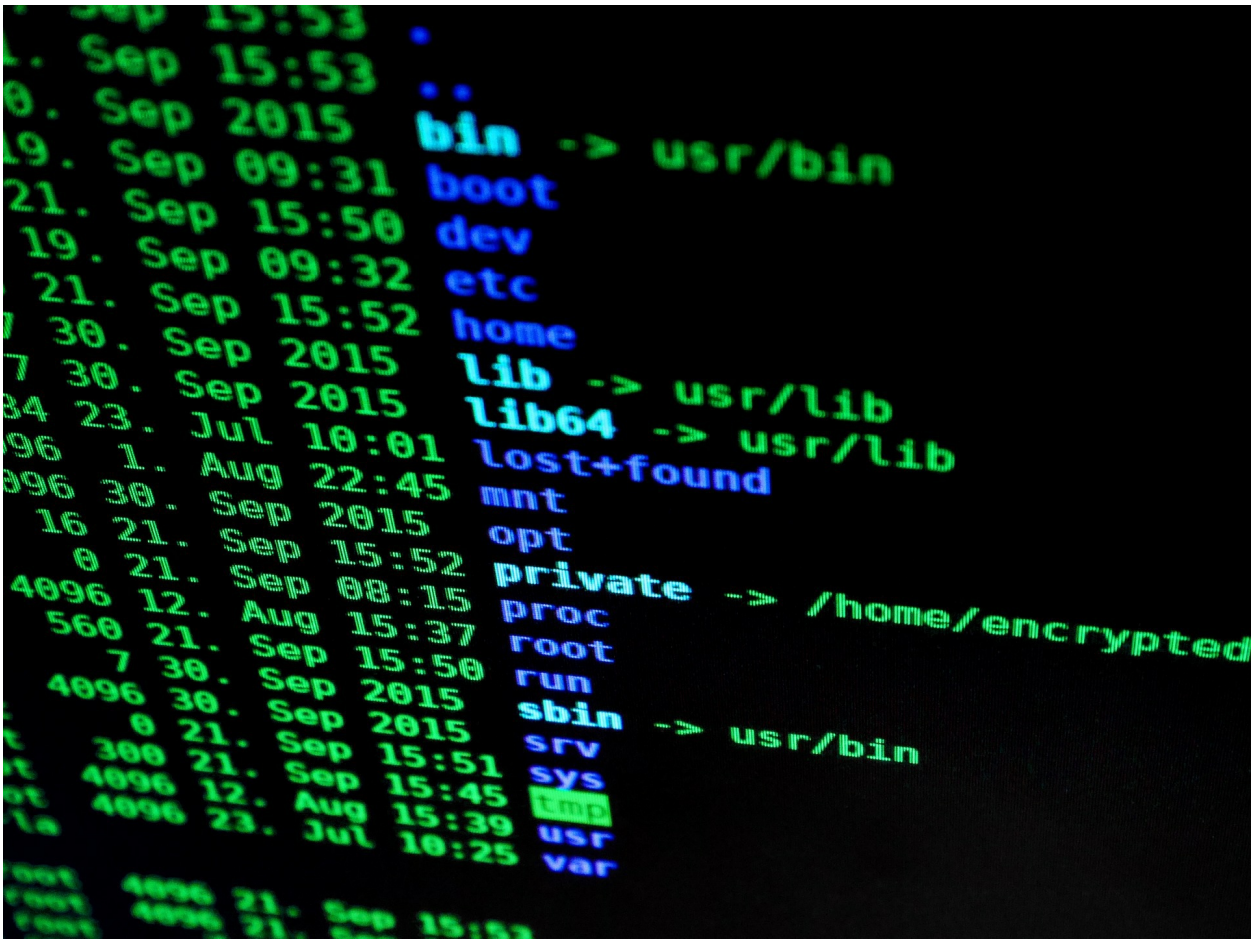
Why should you use a router as DHCP server?

Most of the switches and routers have the capability of providing the following server support for DHCP:

- DHCP client and obtaining an IPv4 address interface from an upstream service of DHCP.

- One relay of DHCP along with forward UDP DHCP messages from the clients directly on a local area network to and from a server of DHCP.
- Running DHCP server on switches and routers consumes all the resources which are available on the device network. Such packets of DHCP are handled by software.
- Does not need the support of dynamic DNS. The switch or router DHCP server will not be able to create an entry into the DNS on part of the client which is based on IPv4 address which was leased for the client.
- No form of redundancy or high availability of the bindings of DHCP. This might result in some serious form of problem if the present DHCP along with the default gateway fails together.

The organizations which have started the implementation of IPv6 need to migrate to the DHCP for IPv4. This change in DHCP will also point out that the organization also wants to have DHCP for operating both the protocols.



Chapter 12: Background and History of TCP/IP

TCP/IP is a protocol set which enables the communication between various computers in a network. Protocols are nothing but the standards or rules which help in governing communications. When two devices in a network want to communicate with each other, both need to use the same protocol. This can also be compared to the communication of human beings. A person who speaks French will not be able to communicate with a person who speaks Chinese as both of them speak different languages. You have the option of selecting from a large pool of network protocols for using in the network. But, when it comes to TCP/IP, it is regarded as the industry standard. All forms of operating systems support TCP/IP. The whole internet works on TCP/IP. It is also called the language of the internet. In case you want a computer to communicate with the internet, you are required to use TCP/IP.

History of TCP/IP

Just before the internet of today, there was ARPAnet. It was created by ARPA or Advanced Research Projects Agency. It was launched at the time of the Cold War in 1969. ARPAnet was created as a response to the rising threat of nuclear attack from the Soviet Union. ARPA's main goal was to create a network which would be fault-tolerant and would enable the leaders of the U.S. military to stay in touch in case of a nuclear war. The protocol which was used for ARPAnet was known as the NCP or Network Control Protocol. As ARPAnet grew in size, another protocol was also required as NCP was unable to meet the growing needs of a large-sized network.

In the year 1974, a paper was published describing the features of TCP or Transmission Control Protocol. NCP was eventually replaced by TCP. After further development and testing of the new language, it led way to a brand new set of protocols which was called TCP/IP or Transmission Control Protocol/Internet Protocol. It was finally in the year 1982 when TCP/IP replaced NCP as the standard language for ARPAnet.

Features of TCP/IP

TCP/IP has been in the industry for more than 35 years. It a proved set of protocols that make it possible for the devices to connect with the internet. It comes with various features that make communication much more easier.

- **Support of multi-vendor:** TCP/IP is being implemented by several software and hardware vendors. It has been now a standard of the industry and is not at all limited to a particular vendor.
- **Interoperability:** Today, people can work in a network which is heterogeneous in nature only due to TCP/IP. While you are using a computer which runs on Windows OS, you can still download your required files from a machine that runs on Linux. This is possible only because both the systems support TCP/IP. It helps in eliminating the boundaries of cross-platform.
- **Logical addressing:** Each and every adapter of the network comes with a unique physical address which is permanent in nature. This permanent address is known as MAC address, also known as the hardware address. This address is being burnt into

the hardware card at the time of manufacturing. The protocols which are low-lying in nature and are hardware conscious on LAN delivers the packets of data with the use of the physical address of the adapter. The local adapter present in each computer tracks each and every transmission on the LAN for determining whether the message has been addressed to its very own physical address.

For a small-sized LAN, this whole thing works very well. But, when a computer is connected with a very large network just like the internet, it will need to listen to billions of transmissions every second. This might result in the failure of the network connection. For avoiding such cases, the administrators of the networks divide the big networks into various smaller networks with the use of devices like routers for reducing the network traffic. It makes sure that the unwanted traffic from any network will not create any kind of problem in some other network. The administrators can again subdivide a network into subnets for efficient travelling of the message directly from the sender to the receiver. TCP/IP comes with great capacity of subnetting which is achieved with the help of logical addressing. The address which is configured by the network software is called the logical address. TCP/IP uses a system of logical addressing which is known as the IP address.

- **Routability:** A router is a device of the network infrastructure which is capable of reading the information of logical addressing and then directs the data through the network right to the destination. TCP/IP is a routable kind of protocol. This means that the data packets of TCP/IP can be easily moved from the segment of one network to another.

- **Flow and error control:** TCP/IP comes with various features that make sure that the data is delivered from the source to the destination reliably. Transmission Control Protocol or TCP also checks many of the error checking and flow control functions along with functions of acknowledgement.

Chapter 13: FTP – File Transfer Protocol

FTP which stands for file transfer protocol is a technique of sending files online. It acts as an application layer protocol which helps in moving the files between the local file system and remote file system. It functions on top of TCP such as HTTP. In order to share a file, two connections of TCP arranged parallel are used by the FTP: data connection and command connection.

FTP belongs to the oldest set of protocols which are still used today. It is a very convenient way of moving your files around. The server of FTP provides all-round access to any directory along with the sub-directories. The users can connect with all these servers with the help of FTP client. FTP client is a software which allows the users to download their required files right from the server and also upload files to the same server. If you are a normal internet user, you will not be requiring FTP. But, in case you are building a full website, it is a very important tool.

What is FTP used for?

FTP is useful for moving of information from the system on which you are working to the server where the website is being hosted. For example, if you want to install WordPress on a server, you need FTP for copying over the files. It is also used as a tool for sharing files. You can upload a document or file on the server of FTP and then share the file link with the person you want. However, this service is not much common today as people prefer cloud file transfer services rather than FTP file sharing. There are various people who prefer to upload their files on the home server and they need to enable FTP for such service.

FTP uses two very basic types of channels: the command channel which carries all relevant information about the task and the data channel which transfers the files between the devices.

- **Command channel:** It is used for sharing all information of controls like the identification of the user, password, commands for changing remote directory, commands for retrieving and storing the files etc. The command channel is started on the port number 21.
- **Data channel:** For the purpose of sending the data file in actual, FTP uses a data channel. It is started at the port number 20.

FTP sends out the information of control out of band because it utilizes a completely separate command channel. Some of the protocols also send in request along with the header lines with the data in the same connection of TCP. That is why FTP sends out control information in the form of bands.

The FTP connection can also function in active and passive mode. Active mode is the most common of all and it allows an open form of communication in between the device and the server over both the channels. In this form of connection, the server assumes the active function for establishing a connection after approval of data requests. However, the active mode can be disrupted easily by the firewalls. So, in such cases, passive mode comes into play where the server attends the connection but doesn’t maintain the connection actively and thus allowing all the devices in that network to perform all the tasks.

FTP session

When a session of FTP starts between the server and the client, the client starts a controlled TCP connection along with server side. The client uses this for sending out information on control. After the server receives this information on control, it starts a connection of data directed to the side of the client. It is to be noted that it is possible to send only one file over one single data connection. However, the connection of control stays active throughout the session of the user. HTTP is stateless in nature which means it does not require to keep detailed tracking of the state of the user. But, in the case of FTP, it is required to maintain the user state all throughout the session.

Data structure in FTP

In FTP, three types of structured data are allowed:

- **File structure:** In this, there is no form of internal structure. The file in this structure is regarded as the continuous sequence of the data bytes.
- **Record structure:** In this, the data files are composed of records in sequence.
- **Page structure:** In this, the data files are composed of indexed pages of independent nature.

Is FTP secured in nature?

No, FTP is not at all secured by its design. FTP is from that time when cyber security was only a study of hypothetical field. In simple words, the transfers made using FTP are not in encrypted format. So, anyone who is capable of sniffing data packets can easily intercept the files. That is the reason why people turn towards FTPS rather than FTP. FTPS works exactly in the same way just like FTP but it helps by encrypting every data files so that the prying eyes cannot read the files even if they intercept the files.

Chapter 14: Remote Login

Remote login, also known as remote access, is the technique which is being used for accessing a system of computers like office network computer or home computer from a location which is remote in nature or is much away from the physical location of the system. This technique allows the office employees to keep up with their work offsite, like at their home or at any other place, while still accessing a network or computer at a distance, for example, office network. Remote login or access can be easily set up with the use of LAN or local area network, WAN or wide area network or even with the help of VPN or virtual private network so that all the systems and resources can be accessed from a remote distance.

Remote login can be created through a line which runs in between the computer of the user and an organization’s or company’s LAN. It is also possible to establish a connection between the LAN of a company and a remote LAN by the use of a dedicated line. This form of lines provides great speeds but also has the drawback of being very expensive. Another way of establishing remote login connection is by the VPN. VPN is a network which uses the internet for connecting with the remote sites and also the users together. This form of network uses encryption and also tunneling for the purpose of accessing the network of a company. This might turn out to be the

best choice for those organizations which are small in size.

There are other means for establishing remote login that includes the using of wireless network, integrate services, cable modem, digital network or digital subscriber line. For the purpose of establishing a remote login connection, both the remote computer or server and the local machine needs to have software of remote-access. There are various service providers that can be found today which provides remote access services via the internet.

Remote desktop software

One of the most sophisticated forms of remote login is remote desktop software. It allows the user of one computer to interact and see the actual desktop interface of another system. For setting up remote desktop access, both the computers, i.e. the computer of the client and the computer of the server need to be configured on the remote desktop software for establishing a connection. After being connected, the software opens up a window directly on the host computer which contains the view of the client's desktop.

The client computer can also maximize the window of the program for taking up the complete screen which will depend on how the software works on both the systems and what is the screen resolution of both the screens. The latest versions of Windows OS offer users with Remote Desktop Software which is only available for those computers which are running on either Enterprise, Professional or Ultimate version of the OS. When it comes to Mac, the Apple Remote Desktop Software is designed only for the business networks and the users are required to buy the same separately. The ecosystem of Linux offers users with various types of solutions regarding remote desktop.

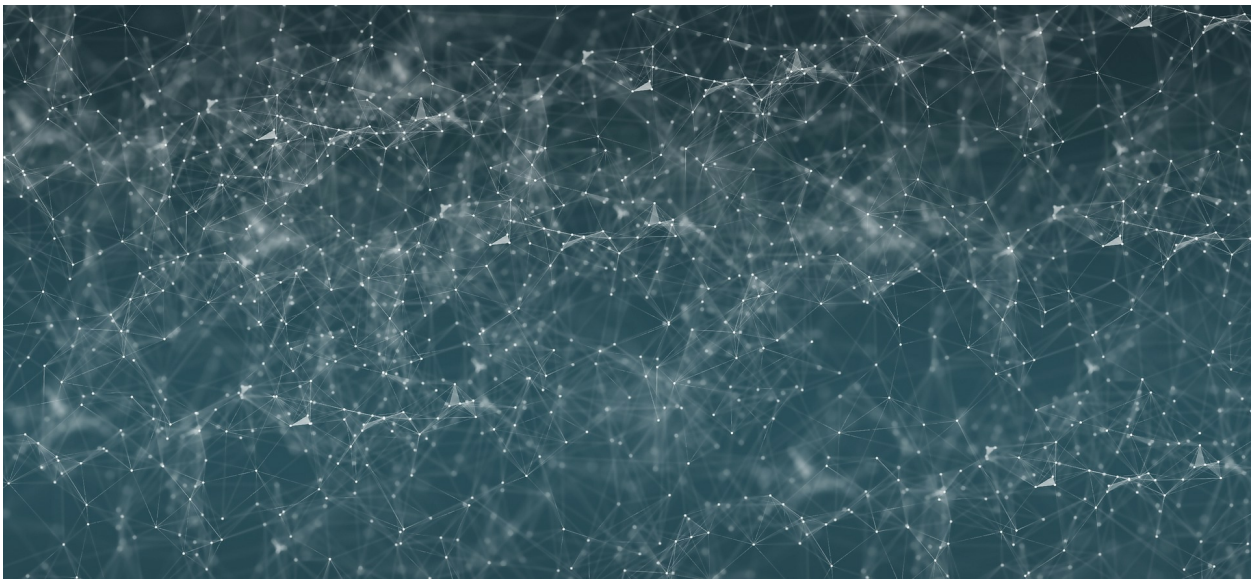
However, there are various types of remote access programs which are non-native in nature which the user can install on their system and then use the same in place of the desktop tools which comes built-in. Most of them function absolutely in the proper way in most of the OS of today. Many of the remote desktop solution today rely on the technique of virtual network computing. The packages of software which are based on virtual network computing works across various OS.

Remote accessing of files

The basic remote login software allows access of files on the system that can be read and also written on the system of the client. The technology of virtual private network offers remote login and functionality of file access across WAN. For a VPN to function properly, the client software is required to be present on both the systems. The client/server software which is based on SSH protocol can be used as an alternative to VPN for remote access of files. SSH offers an interface of command line to the system of the target. The task of sharing files within a local area network such as within home is not actually considered to be an environment of remote access even if it is actually remotely accessing the system of other device.

Is using remote desktop safe?

All the programs which are used for connecting remotely to your computer are most of the times safe. But, like all other software, there are some which go through some malicious process for the purpose of information stealing, installing malicious programs on another system, deleting important files and many others. In order to make sure the security of your system, try to disable those programs of remote desktop which you no longer use. You can also disable some of the functionalities of the program. You can easily disable remote desktop in Windows along with other OS.



Chapter 15: Networking In Detail

Computer networking functions with various components and systematic parts, all of which functions together for making the connection to a network a successful one. Let’s have a look at some of the primary components of networking.

Protocols

Network protocols help in defining the various conventions and rules for the purpose of communication between various devices in a network. The protocols of networking include various mechanisms for all the network devices for identifying and making connections with one another along with formatting the rules which help in specifying how the data is going to be packaged into received and send messages. Some of the network protocols also support compression of data and acknowledgement of the message which is designed for the high performing and reliable form of network communications. The network protocols incorporate all the constraints and requirement of processes for the initiation and accomplishment of communication between the routers, computers, servers and other devices which are network-enabled. The network protocols need to be confirmed as well as installed by both the sender and the receiver for ensuring data or network communication.

The modern network protocols use generally the techniques of packet

switching for sending and also receiving messages in the form of data packets. Data packets are nothing but subdivided messages which are broken into pieces. The data packets are collected at the destination and then reassembled for getting the complete message. There are various types of network protocols which have been developed and designed for some specific functions in specific environments.

Internet Protocol

IP or the internet protocol family is composed of a set of related protocols of networking. Besides having internet protocol itself, there are also various higher class protocols such as UDP, TCP, FTP and HTTP. All such protocols integrate with the internet protocol for the purpose of providing many more added capabilities. There are some lower-level internet protocols as well such ICMP and ARP which coexists within the family. The higher-level protocols which belong to the family of IP have much closer interaction with the applications such as web browsers. The lower-level protocols interact with the adapters of a network along with some other hardware of the computer.

Wireless Network Protocols

The wireless networking system now has turned out to be commonplace which is mainly because of Bluetooth, Wi-Fi and LTE. There are wireless network protocols that check the functioning of wireless networks. The network protocols which have been designed for the purpose of wireless networking needs to support roaming in mobile devices and also deal with various issues like network security and variable rates of data.

Network Routing Protocols

The network routing protocols are the specially designed protocols which have been designed to be used specifically for the network routers. A network routing protocol is capable of identifying several other routers on the network, manage the destination of the messages of a network, manage the message pathways which are called routes and also makes dynamic decisions on routing. Some of the most common protocols of routing include OSFP, EIGRP and BGP.

TCP or Transmission Control Protocol

The TCP or Transmission Control Protocol is regarded as the core protocol of the IP suite. It originates in the implementation of a network in which it has complemented the IP. So, the entire suite is also known as TCP/IP. TCP helps by providing a reliable system of delivery of octet streams over the network of IP. The main characteristics of TCP include checking of errors and ordering. All the major forms of internet-based applications like email and the World Wide Web along with file transfer relies on TCP.

How are networking protocols implemented?

Most of the modern operating system of today comes with in-built software services which help in implementing support for some of the network protocols. Various applications such as web browsers come with software library which supports high-level protocols when needed by the application for functioning. For some of the lower level protocols of routing and TCP/IP, the support is being implemented directly within the hardware for improving the overall performance.

Each of the data packets which are transmitted and received by the destination over the network consists of binary data, zeros and ones which helps in encoding the message contents. Most of the protocols of networking add up small header at the starting of every data packet for the purpose of storing information about the sender of the message along with the intended destination. Some of the protocols also add up footer at the very end of data packets. Each of the network protocols comes with the capability of identifying all the messages of its own form and then process the header along with footer as parts of the moving data across the devices.

A large group of protocols related to networking which functions together at both the higher and lower levels is known as protocol family. Some of the most common protocols which are used are HTTP with default port 80, FTP with default port 20/21, SSH with default port 22, Telnet with default port 23 and DNS with default port 53.

Layers of the OSI Model and Its Functions

The OSI model or the Open System Interconnection model is an architecture of 7 layers in which every layer performs some specific function. All the layers work in close collaboration for the purpose of transmitting data from one system to the other all around the globe.

- **Physical Layer:** The layer at the bottom of the OSI model is the physical layer. It performs the duty of establishing an actual physical connection between the concerned devices in a network. All the information in the physical layer is stored in the form of bits. At the time of receiving the data, the physical layer receives the signal and then converts the same into 1s and 0s. It is then sent to the layer of data link which puts back the frame together. Functions of the physical layer are:

    1. **Bit synchronization:** This layer helps in bit synchronization by providing a clock. The clock provided by the physical layer is responsible for controlling both the sender and the receiver and thus provides synchronization at the level of bit.
    2. **Bit rate control:** This layer is also responsible for defining the rate of transmission which is the total number of bits sent out every second.
    3. **Physical topology:** This layer determines the way in which all the nodes and devices are going to be arranged in the network which are star, bus and mesh topology.
    4. **Transmission mode:** This layer determines how the data is going to flow in between the connected devices. The possible modes of transmission are: simplex, full-duplex and half-duplex.

- **Data Link Layer:** This layer is the second layer right above the physical layer. It is responsible for message delivery from node to node. The primary function of the data link layer is to make sure that the transfer of data is absolutely free from errors while travelling from one node to the other, right over the 1st layer i.e. the physical layer. After a packet has arrived in a network, it is the duty of this layer to transmit the same to the host by using its

MAC address. The data link layer is being divided into two layers: Logical Link Control and Media Access Control.

The packet which is received from the network layer is then divided into frames which depend on the size of the Network Interface Card or NIC. This layer also encapsulates the MAC address of the sender and the receiver in the data header. The functions of the data link layer are:

1. **Framing:** The main function of the data link layer is framing. It provides the sender with a way for transmitting a set of bits which are meaningful for the receiver. This is achieved by the attachment of special patterns of bits right at the beginning of the frame and at the end.
2. **Physical addressing:** After this layer is done with the job of framing, it adds physical addresses also known as MAC addresses for the sender or of the receiver in the frame header of each.
3. **Error control:** This layer comes with the mechanism of controlling errors in which errors are detected and the lost or damaged frames are retransmitted.
4. **Flow control:** The rate of data needs to be constant on both the sides otherwise the data might result in getting corrupted. So, with the help of flow control, the data amount is coordinated which can be sent before receiving the acknowledgement.
5. **Access control:** When a single channel of communication is being shared by various devices, the sub-layer of MAC in the data link layer helps in determining which device has the control of the channel at some given time.

- **Network Layer:** This layer functions for transmitting data from one host to another which is located in some other network. The network layer also looks after packet routing which means it helps in selecting the path which is the shortest of all for the purpose of transmitting the packet, from the total number of

routes which are available. The network layer also places the IP addresses of the sender and the receiver in the header. The functions of the network layer are:

1. **Routing:** The protocol of the network layer determines that which route will be the best for the packet from the source to the destination. This function performed by the network layer is called routing.
2. **Logical addressing:** For the purpose of identifying each of the devices on the internetwork in a unique way, the network layer helps by defining a scheme of addressing. The IP address of the sender and the receiver are placed in the header which helps in distinguishing each and every device in a unique and universal way.

- **Transport layer:** The transport layer helps by providing all the required service to the application layer and also takes up services from the network layer. Segments are those data which are present in the transport layer. It helps in end to end message delivery. This layer is also responsible for providing the acknowledgement after successful transmission of data and also re-transmits any data if any form of error is found.

At the sender side: The transport layer receives the data which has been formatted from the layers above it and performs segmentation. After segmentation is done, it also implements error and flow control for ensuring that the data is transmitted properly. It also adds up port number of the sender and the receiver in the header and then forwards the data which has been segmented to the network layer. The sender of the data needs to have the port number which is associated with the application of the receiver. The destination port number is generally manually configured or is configured by default. For example, when any web application sends any request to the web server, it uses the port number 80 because it is the port number which has been assigned for the web applications by default. Many of the applications come with default assigned port number.

At the receiver side: The transport layer reads up the number of a

port from the header and then forwards the packet of data which it has received for the respective application. This layer also performs reassembling and sequencing of the data which is segmented.

Functions of the transport layer:

1. **Segmentation:** The transport layer accepts the sent message from the session layer and then breaks it onto several smaller units. The segments which are produced after segmentation comes with a header associated with every segment. The segmented message is reassembled by the transport layer at the destination.
2. **Service point addressing:** For the purpose of delivering message to the proper process, the header of the transport layer also includes an address type which is called the port address or service point address. By determining this specific address, the transport layer makes sure that the intended message gets delivered to the right process.

Services provided by transport layer:

1. **Service oriented to connection:** This whole process is done in three phases:

-Connection establishment

-Transfer of data

-Disconnection or termination

In this form of transmission, the device on the receiver's side sends out an acknowledgement intended for the source right after a data packet or group of packet has been received by the destination. This form of transmission is very secure and reliable as well.

2. **Connection less service:** This process is one phase in

nature and it includes transfer of data. In this form of transmission, the receipt of a packet is not at all acknowledged by the receiver. This form of transmission approach allows a faster mode of communication in between the devices. However, the connection oriented service is much more reliable than the connection less service.

- **Session layer:** The session layer serves the function of connection establishment, session maintenance, authentication and also security of the session. The functions of this layer are:

    1. **Establishment of session, maintenance of session and termination:** This layer helps in the establishment of the two processes, uses and also terminates the connection.
    2. **Synchronization:** The session layer helps in adding up checkpoints which are regarded as the points of synchronization by a process into the data. The points of synchronization help in identification of the errors in order to ensure that the data has been re-synchronized in the proper way. It also ensures that the message ends are not prematurely cut for avoiding loss of data.
    3. **Dialog controller:** This layer allows the two systems to begin the communication with one another in full-duplex or half-duplex.

- **Presentation layer:** The presentation layer is also known as the translation layer. The data which is received from the application layer is extracted in this layer and is also manipulated as per the requirements of the format for transmitting the same over the network. The functions of this layer are:

    1. **Translation:** It helps in the process of translation such as from ASCII to EBCDIC.
    2. **Encryption and decryption:** The encryption of data translates the whole data into some other form or code. The

data which is encrypted is known as the cipher text. The data which is decrypted is known as the plain text. For the purpose of data encryption and data decryption, a key value is used by this layer.

3. **Compression:** This layer helps in reducing the total number of bits which is to be transmitted into the network.

- **Application layer:** At the top of the stack of layers of the OSI model exists the application layer. It is a layer which is implemented by the applications in a network. The applications of the network produce the data which is to be transferred across the network. The application layer serves as a window for the services of applications for accessing the network and also for the purpose of displaying the information which is received to the user. Some examples of network applications are web browsers, messengers etc. The functions of this layer are:

  1. Mail services
  2. Network virtual terminal
  3. FTAM or file transfer access and management
  4. Directory services

The OSI model as the reference model and is not at all implemented for the internet as it is considered as being outdated. TCP/IP model is used in place of the OSI reference model.

VLAN

VLAN or virtual LAN is a group composed of devices on one or more than one LANs which are configured for communicating in a way as if all of them are attached with the same wire whereas they are located at several different segments of a LAN. VLANs are extremely flexible in nature as it is based on a logical connection in place of a physical connection. VLANs help in defining the domains of broadcasting in a network of Layer 2 nature. A broadcast domain is nothing but a set of all the devices which will be receiving frames of broadcast originating from any of devices within that set.

The broadcast domains are bounded typically by the routers as the routers will not be forwarding the frames of the broadcast.

The switches of Layer 2 create broadcast domains which are completely based on the switch configuration. Switches are the multiport bridges which allow in creating several broadcast domains. Each of the broadcast domains is similar to a distinct form of a virtual bridge which can be found within a switch. You can easily define one single or many bridges of virtual nature which are available within a switch. Each of the virtual bridge which a user creates within the switch helps in defining a new VLAN or broadcasting domain. It is not possible for traffic to directly pass to some other VLAN between two switches or within that switch.

VLAN acts just like a sub-network. VLAN eases up the job for the network administrators to divide one single switched network for matching the security and functional requirements of the systems without the need of running new cables or without making any major changes in the present infrastructure of the network. VLANs are generally set up by the large-sized businesses for the purpose of re-partitioning the devices for the better management of traffic.

VLANs also help in improving the all-round performance of the network simply by grouping all the devices together which communicates the most. VLANs also provide proper security for the large-sized networks by providing a greater degree of control across which the devices have access to each other. One or more than one network switch can support several independent VLANs by creating Layer 2 subnet implementation.

VLANs and its types

There are various types of VLANs present. Let’s have a look at them.

- **Protocol VLAN:** This type of VLAN comes with traffic handled base on the protocol. The switch on the network will either forward or segregate the traffic based on the protocol of the traffic.
- **Static VLAN:** It is also known as port-based VLAN. It requires the administrator of a network for assigning the ports on the

network switch to a network of virtual nature.

- **Dynamic VLAN:** It allows the network administrator to define the membership of the network which is based on the characteristics of the device which is in opposition to the switch port location.

How does VLAN work?

Ports or interfaces on the switches can be assigned to one single or more than one VLANs which enable the systems to get divided into various logical groups which are based completely on the departments with which they are associated with. It also establishes the rules about the systems about how the systems in the separate groups are going to communicate with one another. These separate groups can range from practical and simple to legal and complex. Each of the VLAN provides access of data link to all the hosts which are connected to the switch ports configured with the similar VLAN ID. The VLAN tag is a field of 12-bit in the header of the Ethernet which provides support for 4,096 VLANs per domain switching. The tagging of VLAN is standardized in the IEEE 802.1Q and is also called Dot1Q.

When a frame is received of untagged nature from a host which is unattached, the VLAN ID which is configured on the interface is added up in the header of the data link frame by using the format 802.1Q. The frame of 802.1Q is forwarded towards the proper destination. Each of the switches uses the tags for keeping each traffic of the VLAN separate from the traffic of the other VLANs, forwarding the same only to the place where VLAN is configured.

The trunk lines in between the switches can handle several VLANs by using the tags for keeping them all segregated. A trunk line is a line of communication which has been designed for carrying several signals for the purpose of providing network access in between two different points. When the frame reaches the ultimate switch port of the destination, the tag of VLAN is removed just before the frame is transmitted to the device of destination.

It is possible to configure multiple VLANs on one single port with the use of trunk configuration in which each of the frames sent through the port is being tagged with the VLAN ID. The interface of the neighboring device which

might be on some other switch or host which supports 802.1Q tagging will require to support the configuration of trunk mode for transmitting and receiving the frames which have been tagged. Any of the Ethernet frames which are untagged are assigned to a VLAN of default nature which can also be designated in the configuration of a switch.

When a switch which is VLAN-enabled receives an Ethernet frame of untagged nature from an attached host, it adds up the VLAN tag which is assigned to the interface. The frame is then sent forward to the host port along with the MAC address of the destination. Broadcast multicast and unknown unicast is then forwarded to all the ports in the VLAN. When any previously unrecognized or unknown host replies to an unknown frame of unicast, the switches get to know about the host location and do not flood the host with the subsequent frames which were addressed for that host.

The STP or Spanning Tree Protocol is being used for creating a topology of loop-free nature among all the switches in every Layer 2 domain. As per the regulations of VLAN, an instance of STP can be used which in turn enables the various topologies of Layer 2 or a MISTP or multi-instance STP can be used for reducing the overhead of STP in case the topology is also the same among the multiple VLANs. STP blocks away the forwarding on the links which might produce some forwarding loops and thus creating a spanning tree from the selected switch of root. The concept of blocking means that some of the links will not at all be used for the purpose of forwarding unless and until there is a failure in some other part of the network which causes the STP to turn the link a part of any forwarding path of active nature.

Advantages and disadvantages of virtual LAN

VLAN comes with some basic advantages such as reduced traffic of broadcast, proper security of network, confinement of broadcast domain and easy administration of network.

When it comes to the disadvantages of VLAN, it comes with the limitation of 4,096 VLANs only for per switching domain which creates lots of problems for the large-sized providers of hosting, which also often comes with the need to allocate hundreds of VLANs for the customers. For addressing this limitation, several other protocols such as NVGRE, VXLAN and Geneve supports larger sized tags and also comes with the ability of tunneling frames

of Layer 2 within the packets of Layer 3.

Routing

Routing is the process by which path is selected along which the requested data is to be transferred from the source of origin right to the receiver or destination. Routing is done by a special network device which is known as a router. The router functions at the networking layer in the OSI reference model and in the internet layer in the model of TCP/IP. A router is a device which is used in networking which helps in forwarding the data packets based completely on the available information within the header of the packet along with the forwarding table. For the purpose of routing the data packets, various routing algorithms are used. The routing algorithm is a software which helps in deciding the path which will be the optimal one for the data packet to be transmitted to the destination.

The protocols regarding routing use metric for determining the perfect and fastest path for the delivery of the packet. Metric is nothing but the standard which is used for measurement such as bandwidth, hop count, current path load, delay etc. which is being used by the algorithm of routing for determining the optimal delivery path. The algorithm of routing maintains and also initializes the table of routing which is required for the process regarding the determination of path.

Metrics of routing

Routing metrics along with costs are used by the router for determining the most suited route up to the destination. The factors which are used by the routing protocols for determining the fastest path are known as metrics. For some of the routing protocols, they use static form of metrics whose value cannot be changed and some of the protocols use the dynamic version of metrics whose value can be changed and then assigned by the administrator of the system. The most common values of metrics are:

- **Hop count:** It is the metric which helps in specifying the total number of passes across the devices of internetworking like the router. A data packet needs to move in a route for travelling right

from the source to the destination. If the protocol of routing takes the hop as a primary value of the metric, the path which comes with the least hop count is going to be considered as the fastest and the best path for moving the data packet from the source to the destination.

- **Delay:** It is the time which is taken by the network router for processing, queuing and transmitting one datagram to the interface. The protocols of routing use this form of metric for determining the values of delay for each and every link which are in the path from end-to-end. The path which will be having the lowest value of delay will be taken as the best path for the data packet.
- **Bandwidth:** The capacity that a link has is called the bandwidth of that link. The link bandwidth is measured as bits per second. The link which has the highest rate of transfer such as gigabit will be preferred over any other link which comes with a link capacity of like 52 kb. The protocol of routing will be determining the capacity of bandwidth for each and every link along the path and the link which comes with overall higher bandwidth will be taken as the perfect route for moving the packet from source to destination.
- **Load:** Load is the measurement with which it is measured that the resource of a network like network link or router is busy to which extent. The load can be measured in various ways such as packets processed every second, utilization of CPU etc. In case the traffic increases, the value of load will also increase. In simple words, the load value will change in relation to the change in the network traffic.
- **Reliability:** It is a factor of metrics which might be composed of only one fixed value. It depends on the links of the network along with its value which is dynamically measured. There are some forms of networks which go down more often when compared to others. After a network fails, there are some links of the network which gets repaired more easily when compared with the other links of the network. Any factors of reliability can

be considered reliability rating assignment which is in numeric values in general and is assigned by the administrator of the system.

Routing and its types

Routing is of various types and it can be easily classified into three broad categories:

- **Static routing:** It is also known as the nonadaptive form of routing. With this routing technique, the administrator of a network manually adds the preferred routes within the table of routing. A router sends the data packets towards the destination by following the route which is defined by the administrator. In this routing technique, the decisions of routing are not at all made based on the topology or conditions of a network.

Advantages:

1. **No overhead:** It has no form of overhead on the usage of the CPU of the network router. Therefore, a cheaper variant of the router can easily be used for obtaining static routing.
2. **Bandwidth:** It has no usage of bandwidth between the network routers.
3. **Security:** It provides proper security as the administrator of the system is allowed control only over the process of routing to a specific network.

Disadvantages:

1. For a large-sized network, it turns out to be a very difficult task for manually adding each of the routes to the table of routing.
2. The administrator of the system is required to have proper knowledge of the network topology as he needs to manually

add each of the routes.

- **Default routing:** It is a technique in which the network router is configured for sending all the data packets to the exact same hop device and it is not necessary that whether it belongs to that specific network or not. A data packet is being transported to the device for which it has been configured in the default form of routing. Default routing is being used when the networks only deal with one single point of exit. It is very helpful in situations when the transmission network bulks need to transmit the packet of data to a similar hop device. When any particular route has been mentioned in the table of routing, the network router will be selecting the route which has been specified rather than using the default route. The default path or route is selected by the router only when any specific route has not been mentioned in the table of routing.
- **Dynamic routing:** It is also called adaptive routing. In this technique of routing, the network router adds up a new route in the table of routing for every single data packet in response to all the changes which has been made in the topology or condition of the network. The dynamic protocols are being used for the purpose of discovering the brand new routes for reaching the destination. In this form of routing, OSPF and RIP are the only protocols which are used for the purpose of discovering new routes. In case any of the routes go down, the automatic adjustment will be done for reaching the destination.

Advantages:

1. It is very easy to configure.
2. It is the most effective of all for selecting the perfect and best route in response to all the changes in the topology or condition of the network.

Disadvantages:

1. It is very expensive with respect to the bandwidth and CPU usage.
2. It is not much secure when compared with static and default routing.

The dynamic protocol needs to have these features:

- All the network routers need to have the similar protocol of dynamic protocol for the purpose of exchanging the routes.
- In case the network router discovers any form of change in the topology or condition of the network, the router needs to broadcast this information among all the other routers.

Network Services

DHCP

Also known as Dynamic Host Configuration Protocol, is a protocol for network management which is used dynamically for the purpose of assigning IP address for the devices or for any node on any network so that is possible to establish communication by using the IP. DHCP manages centrally and also automates all of these configurations instead of having the administrators of a network to manually assign the IP addresses for all the networking devices. It is possible to implement DHCP on small-sized local networks and also on large-sized enterprise networks. DHCP helps in assigning new IP addresses for every location when the networking devices are moved from one place to another. This means the administrators of the networks are not required to manually configure the devices with new IP addresses when it is moved to a completely new location within the network.

How does DHCP work?

DHCP functions at the application layer of TCP/IP model for dynamic assigning of the IP addresses to the DHCP clients and for allocating TCP/IP configuration to the clients of DHCP. This is composed of subnet mask, IP

addresses, default gateway and DNS address. DHCP serves as a client-server protocol. In this, the servers manage a unique pool of IP addresses along with various information regarding the configuration parameters of the clients and also assign address from those pools of address only. The clients which are DHCP enabled send out requests to the server of DHCP whenever they connect with the network.

The clients which are configured with DHCP broadcast requests to the server of DHCP and requests information regarding network configuration for that local network with which they are connected or attached. The clients generally broadcast their query for information as soon as they boot up. The server of DHCP responds to the requests of the clients by providing information regarding IP configuration which was specified previously by the administrator of a network. This also includes one particular IP address as well for that time period which also called a lease and the allocation is valid for this one. At the time of refreshing any assignment, a client of DHCP requests out for the same parameters but the server of DHCP might also assign a new IP address completely based on the policies which are set by the administrators of the network.

The server of DHCP also manages a proper record of all those IP addresses which it allocates to the nodes of a network. In case any node is relocated within the network, the server of DHCP identifies it quickly by using MAC address which helps in preventing the accidental configuration of several devices by using the same IP address.

DHCP is not at all a routable form of protocol nor is it secure. DHCP is limited within a LAN which means one server of DHCP every LAN is enough for usage in case of any failover. The larger form of networks might also have WAN which contains several individual locations. Depending completely on the connections in between the points and the total number of clients in every location, several servers of DHCP can be set up for the purpose of handling address distribution.

In case the administrators of a network want a server of DHCP to provide IP addresses for multiple subnets on any given network, they are required to configure the relay services of DHCP which located on the interconnecting routers across which the requests of DHCP needs to cross. These agents help

in relaying the messages between the clients of DHCP and servers which are located on various subnets. DHCP lacks the feature of built-in mechanism which would have allowed the clients and the servers to authenticate one another. Both the clients and the servers are susceptible to deception and to attacks as well.

Static DHCP leases VS. Dynamic DHCP leases

By having a dynamic DHCP, the client does not own an IP address which has been assigned but instead of that leases the address for a period. Every time when a device with a dynamic form of IP address gets powered up, it needs to communicate with the server of DHCP for leasing another IP address. The wireless types of devices are the examples of those clients which are assigned with dynamic IP addresses whenever they connect with the network. The devices which are assigned with a static form of IP address have permanent IP addresses. They are used for various devices such as switches or web servers.

Under a setup of dynamic DHCP, the clients need to perform certain tasks that result in termination of its address and then reconnect with the network with the use of other IP address. The lease times of DHCP varies depending on the period of time for which a user needs the internet connection at one specific location. The devices with a dynamic IP address, release the IP addresses when the lease of their DHCP expires and then the devices request for renewal of IP addresses from the server of DHCP in case they want to stay online for a longer time. The server of DHCP might assign a completely new IP address instead of just renewing the old IP address.

NAT

For accessing the internet, a user needs one IP address which is public in nature. Private IP addresses can be used in those networks which are private in nature. The primary goal of NAT is to permit several devices to get access to the internet by using one public address only. For the purpose of achieving this, it is required to translate the IP address to a public IP address. NAT or Network Address Translation is the process by which one or more than one local form of IP address is readily translated into one or more than one

Global form of IP address and vice versa for the purpose of providing internet access to all the local hosts.
Also, NAT translates the port numbers which means it helps in masking the port number of the host with some other port number within the data packet which will be moved to the destination. NAT then makes the required entries of port numbers and IP addresses in the table of NAT. It operates on the firewall or router generally.

Types of NAT

There are three ways in which NAT can be configured.

- **Static NAT:** In this form of configuration, one private IP address is mapped with one public IP address which means one-to-one mapping between the local and the global address. This form of configuration is generally used for the purpose of web hosting. This form of configuration is not at all used in the organizations as there will be various devices which will need access to the internet at the same time.
- **Dynamic NAT:** In this form of NAT configuration, one private IP address is being translated into one public IP address from a huge pool of IP addresses of public nature. In case any IP address from a pool is not free, the packet will be dropped off as only a specific number of IP addresses can be translated from private to public.
- **Port address translation or PAT:** This configuration is also called NAT overload. In this form of configuration, various private IP addresses are translated into one single public IP address. For the purpose of distinguishing the traffic, port numbers are used.

Advantages of NAT

- NAT helps in conserving public IP addresses.
- It helps in maintaining proper privacy as the IP address of the

device which will be receiving and sending traffic will be in hidden form.

- It helps in the renumbering of address when any network evolves.

Disadvantages of NAT

- The translation of IP addresses might result in delay in path switching.
- There are various applications which will not be functioning when NAT is enabled.
- It complicates various protocols of tunneling like IPsec.

Switching

VLAN Trunking Protocol

VTP or VLAN trunking protocol is used for maintaining proper continuity and consistency throughout a network. VTP allows the users to add up, remove or rename VLANs which is propagated to some other switches within the domain of VTP. However, there are certain requirements for the VTP to communicate about VLAN information between the switches. The version of VTP needs to be on similar on all the switches which the user needs to or wants to configure. Also, the domain name of VTP needs to be same on all the switches. For VTP communication, one of the switches needs to act like the server or be the server.

Modes of VTP

There are three different modes of VTP:

- **Server:** All the switches are set for this mode by default. This mode allows the users to add, delete or create VLANs. Any kind of change that the user wants to make needs to be done in this mode. Each and every change which is made in this mode will be propagated to every switch which belongs to the same domain of VTP.

- **Client:** In this mode of VTP, the switches receive all the updates and are also capable of forwarding all those updates to the other switches.
- **Transparent:** This mode of VTP forwards only the summary of VTP advertisements via the trunk line. The switches of this mode can create their own database of local nature which can keep secrets from all the other switches.

Spanning Tree Protocol

STP or spanning tree protocol is being used for creating a loop-free network by the process of network monitoring for tracking all of the links and then shutting down those which are less redundant in nature.

STP and its types

- **802.1D:** This type of STP is also called CST or common spanning tree. This is a standard of STP which has been developed by the IEEE which selects one single root bridge only for every topology. All of the traffic in the network flows in the same path but this might not be good always as there might be issues in which the path which has been optimized for reaching the VLAN is completely different from the path which has been obtained after electing root bridge. It is also very slow in nature as it takes minimum 32 seconds of time for converging.

  Advantages:

  It requires very less CPU and memory.

  Disadvantages:

  It comes with a lesser percentage of optimization as the path which is calculated as the perfect one to root bridge might turn out to be not the best path for reaching the network. It also offers no form of load balancing.

- **802.1w or RSTP:** RSTP or rapid spanning tree protocol is the

standard which has been developed by the IEEE for providing a faster rate of convergences that CST. However, it also holds a similar idea of finding a single root bridge within the topology.

- **RPVST:** Also known as rapid per VLAN spanning tree, is a standard which has been developed by Cisco for providing faster rates of convergence than RSTP and also finds out separate instances for 802.1w for every VLAN. However, it needs more memory along with CPU when compared with the other standards of STP.

Routing Configuration

OSPF

Also known as Open Shortest Path First protocol, is a form of link-state routing protocol which helps in finding the best path between the destination and the source router by using up its own shortest path first. OSPF protocol has been developed by IETF as an IGP or interior gateway protocol which is the protocol for moving the packets within a very large system of autonomous nature or domain of routing. It acts in the network layer and works on the protocol number 89.

Terms of OSPF

- **Router ID:** It represents that IP address on the router which is the most active of all. The highest address of loopback is considered at the first place and in case no form of loopback has been configured, the IP address which is the highest active within the interface is considered.
- **Router priority:** It is a value which is assigned to the router which is operating OSPF. It is 8 bit in nature and helps in electing BDR and DR within a broadcast network.
- **DR or designated router:** It is elected for minimizing the total number of adjacency which has formed.
- **BDR or Backup designated router:** BDR acts as the backup of DR within a broadcast network. Whenever DR performance goes down, BDR assumes the role of DR and starts to perform the

functions of DR.

BDR and DR election

The election of BDR and DR takes place within a broadcast network or within a multi-access network. The criteria for election are:

- The router which has the highest priority of router will be elected as the DR.
- In case there is any form of a tie in choosing the router priority, the router ID which is the highest will be considered.

EIGRP

EIGRP or enhanced interior gateway routing protocol is a form of dynamic routing protocol which is being used finding the best route between two devices of layer 3 for delivering the data packet. It functions at the network layer of the OSI reference model. It uses up protocol number 88 for functioning. EIGRP uses the method of metric for finding out the perfect path between the two devices which operates EIGRP.

Characteristics of EIGRP

EIGRP functions with the following characteristics:

- It works with an advanced form of operational efficiency.
- It acts as a classless protocol of routing.
- It comes with the capability of both distance vector and link state.
- It comes with some unique features like RTP or reliable transport protocol, DUAL or diffusing update algorithm and all forms of updated information about the neighbors.

- It offers a faster rate of convergence as it precalculates all the routes and also does not broadcast timer packets prior to convergence.

It uses delay, load, bandwidth and reliability for calculating the metrics for the table of routing.

Chapter 16: Troubleshooting of Network

A complete setup of network uses up various components, hardware, configurations of network, setups and operating systems which works together for making a network successful. However, it might happen that some of the components stop functioning due to some glitch or error. Such a situation might result in the complete shutdown of a network which can also call up huge losses for the large-sized networks. So, all that is needed in such a situation is troubleshooting of the network for making the network functional again.

Adapter resources

Try to make sure that the adapter of the network has been installed properly and has also been detected by the computer without any hassle. If you are using Windows OS, open up the device manager and then verify that there is no form of error. In case there is any form of discrepancy in the adapter of the network or if it has been detected by the computer as other device, you need

to check that whether the adapter has been installed properly or not.

Verifying the connections

In case you are using a wired form of network, make sure that the network cable has been connected properly and the LED indicator right next to the network jack is blinking. A solid green LED or light means that the cable has been attached properly and it is receiving signals from the network. In case there is no light in the indicator, it might indicate that the card is not good or it has not been connected in the proper way or there is any form of error in the network signal. If you are on a small-sized local network, check all the hubs and routers and make sure that the cables are connected properly in all.

In case you are using a wireless network like a laptop, make sure that the Wi-Fi option in your laptop has been turned on. If you are still facing any issue, make sure that you have selected the proper Wi-Fi network. Also, check the connection of the Wi-Fi router for ensuring that the router is receiving signal from the internet.

Functionality of adapter

You need to verify that the card of the network is able to ping itself by the use of ping command. If the local host is properly functioning you will receive replies from the host. In case you receive any error such as time out, check that the network card has been properly installed and the drivers are updated as well.

Chapter 17: Networking on PC and MAC

PC and MAC are completely two different forms of system which uses two different operating systems. A PC generally runs of Windows or Linux whereas MAC uses its own OS for functioning. There is a very common question that is it possible to establish a network between PC and MAC and the answer to this question is yes. It is not at all a strenuous job and can be done within a few minutes.

Steps to follow

- Right before you start with the process, make sure that you have set up the IP in both the PC and MAC systems. Note down both the IP addresses as it will be used in setting up the connection.
- Set up a password for your PC sharing system which can be found in the network and sharing option.

- Put the PC running on Windows or Linux and the MAC system in the same workgroup.
- In the MAC system, open up system preferences and then select the adaptor of the network. Select the advanced option which is available on the right pane and select wins tab and type in the same name of the workgroup as you are using in the system of PC.
- Create a folder named as shared in the PC system.
- Create a folder named as shared in the MAC system.
- The next step is to open system preferences in the MAC system and select the option sharing under the option of internet & network. Check out the option of file sharing.
- Under the file sharing option, check share folder and file by using SMB.
- Now you will be able to connect both the systems and transfer files and folder between your PC running on Windows or Linux and the MAC system.

Make sure that nothing is in the encrypted format while sharing as with encryption turned on, the system of PC will not be able to log in the MAC system and share files and folders.

Conclusion

As you have completed reading the whole eBook, you have developed a clear perception about the basics of networking along with various protocols of the same. By now, you must have learnt the basic requirements for setting up a network and how can you speed up the functioning of your network. The protocols and the types of system that you choose will ultimately determine how your network is going to function. You are the one who can make a network function to its fullest.

With the help of various tools of networking along with its components, you can create your own network, whether you need one for your home or you need a large network for your business place. You have also learnt about various components of a network and how each of them functions in different forms of environment.

As you have leant about the basics of networking in this eBook, you can try out the other eBook on *Hacking With Kali Linux* from which you can learn about the various concepts of network hacking along with the security of your network. Kali Linux can help in testing the vulnerabilities in your network system which you can ultimately use for securing up your network. As the number of prying eyes is increasing day by day, it is very important for the network administrators to use the best components of networking and also perform regular security checks for the ultimate security infrastructure.

If you find this book helpful for your business in any way, kindly leave a review on Amazon.