



Telecommunication System for Next Generation Network

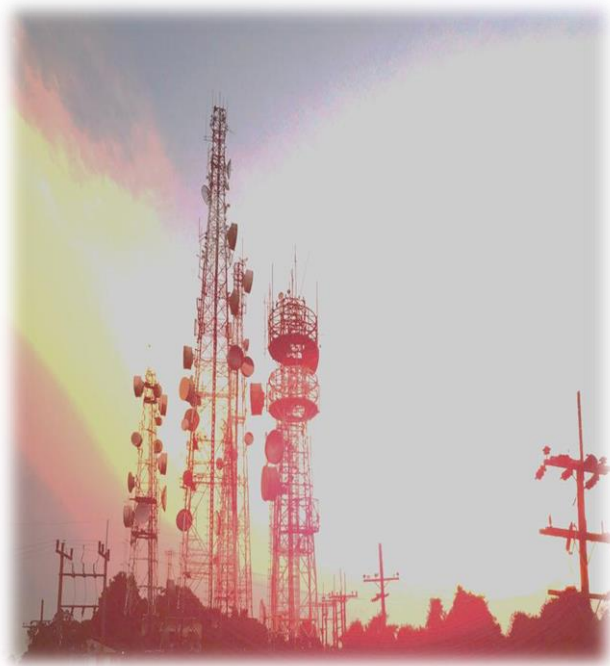
A Q&A Note with Info Graphic and
Practical Activities

eBook Edition

SYAMSUL BAHRI MOHAMAD

TELECOMMUNICATION SYSTEM FOR NEXT GENERATION NETWORK

A Q&A Note with Info Graphic and
Practical Activities



SYAMSUL BAHRI MOHAMAD

©ePembelajaran Politeknik Merlimau

Writer

SYAMSUL BAHRI MOHAMAD

Published in 2021

All rights reserved. No part of this article, illustration or book may be reproduced in any form or by any means, electronic, photocopying, mechanical, or other means without the prior written permission from Syamsul Bahri Mohamad. Negotiations are subject to royalty or honorarium arrangements.

Perpustakaan Negara Malaysia

Cataloguing-in-Publication Data

Syamsul Bahri Mohamad

Telecommunication System for Next Generation Network A Q&A Note with Info Graphic and Practical Activities / SYAMSUL BAHRI MOHAMAD. – eBook Edition.

Mode of access: Internet

eISBN 978-967-2241-75-1

1. Telecommunication systems.
2. Computer networks.
3. Government publications--Malaysia.
4. Electronic books.

I. Title.

621.382

Published by:

Politeknik Merlimau, Melaka

KB1031 Pej Pos Merlimau

77300 Merlimau Melaka

PREFACE

Telecommunication System for Next Generation Network: A Q&A Note with Info Graphic and Practical Activities is a reference book that developed to help students as a learning process tool in the field of telecommunications engineering of new/ next generation network or NGN. The New Generation Network or Next Generation Network (NGN) is a future technology platform that integrates all telecommunication network systems, i.e., cellular, Plain Old Telephone Network (POTS), Public Switching Telephone Network (PSTN), IP internet network, fibre optic network, microwave network, satellite network and others onto the same dedicated path system. The presence of NGN will definitely provide great benefits to network operators in terms of cost savings while facilitating the communication between two users by improving the connection speed and access.

The purpose of publishing this book is to make it easier for students or readers understand the important concepts of telecommunication network systems. The main uniqueness of this book is that it is a reading note based on Q&A (Questions and Answers). Through the use of Q&A notes, reading comprehension is more focused on important information rather than lengthy descriptions. The questions on Q&A are based on the appropriate level of cognitive learning for diploma students, i.e., level of knowledge, level of understanding and level of application.

In addition, this book provides simple and interactive info graphics to help students' readers to understand topics, especially those involving network infrastructure compared to the others main notes that display complex and intricate info graphics that are difficult for students and readers to remember.

Another advantage of this book is that it provides exercise activities on each sub-topic as a medium for revision and the abbreviated list. This list of abbreviations is important because this field of study has almost hundreds of abbreviations that students need to know. As an added advantage, this book also provides practical activities to complement the theoretical knowledge they have learned on the topics described in this book.

APPRECIATION

The highest appreciation and a sign of gratitude to God because with His bounty and permission, the book Telecommunication System for Next Generation Network: A Q&A Note with Info Graphic and Practical Activities was successfully published to meet the needs of educators, students and the public, especially polytechnic students who is pursuing a diploma in electronic engineering (communications). Many thanks and appreciation to the whole family, friends and the E-learning Unit of Politeknik Merlimau, Melaka who gave a lot of encouragement and support as well as views to perfectly produce of this book. Finally, millions of thanks are extended to all parties who have assisted us either directly or indirectly in the successful publication of this book.

Syamsul Bahri Mohamad
Electrical Engineering Department
Politeknik Merlimau, Melaka (PMM)
2021

CONTENTS

<i>Preface</i>	v
<i>Appreciation</i>	vi
Chapter 1 - Introduction to NGN	1
1.1 Understand Traditional Telecom World	2
1.2 Apply Public Switched Telephone Network (PSTN)	3
1.2.1 Show Pulse Code Modulation	5
1.2.2 Show Architecture of the Telephone Network	8
1.2.3 Show Switching Technique in Telephone Network	10
1.3 Understand Signalling Network	12
1.3.1 Explain SS7 Architecture	13
1.3.2 Explain SS7 Protocol Model	14
1.4 Apply understanding of Transmission Systems	16
1.4.1 Show Multiplexing of Digital Channels	16
1.4.2 Show Time Division Multiplexing in PSTN	18
1.4.3 Plesiochronous Digital Hierarchy (PDH)	20
1.4.4 Synchronous Digital Hierarchy (SDH)	21
1.4.5 Dense Wavelength Division Multiplexing (DWDM)	22
1.5 Understand the Convergence of the Two Worlds: Next Generations Networks	23
1.5.1 Explain Characteristic of NGN	23
1.5.2 Explain Architecture of NGN with an Illustration	24
Chapter 2 - Internet Fundamentals by IETF	25
2.1 Understand Internet Architecture of IETF Standardization	26
2.1.1 Discuss Internet Protocol Architecture	26
2.1.2 Explain Internet Network Architecture	27
2.2 Understand Fundamental Internet Protocols	28
2.2.1 Internet Protocol Version 4 (IPv4)	30
2.2.2 Internet Protocol Version 6 (IPv6)	32
2.2.3 User Datagram Protocol (UDP)	34
2.2.4 Transmission Control Protocol (TCP)	35
2.2.5 Stream Control Transmission Protocol (SCTP)	37

2.3 Apply Addressing and Numbering	38
2.3.1 Apply Network Address Translation	42
2.3.2 Show Dynamic Host Configuration Protocol	43
2.3.3 Show Domain Name System	45
2.3.4 Apply ENUM	46
2.3.5 Show IPv6 Addressing Architecture	47
Chapter 3 - NGN Standards and Transition to NGN	49
3.1 Understand Main Drivers to Next Generation Networks	50
3.1.1 Explain Fixed and Mobile Broadband Internet Access	50
3.2 Remember Standardization Synergy of IETF, ETSI, 3GPP and IEEE	53
3.2.1 Identify the IETF Role	53
3.2.2 Identify the ETSI Role	54
3.2.3 Identify the 3GPP Role	54
3.2.4 Identify the IEEE Role	55
3.3 Understand All-IP Network Concept for NGN	56
3.3.1 Explain All-IP Network Concept for NGN	57
3.4 Apply the understanding of Migration in PSTN Networks to NGN	57
3.4.1 Evolution of PSTN/ISDN to NGN	58
3.5 Understand signaling protocols for NGN	59
3.5.1 Explain the SIP	59
3.5.2 Explain the H.323	60
3.5.3 Explain the SIGTRAN	61
3.5.4 Explain the H.248	61
3.5.5 Explain the Diameter	62
Chapter 4 - Broadband Internet: The Basic for NGN	63
4.1 Remember ITU's Work on Broadband	64
4.1.1 Identify the Work of ITU-T, ITU-R and ITU-D	65
4.2 Apply DSL and Cable Access Networks	68
4.2.1 ADSL Network and Access Architectures	70
4.2.2 ADSL Frequency Bands and Modulation	70
4.2.3 Cable Access Network	73
4.3 Understand Mobile Broadband: Next Generation Mobile Networks	74
4.3.1 Evolution of Mobile Broadband	74

4.3.2 4G Standard by 3GPP: LTE	75
4.3.3 4G Standard by 3GPP: LTE-Advanced	76
4.3.4 4G Standard by IEEE: Mobile WiMAX 2.0	80
4.3.5 IP Multimedia Subsystem (IMS) for NGN	83
4.3.6 Next Generation Mobile Services	84
Chapter 5 - NGN Services	86
5.1 Apply the understanding of VoIP	87
5.1.1 Show Differences between VoIP and PSTN	88
5.1.2 Session Initiation Protocol (SIP) scenarios for VoIP	89
5.2 Understand IPTV over NGN	91
5.2.1 IPTV Functional Architecture	91
5.2.2 Multicast and Unicast Based IPTV Content Delivery	92
5.3 Apply the Understanding of Web Services in NGN	95
5.4 Understand Fixed-Mobile Convergence	96
5.5 Apply the Understanding of Ubiquitous Sensor Network (USN) Services	98
5.5.1 USN Applications	99
5.6 Understand VPN Services in NGN	100
5.7 Understand Various Concepts in NGN	102
5.7.1 Internet of Things (IoT)	102
5.7.2 Web of Things (IoT)	104
5.7.3 Software Defined Networking (SDN)	106
5.7.4 Network Functions Virtualization (NFV)	108
Practical Activities	111
A. Installation Tools in Ethernet LAN Network	112
B. Fixed and Mobile Broadband Internet Access	119
C. IPTV with VPN Services	125
D. VPN Services with IPv4 Addressing	132
E. IPv4 in VoIP Services	139
F. LED Control Using Web of Thing (WoT)	146
<i>Abbreviation</i>	155
<i>References</i>	160

Chapter 1

Introduction to NGN

World-Traditional Telecommunication – PSTN – PCM – Signalling Network –
SS7 – Multiplexing – TDM in PSTN – Characteristic & Architecture of NGN

1.1 Understand World-Traditional Telecommunication Scenario

Explain the information about the Traditional Telecommunication World?

- Traditional telecom world is mainly based on the telephony, which is the most important service in it. Hence, on the way toward the NGN, the telephony is still one of the most influential services.
- The other important traditional telecommunication service is television (also, coming from the first half of the twentieth century).
- However, from the beginning the television was not offered by telecom operators which provided the telephony. Instead, the television was provided via separate broadcast networks, either terrestrial or cable. Traditional telecommunication networks are in fact the telephone networks.

HISTORY OF TELEPHONY	
Started 19th Century (1876)	Invent the telephone by Alexander Graham Bell - Manual switching (based on operator)
End of 19th Century	First Automatic switching used base one step by step switch called Strowger switches. (analog system)
First half of 20th Century	Step by step replaced by Crossbar switches. Crossbar stayed in operation worldwide until the 1990s (transition from analog to digital telephony)
1990s	<ul style="list-style-type: none"> ▪ Switching was done with digital system (SPC – store programme control switches) ▪ Telecommunication network – digital ▪ Local loop (PSTN) subscriber line) – remain analog ▪ The digitalization of the subscriber line began with ISDN (for internet and voice) ▪ ISDN could not satisfy such requirements for higher data rates for emerging internet services.
2000 and 2010	Replacement ISDN with the xDSL technologies. (Digital Subscriber Line). Most widespread DSL was ADSL (Asymmetric DSL)

Activities:

List out the differences between old and new telecommunication technologies

Old telecommunication technologies	New/recent telecommunication technologies

1.2 Apply Public Switched Telephone Network (PSTN)

What is Public Switched Telephone Network (PSTN)?

PSTN or Public Switched Telephone Network, also known as the plain old telephone system (POTS) is generally is the inter-connected telephone system use for house telephone calls via copper wires.

How PSTN works?

PSTN is stands for Public Switched Telephone Network, and it's an old circuit-switched telephone network that works via underground or overhead copper wires from homes and businesses premise to switching centres (central office or main office or exchange) where the phone calls are inter-connected between each other.

What is a PSTN line used for?

Public Switched Telephone Network (PSTN) is the analogue network for residential and business customers. Analogue lines are single lines that are primarily used for making voice calls, connecting to fax machines and connecting to a modem for dial up internet.

What are the six main components of the PSTN?

The Public Switched Telephone Network components are (i) signaling counterpart, (ii) SS7, (iii) connect, (iv) monitor, (v) bill, and (vi) disconnect calls.

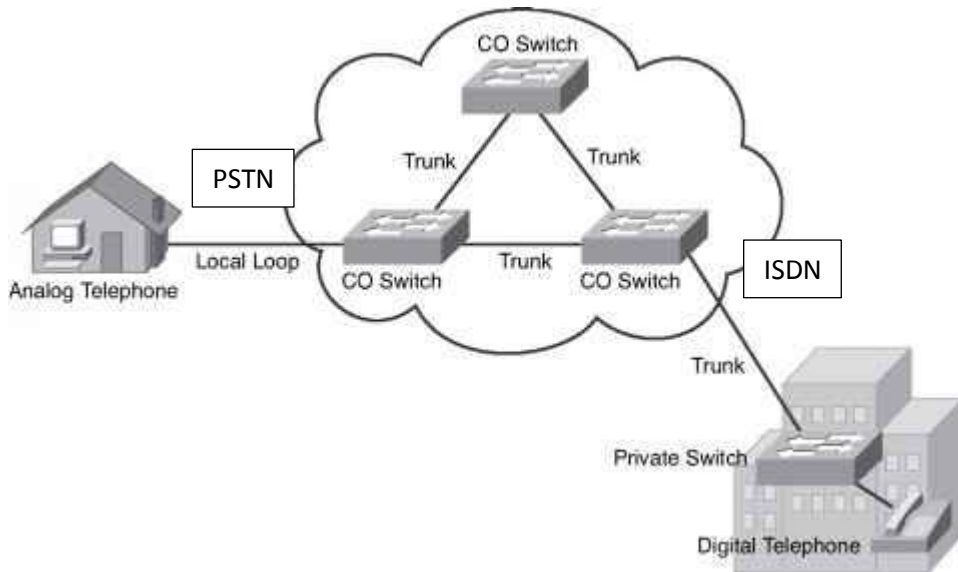


Figure 1.1: PSTN to ISDN architectures

What is ISDN?

Integrated Services Digital Network (ISDN) is a set of communication standards used for simultaneous digital transmission of voice, video, data, and other network services over the digitalised circuits (packet switching) of the public switched telephone network.

What is the difference between ISDN and PSTN?

The main differences between these two services is that PSTN are analogue systems while ISDN are made digital networking systems. ISDN provides better voice quality compared to PSTN.

PSTN	300 ... 3400 Hz analogue transmission band "poor-performance" subscriber signaling
Basic Rate Access ISDN	2 x 64 kbit/s digital channels (B channels) 16 kbit/s channel for signaling (D channel)
Primary Rate Access ISDN	30 x 64 kbit/s digital channels (B channels) 64 kbit/s channel for signaling (D channel) concatenation of B channels possible

Figure 1.2: PSTN vs ISDN channels

Activities:

List out THREE (3) differences between PSTN and ISDN

PSTN	ISDN

1.2.1 Show Pulse Code Modulation

What is PCM?

PCM or Pulse-code modulation is a digital method used to represent the sampled analog signals. It is the standard form of digital audio often used in computers, compact discs and digital telephony. In a PCM stream, the amplitude of the analog signal is sampled in uniform intervals shape where each sample is quantized to the nearest value within a range of digital steps.

Filename extension	.L16, .WAV, .AIFF, .AU, .PCM
Internet media type	audio/L16, audio/L8, audio/L20, audio/L24
Type code	"AIFF" for L16,
Magic number	Varies
Type of format	Uncompressed audio
Contained by	Audio CD, AES3, WAV, AIFF, AU, M2TS, VOB, and many others

Figure 1.3: Other information about PCM

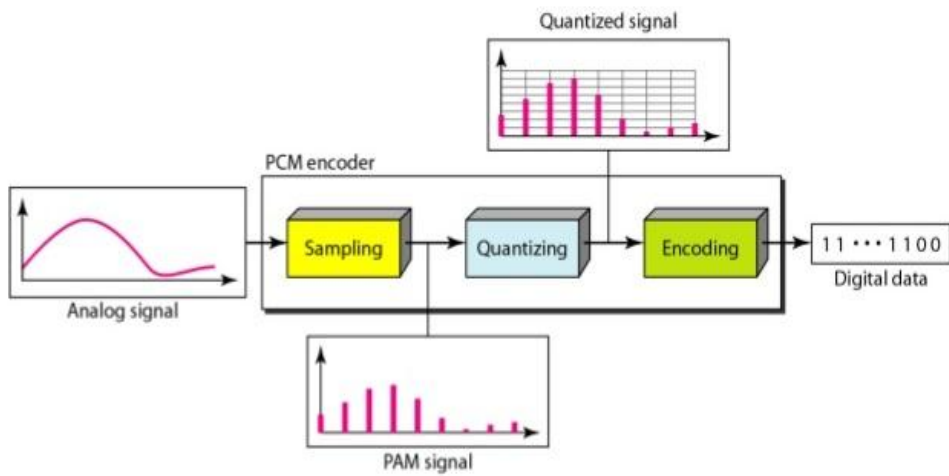


Figure 1.4: PCM process

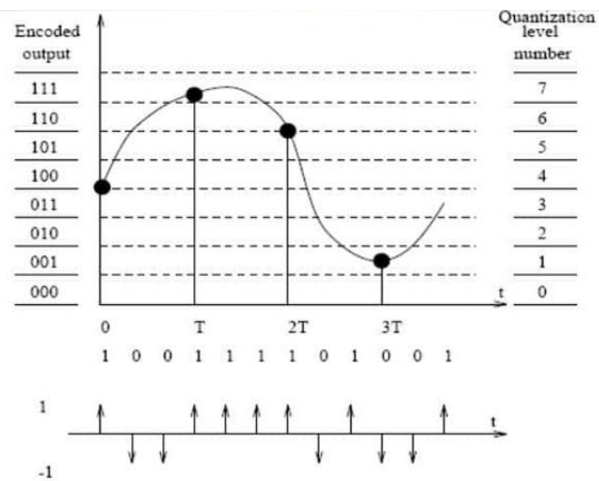


Figure 1.5: PCM quantization technique

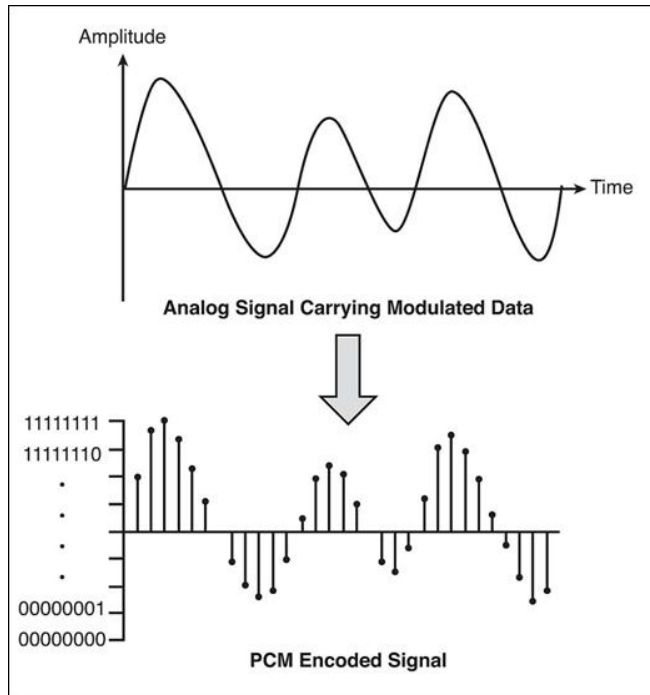


Figure 1.6: PCM encoded signal

What is the principle of PCM?

Pulse code modulation (PCM) involves three important principles, (i) sampling, (ii) quantizing, (iii) encoding. Some of the note state the use of filtering in the initial step of the process. This signal is merely a sequence of on-off pulse amplitude.

What are the applications of PCM?

The example PCM applications are used in the satellite transmission system, local telephony and compact disc (CD).

Activities:

Sketch the Pulse Code Modulation process with labelling.

1.2.2 Show Architecture of the Telephone Network

Explain the Local Loop or Subscriber line (Twisted Pair) Network?

- Local Loop / Subscriber line was usually analog.
- A/D conversion (PCM) was completed at the local exchange (central office) (exchange to which the user was connected)
- Telephone device (home or office) receives its power supply (-48V) from the local exchange.
- When the telephone is off-hook, the circuit between the telephone device and the exchange is closed, and electric current from local exchange flows over it. (DC – direct current).
- The two wires in the local loop are twisted to eliminate the crosstalk effect from electromagnetic current.
- Analog signals are converted into digital signals at local exchange.
- Then, the digital signals are transferred via the PSTN to end receiver for decoding (e.g. in local exchange on the other side which performs D/A conversion) at 64kbit/s bit rate.

RJ 11

- RJ stand for Registered jack
- Telephone connection interface

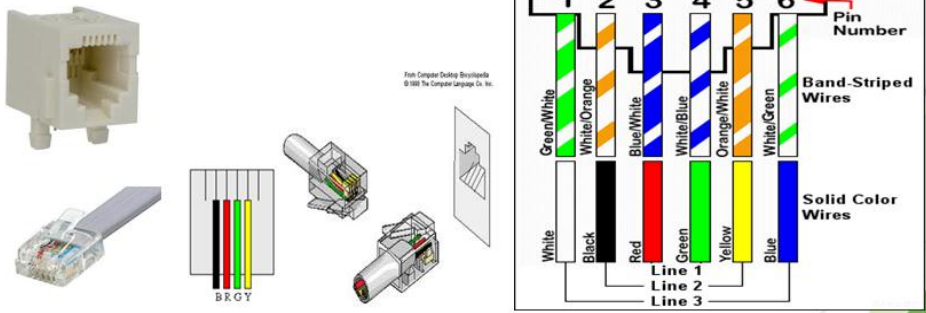


Figure 1.7: Register Jack (RJ-11) is a basic telephone set that requires minimum two wires (one pair) from the exchange to operate.

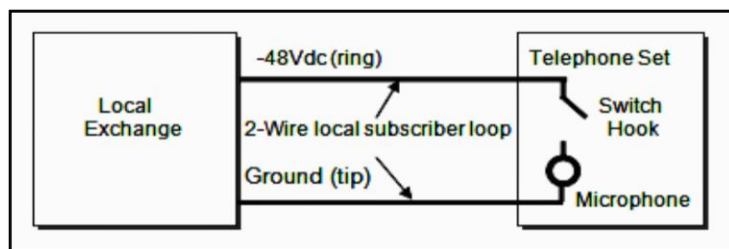


Figure 1.8: Local Loop/Subscriber Line

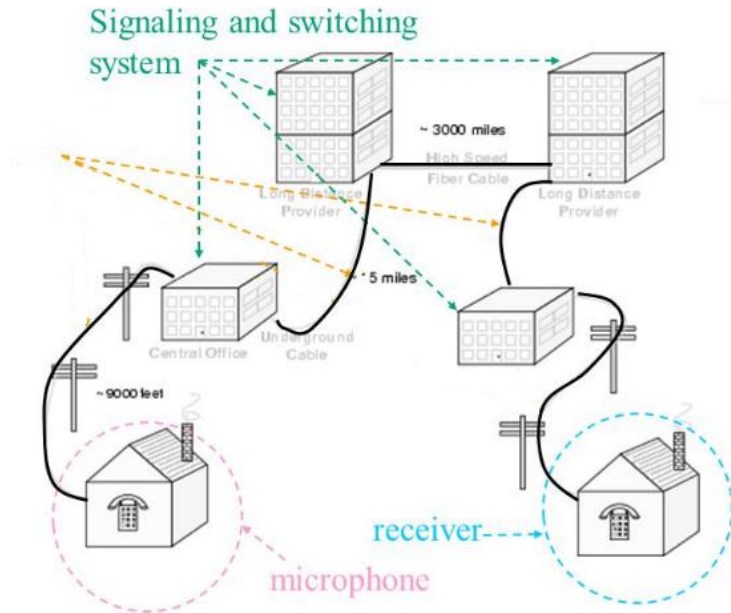


Figure 1.9: Architecture of the local telephone networking

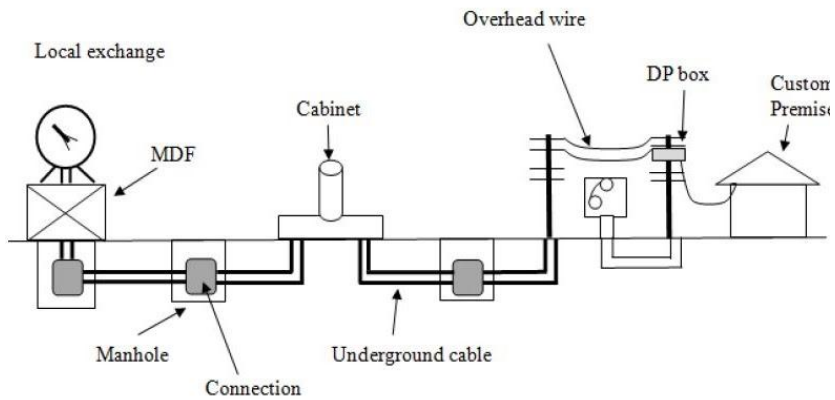


Figure 1.10: Connectivity of telephone network architecture

Activities:

Define the functionalities of cabinet, DP Box and MDF.

1.2.3 Show Switching Technique in Telephone Network

What is switching?

Switching is the technique uses to control and monitor the telephone call process between nodes.

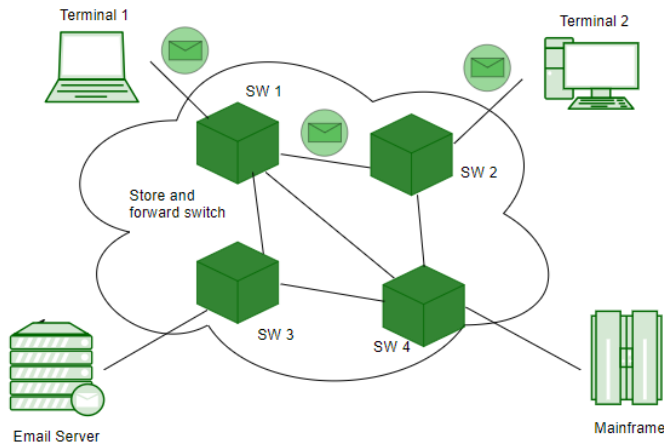


Figure 1.11: Example of message switching techniques

What are the switching techniques?

There are 3 common types of switching techniques:

- Circuit Switching.
- Packet Switching.
- Softswitch Switching.

What is circuit switching?

The switching that uses component electronic device to control the telephone call process and common used in PSTN. It is used for voice transmission. Fixed data can be transferred at in circuit switching technology by embedded the ISDN into PSTN.

What is packet Switching?

Packet switching is a method of switching that uses a grouping transmitted data into packets in digital network. Packets consist of header and a payload obtain from networking hardware to direct the packet to the destination. Packet switching is the primary basis technique for data communications in computer networks.

What is the classification of packet switching?

Packet switching is classified into connectionless switching and the example of the use of connectionless switching are in Internet Protocol (IP), Ethernet and the User Datagram Protocol (UDP).

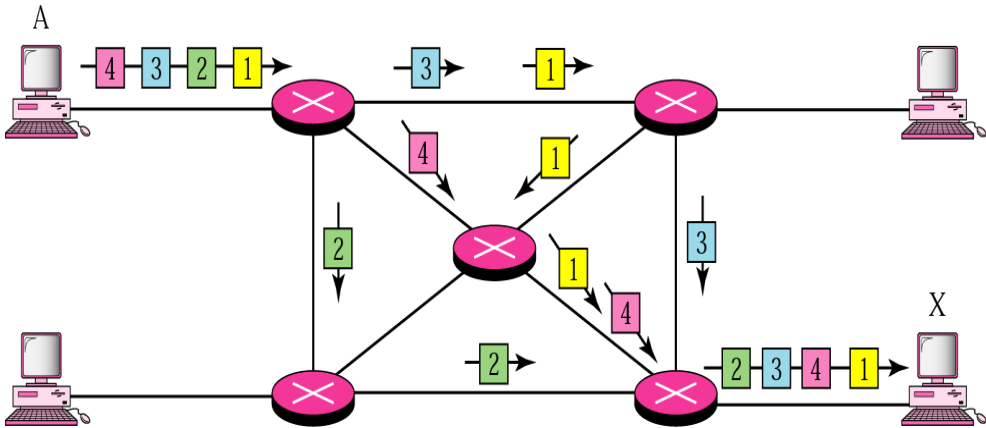


Figure 1.12: Packet switching technique in telephone network

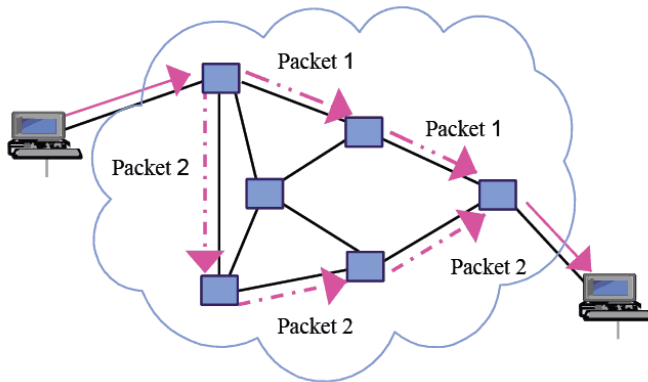
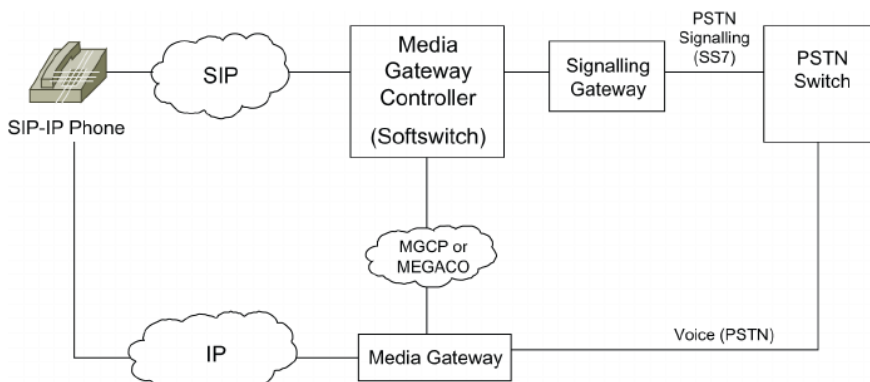


Figure 1.13: Example dataflow in Packet switching



Source: Collins (2003)

Figure 1.14: The Softswitch architecture

What is Softswitch switching?

The Softswitch switching is a call-switching that implemented in software running like a computing platform. The example of Softswitch switching is voice over IP (VoIP) technologies.

Activities:

State TWO (2) differentiation between Packet Switching & Softswitch Switching

Packet Switching	Softswitch Switching

1.3 Understand Signalling Network

What is Signaling Network?

- Signaling is **mediated exchange of control information signals** using certain signaling alphabet (set of signal or messages) on a telecommunications circuit.
- Signaling can be done using **analog signals** (e.g., electrical signals) or **digital signals** (e.g., bits, bytes, or messages/packets).
- The line signalling is refer to networking between the user telephone and the local exchange.
- In many PSTNs the line signaling is still analog, while signaling between exchanges is digital.

CLASSIFICATION OF SIGNALING IN PSTN	
Channel Associated Signaling (CAS)	Common Channel Signaling (CCS)
Certain signaling information is associated with the voice channels over the same transmission medium.	Signaling information from many users is multiplexed over a common channel and can be carried separately from the voice traffic

1.3.1 Explain SS7 Architecture

What is SS7?

SS7 or Signalling System No. 7 is a **signalling protocols** that developed in 1975, which is used to set up and terminate the telephone calls at public switched telephone network.

What is SS7 and how it works?

The SS7 is a signalling protocols that allowing phone networks to exchange the information that are needed for passing calls and text messages between each other. Is also used to ensure the correct billing and to roam on another, such as when travelling outside of the country.

What is SS7 architecture?

Signaling System 7 (SS7) architecture consist of (i) call-establishment, (ii) billing, (iii) routing, and, (iv) information exchange functions of PSTN.

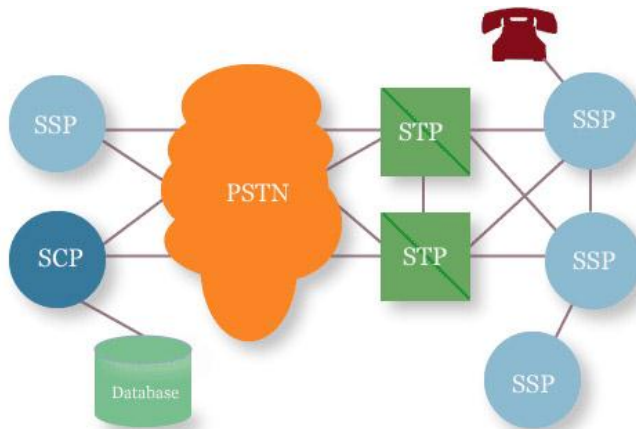


Figure 1.15: SS7 architectures

*What are three types of nodes used in SS7 network architecture?

- Service Switching Point (SSP);
- Signal Transfer Point (STP);
- Signal Control Point (SCP).

What is Service Switching Point (SSP)?

- SSP is a network element in SS7, which is integrated with local telephone exchanges (with attached subscriber lines to them).
- SSP converts dialled number (called B-numbers or Global Titles according to SS7 terminology) into SS7 signaling messages and establishes signaling connection with the SSP of the called user.
- SSP establishes, manages, and terminates voice connections. It sends signaling messages to another SSP via the STP node to which it is connected.

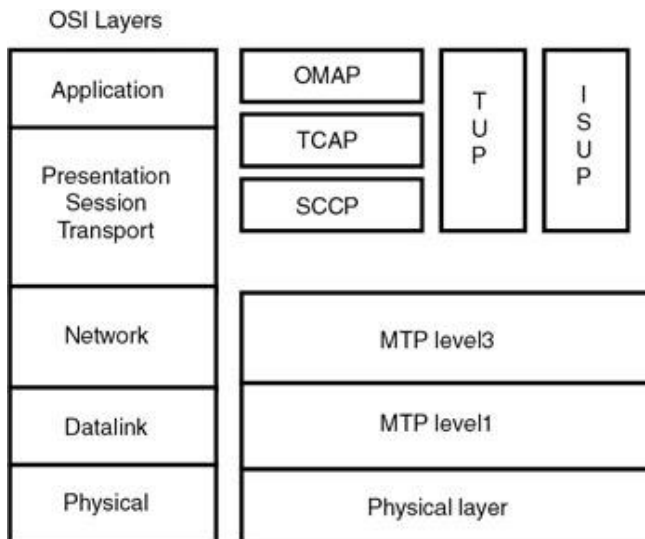
What is Signal Transfer Point (STP)?

- STP is a router of signalling gateway used in the SS7 network.
- This node (STP) has main task to route signaling messages between so-called signaling points in the network.
- Those STPs who act as gateway nodes actually connect signaling network of one telecommunications network (e.g., belonging to a telecom operator) with signaling network of another telecommunications network (e.g., belonging to another telecom operator).

What is Signal Control Point (SCP)?

- SCP provides access to certain application in SS7. In fact, SCP can be viewed as a database with an appropriate interface for database access by other signaling points in SS7.
- Typical usage of SCP is for special B-numbers such as the 0800 series (when the called party is charged for calls), or for the provisioning of roaming in PLMN.

1.3.2 Explain SS7 Protocol Model



*Figure 1.16: SS7 Protocol Model

PART	DESCRIPTION
ISDN User Part (ISUP)	The ISUP is a part of SS7 used to set up telephone calls in the public switched telephone network.
Telephone User Part (TUP)	Telephone User Part (TUP) is an analog protocol that performs basic telephone call connection and termination .
Transaction Capabilities Application Part (TCAP)	Transaction Capabilities Application Part (TCAP) is the SS7 protocol that carries application data to be exchanged between each nodes .
Signaling Connection Control Part (SCCP)	The Signalling Connection Control Part is a network layer protocol that provides extended routing, flow control, segmentation, connection-orientation, and error correction facilities . SCCP also provides the services of basic routing and error detection.
Operation, Maintenance, & Administration Part (OMAP)	OMAP is a set of functions and processes in SS7 network that are used to identify, control, configure, and manage network components.
Message Transfer Part (MTP)	MTP is part of SS7 that responsible for reliable, unduplicated and in-sequence transport of SS7 messages between communication partners .

Activities:

Explain the each function of SS7 in telecommunication network.

1.4 Apply understanding of Transmission Systems

What is meant by transmission system?

The transmission system is a **system that transmits a signal between two nodes**. The signal can be in form of radio signal, electrical signal or optical signal.

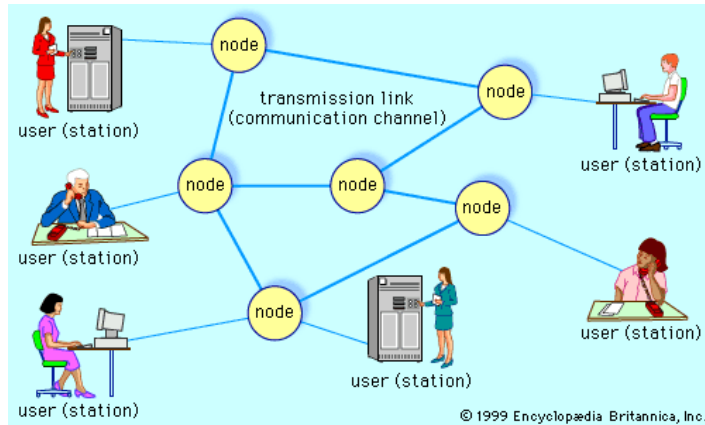


Figure 1.17: Telecommunications network

1.4.1 Show Multiplexing of Digital Channels

What is multiplexing?

Multiplexing is a technique of placing many signals over one transmission medium (e.g., copper, optical fiber, or radio).

Multiplexing	Description
FDM (Frequency Division Multiplexing)	Different frequency bands are assigned for each separate channels over the same transmission medium.
TDM (Time division multiplexing)	Different time intervals, called time slots , are assigned to different users over the same transmission medium and using the same frequency in the case of copper cables or radio transmission, or the same wavelength in the case of fiber.
Wavelength Division Multiplexing (WDM)	WDM used to increase the bandwidth by allowing different data streams at different frequencies is sent into a single optical network . Signals at WDM are independent from each other.
Code division multiplexing (CDM)	Code division multiplexing (CDM) is a networking technique which a multiple data signals are combined for simultaneous transmission over a common frequency band. The CDM is used to allow multiple users to share a single communications channel. CDM often used in cellular communication.

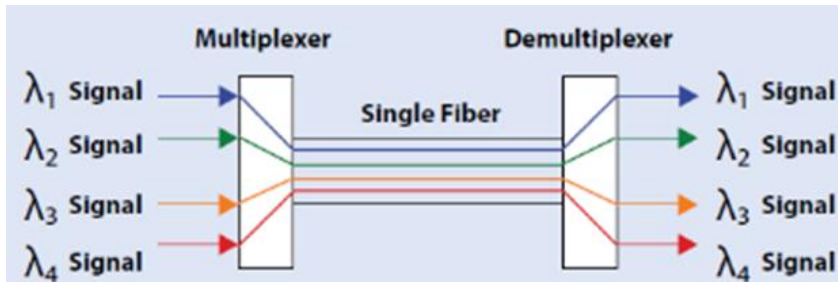


Figure 1.18: Wavelength Division Multiplexing

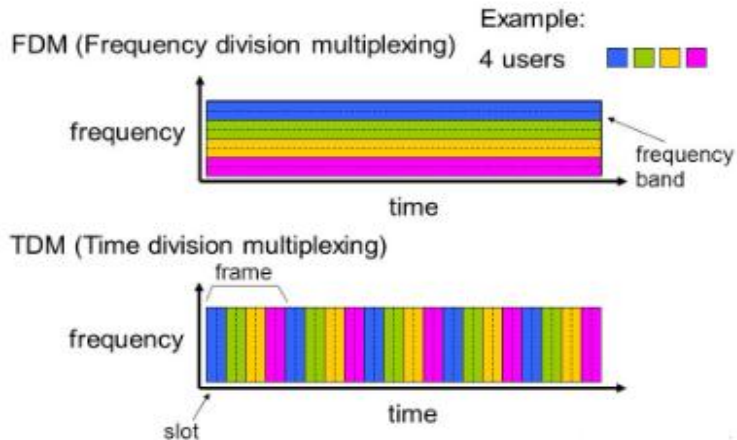


Figure 1.19: Differentiation between TDM and FDM

FDM has multiple data signals combined for simultaneous transmission via a shared communication medium.	TDM allows multiple users to send signals over a common channel by allocating fixed time slot for each user.	WDM modulates data streams, optical carrier signals of varying wavelengths into a single light beams via a single optical fiber.
FDM uses analog signals.	TDM uses digital and analog signals.	WDM uses optical signals.

Figure 1.20: Differentiation between TDM, FDM & WDM

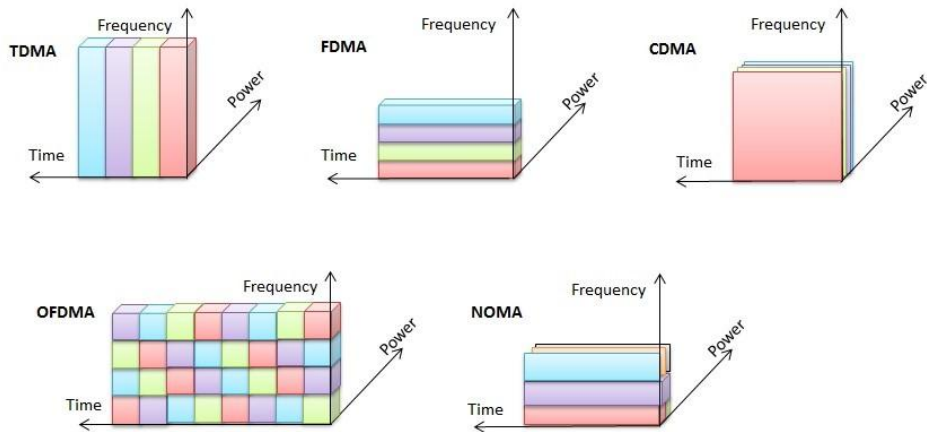


Figure 1.21: Differentiation in multiple access technique

Activities:

Explain why the multiplexing technique is upgrading from TDM until CDM?

1.4.2 Show Time Division Multiplexing in PSTN

What is PCM TDM?

A TDM PCM communication system uses a switching network and CPU for controlling and establishing the transmission paths between the user terminals.

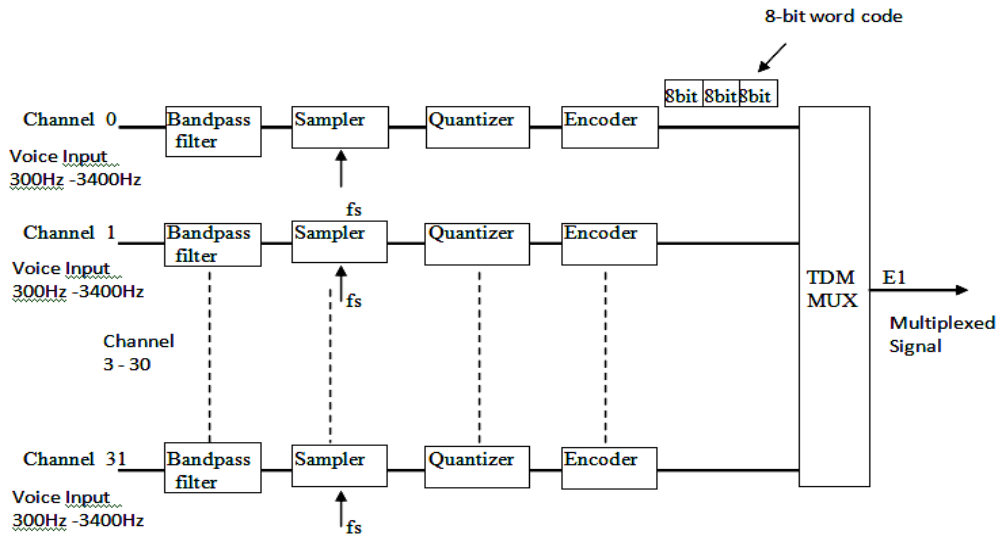
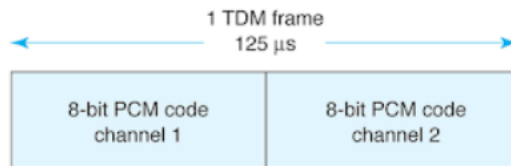


Figure 1.22: PCM-TDM for European (E1-Line) where E refers to European standard

What are the characteristic details about (PCM –TDM)?

- Using TDM, the transmissions from multiple sources can occur on same input but not at the same time.
- Figure 1.22 shows that for a PCM carrier system it's comprised of two DS-0 channels consolidated in time division multiplexed. Each input channel is sampled at 8 kHz rate and then converted to 8 bit PCM code.
- While PCM code for channel 1 is being transmitted, the channel 2 is sampled and converted to a PCM code. Then, while the PCM code from channel 2 is being transmitted, the next sample is taken from channel 1 and converted to PCM code.
- The process continues and samples are taken alternately from each channel, converted to PCM codes and transmitted.
- Multiplexer is an electronic controlled digital switch that consist two or more inputs with one output. Channel 1 and channel 2 are alternately selected and connected to transmission line through the multiplexer.



TDM Frame

- One 8-bit PCM code from each channel (16-bits total) is called a TDM frame, and time it takes to transmit one TDM frame is called frame time.
- Frame time is reciprocal of sample rate ($1/f_s$) or $1/8000 = 125\mu$ s.

- The PCM code for each channel occupies a fixed time slot within the total TDM frame.
- With Two channel system, one sample is taken from each channel during each frame, and time allocated to transmit PCM bits from each channel is equal to one half the total frame times. Therefore eight bits from each channel must be transmitted during each frame (a total of 16 PCM bits per frame). Thus line speed at output of multiplexer is

$$\frac{2\text{Channels}}{\text{frame}} \times \frac{8000\text{sample}}{\text{second}} \times \frac{8\text{bits}}{\text{channel}} = 128\text{Kbps}$$

- Each channel is producing and transmitting only 64Kbps, the bits must be clocked out onto line at a 128 KHz rate to allow eight bits from each channel to be transmitted in a 1211µs time slot.

1.4.3 Plesiochronous Digital Hierarchy (PDH)

What does Plesiochronous mean?

Almost synchronous: A transmission of sending and receiving devices are synchronized but being set to different clocks. Although the bits may not arrive in the same time slot, the transmission are arrive within a certain range or can be said as almost synchronous.

What is Plesiochronous digital hierarchy?

The PDH is an optical technology network that used in telecommunications networks to transport a large quantities of data over digital transmission equipment such microwave radio or fibre optic systems.

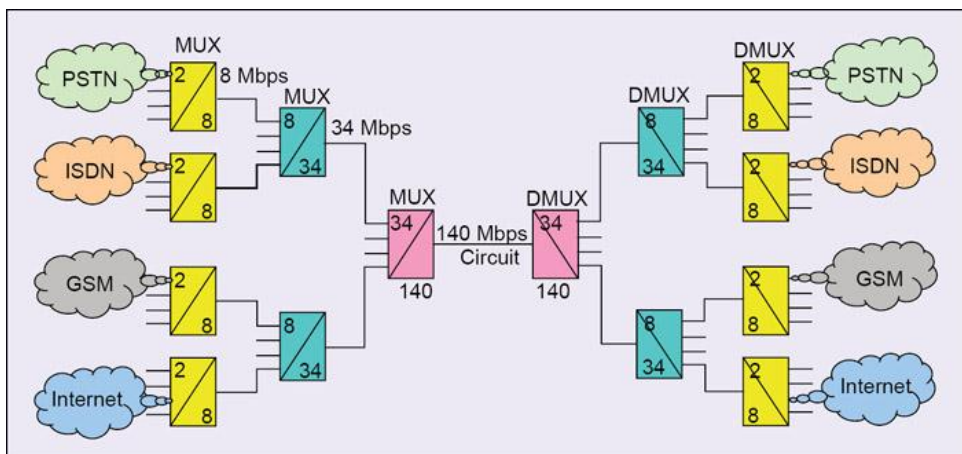


Figure 1.23: Plesiochronous Digital Hierarchy (PDH) used as a circuit provider

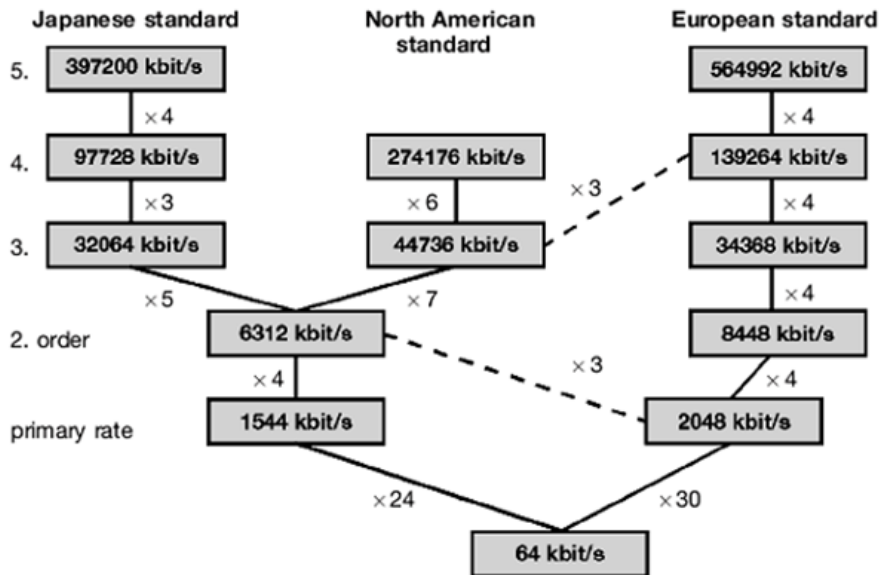


Figure 1.24: Plesiochronous Digital Hierarchies (PDH)

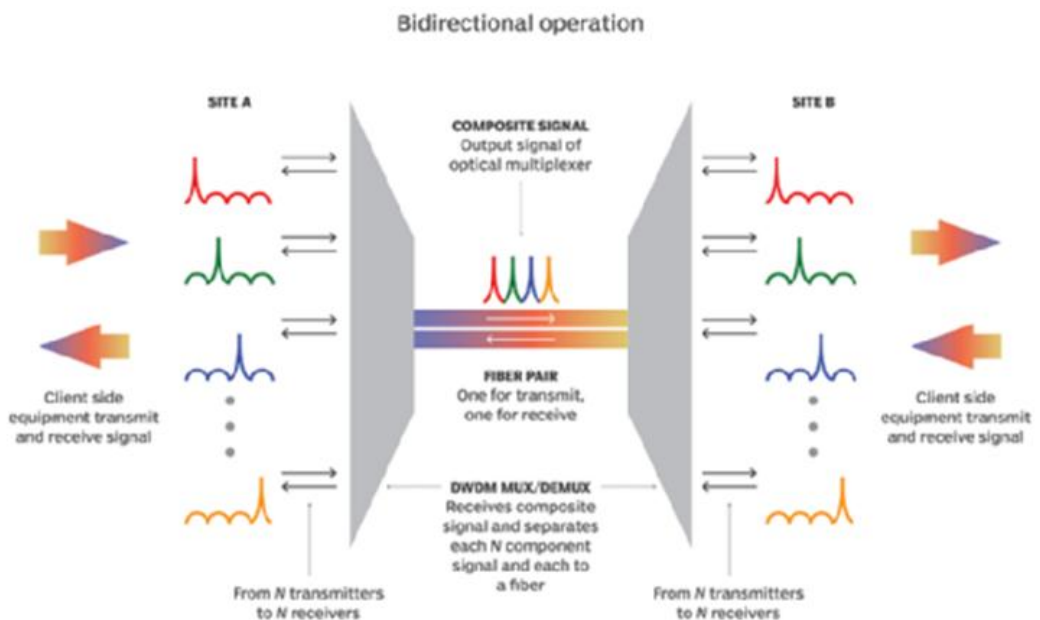


Figure 1.25: Dense Wavelength Division Multiplexing (DWDM) operation

1.4.4 Synchronous Digital Hierarchy (SDH)

What is Synchronous Digital Hierarchy (SDH)?

The SDH is a networking technologies standard that used for multiplexing the low rate of digital traffic channels into a single higher rate channels.

1.4.5 Dense Wavelength Division Multiplexing (DWDM)

What is DWDM?

DWDM is an optical multiplexing technology that used to increase bandwidth over existing fiber networks. It's works by combining and transmitting the multiple signals simultaneously at different wavelengths on the same optical fibre.

Activities:

State ONE (1) differentiation between SDH & PDH

Plesiochronous Digital Hierarchy (PDH)	Synchronous Digital Hierarchy (SDH)

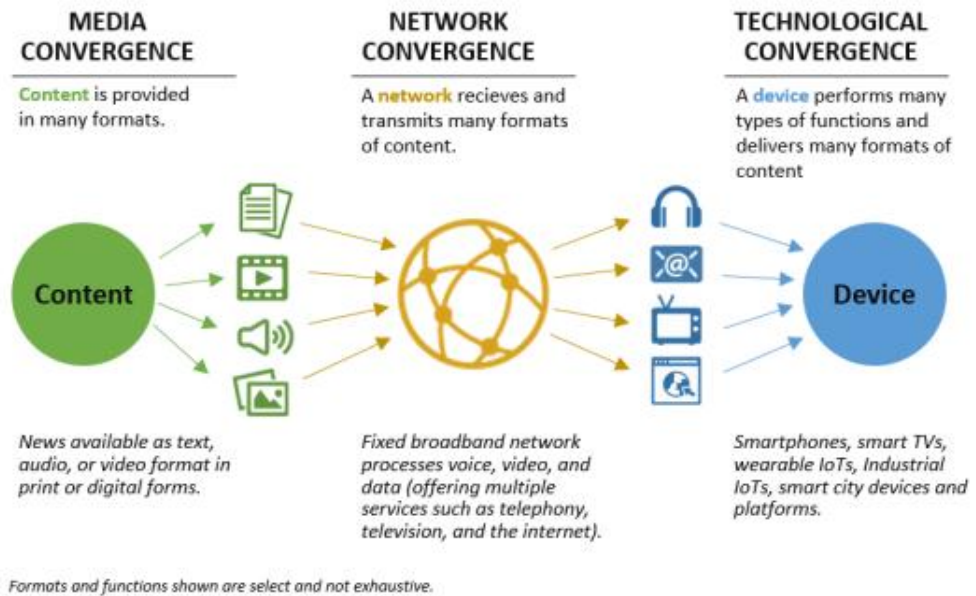


Figure 1.26: Network convergence in NGN between two worlds

1.5 Understand the Convergence of the Two Worlds: Next Generations Networks

What is convergence in a network?

Convergence in networking defines as a single combining network technologies that related to delivers networking services for voice, data, and video. These merging of standard and specification allows a user's and operators to use only one network technologies suitable for all communication devices and cloud-based services.

1.5.1 Explain Characteristic of NGN

What the fundamental aspect of Next Generation Network?

The fundamental aspects of NGN are:

1. Packet-based transfer.
2. Single service provision from the network with provision of open interfaces.
3. Using separation of control functions among bearer capabilities, call/session, and application/ service.

*What are the characteristic of NGN?

1. Packet-Based Network
2. Unified Global Networking Platform
3. Services are independent of transport layer technologies.
4. Low Delay, High Throughput and Strong Reliability
5. Unfettered access for users to network and services.
6. Generalized mobility that allow consistent services to users.
7. Provides Telecommunication Services to Users
8. Higher QoS – for enabling Transport Technologies

Differences between throughputs and data rates?

Throughputs is a network speed based on theoretical but data rates is an actual speed base of reality providing network.

	PSTN/IN	Internet	NGN
Multimedia Services	NO	YES	YES
QoS support	YES	NO	YES
Network Intelligence	YES	NO	YES
Intelligent Terminal Equipment	NO	YES	YES
Integrated Supervision & Control	YES	NO	YES
Reliability	High	Low	High
Service Creation	Complex	ad-hoc	Systematic
Simplicity of Services use	Medium	High	High
Modularity	Low	Medium	High
Time of Service Introduction	Long	Short	Short
Openness of Architecture	Small	High	High

Figure 1.27: Comparison between PSTN and NGN

1.5.2 Explain Architecture of NGN with an Illustration

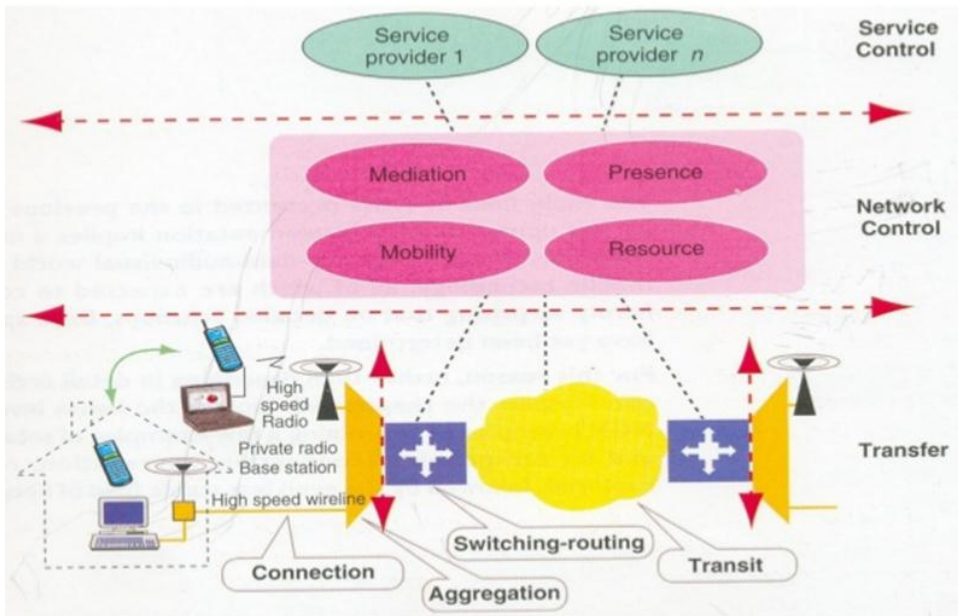


Figure 1.28: NGN architectures

Activities:

Explain THREE (3) characteristic of NGN bellows.

NGN Characteristic	Explanation
Packet-Based Network	
QoS-enabled Transport Technologies	
Delay, Throughput and Reliability	

Chapter 2

Internet Fundamentals by IETF

IETF Standardization – Internet Protocol – Internet Architecture – IPv4 – IPv6 –
UDP – TCP – SCTP – IPv4 Addressing – Network Address Translation –
Dynamic Host Configuration Protocol – Domain Name Services – ENUM –
IPv6 Addressing Architecture

2.1 Understand Internet Architecture of IETF Standardization

What is IETF stand for?

The IETF is community organization and the Internet technical standardization body that decentralized the structure and derives the Internet specification.

What are IETF role?

The IETF is the primary Internet standards organization that do the collaboration of autonomous, interconnected networks, supports communication through voluntary adherence to open protocols and procedures.

What is the mission of IETF?

The mission of the IETF is to ensure the Internet works better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

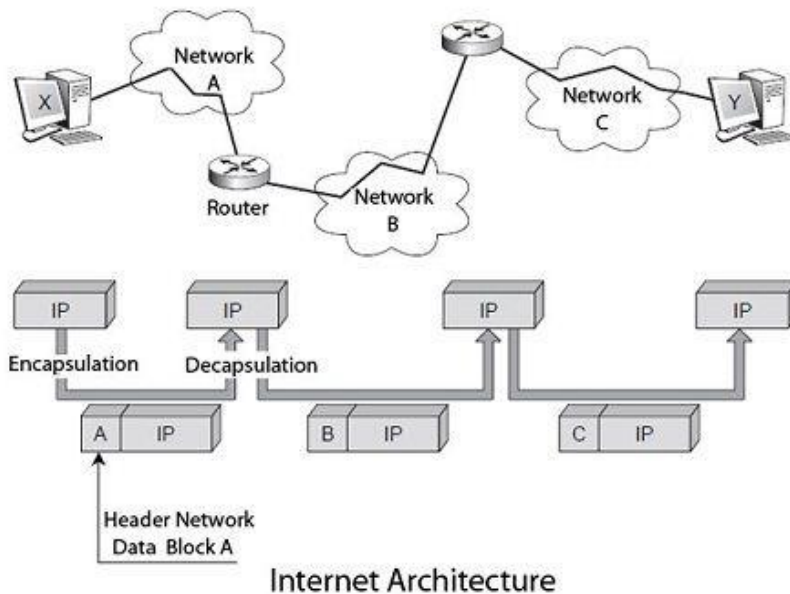


Figure 2.1: Internet architectures

2.1.1 Discuss Internet Protocol Architecture

What is the basic concept in Internet Protocol?

The Internet protocol is a conceptual model of communications protocols that used in computer networks. It is also known as **TCP/IP** or Transmission Control Protocol (TCP) / Internet Protocol (IP) which are fundamental protocols in internet network.

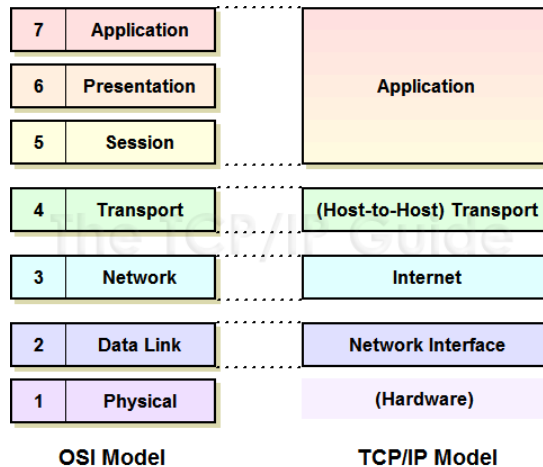


Figure 2.2: OSI Model and Internet Protocol Model

Explain the internet protocol layers?

The Internet Protocol is the first layer that introduces the virtual network abstraction in basic principle of the Internet model. The IP layer provides unreliable, connectionless delivery systems that not provide any functionality for error datagrams recovery either for duplicated or lost packet. If no such errors occur in the physical layer, the IP protocol guarantees that the transmission is successfully terminated.

2.1.2 Explain Internet Network Architecture

What is Network architecture?

- Network architecture is defines as a computer network design. The network architecture of the internet is expressed by the internet protocol suite
- The Internet architecture also called as TCP/IP architecture consists of two main protocols is depicted in Figure 2.4 which is TCP and UCP.

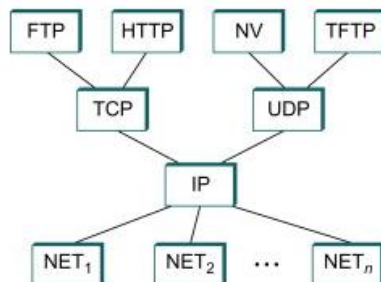


Figure 2.4: Internet protocol graph

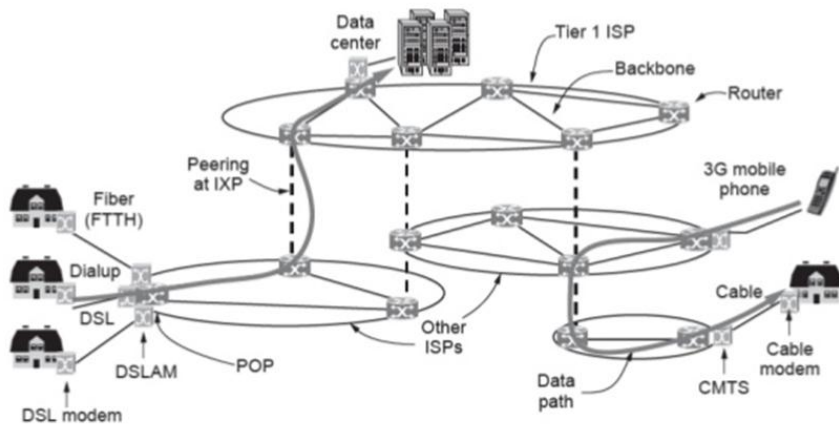
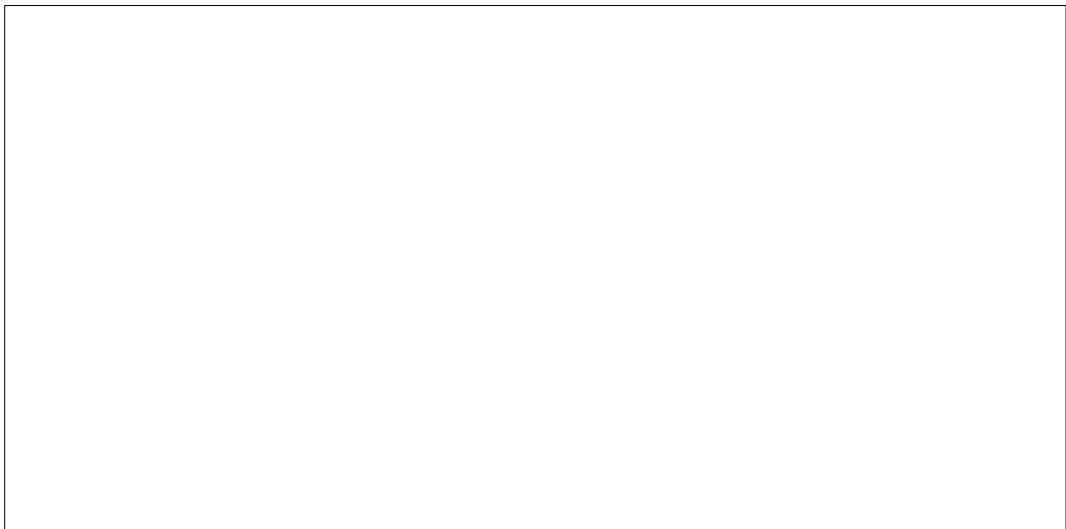


Figure 2.5: Architectures of Internet

Activities:

Sketch briefly the internet architecture with labelling.



2.2 Understand Fundamental Internet Protocols

What is Internet protocol?

Internet Protocol (IP) is a set of rules that dictate how data is delivered over the public network (Internet).

What are the basic protocols used in Internet protocols?

Common Internet protocols include

- a) TCP/IP (Transmission Control Protocol/Internet Protocol),
- b) UDP/IP (User Datagram Protocol/Internet Protocol),

- c) HTTP (HyperText Transfer Protocol) or HTTPS example
`http://spmp.pmm.edu.my/login.jsp`
- d) FTP (File Transfer Protocol).

What are the important protocols use in Computer Protocol?

The most important computer protocol is OSI (Open Systems Interconnection). OSI is a set of **guidelines for implementing networking communications between computers**. Among the most important sets of Internet protocols are TCP/IP, HTTPS, SMTP, and DNS.

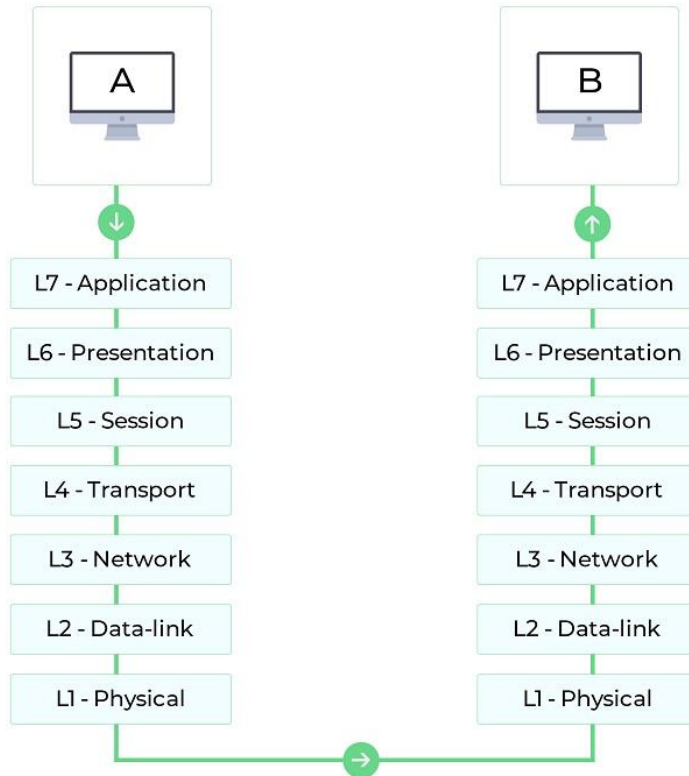


Figure 2.6: OSI model connection from PC A to PC B

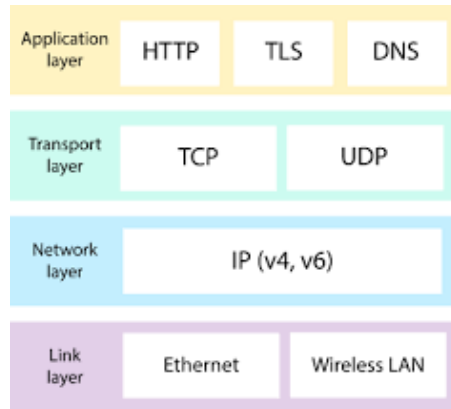


Figure 2.7: Internet protocol and layer involvement

2.2.1 Internet Protocol Version 4 (IPv4)

What is IPv4?

Internet Protocol version 4 is the fourth version of the Internet Protocol that refer to standards inter-networking based methods for packet-switched networks. IPv4 was first implementing in SATNET at 1982 and ARPANET at 1983.

What is purpose of IPv4?

IPv4 is created for underlying the internet technology to connect the devices to the website. Its enable a process of sending data from one computer through the website that containing the IP addresses of both devices.

How IPv4 work?

IPv4 works on the network layer of the TCP/IP protocol stack. The main task of the protocol is to transfer data blocks from the sender to the destination, where the senders and receivers are assigned with uniquely IP addresses.

What is IPv4 example?

IP (version 4) addresses are **32-bit integers** that **expressed in decimal notation**. The more common format, known as dotted quad or **dotted decimal**, is x.x.x.x, where each x can be any value between 0 and 255. For example, 192.0.2.146 is a valid IPv4 address.

*List out Characteristics of IPv4?

- IPv4 has 32-bit IP Address with 4 octets.
- IPv4 uses numeric decimal address, and its bits are separated by a **single dot**.
- The numbers of **header fields are 12** and the **length of the header filed are 20** which total up to 32.

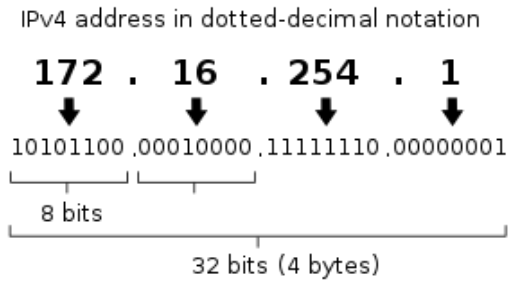


Figure 2.8: IPv4 notation (8 bits = 1 byte)

IPv4 Address Example				
Decimal Notation	131 . 153 . 40 . 106			
Binary Notation	10000011	10011001	00101000	1101010
	1 byte = 8 bits (Octet)	1 byte = 8 bits (Octet)	1 byte = 8 bits (Octet)	1 byte = 8 bits (Octet)
32 bits (4x8) = 4 bytes				

Figure 2.9: IPv4 address example

IPv4	IPv6
Deployed 1981	Deployed 1998
32-bit IP address	128-bit IP address
4.3 billion addresses Addresses must be reused and masked	7.9x10 ²⁸ addresses Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18	Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration	Supports autoconfiguration

*Figure 2.10: Differences between IPv4 and IPv6

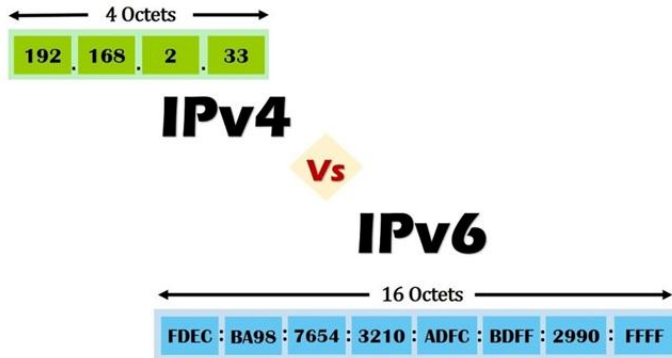


Figure 2.11: Other differences between IPv4 and IPv6

2.2.2 Internet Protocol Version 6 (IPv6)

What is IPv6?

Internet Protocol version 6 is the recent version of the Internet Protocol that provides an identification and location system for devices on networks and routes traffic across the Internet.

Which is faster IPv4 or IPv6?

Without network-address translation or NAT, IPv6 is faster than IPv4.

What is the purpose of IPv6?

The primary function of IPv6 is to allow for more unique IP address to be created where now 4.3 billion IPv4 has been created which insufficient for global uses. Other reasons are to provide the need of the Internet of Things (IoT) and 5G.

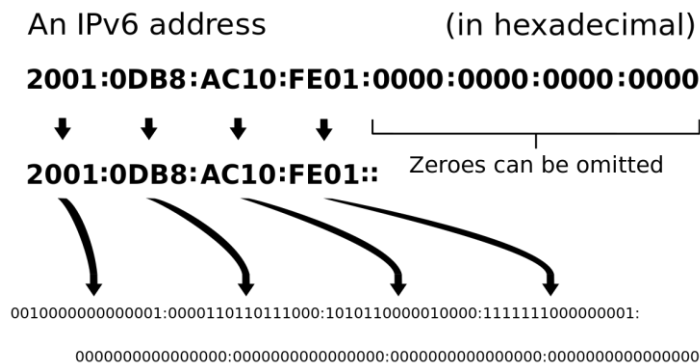


Figure 2.12: IPv6 addressing

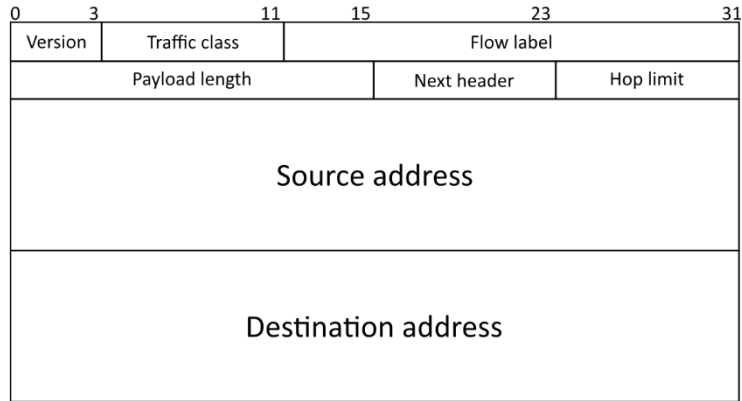


Figure 2.13: IPv6 frame format

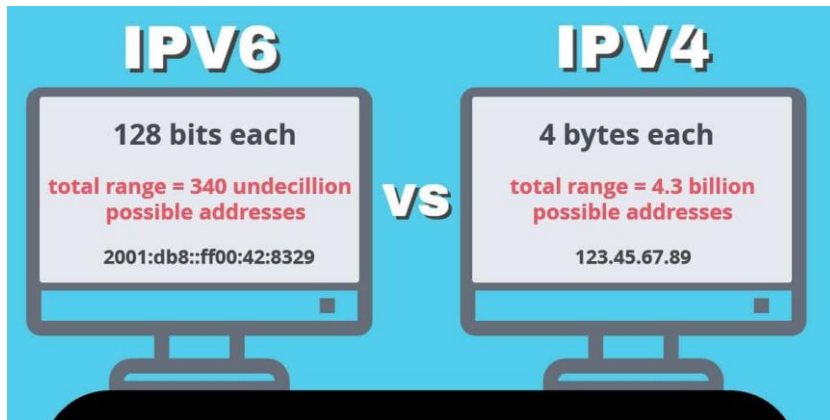


Figure 2.14: IPv4 vs. IPv6

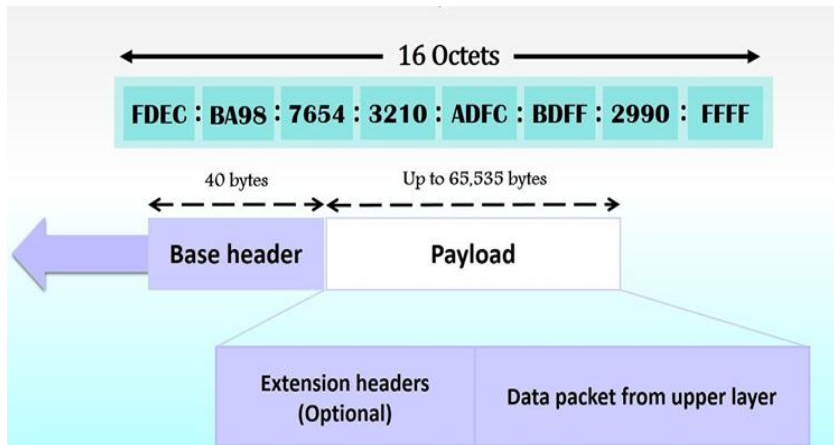


Figure 2.15: Other details about IPv6

Activities:

State THREE differences between IPv4 and IPv6

IPv4	IPv6

2.2.3 User Datagram Protocol (UDP)

What is User Datagram Protocol (UDP/IP)?

UDP is defined as a communication protocol that uses for time-sensitive transmissions such as video playback or DNS lookups.

How does UDP work?

UDP works by gathering all data in a packet and adding its own header information to the packet. These data consists of the source and destination ports with the packet length and a checksum (error checking) and transferred to their destinations.

Where is UDP protocol used?

UDP is commonly used for applications such as audio and video streaming. It is also used for query-response applications, such as DNS (Domain Name Services) queries example for www.google.com.my.

What is the disadvantage of UDP?

UDP does not provide assurance of delivery of packet and reliability of delivery. Thus the UDP provides low overhead and higher speed of delivery.

What is an example of UDP?

Examples of UDP services are Voice over IP (VoIP), online games, and media streaming.

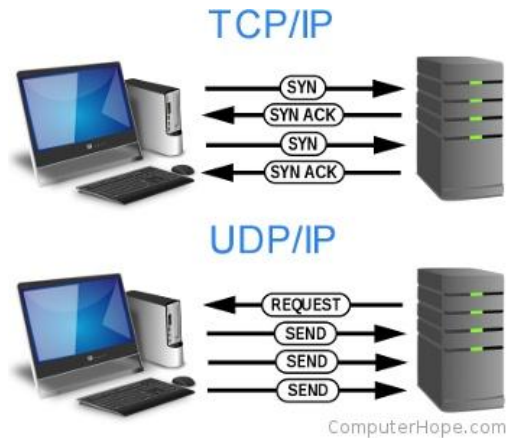


Figure 2.16: UDP vs. TCP

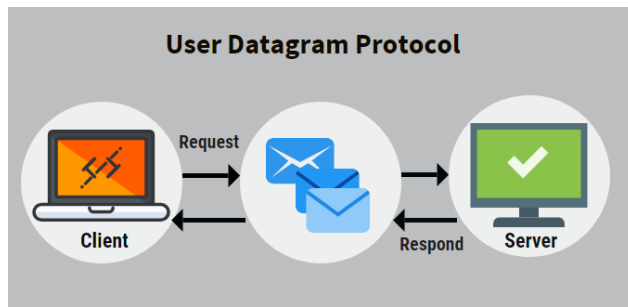


Figure 2.17: UDP dataflow

2.2.4 Transmission Control Protocol (TCP)

What is TCP?

Transmission Control Protocol (TCP) is **a connection-oriented** communications protocol that facilitates the exchange of messages between networking devices. It is the most common protocol in networks that use the Internet Protocol (IP) referred as TCP/IP.

Why TCP is are used?

TCP protocol is designed to send packets across the internet and **ensuring the successful delivery** of data and messages over networks.

How TCP work?

TCP is a program where the higher layer disassembles message content into small data packets to be transmitted over the Internet and then re-assembled back into the message's original form and **ensuring the successful message delivery**.

What is the main difference between TCP and UDP?

TCP is a connection oriented protocol and UDP is a connection less protocol. TCP provides an error checking support and also guarantees delivery of data to the destination where make it more reliable as compared to UDP.

2.2.5 Stream Control Transmission Protocol (SCTP)

What is SCTP?

The Stream Control Transmission Protocol (SCTP) is a computer networking communications protocol in the Transport Layer of OSI model. Its developed **intended for Signaling System 7 (SS7)** for message transport in signalling process. The SCTP provides the message-oriented feature of and **ensuring reliable** transport of messages mere to TCP.

What is SCTP protocol used for?

SCTP is a transport-layer protocol that ensures reliable, in-sequence transport of data and provides multi-homing support for both endpoints connection which consist more than one IP address. The SCTP enables transparent failover between redundant network paths.

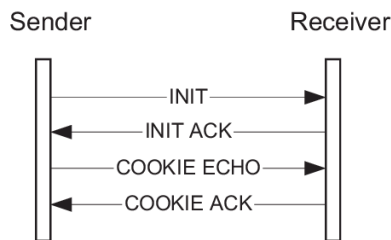


Figure 2.22: Dataflow in SCTP

	TCP	UDP	SCTP
Reliability	trustworthy	Unreliable	Trustworthy
Connection type	Connection-oriented	Connectionless	Connection-oriented
Transmission type	Byte-oriented	News-oriented	News-oriented
Transfer sequence	Strictly ordered	Disordered	Partially ordered
Overload control	Yes	No	Yes
Error tolerance	No	No	Yes

Figure 2.21: Differences between TCP, UDP and SCTP

What are the characteristics of SCTP?

- Unicast and multicast properties.
- Reliable transmission.
- Message oriented.
- Rate adaptive.
- Multi-homing & Multi-streaming.

Is SCTP better than TCP?

SCTP is a connection-oriented protocol which similar to TCP but provides message-oriented data transfer that similar to UDP. The SCTP is most likely combination of the advantages of TCP and UDP.

Who uses SCTP protocol?

SCTP is used mostly in telecom switches that use SS7 (Signaling System No. 7).

2.3 Apply Addressing and Numbering

What is addressing and numbering?

- An IP addressing is a numerical label assigned to each networking devices that uses the Internet Protocol. An IP address serves two main functions which are **host address and network** address.
- IP address in IPv4 uses **32-bit**. However, IPv6 using **128 bits** for the IP address.
- IP addresses are written and displayed in **human-readable notations** such as **172.16.254.1 in IPv4**, and **2001:db8:0:1234:0:567:8:1 in IPv6**.
- The size of the routing prefix of the address is designated in CIDR notation by suffixing the address with the number of significant bits.
- Example 192.168.1.15/24, which is equivalent to the historically used **subnet mask 255.255.255.0**.

Important terms in IPv4 addressing

1. Class of IP
2. Host address
3. Network address
4. Subnet Mask
5. Broadcast address

IPv4 addressing

IPv4 addresses are 32-bit numbers that are typically displayed in dotted decimal notation. A 32-bit address contains two primary parts: the network prefix and the host number. All hosts within a single network share the same network address. Each host also has an address that uniquely identifies it.

How do you write an IPv4 address?

IPv4 addresses are represented in **dot-decimal notation**, consists of 4 decimal numbers which ranging from **0 to 255** and separated by dots. Example address is 171.15. 253.1 each part represents a group of **8 bits** of the address.

What are the categories types of IPv4 addresses?

There are TWO different categories of IP addresses:

1. Public IP or private (internal network) IP
2. Static IP (manual) or dynamic IP / DHCP (automatic).

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.

Figure 2.23: IPv4 classes

What is Broadcast address?

A broadcast address is a network address that used to transmit to all devices connected to a multiple-access communications network. A message sent to a broadcast address may be received by all network-attached hosts.

192.16.20.20 255.255.255.0 Broadcast Address = 192.16.20.255 Class C : X.X.X.255 Class B : X.X.255.255 Class A : X.255.255.255
--

Figure 2.26: Another example of broadcast address and example of broadcast IP address at different classes

What is Network Address and Host Address?

An IP address consists of two components which are the network address and the host address. The network address is used to find and locate the subnet of the device and the host address is used to find the computer or the device in the subnet.

What is Subnet mask?

A subnet mask is a number that defines a range of IP addresses available within a network.

Calculations

- Perform calculations for 192.168.15.100
 - Network address (all host bits are 0s)
 - 192.168.15.0
 - Broadcast address (all host bits are 1s)
 - 192.168.15.255
 - Host addresses
 - Range → Network +1 to Broadcast -1
 - 192.168.15.1 to 192.168.15.255
 - Number of hosts in network = $2^h - 2$
 - $2^8 - 2 = 254$ host addresses

Figure 2.24: Example of host and network addresses

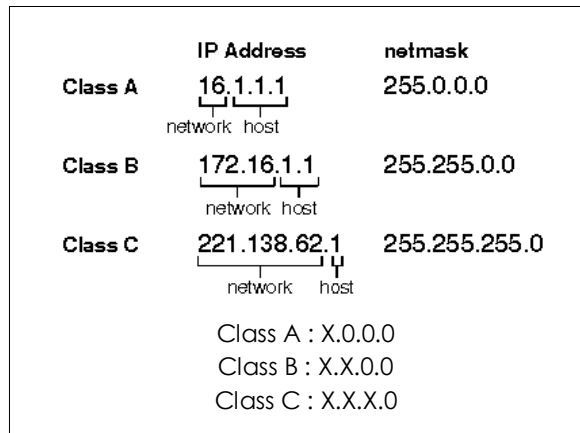


Figure 2.25: Other examples of positioning of host and network addresses and the example of Network IP Address at different classes

Activities:

Answer all questions

Address Class Identification

Address	Class	Subnet Mask	Network Address
10.250.1.1	<u>A</u>	_____	_____
150.10.15.0	<u>B</u>	_____	_____
192.14.2.0	_____	_____	_____
148.17.9.1	_____	_____	_____
193.42.1.1	_____	_____	_____
126.8.156.0	_____	_____	_____
220.200.23.1	_____	_____	_____

2.3.1 Apply Network Address Translation (NAT)

Definition / function / characteristic / example

What is NAT?

Network address translation is defined as a method of IP address mapping into another type of modifying network address information from local IP to public IP that change the IP header of the packets.

What does Network Address Translation do?

NAT allows a device such as a router to act as an agent between the Internet (public network) and a local (private) network. Only a single unique IP address is required to represent an entire group of local network.

What is NAT in networking with example?

NAT translates the IP addresses of computers in a local network to a single IP address for public network. This address is often used by the router that connects the networking device to the Internet.

Why is NAT used?

The use of NAT is to limit the number of public IP addresses of organization used for security purposes. The common form of large private network is in a range of 10.0.0.0 to 10.255.0.0. NAT generally operates on router or firewall.

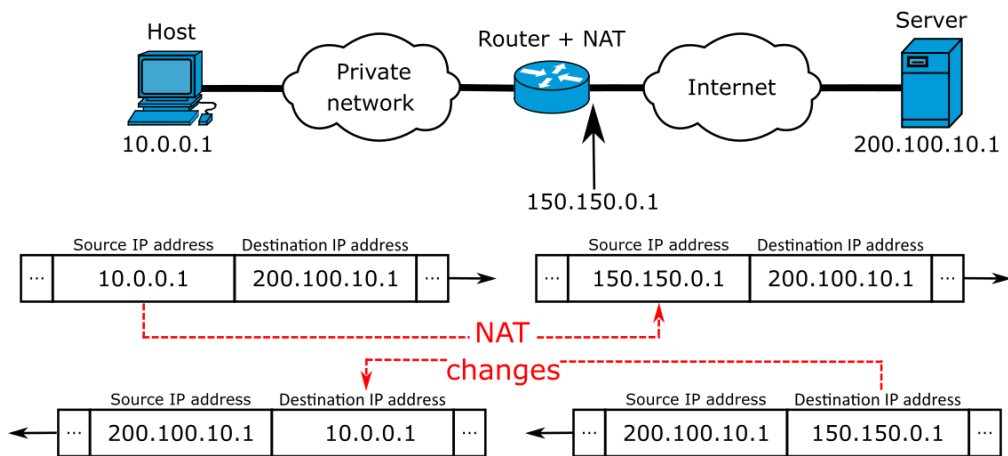


Figure 2.26: NAT architectures

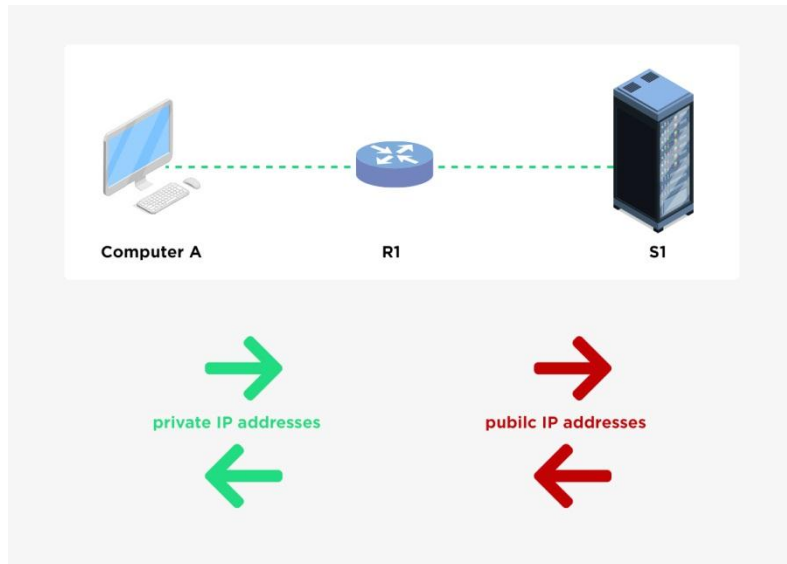


Figure 2.27: NAT connections

2.3.2 Show Dynamic Host Configuration Protocol

What is DHCP?

Dynamic Host Configuration Protocol (DHCP) is a client or server protocol that **automatically** set an Internet Protocol (IP) and other related configuration information such the subnet mask and default gateway IP.

How DHCP works?

DHCP works by automatically assigns an IP address and other information to each host on the network to enable a networking efficiently.

Why DHCP is used?

DHCP used to automate the process of configuring devices on IP networks by allowing the network services such as DNS to communicate based on UDP or TCP.

What are the 4 phase in DHCP?

DHCP operations fall into four phases:

- i) Server discovery,
- ii) IP lease offer,
- iii) IP lease request, and
- iv) IP lease acknowledgement.

These stages are often abbreviated as DORA for Discovery, Offer, Request, and Acknowledgement.

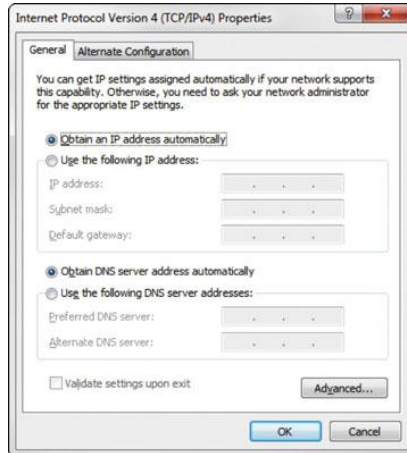


Figure 2.28: The DHCP setup in Internet Option for windows

Should DHCP to be set ON or OFF?

DHCP is ON means it hands out IP addresses for the computer to determine. If DHCP is OFF, the configuration is manually.

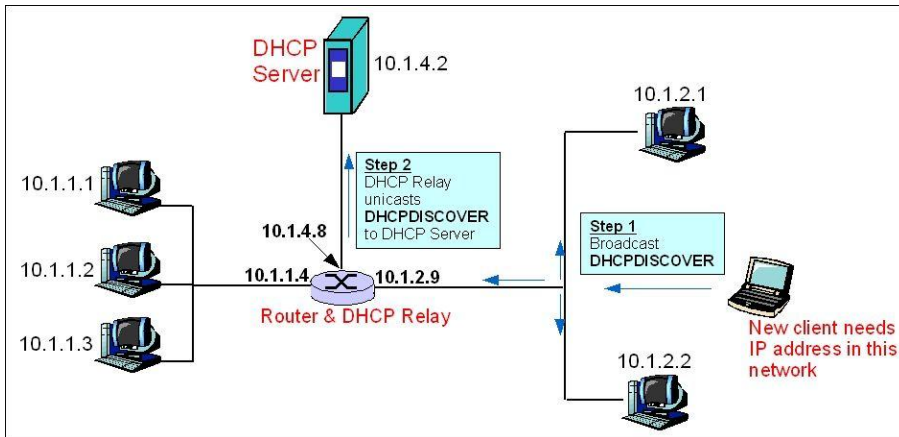


Figure 2.29: DHCP connections



Figure 2.30: DHCP links

2.3.3 Show Domain Name System

What is DNS?

The domain name system (DNS) is a naming database where the internet domain names are located and translated into internet protocol (IP) addresses. The domain name system help people use to locate a website easily.

What is example of domain name system?

DNS use mapping alphabetic names to replace the numeric Internet Protocol (IP) addresses example `www.example.com` is the URL where `example.com` is the domain name, and `www` is the hostname. Other example is `www.amazon.com` that refers to `192.0. 2.44`.

How do I find my DNS?

Open the Command Prompt from the Start menu or type "Cmd" into the search in the Windows task bar. Next, type `ipconfig/all` into the command prompt and press "Enter". Look for the field labelled "DNS Servers." The first address is the primary DNS server, and the next address is the secondary DNS server.

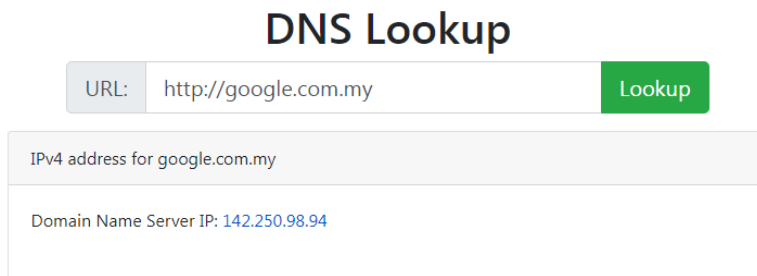


Figure 2.31: This website can search the actual IP address for DNS <https://www.whatismyip.com/dns-lookup/>

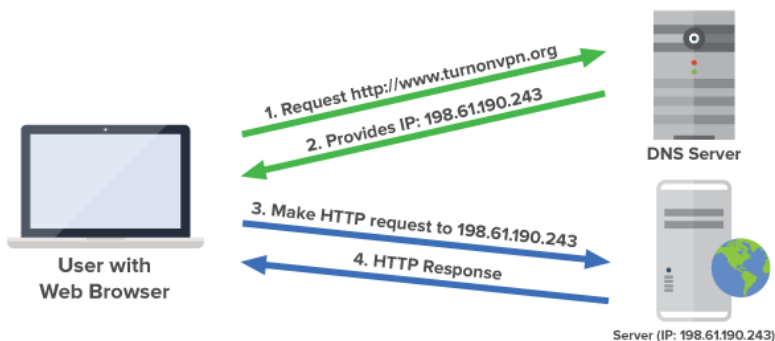


Figure 2.32: Example of DNS connections

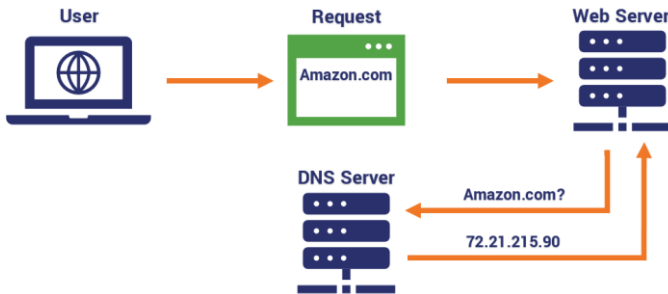


Figure 2.33: Other example of DNS connections

2.3.4 Apply ENUM

What is ENUM and how it works?

ENUM defines as the international telephone number that integrates the public switched telephone network (PSTN) call with IP addressing telephony. Its works by translating standard telephone numbers into special IP addresses.

What is ENUM in VoIP?

ENUM or called as **E.164** standard works by translates telephone numbers into Internet addresses. ENUM is supported by certain **SIP Proxies** technologies such Skype, Kamailio, OpenSIPS and others.

Discuss the types of ENUM?

There are three different types of ENUM:

- Public User ENUM
This type allows the users to manage their own account into the ENUM registry.
- Private Infrastructure ENUM
This type is used by a specific group without using the public domain. This group creates a domain name for each telephone number and links it to a Uniform Resource Identifier (URI).
- Public Infrastructure ENUM
This type is centrally managed by a National Number Administrator. This authority delegates a telephone number to a carrier, which in turn assigns the telephone number to an end-user.

Registration of ENUM number

An ENUM number is registered same like a domain registration. Now, some providers are providing this as free services. Registration needs to be done through a registration service using the standardized ENUM request form. This is then registered with the International Telecommunication Union, Telecommunication Standardization Sector, Telecommunication Standardization Bureau (ITU-T TSB). After this the number is registered, it's ready for international use.



Figure 2.34: Origin word of ENUM

Phone number setup

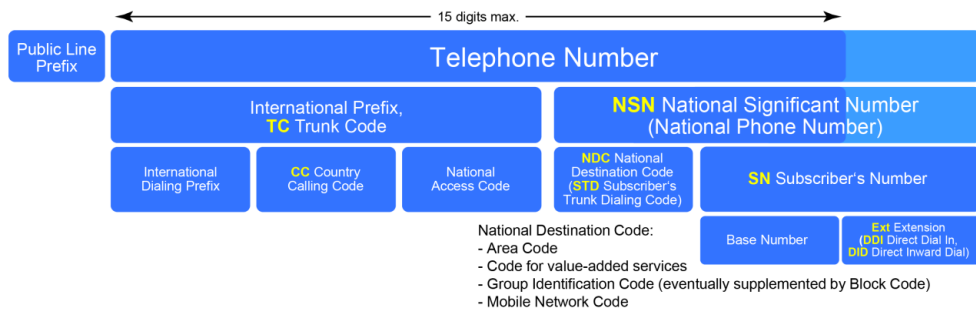


Figure 2.35: ENUM configuration numbers

2.3.5 Show IPv6 Addressing Architecture

What are the major categories in IPv6?

There are three major categories of IPv6 addresses:

- Unicast : For point-to-point networking.
- Multicast : For networking so selected audience (destination).
- Anycast : For open networking to any destinations.

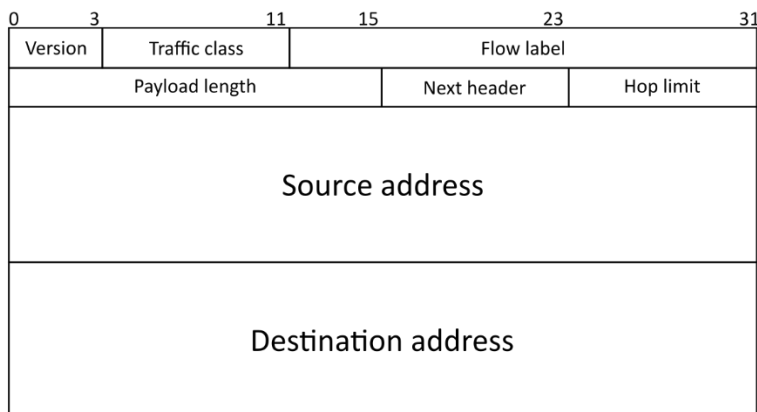


Figure 2.36: IPv6 format frame

How is an IPv6 address constructed?

IPv6 is represented in **8 groups** of 4 hexadecimal digits where each group representing 16 bits (2 octets). These groups are separated by colons (:). The example of an IPv6 address notation is 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

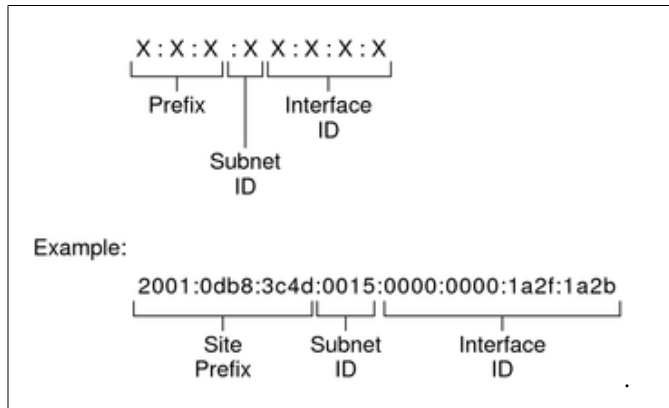


Figure 2.37: IPv6 address architecture

Activities:

Give FOUR (4) example application of IPv6 in technology of NGN.

Chapter 3

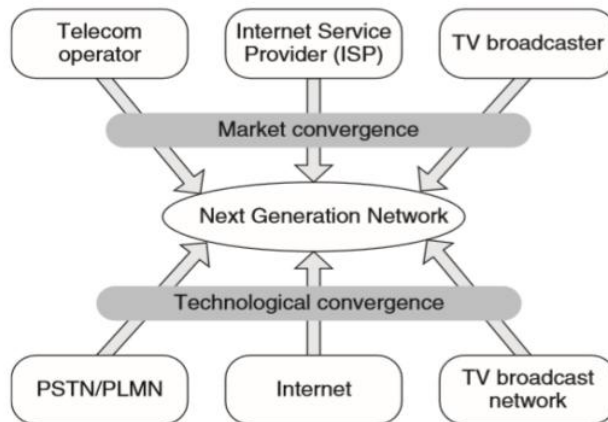
NGN Standards and Transition to NGN

Fixed Broadband Internet Access – Mobile Broadband Internet Access –
IETF Role – ETSI Role – 3GPP Role – IEEE Role – All-IP Network Concept for
NGN – Evolution of PSTN/ISDN to NGN – Session Initiation Protocol (SIP) –
H.323 – SIGTRAN – H.248 – Diameter

3.1 Understand Main Drivers to Next Generation Networks

Drivers	Operators' Motivation
<ul style="list-style-type: none"> ▪ massive growth of data traffic ▪ flat growth of voice market ▪ massive access competition ▪ maturity of IP technology ▪ open standards and architectures 	<ul style="list-style-type: none"> ▪ develop new services easier and faster ▪ enhance flexibility ▪ reduce operational expenditures ▪ replace of old platforms at their end of lifecycle

Picture 3.1: External drivers and internal motivation put pressure on operator's NGN deployments



Picture 3.2: Particular drivers for NGN

3.1.1 Explain Fixed and Mobile Broadband Internet Access

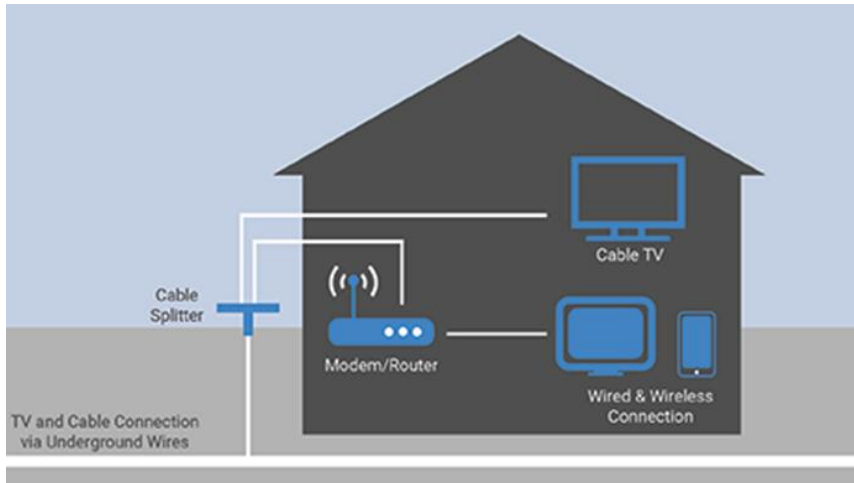
What is Fixed Broadband Internet Access?

Fixed broadband Internet Access is referred to any high-speed data transmission for home or business premise at a fixed location using a variety of technologies, including DSL, fibre optics or wireless. It also refers as a high-speed home internet connections that are "always on" at fixed locations.

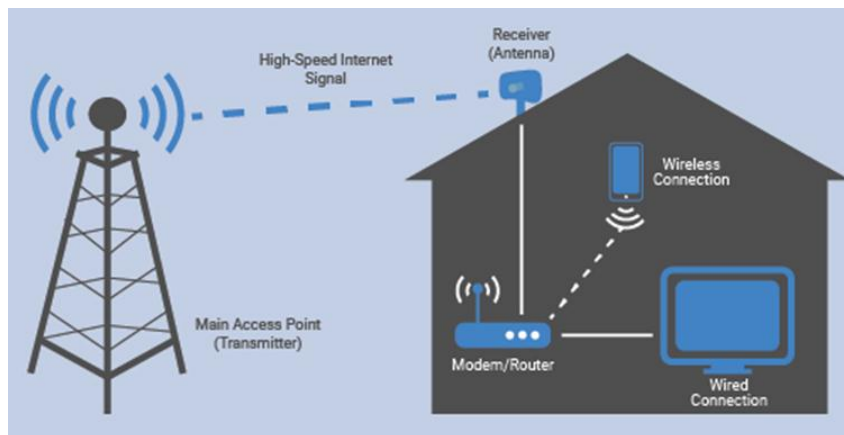
Types of Fixed Broadband Connections

The types of fixed broadband connection are depending on location, packages and prices. The most common are:

- i. Digital Subscriber Line, DSL (Streamyx)
- ii. Fibre optic (Unifi)
- iii. Fixed wireless
- iv. Satellite (<https://connectme.my/home>)
- v. Broadband over power lines, BPL (TNB)



Picture 3.3: Illustration on how cable internet home network works



Picture 3.4: Illustration on how fixed wireless internet home network works

What is Mobile Broadband Internet Access?

- Mobile Broadband Internet Access is referred to wireless Internet access existed in portable or moving devices such a portable modem, USB modem, tablet, smartphone or other mobile or moving device. Mobile broadband often uses a frequency spectrum from 200 MHz to 4000 MHz.

Second generation (2G) from 1991:

	Speeds in kbit/s	
	down	up
• GSM CSD	9.6	
• CDPD	up to 19.2	
• GSM GPRS (2.5G)	56–115	
• GSM EDGE (2.75G)	up to 237	

Third generation (3G) from 2001:

	Speeds in Mbit/s	
	down	up
• UMTS W-CDMA	0.4	
• UMTS HSPA	14.4	5.8
• UMTS TDD	16	
• CDMA2000 1xRTT	0.3	0.15
• CDMA2000 EV-DO	2.5–4.9	0.15–1.8
• GSM EDGE-Evolution	1.6	0.5

Fourth generation (4G) from 2006:

	Speeds in Mbit/s	
	down	up
• HSPA+	21–672	5.8–168
• Mobile WiMAX (802.16)	37–365	17–376
• LTE	100–300	50–75
• LTE-Advanced:		
• while moving at high speeds	100	
• while stationary or moving at low speeds	up to 1000	
• MBWA (802.20)	80	

Fifth generation (5G) from 2018:

	Speeds in Mbit/s	
	down	up
• HSPA+	400–25000	200–3000
• Mobile WiMAX (802.16)	300–700	186–400
• 5G	400–3000	500–1500

Picture 3.5: Mobile network generations and standards with average rate of transmission

MOBILE BROADBAND	FIXED BROADBAND
• 100% mobility/Portable	• Fixed at Homes and Offices
• Affordable communication service	• Priced depend on speed subscription
• Simple and free to set up	• Involves initial installation cost
• Coverage limitations	• Wider coverage and connection stability
• Mobile Device should be 4G compatible	• Device compatibility is unnecessary
• Maximum speed up to 100mbps dependent on the coverage area.	• On Normal Ethernet cable maximum speed is 100mbps and on Fibre Gigabyte speed is assured.
• Limited multiple usage	• Multiple usage
• Always have restrictive usage caps with high costs when you exceed them	• Guaranteed Unlimited data

Activities:

List down (THREE) 3 broadband internet providers that exist in Malaysia for both Fixed and Mobile network

Fixed Broadband Internet Providers	Mobile Broadband Internet Providers

3.2 Remember Standardization Synergy of IETF, ETSI, 3GPP and IEEE



Picture 3.6: General information about IETF

3.2.1 Identify the IETF Role

What is IETF?

The Internet Engineering Task Force (IETF) is an open standards organization that develops and promotes the Internet standards for world wide application.

What is the role of the IETF?

An IETF role is to develop an open standard through open processes to make the internet network in better application.

3.2.2 Identify the ETSI Role



Picture 3.7: General information about ETSI

What is ETSI?

The ETSI or European Telecommunications Standards Institute is an independent and non-profit organization for standardize the devices and system for the use of field of information and communication system.

What is the role of ETSI?

ETSI roles are to test and support the development of global technical standards for ICT technologies, applications and services.

3.2.3 Identify the 3GPP Role



Picture 3.8: General information about 3GPP

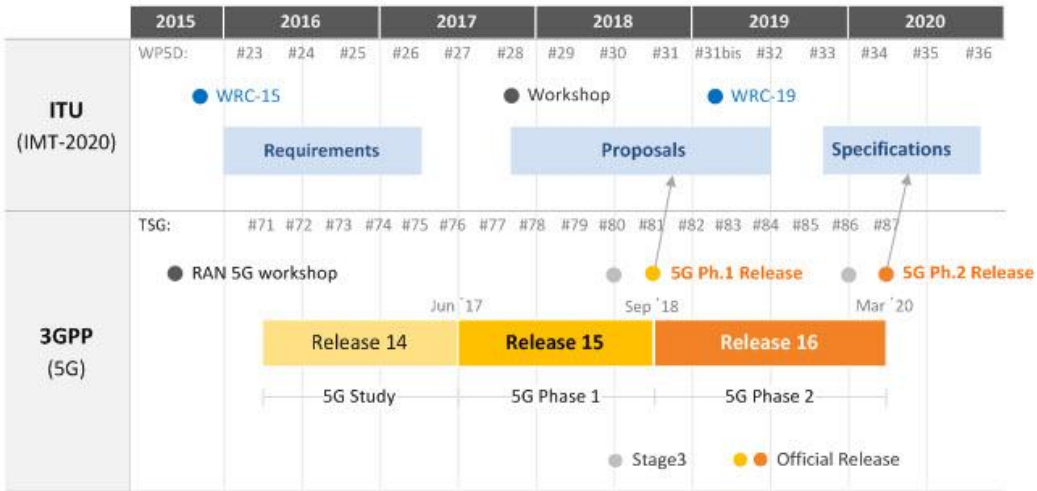
What is 3GPP?

The 3rd Generation Partnership Project or 3GPP is an organization that develops the **term, protocol and specification for global mobile communication standards**. 3GPP is a consortium with several regional telecommunication organizations as primary members and

a variety of other mobile communication organizations as associate members and market representation partners.

What is the role of 3GPP?

3GPP roles are to collaborate between world mobile telecommunication organization and telecommunication scholar by creating a mobile communications standard and beyond. The 3GPP organizes its work into three different fields: Radio Access Networks, Services and Systems Aspects, and Core Network and Terminals.



Picture 3.9: Timeline 3GPP and ITU current project stage of 5G standard and specification

3.2.4 Identify the IEEE Role

Institute of Electrical and Electronics Engineers
Professional association



spectrum.ieee.org

Location: New York, New York, US;
Headquarters: Piscataway, New Jersey, United States
Customer service: 00 1 732-981-0060

Picture 3.10: General information about IEEE

What is IEEE?

The Institute of Electrical and Electronics Engineers (IEEE) (pronounced I-triple-E) is a professional association for electronic engineering and electrical engineering engineer and scholar. The IEEE main office is in New York City and its operations center in Piscataway, New Jersey. It was formed in 1963 from the amalgamation of the American Institute of Electrical Engineers and the Institute of Radio Engineers.

What is the role of IEEE?

The IEEE is a professional association that develops, defines, and reviews the electronics and computer science specification and standards. The IEEE mission is to foster the technological innovation, research and engineering development for the benefit of humanity.

Activities:

List down briefly the purpose of the standardization bodies of telecommunication network below:

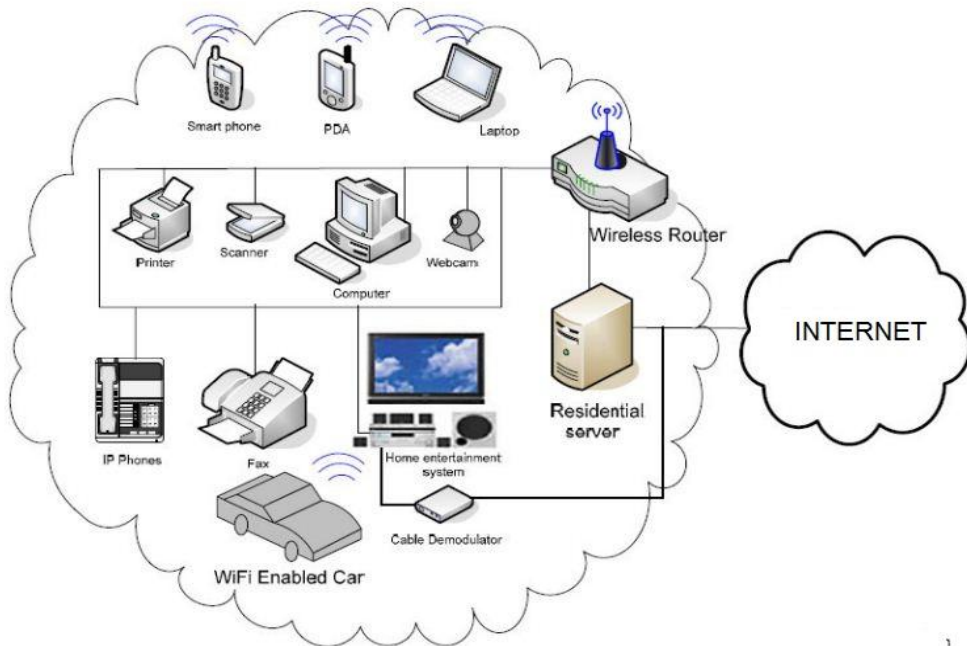
Standardization bodies	Purpose / Role
IETF	
ETSI	
3GPP	
IEEE	

3.3 Understand All-IP Network Concept for NGN

What is All-IP Network?

An all-IP network is an IP packet-based network that access inter-connected to different types of devices simultaneously at a particular networking system. The all-IP network is one of key features towards the next generation networks (NGN).

3.3.1 Explain All-IP Network Concept for NGN



Picture 3.11: All IP home network environments

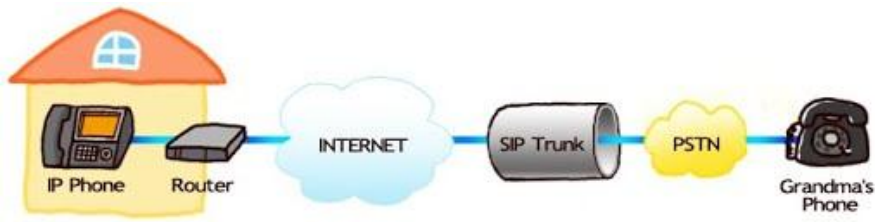
Activities:

In your opinion, in the coming technology, what are the electrical and electronic appliances will be given IP in telecommunication networks. List down THREE (3) appliances

All IP future appliances network
1.
2.
3.

3.4 Apply the understanding of Migration in PSTN Networks to NGN

Although a traditional analog phone line in PSTN and the IP phone are designed with very different networks, a call from both sides can be establish due to the migration of PSTN network in NGN. Several protocols need to apply in between of both systems to connect and convert the analog voice or data to digital data or vice-versa.

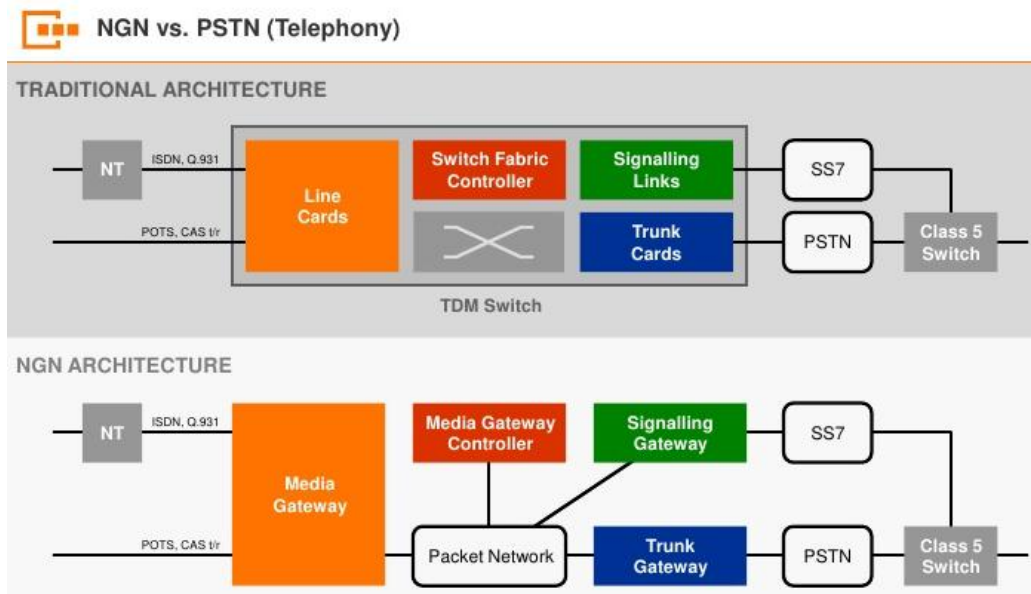


Picture 3.12: Telecommunication network between IP Phone and Grandma's Phone using SIP Trunk

There are a few ways to connect an analog phone line and an IP network:

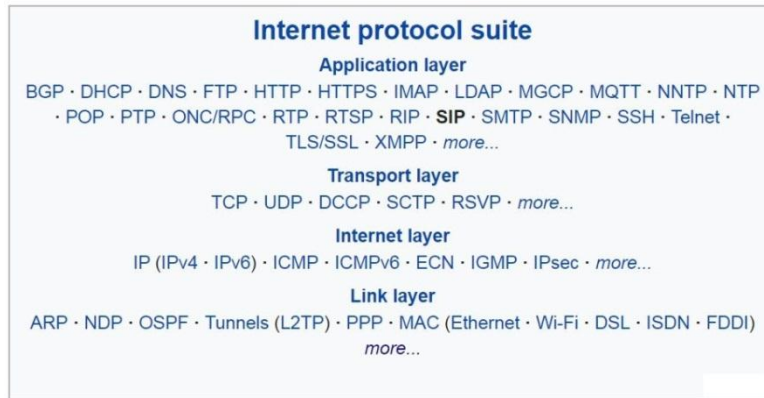
- i. Using Analog Telephony Adaptor (ATA). The ATA is a device for connecting traditional analog telephones, fax machines, and other similar functioning devices to a digital telephone system.
- ii. Using Media Gateway protocols. There is few media gateway protocol can be implement to translation and converts media streams from POTS, SS7, 2G and private branch exchange (PBX) systems to digital formatting standard such HSPA+ and LTE.
- iii. Using Session Initiation Protocol such SIP Trunk. A SIP trunk is the method conversation from an analog phone line transmission to digital medium.

3.4.1 Evolution of PSTN/ISDN to NGN



Picture 3.13: PSTN Networks to NGN network architecture (where NT refer to user)

3.5 Understand Signaling protocols for NGN



Picture 3.14: The list of internet protocols in different OSI layer and the location of SIP

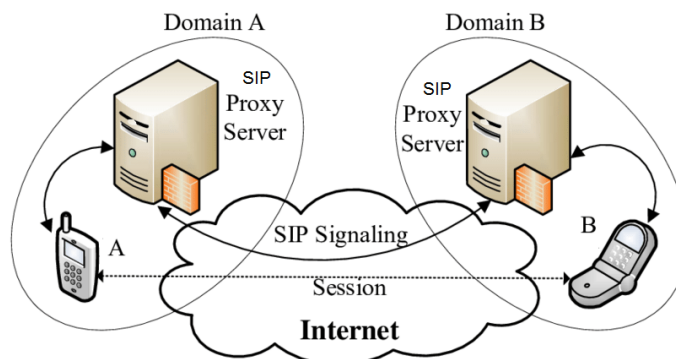
3.5.1 Explain the SIP

What is SIP?

The Session Initiation Protocol or SIP is defined as a signaling protocol used for initiating, maintaining, and terminating real-time sessions include voice, video and messaging/data applications.

Where the Session Initiation Protocol used for?

The SIP used to enable the Voice over Internet Protocol (VoIP) and supports voice calls, video conferencing, instant messaging, and media distribution. The SIP also used to control the interactive communication sessions such chat and instant messaging, as well as interactive games and virtual reality.

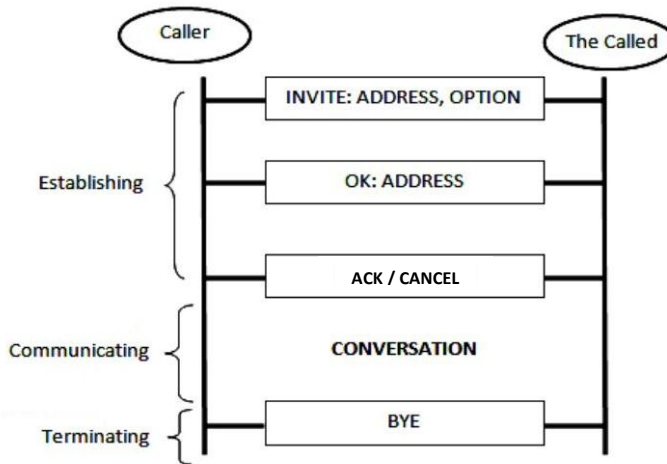


Picture 3.15: Simplified architecture of a SIP network

Example of SIP Protocol Addresses

SIP is flexible in specifying the address. Below are sample of SIP standard format use in IPv4, email and IP call;

- i. IPv4 address : sip:rais@201.23.45.76
- ii. E-mail address : sip:rais@polisas.edu.my
- iii. Phone Number : sip:rais@09-5655300



Picture 3.16: A simple session or process using SIP

*Table 3.1: Detail description of simple session/process using SIP

Terms	Function
INVITE	These messages are used by the caller to initialize a session.
OPTIONS	These messages are used to request information about the caller capabilities.
ACK	The caller acknowledges the answer of the call by the called party.
BYE	These messages are used to terminate an established session.
REGISTER	These messages are used by SIP user agent to register the current IP address.
CANCEL	These messages are used to cancel the initialization process.

3.5.2 Explain the H.323

What is H.323?

H.323 is protocol define by ITU Telecommunication Standardization Sector (ITU-T) to provide an audio-visual communication sessions on any packet network in synchronized manner.

What is H.323 used for?

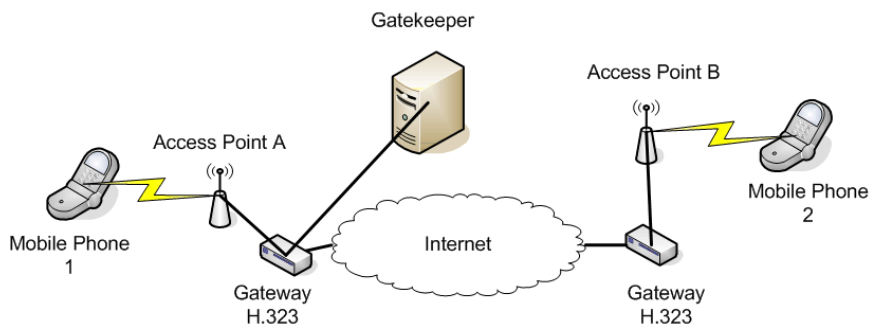
H.323 provides a specification and standards for equipment and services to multimedia packet based data into the networks and specifies transmission protocols for real-time delivery for video, audio and data.

What is example application of H.323?

H.323 are commonly used in IP based video conferencing, Voice over Internet Protocol (VoIP) and Internet telephony.

What layer do H.323 involved?

H.323 are located at session layer protocol, which help to set up, support, and tear down the voice or video connection.



Picture 3.17: Example of a H.323 network with a Gatekeeper

*The gatekeepers functions are for call admission control call signaling and bandwidth management as a co-located unit.

3.5.3 Explain the SIGTRAN

What is SIGTRAN?

SIGTRAN is an acronym derived from word SIGNALING TRANSPORT. SIGTRAN is a former IETF working group that produced specifications for protocols that provide reliable datagram service and user adaptations for Signaling System and ISDN communications protocols.

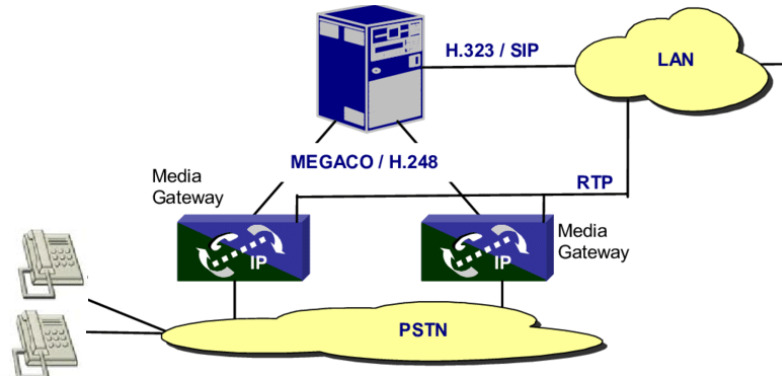
How SIGTRAN works?

SIGTRAN use the same application and call management in SS7 but uses SCTP to carry PSTN signalling over IP.

3.5.4 Explain the H.248

What is H.248?

H.248 or other name is Megaco is media gateway control protocol architecture for providing telecommunication services across a converged internetwork consisting of the traditional public switched telephone network (PSTN) and modern packet networks such DSL. H.248 is designed and developed as a recommendation by the ITU-T.



Picture 3.18: General Scenario for MEGACO/H.248 Usage (where RTP is Real-time Transport Protocol)

3.5.5 Explain the Diameter

What is Diameter?

Diameter is protocol for authentication and authorization management of the use of network. Diameter protocol is evolved from Remote Authentication Dial-In User Service or RADIUS protocol that belongs to the application layer protocols in the internet protocol suite.

What is Diameter protocol used for?

Diameter is a next generation industry standard that used in Long-Term Evolution (LTE) and IP Multimedia Subsystems (IMS) and beyond networks specification.

Activities:

State the function or purpose of all Signaling protocols in NGN below;

Signaling protocols	Function or purpose
SIP	
H.323	
SIGTRAN	
H.248	
Diameter	

Chapter 4

Broadband Internet: The Basic for NGN

ITU – DSL – ADSL – Cable Access Networks – Evolution of Mobile Broadband
– 4G – LTE/LTE Advanced – WiMAX 2.0 – IP Multimedia Subsystem (IMS) –
Next Generation Mobile Services

4.1 Remember ITU's Work on Broadband

International Telecommunication Union



What is ITU?

ITU or International Telecommunication Union is a specialized agency of the United Nations that responsible for all issue related to information and telecommunication technologies. ITU Established in 1865 as the International Telegraph Union before turn up as International Telecommunication Union is one of the oldest international organizations in operation in the world.

What is the work of ITU?

ITU objectives are to promote and develop the telecommunication networks, access and services by fostering cooperation among governments and non-governmental organizations includes the network operators, service providers, equipment manufacturers, scientific and technical organizations, financial organizations and development organizations.

What are the 3 ITU sectors?

The ITU are divided into 3 main sectors:

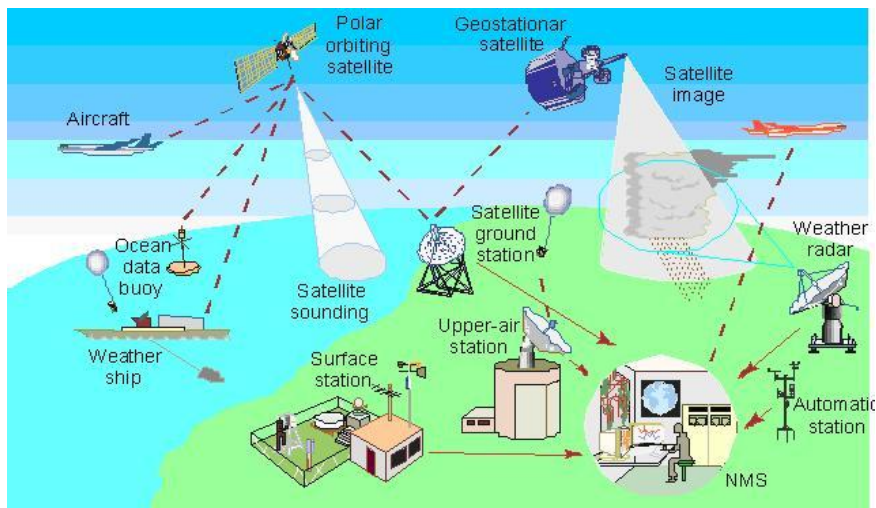
- i. ITU-R – For allocating the radio frequencies and managing the satellite orbit and access technologies;
- ii. ITU-T – For developing technical telecommunication specification and standards;
- iii. ITU-D – To support and improve the development of global access efforts in ICT.

What is the function of International Telecommunication Union?

ITU role are to act as a catalyst in fostering the cooperation among the government in order to promote the global telecommunication technologies.

Who are the members in ITU?

Currently there are 193 members represent each different country in ITU. The recent member is South Sudan.



Picture 4.1: ITU-R works on Global Observing System

* NMS refer to Network Management System that designed for monitoring, maintaining and optimizing the network.

4.1.1 Identify the Work of ITU-T, ITU-R and ITU-D

What does ITU-R stand for?

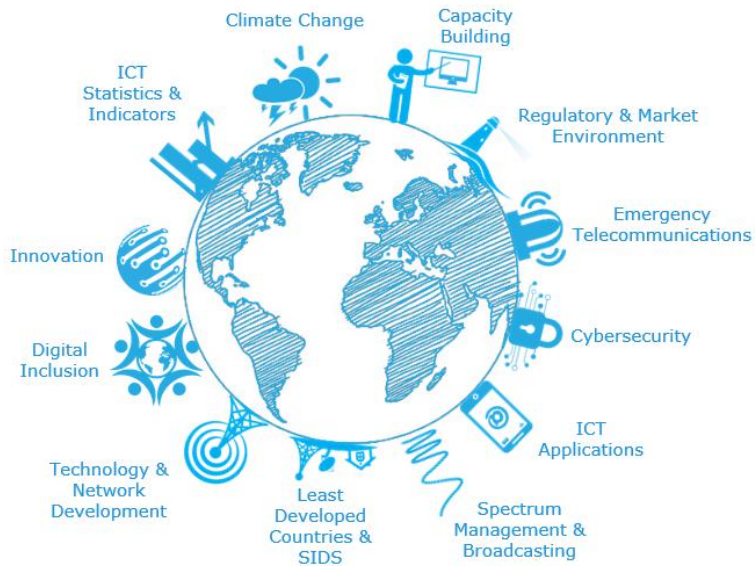
The ITU-R is ITU Radio Communication Sector is one of the divisions that responsible for radio communication.

What is role of ITU-R?

ITU-R role are to manage the international radio frequency spectrum and satellite orbit resources. It also are role to develop the standardization for radio communication systems and ensuring the effective use of the spectrum.

What is ITU-D?

The ITU-D refers to ITU Telecommunication Development Sector that responsible for creating the policies, regulation and providing training programs and financial strategies for developing countries.



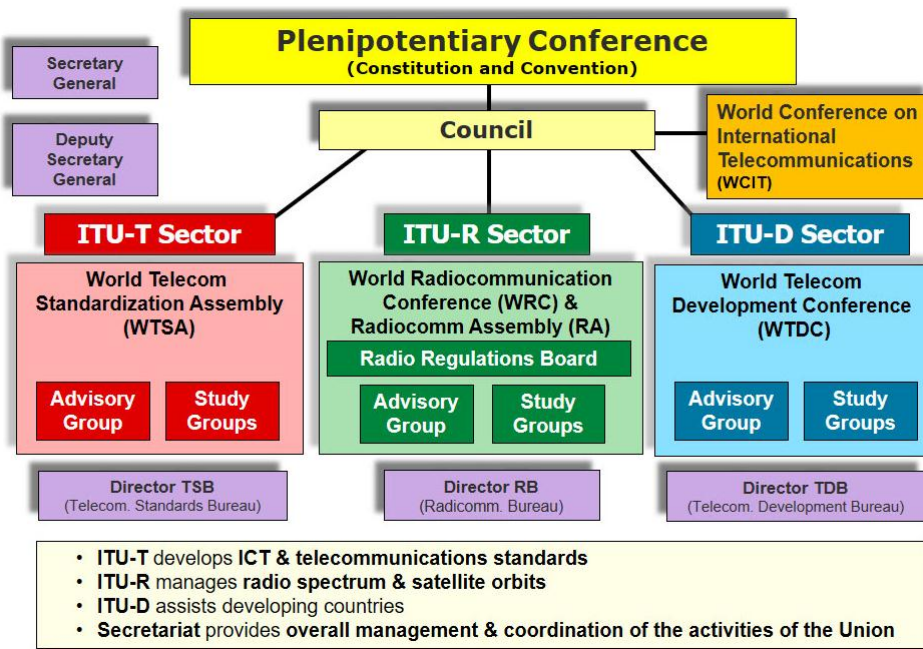
Picture 4.2: ITU-D focus area
*SIDS is Small Island Developing States

What is ITU-T?

ITU-T refer to ITU Telecommunication Standardization Sector that fostering the cooperative standards of telecommunications equipment and systems. It was formerly known as CCITT (Consultative Committee for International Telephony and Telegraphy) and located in Geneva, Switzerland.



Picture 4.3: ITU-T collaboration partnerships



Picture 4.4: ITU organization structure

Activities:

State the difference role of ITU-T, ITU-R and ITU-D.

Type of ITU	Role
ITU-R	
ITU-D	
ITU-T	

4.2 Apply DSL and Cable Access Networks

What does DSL mean for Internet?

DSL or Digital Subscriber Line is internet technologies and the predecessor to dial-up that uses the local phone line to transfer data via internet. DSL connections can be in symmetric and asymmetric.

What is DSL used for?

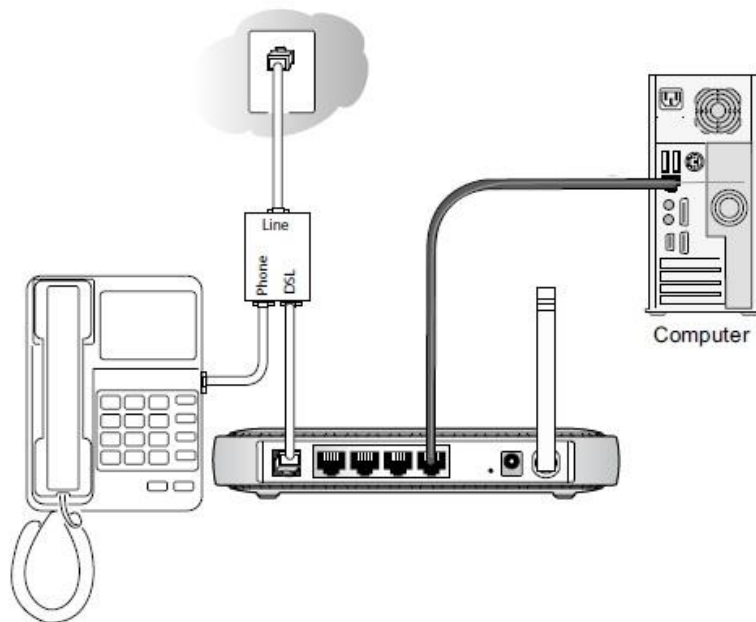
DSL is an internet connection working through telephone lines and allows the telephone calls at the same time. It works by separates the telephone signals into different slot of frequencies frame.

How DSL works?

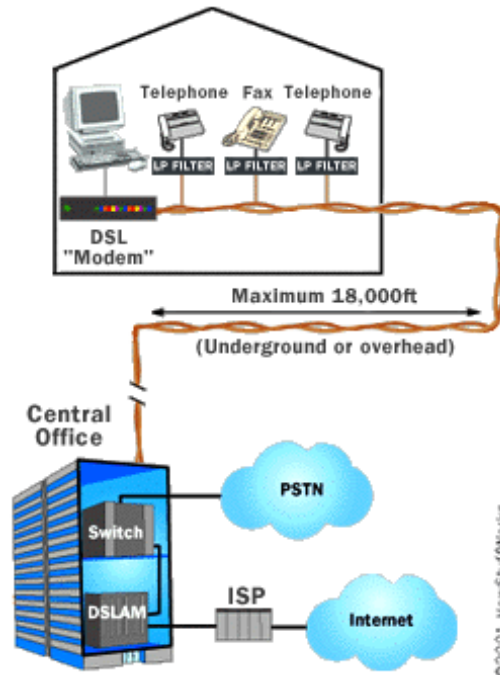
DSL enable the high speed bandwidth connection from an existing telephone network. DSL works within the frequencies that the telephone doesn't used while making a phone calls.

How is DSL installed?

The DSL technology comes with modem kit that provides from the provider. The kit contains a DSL modem, a phone cable, an Ethernet cable, and DSL splitters (with filters). DSL is installed using Ethernet cable to a splitter and wall jack that serves the phone connection.



Picture 4.5: Simple connection of DSL



Picture 4.6: DSL network connection from CO to home

What is DSLAM?

DSLAM is Digital Subscriber Line Access Multiplexer that defined as a network device that located central office purposes to receive the signals from multiple customer of DSL connections and transferred the signals on a high-speed backbone line using multiplexing techniques.

What is difference between DSL and ADSL?

ADSL is one of several types of DSL technologies. ADSL allows the download data transmission much faster than upload.

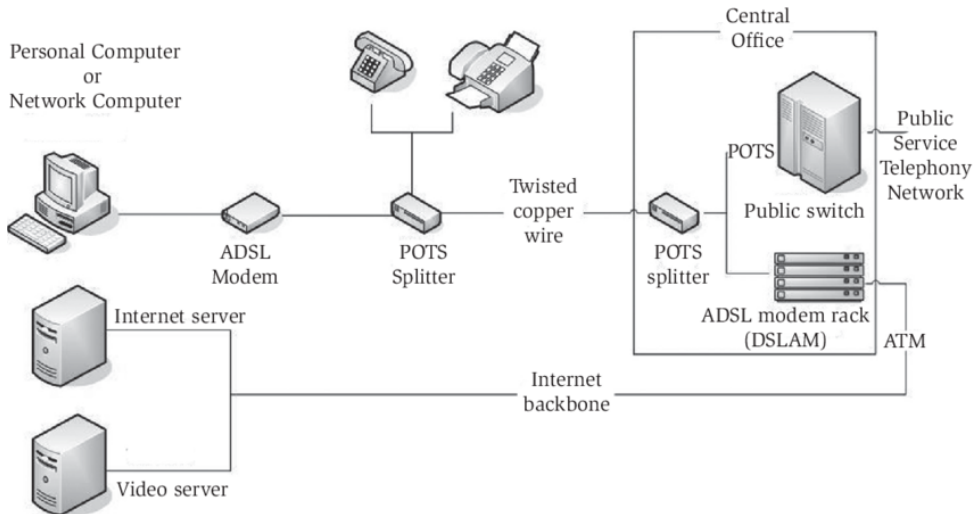
Table 4.1: Types of DSL

Type	Download Speed	Upload Speed	Distance from CO
ADSL	1.5 to 9 Mbps	16 to 640 Kbps	18,000 feet
SDSL	1.544 Mbps	1.544 Mbps	10,000 feet
HDSL	1.544 Mbps	1.544 Mbps	10,000 feet
VDSL	20-50+ Mbps	Up to 20 Mbps	< 5,000 feet

4.2.1 ADSL Network and Access Architectures

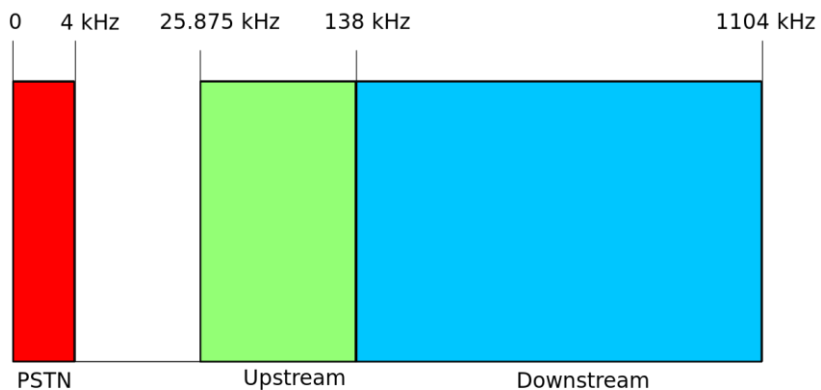
What is ADSL connection?

ADSL is a term stand for Asymmetric Digital Subscriber Line that allowed the broadband connection that works through the existing copper wires of telephone lines. ADSL designed mainly for the use of home broadband and small business premise.

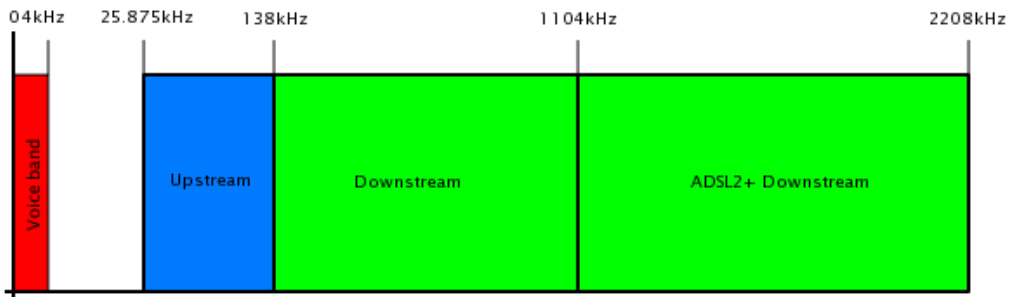


Picture 4.7: ADSL Network and Access Architectures

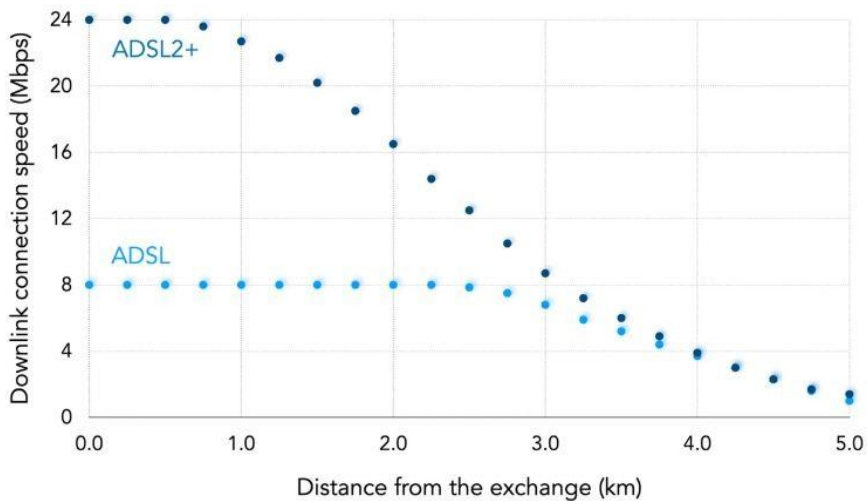
4.2.2 ADSL Frequency Bands and Modulation



Picture 4.8: Frequency plan for ADSL



Picture 4.9: Frequency plan for ADSL2+



Picture 4.10: Differences between ADSL and ADSL2+

Why always get low speed for ADSL compare to its capability?

The reduction speed happens because of higher latency between the connections. Other reason is cause by overloaded systems when too many user online using the same transmission at the same time simultaneously.

What is ADSL modulation type?

ADSL uses DMT or Discrete Multitone modulation.

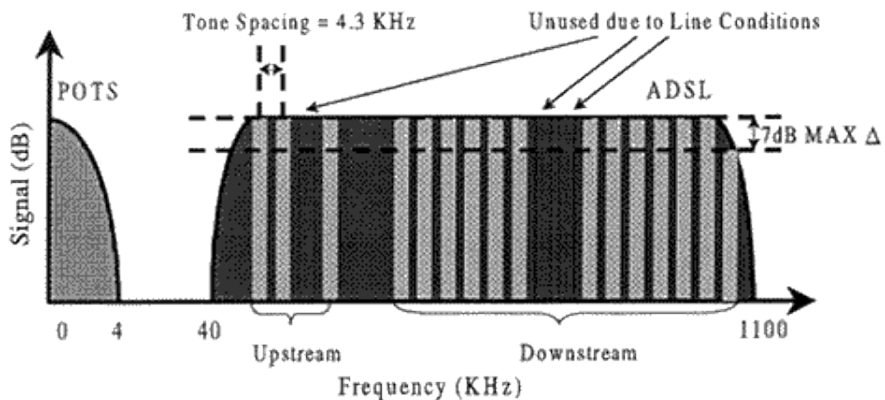
What is Discrete Multitone technique?

Discrete Multitone is a method that separating a DSL spectrum signal so that the usable frequency range is separated into 256 frequency bands (or channels) of 4.3125 kHz each. DMT uses the fast Fourier transform (FFT) algorithm for modulation and demodulation.

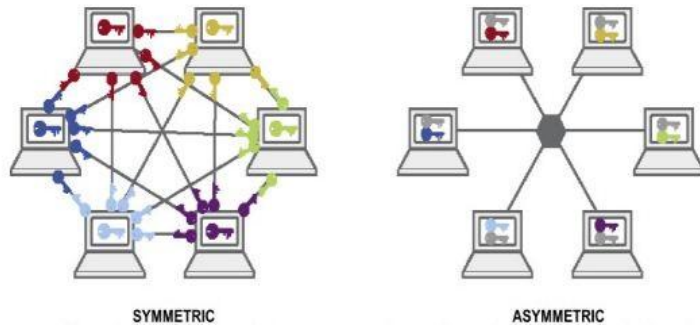
ADSL standards

Version	Standard name	Common name	Downstream rate	Upstream rate	Approved in
ADSL	ANSI T1.413-1998 Issue 2	ADSL	8.0 Mbit/s	1.0 Mbit/s	1998
	ITU G.992.2	ADSL Lite (G.lite)	1.5 Mbit/s	0.5 Mbit/s	1999-07
	ITU G.992.1	ADSL (G.dmt)	8.0 Mbit/s	1.3 Mbit/s	1999-07
	ITU G.992.1 Annex A	ADSL over POTS	12.0 Mbit/s	1.3 Mbit/s	2001
	ITU G.992.1 Annex B	ADSL over ISDN	12.0 Mbit/s	1.8 Mbit/s	2005
ADSL2	ITU G.992.3 Annex L	RE-ADSL2	5.0 Mbit/s	0.8 Mbit/s	2002-07
	ITU G.992.3	ADSL2	12.0 Mbit/s	1.3 Mbit/s	2002-07
	ITU G.992.3 Annex J	ADSL2	12.0 Mbit/s	3.5 Mbit/s	2002-07
	ITU G.992.4	Splitterless ADSL2	1.5 Mbit/s	0.5 Mbit/s	2002-07
ADSL2+	ITU G.992.5	ADSL2+	24.0 Mbit/s	1.4 Mbit/s	2003-05
	ITU G.992.5 Annex M	ADSL2+M	24.0 Mbit/s	3.3 Mbit/s	2008

Picture 4.11: Evolution standards of ADSL



Picture 4.12: DMT Source

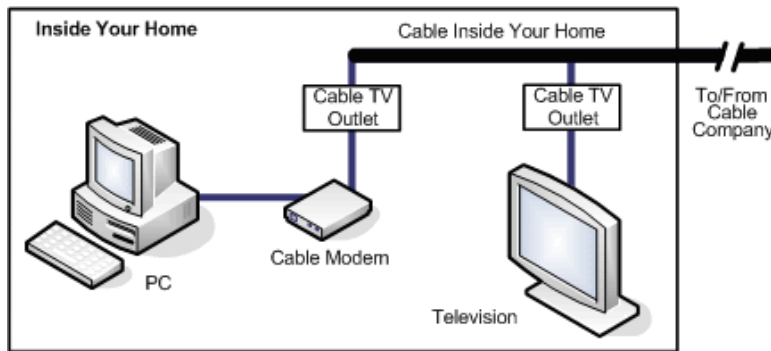


Picture 4.13: Symmetric vs. Asymmetric

4.2.3 Cable Access Network

What is cable access network?

Cable access network or CAS mostly called by cable Internet. It is a form of broadband Internet access that uses commonly the same infrastructure for cable television. Like Digital Subscriber Line and fiber, CAS provides IP network connectivity from provider to user.

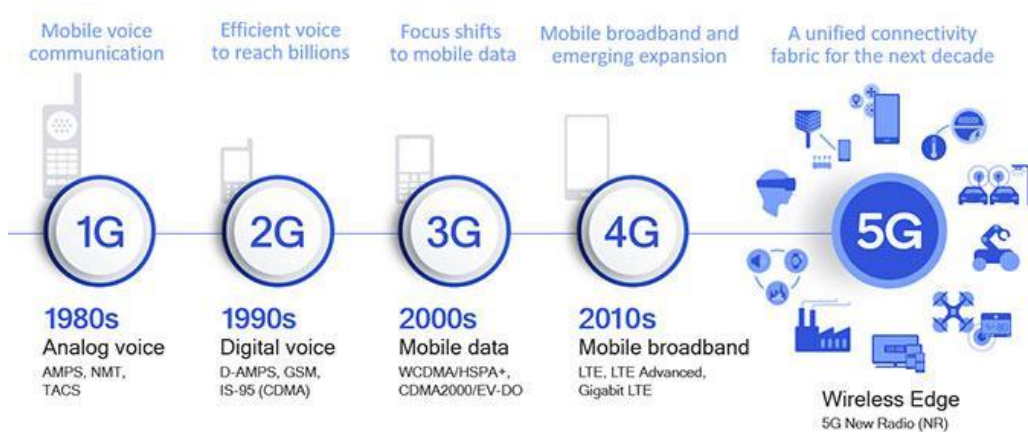


Picture 4.14: Illustration of Cable Access Network

Activities:

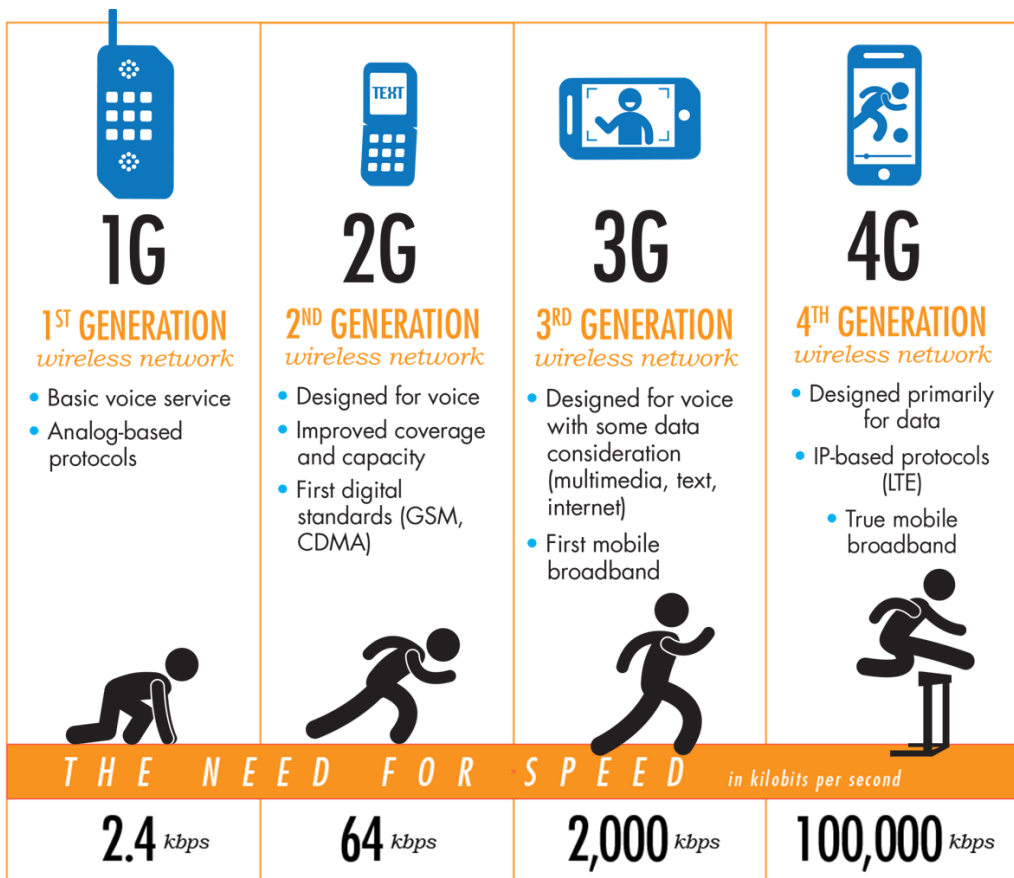
Sketch an ADSL network block diagram with label from central office (CO) to home user.

4.3 Understand Mobile Broadband: Next Generation Mobile Networks



Picture 4.15: Mobile Evolution 1G to 5G

4.3.1 Evolution of Mobile Broadband



Picture 4.16: Mobile Evolution 1G to 4G

4.3.2 4G Standard by 3GPP: LTE



Picture 4.17: LTE logo

What is LTE?

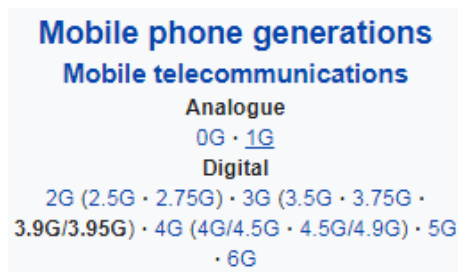
LTE or Long-Term Evolution is a wireless broadband communication standard for mobile devices that evolve based on the GSM, EDGE and UMTS/HSPA+ technologies. It increases the capacity and transmission speed using a different radio interface with core network improvements.

What the LTE definition by 3GPP?

LTE is a mobile standard create by 3GPP in Release 8 documentation in 2008 that has been the basis for the early wave of 4G technologies which are very stable and added with several benefit of enhancements.

What are the motivation for LTE?

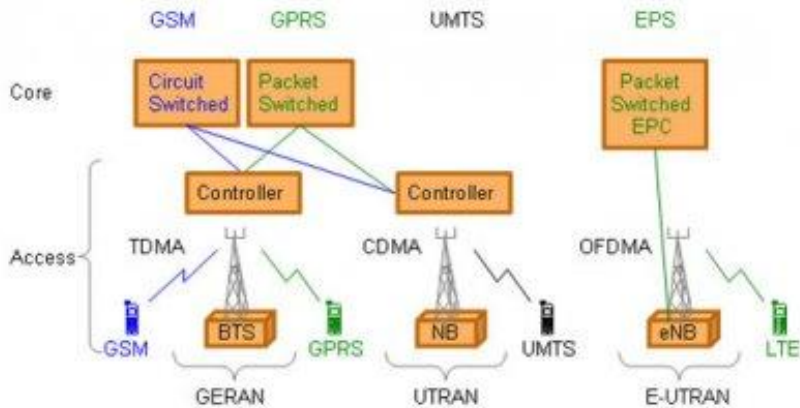
- i. Ensuring the continuity of competitiveness of 3G system for future technologies.
- ii. User demand for higher data rates and higher QoS (quality of service).
- iii. Fully Packet Switched optimised system.
- iv. Demand for cost reduction (CAPEX and OPEX).
- v. Low complexity circuit.



Picture 4.18: The exactly location generation of LTE technology

What is the difference between LTE and LTE-A?

LTE-Advanced is a 4G standard for mobile communication that is one generation beyond LTE.



Picture 4.19: Network Solutions from GSM to LTE
 Where: GERAN stands for GSM EDGE Radio Access Network
 OFDMA stands for Orthogonal Frequency Division Multiple Access
 UTRAN stand for UMTS Terrestrial Radio Access Network

4.3.3 4G Standard by 3GPP: LTE-Advanced



Picture 4.20: LTE-A Logo

LTE-Advanced by 3GPP

LTE-A or LTE-Advanced is created by 3GPP to focus more on higher capacity. It also focuses on higher bit rates in a cost efficient way and at the same time fulfil the requirements from ITU for IMT Advanced or so called as 4G. There is 4 targeted objectives in developing LTE-A such;

- i. Increased peak data rate such Downlink at 3 Gbps and uplink at 1.5 Gbps
- ii. Higher spectral efficiency for maximum at 16bps/Hz to 30 bps/Hz.
- iii. Increased the number of simultaneously active subscribers.
- iv. Improved performance at cell edges, e.g. for DL 2x2 MIMO at least 2.40 bps/Hz/cell.

*What are the main characteristic of LTE-A?

The main new technologies introduced in LTE-Advanced are:

- i. Carrier Aggregation (CA),
- ii. Multi-antenna techniques (MiMO),
- iii. Relay Nodes (RN) and
- iv. Coordinated multi point operation.

*What is other defining of LTE-A?

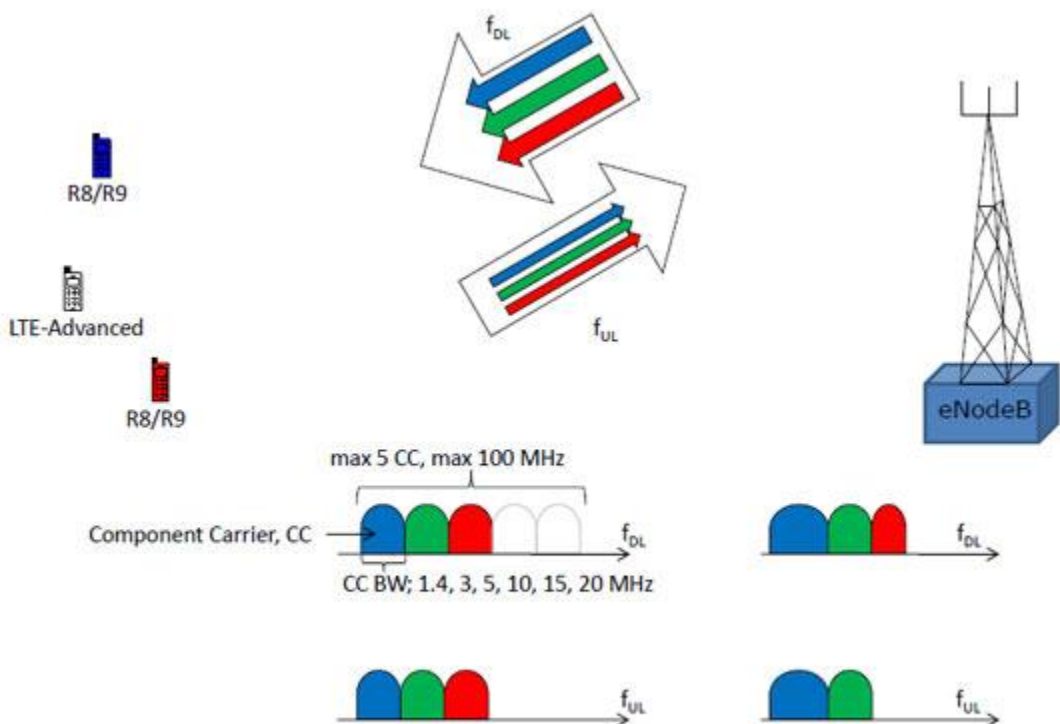
LTE Advanced is a mobile communication standard that formally submitted as a candidate 4G to ITU-T in late 2009 as requirements of the IMT-Advanced. It was standardized by the 3GPP in March 2011 as Release 10.

What is Carrier Aggregation?

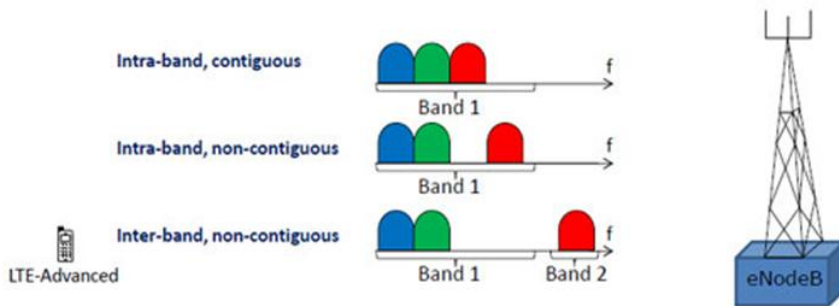
Carrier Aggregation is the most straightforward way to increase capacity by adding more bandwidth. For backward compatibility with R8 and R9 mobiles standard, the LTE-A use the aggregation of R8/R9 carriers. Carrier aggregation can be done in both FDD (Frequency Division Duplex) and TDD (Time Division Duplex).

How Carrier Aggregation is done?

CA works by aggregated two or more carriers that are referred as a component carriers. The component carriers can have a bandwidth of 1.4, 3, 5, 10, 15 or 20 MHz and a maximum of five component carriers can be aggregated. Hence the maximum bandwidth is 100 MHz; the number of aggregated carriers can be different in DL (downlink) and UL (uplink). However, the number of UL component carriers is never larger than the number of DL component carriers. See picture 4.21.



Picture 4.21: In Carrier Aggregation, the UE (user equipment) can allocate the resources of DL and UL up to 5 Component Carriers (CC). The CCs can be in different bandwidths.



Picture 4.22: The Carrier Aggregation of intra-band and inter-band

What is MIMO, Multiple Input Multiple Output?

MIMO or also called as *spatial multiplexing* is used to increase the bit rate through transmission of two or more different data streams using two or more antennas.

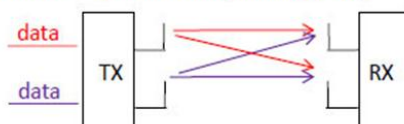
How MiMO works?

MiMO works by using transmitting the same resources in both frequency and time, separated only through use of different reference signals and then receives any resources from that two or more antennas. See Picture 4.23.

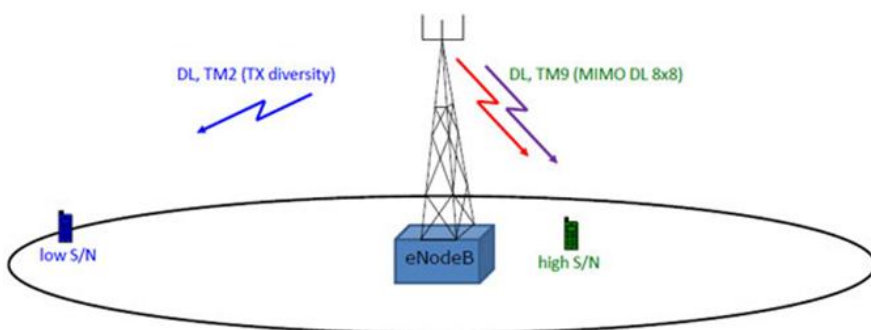
How MiMO can increase bit rate?

MIMO increase bit rate by lowered and improves the S/N (Signal to Noise ratio) which increase the quality of radio channel. See Picture 4.24.

MIMO – Spatial Multiplexing (2x2)



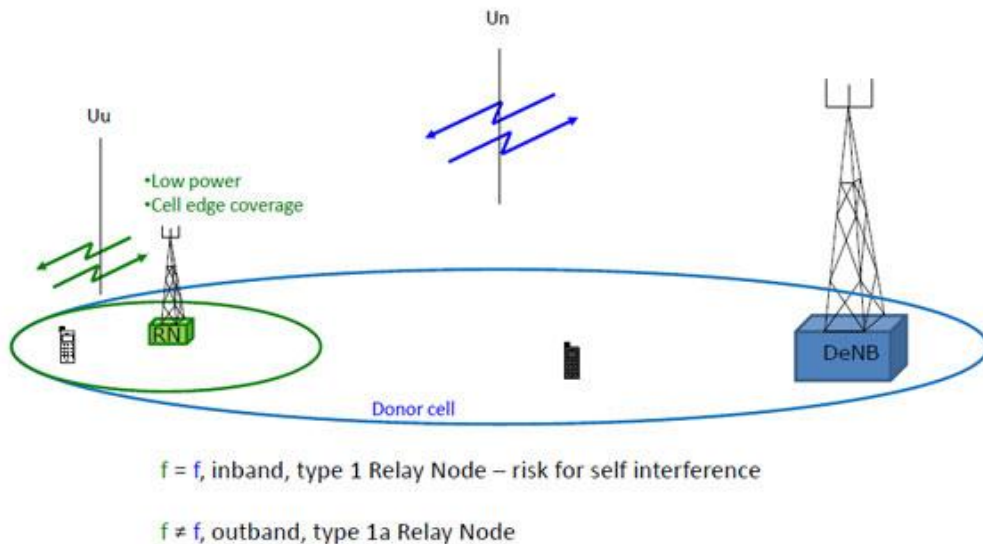
Picture 4.23: The example of 2x2 MIMO (Spatial Multiplexing) where 2 different data streams are transmitted on 2 TX antennas and received by 2 RX antennas. MIMO uses the same frequency and time but separate the use of reference signals.



Picture 4.24: MIMO scenario for high S/N and TX versus low S/N scenarios.

What is Relay Node?

One of characteristic of LTE-A is the efficiency of heterogeneous network planning for large and small cells. It can be done by implementing a devices called Relay Nodes (RNs). The Relay Nodes are low power base stations that provide enhanced coverage and capacity at cell edges and hot-spot areas. It also helps the connection to remote areas without fibre connection.



Picture 4.25: The Relay Node (RN) is connected to the DeNB via the radio interface, Un.

How Relay Node is connected?

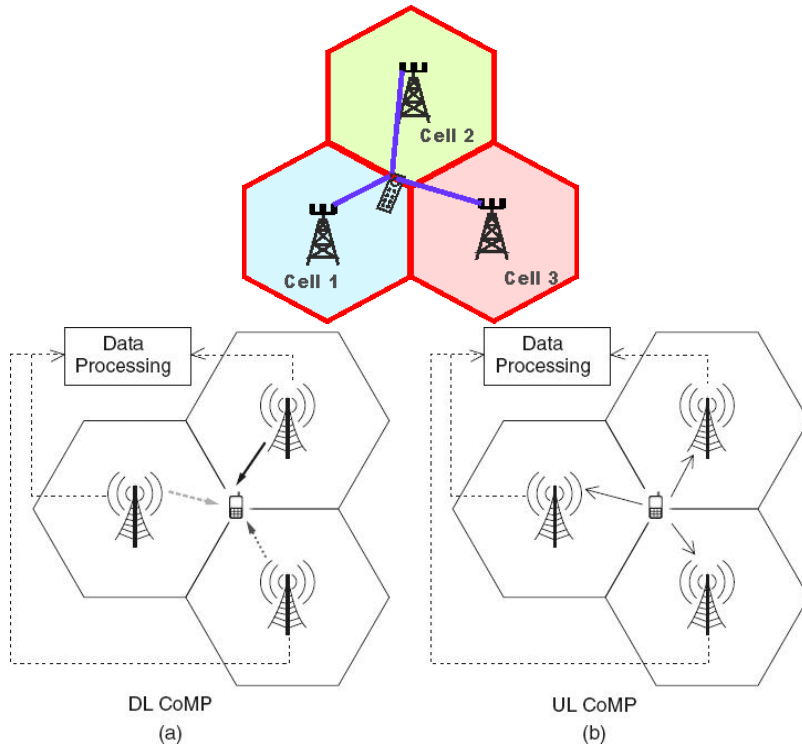
User at the cell edge of the donor cell are connected to the RN via Uu. When the user is closer to the DeNB, it directly connected to the DeNB via the Uu interface. The frequencies used on Un and Uu can be different either outband or inband.

What is Coordinated Multi Point operation (CoMP)?

Coordinated Multi Point operation or CoMP is defined by 3GPP in R11. The main reason to introduce CoMP is to improve network performance at cell edges. In CoMP, a number of TX (transmit) points are provide in coordinated transmission for DL, and a number of RX (receive) points are provide in coordinated reception position for UL.

How CoMP works?

The TX/RX location point is co-located to provide a better coverage in the same sector. CoMP can be done in homogenous networks as well as heterogeneous networks. CoMP is divided into 2 types; a) Joint Transmission; two TX-points transmit to one UE in the same radio resource, b) Dynamic Point Selection; two TX points are ready to transmit, but only one will be scheduled in each subframe.



Picture 4.26: CoMP

4.3.4 4G Standard by IEEE: Mobile WiMAX 2.0



Picture 4.27: IEEE 802.16 working group logo

What is IEEE 802.16?

IEEE 802.16 is a series of wireless broadband standards issued by the IEEE for wireless broadband in metropolitan area networks. IEEE 802.16 family working group also called as WirelessMAN and then commercialized under the name WiMAX or Worldwide Interoperability for Microwave Access.

**WiMAX (Worldwide Interoperability
for Microwave Access)**



Picture 4.28: WiMAX logo

What is WiMAX?

WiMAX or Worldwide Interoperability for Microwave Access is a family of wireless broadband communication standards based on the IEEE 802.16 standards which provide multiple physical layer (PHY) and Media Access Control (MAC) options.

What are the features of WiMAX 4G?

WiMAX offers a set of features with a lot of flexibility in terms of deployment options and potential service offerings. The highlighting features are;

- (1) WiMAX can provide two forms of wireless service;
 - i. Non-line-of-sight (NLOS)– such Wi-Fi using small antenna devices that connects to the WiMAX tower. In this mode, WiMAX uses a lower frequency range – 2 GHz to 11 GHz.
 - ii. Line-of-sight (LOS) – using fixed dish antenna points straight to WiMAX tower. The LOS connection is stronger and more stable with fewer errors. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible of 66 GHz.
- (2) OFDM-based
The WiMAX physical layer is based on orthogonal frequency division multiplexing that offers good resistance to multipath and allows WiMAX to operate in NLOS conditions. Mobile WiMAX uses orthogonal frequency division multiple access (OFDM) as a multiple-access technique, whereby different users can be allocated different subsets of the OFDM tones.
- (3) High Peak Data Rates
WiMAX capable supporting high peak data rates as high as 74Mbps when operating using a 20MHz wide spectrum.
- (4) Scalable Bandwidth
WiMAX has a scalable physical-layer architecture that allows for the data rate to scale easily with available channel bandwidth.
- (5) Adaptive Modulation and Coding (AMC)

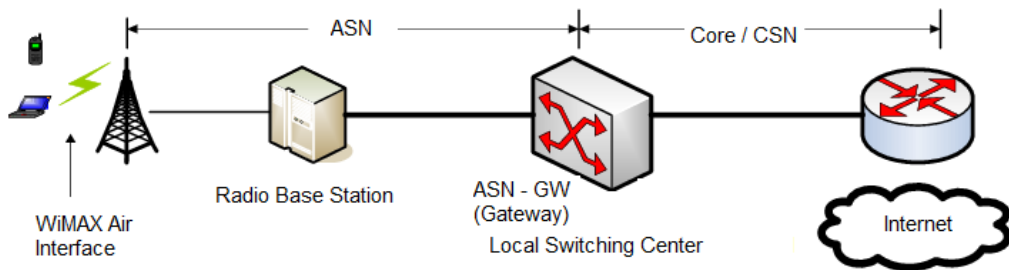
WiMAX supports a number of modulations and forward error correction (FEC) coding schemes and allows the scheme to be changed as per user and per frame basis, based on channel conditions.

- (6) **Link-layer Retransmissions**
WiMAX supports automatic retransmission requests (ARQ) at the link layer for connections that require enhanced reliability. ARQ-enabled connections require each transmitted packet to be acknowledged by the receiver; unacknowledged packets are assumed to be lost and are retransmitted.
- (7) **Support for TDD and FDD**
IEEE 802.16-2004 and IEEE 802.16e-2005 supports both time division duplexing and frequency division duplexing, as well as a half-duplex FDD, which allows for a low-cost system implementation.
- (9) **Flexible and Dynamic per User Resource Allocation**
Both uplink and downlink resource allocation are controlled by a scheduler in the base station. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme.
- (10) **Support for Advanced Antenna Techniques**
The WiMAX solution has a number of hooks built into the physical-layer design, which allows the use of multiple-antenna techniques such as beamforming, space-time coding, and spatial multiplexing.
- (11) **Quality-of-service (QoS) Support**
The WiMAX MAC layer has a connection-oriented architecture that is designed to support a variety of applications, including voice and multimedia services.
- (12) **Robust Security**
WiMAX supports strong encryption, using Advanced Encryption Standard (AES), and has a robust privacy and key-management protocol.
- (13) **Support for Mobility**
The mobile WiMAX variant of the system has mechanisms to support secure seamless handovers for delay-tolerant full-mobility applications, such as VoIP.
- (14) **IP-based Architecture**
The WiMAX Forum has defined a reference network architecture that is based on an all-IP platform. All end-to-end services are delivered over an IP architecture relying on IP-based protocols for end-to-end transport, QoS, session management, security, and mobility.

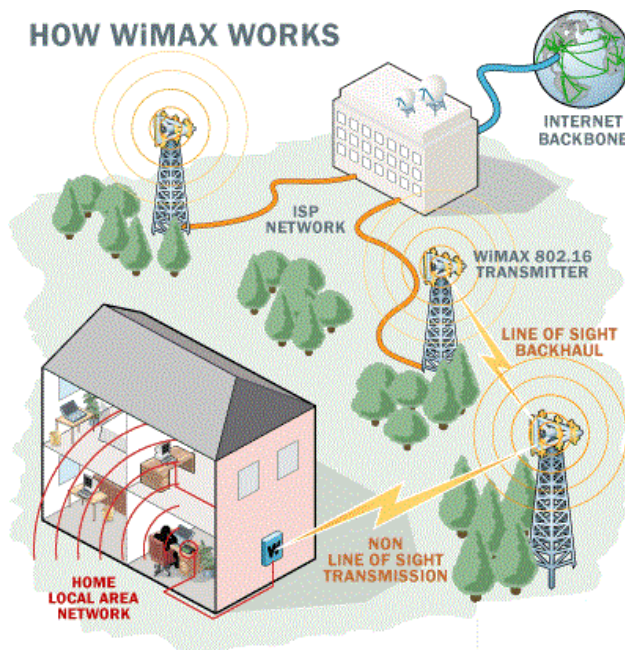
Explain the WiMAX Architecture Network?

WiMAX Architecture Network consisted of three main parts:

- i. Access Service Network (ASN),
- ii. Connectivity Service Network (CSN),
- iii. Mobile Stations (MSs).



Picture 4.29: Mobile WIMAX network Node



Picture 4.30: WiMAX network from CO to home user

4.3.5 IP Multimedia Subsystem (IMS) for NGN

What is IMS?

The IP Multimedia Subsystem or other name IP Multimedia Core Network Subsystem is an architectural framework for delivering IP multimedia services.

Where is IMS used for?

IP Multimedia Subsystem used for delivering multimedia communications services such as voice, video and text messaging over IP networks.

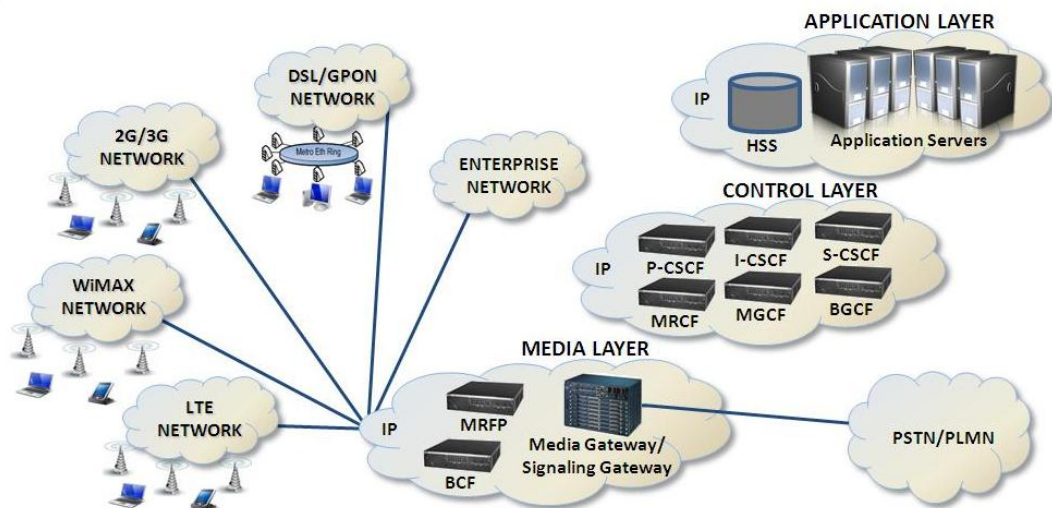
What are the components of IMS?

IMS consists of three components:

- i. The Database Manager (IMS DB)
- ii. The Transaction Manager (IMS TM)
- iii. A set of system services that provide common services to IMS DB and IMS TM.

Why is IMS needed?

IMS approached as an important network for mobile operators future applications. The goal of IMS is to replace the operator's current back-end network architecture with an all IP-based for easier deployment applications.



Picture 4.31: IP Multimedia Subsystem (IMS) network market for NGN

4.3.6 Next Generation Mobile Services

What is Next Generation Mobile Services?

Next-generation mobile networks or NGMN defines as a new concept of wireless communications to deliver voice calls, video streams, website visits, data services and others through the same particular device on a transparent network.

What is NGN network concept?

The concept of NGN is based on packet network which provide a telecommunication services includes the multiple broadband, QoS (quality of service) and enabled transport technologies which are independent from underlying transport-related technologies.

What is the latest generation of mobile network?

5G is the latest generation mobile network. It is a new global wireless standard after 4G networks. 5G enables a new kind of network that is designed to connect virtually everyone and everything together including machines, objects, and devices.



Picture 4.31: NGN and mobile services

*SaaS is Software as a service that serve the software licensing and delivery model.

Activities:

Explain briefly FOUR (4) features in LTE-A and Mobile WiMAX 2.0.

Technology	Features
LTE-A	
Mobile WiMAX 2.0	

Chapter 5

NGN Services

VoIP – VoIP vs. PSTN – SIP in VoIP – IPTV Architecture – Web Services –
Ubiquitous Sensor Network – VPN – IoT – WoT – Software-Defined
Networking (SDN) – Network Functions Virtualization (NFV)

5.1 Apply the Understanding of VoIP

What is VoIP and its purpose?

Voice over Internet Protocol (VoIP) is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular analog phone line.

How VoIP work?

VoIP works by converting the voice into a digital signal and allowing a call directly from a computer.

What are the examples of VoIP?

Skype or Facebook Messenger is examples of VoIP applications. Here are the most common examples of VoIP apps:

- i. Skype.
- ii. Facebook Messenger.
- iii. Google Hangouts.
- iv. Viber.

What are the advantages of VoIP?

- i. Cost savings
With VoIP, the cost only refer to the cost of internet network connection.
- ii. Multi features
VoIP offers a huge range of features such call forwarding, blocking, caller ID and voicemail. VoIP also offers remote management, automatic call distribution and interactive voice recognition.

How do I build a VoIP service provider?

How to Start a Mobile VoIP Business?

Step 1: Set up a VoIP Infrastructure (Hardware and Software).

Step 2: Mobile VoIP Applications.

Step 3: Own Website, with Credit Card Payment Gateway Support.

Step 4: Inter-Connecting with Terminating Carriers.

Step 5: Find Customers.

Step 6: Customer Support.

What is the main disadvantage of VoIP?

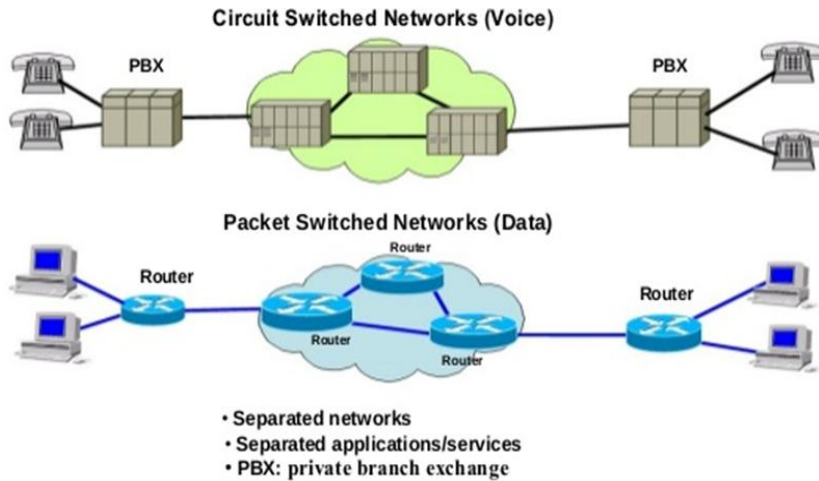
The main disadvantages are weak call quality, call drop and latency.

How much Internet speed do I need for VoIP?

According to the FCC (Federal Communications Commission), VoIP calls require at least 0.5 Mbps download. For streaming video, it uses at least 3 to 4Mbps download speed.

How do I get a VoIP number?

A VoIP phone service provider are provided with VoIP phone number by sign up the VoIP service plan. Most of plans are less expensive compared with cell phone or regular telephone service.



Picture 5.1: PSTN versus Internet (VoIP)

Can a VoIP call be traced?

All VoIP calls are traceable. Even the call has to traverse from the internet to PSTN on its journey.

Who is the best VoIP provider?

Base on internet survey last April 2021, here are the best provider so far:

- i. Nextiva – Best for remote teams.
- ii. RingCentral – Best for growing teams of 50+.
- iii. Ooma – Best for Adding VoIP to Existing SMB Phone Systems.
- iv. Verizon – Best for Adding VoIP to Existing Enterprise Phone Systems.
- v. Grasshopper – Best for Businesses with Fewer Than 10 Employees.

How do I test VoIP quality?

Most Popular VoIP Speed and Quality Test Tools in 2021

- #1) ZDA NET. This tool provides a very good interface.
- #2) Speed Test. SpeedTest is a product by Ookla.
- #3) FreeOLA.
- #4) Ping-test.net.
- #5) 8x8 VoIP Test.
- #6) OnSIP VoIP Test.
- #7) MegaPath Speed Test Plus.
- #8) Bandwidth Place.

Is VoIP and SIP the same?

SIP and VoIP is a different terms, terminology and devices. VoIP stands for Voice over Internet Protocol which covers any phone calls made from the Internet as opposed to traditional telephone lines. SIP is a protocol that used to enable the VoIP.

5.1.1 Show Differences between VoIP and PSTN

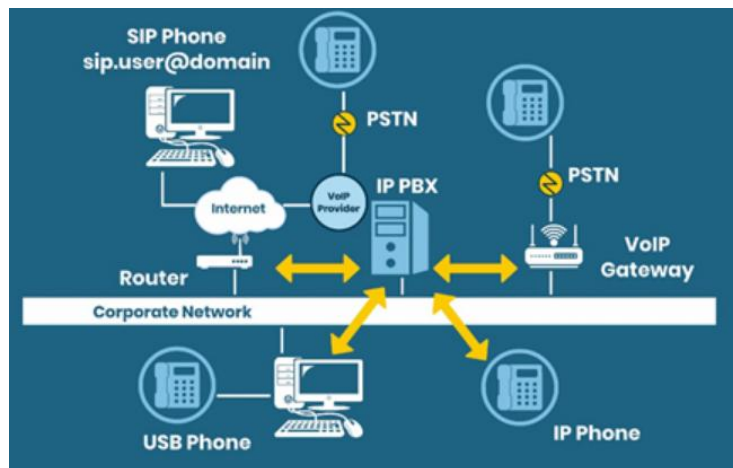
What is the difference between VoIP and PSTN?

The VoIP calls make a call from a computer to a local phone or same VoIP location. While PSTN, uses circuit-switched telephony make a call from between two least line points. VoIP uses the internet to connect but PSTN uses a landline.

PSTN	VoIP
<ul style="list-style-type: none">▪ Voice networks use circuit switching.▪ Dedicated path between calling and Called party.▪ Bandwidth is reserved in advance. Each line is 64kbps.▪ Cost is based on distance and time.▪ Features such as call waiting, Caller ID and so on are usually available at an extra cost	<ul style="list-style-type: none">▪ VoIP uses packet switching.▪ No dedicated path between sender and receiver.▪ It acquires and releases bandwidth, as it is needed.▪ Cost is not dependent on time and distance.▪ Features such as call waiting, Caller ID and so on are usually included free with service

Picture 5.2: Differences between PSTN and VoIP

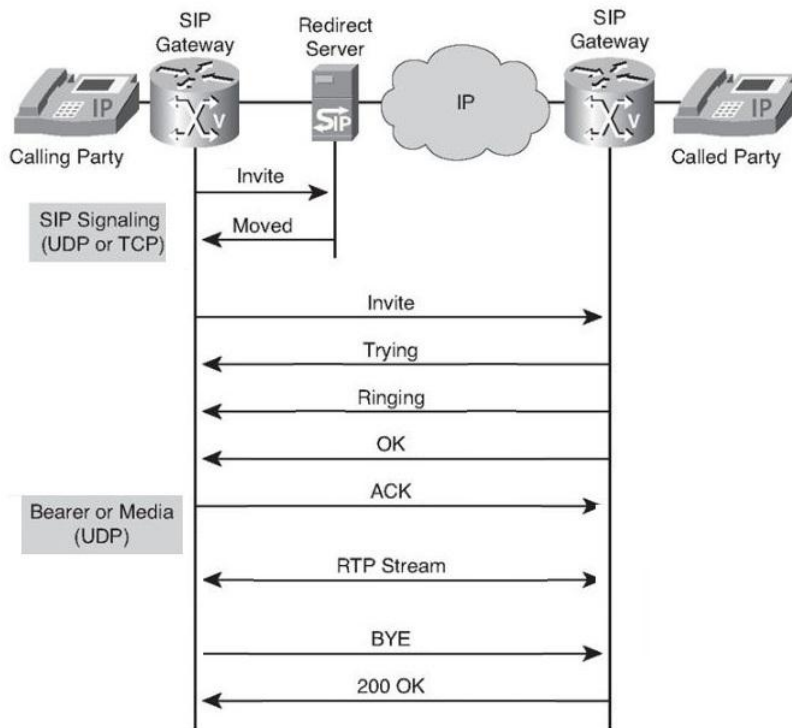
5.1.2 Session Initiation Protocol (SIP) scenarios for VoIP



Picture 5.3: SIP involvement from PSTN to VoIP network

What is SIP protocol in VoIP?

The SIP is a signaling protocol that enables the VoIP by allowing the messages sent between endpoints and managing the call. SIP supports voice calls, video conference, instant messaging, and media distribution.



Picture 5.4: SIP session scenarios between two parties

Activities:

State three (3) difference features between VoIP and PSTN;

VoIP	PSTN

5.2 Understand IPTV over NGN

What is IPTV?

Internet Protocol television or IPTV is the media delivery of television content IP networks. Unlike downloaded media, IPTV offers the ability of streaming the source of media continuously either live or on demand. The client media player can begin playing the content such as a TV channel almost immediately known as streaming media. IPTV can be in form of digital television service that delivered to the subscriber through Internet protocol technology via internet connection.

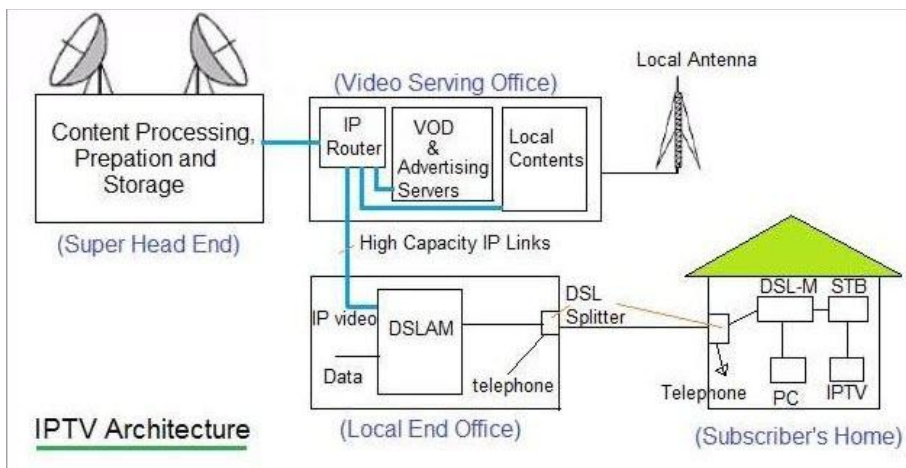
What do I need to set up an IPTV?

To use an IPTV service, a broadband internet connection and a device to view IPTV content on, e.g., a desktop PC, laptop, smartphone, or Smart TV device are needed.

Is YouTube TV an IPTV?

YouTube TV is an IPTV service that offers live and on-demand content. It provides users with live television through over 70 channels right to your preferred device. YouTube TV is compatible with most popular devices such as the Amazon Firestick, which is perfect for cord-cutters.

5.2.1 IPTV Functional Architecture



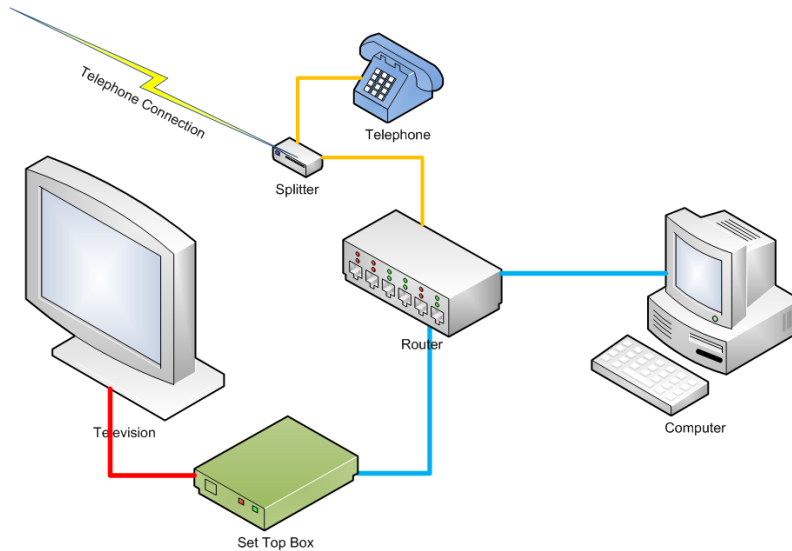
Picture 5.5: IPTV architectures

Where:

VoD = Video on demand.

STB = set-top box.

DSL-M = DSL Modem.



Picture 5.5: A simplified network diagram for IPTV

What is the future of IPTV?

The number of IPTV subscribers had finally exceeded the number of cable TV and satellite TV users and grew 23% between 2015 and 2018. It is predicted that by 2021, IPTV audiences will cover 32.5 million homes and IPTV revenues will reach USD 5.77 billion. However, this is still no match with its big rival OTT (over-the-top).

5.2.2 Multicast and Unicast Based IPTV Content Delivery

What are the differences between unicast and multicast streaming?

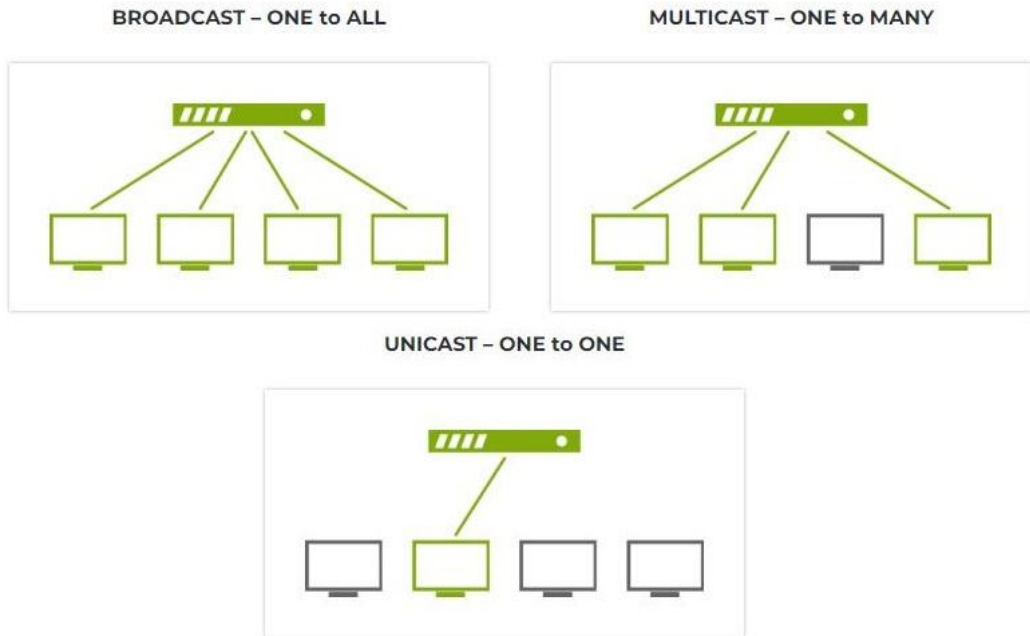
The differences are; the unicast transmission sends an IP packets to a single recipient on a network while a multicast transmission sends IP packets to a group of hosts on a network. Multicast is similar to broadcasting, but only transmits information to specific users. The simple way to send data to multiple users simultaneously is to transmit individual copies of the data to each user.

How does multicast IPTV work?

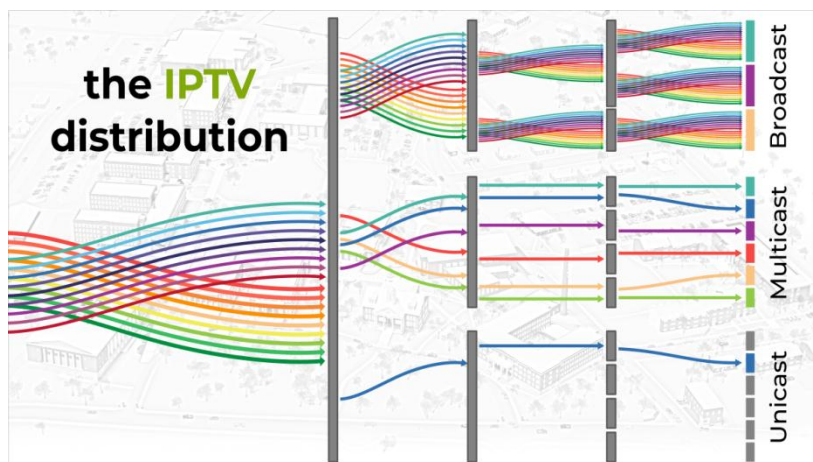
The multicast IPTV stream use a replicated data to network's routers and switches and allow a number of client devices to subscribe to the multicast address and receive the broadcast. Broadcast multicast IP addresses range are from 224.0. 0.0 to 239.255. The best practice for streaming are range from 234.0.

What is Unicast streaming?

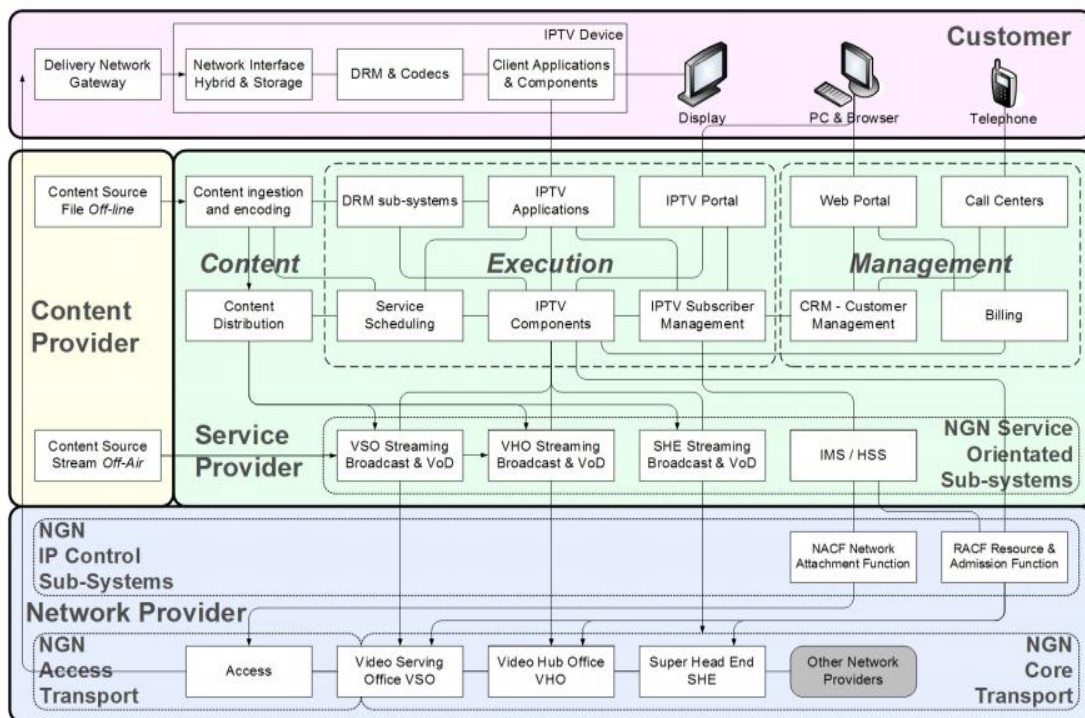
The unicast streaming involves a point-to-point connection between a server and a client where each client gets its own unique data stream and only those clients that request the stream will receive it.



Picture 5.6: Illustration concept of broadcast, multicast and unicast



Picture 5.7: Other Illustration concept of broadcast, multicast and unicast



Picture 5.8: IPTV to NGN Mapping

What are others IPTV services?

Besides IPTV, the other similar services are:

- i. Video on Demand (VoD): This services allows the users to watch any movie from the VoD server's media library. The subscriber can use the pause and rewind features.
- ii. Near Video on Demand (nVoD): This services refer to pay-per-view video service like VoD but intended for multiple users subscribed. The subscribers can look through schedule and plan watching the content of interest.
- iii. TV on Demand (TVoD): This services uses the selected TV channels to be recorded to be viewed whenever the customer finds free convenient time.

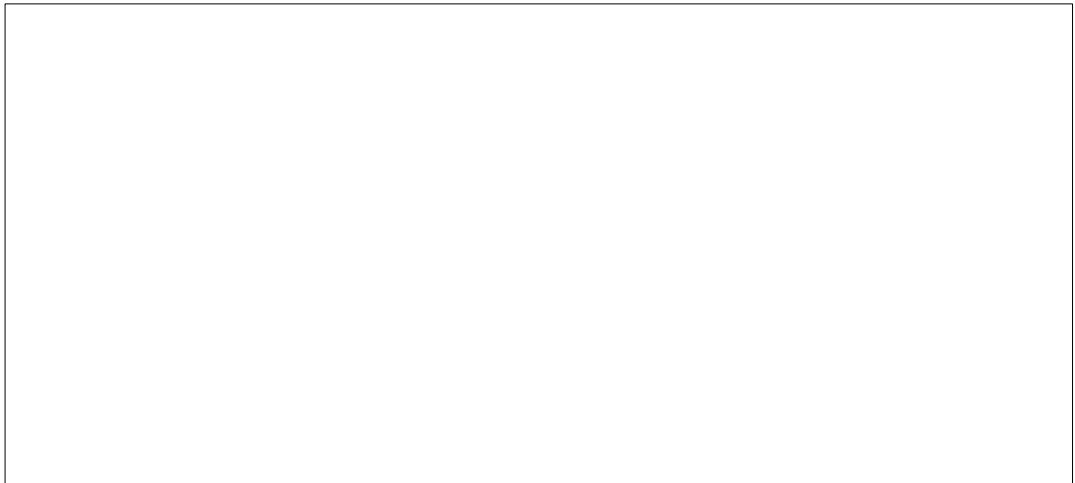
Explain the IPTV Delivery Mechanisms?

IPTV delivery mechanism are divided into 2 categories;

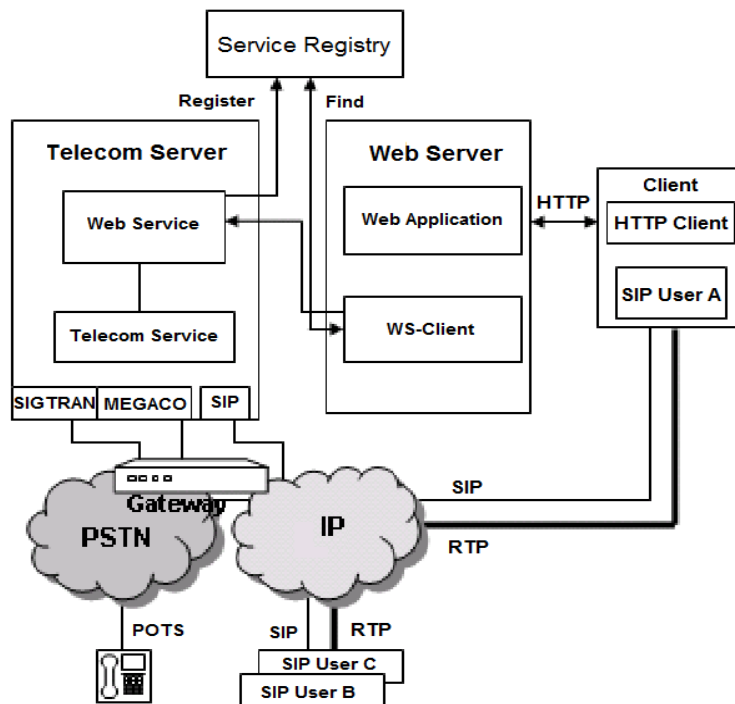
- i. Unicast-Based IPTV Content Delivery
In this category, the users are nomadic within the network, and the IPTV service provider is not located in the network provider domain of the end user.
- ii. Multicast-Based IPTV Content Delivery
In this category, the media delivery of IPTV packets are simultaneously delivered to multiple destinations by using transmission from a single source.

Activities:

Sketch the network connection relation of IPTV from provider to user;



5.3 Apply the Understanding of Web Services in NGN



Picture 5.9: Web Services (WS) based architecture for NGN services delivery

What do you mean by Web services?

A web service is an application or data source that allow the accessible of data via a standard web protocol such HTTP (Hypertext Transfer Protocol) or HTTPS (Hypertext Transfer Protocol Secure).

What is the definition of Web Services for NGN?

A Web service for NGN is a software system that designed to support the interoperable device to device interaction over the internet network. It has an interface described in format of WSDL or Web Services Description Language.

Explain the Web Services Architecture Models?

Four types of Web Services Architectural Models:

- i. Message Oriented Model
- ii. Service Oriented Model
- iii. Resource Oriented Model
- iv. Policy Model

5.4 Understand Fixed-Mobile Convergence

What is Fixed-mobile convergence (FMC)?

Fixed-mobile convergence (FMC) is a change in telecommunications that removes differences between fixed and mobile networks.

Definition from Fixed-Mobile Convergence Alliance (FMCA):

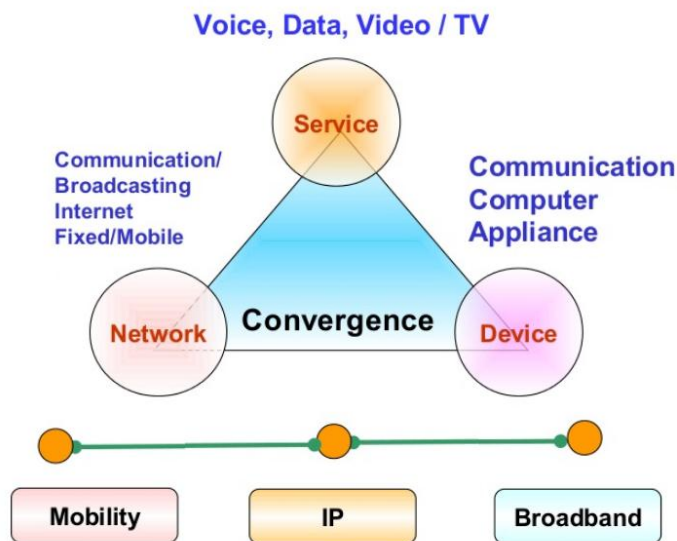
"Fixed Mobile Convergence is a transition point in the telecommunications industry that will finally remove the distinctions between fixed and mobile networks, providing a superior experience to customers by creating seamless services using a combination of fixed broadband and local access wireless technologies to meet their needs in homes, offices, other buildings and on the go."

Components of Fixed-Mobile Convergence

Each vendor appears to have its own definition of enterprise FMC, but all their products consist of one or more of the following capabilities:

- i. Session redirection
Session redirection means moving a call in progress from a cell phone to a desk phone or vice versa, in much the same way as a call can transfer from one extension to another.
- ii. PBX mobility
Treating the mobile phone as an analog extension to the PBX opens up several more possibilities. Various flavours of this service might include features like single number, simultaneous ringing and single voicemail.
- iii. Single number

- Single number means that the mobile phone and the desk phone share an extension number. Only one phone number need be given out to receive calls on either a mobile or desk phone.
- iv. Single voicemail
Single voicemail is the option to use the corporate voice mail rather than the cell phone's voice mail. This only works on calls made to an office number.
 - v. Simultaneous ringing
Simultaneous ringing means that when someone calls an office number, a desk phone and a mobile phone ring simultaneously.
 - vi. Client software
PBX mobility on a regular cell phone is not particularly user friendly, what with the touch-tone interface and the access number prefixing. With a smartphone things get a lot better. The definition of a smartphone is that it can run third-party software..
 - vii. Dual-mode support
A dual-mode phone is a cell phone that also has Wi-Fi. The Wi-Fi can be for data only, voice only, or for both.
 - viii. Session continuity
Dual-mode handset clients can fully hide their split personality, taking the onus of session redirection off the user, and handling it automatically.
 - ix. Mobility controller
Session redirection and session continuity need a device in the network that routes and reroutes the call over either the fixed or mobile network as needed.



Picture 5.10: Fixed Mobile Convergence concept

Activities:

Explain briefly the motivation and objective Fixed Mobile Convergence.



5.5 Apply the Understanding of Ubiquitous Sensor Network (USN) Services

What means ubiquitous?

Constantly encountered, existing or being everywhere at the same time.

What is meant by sensor networks?

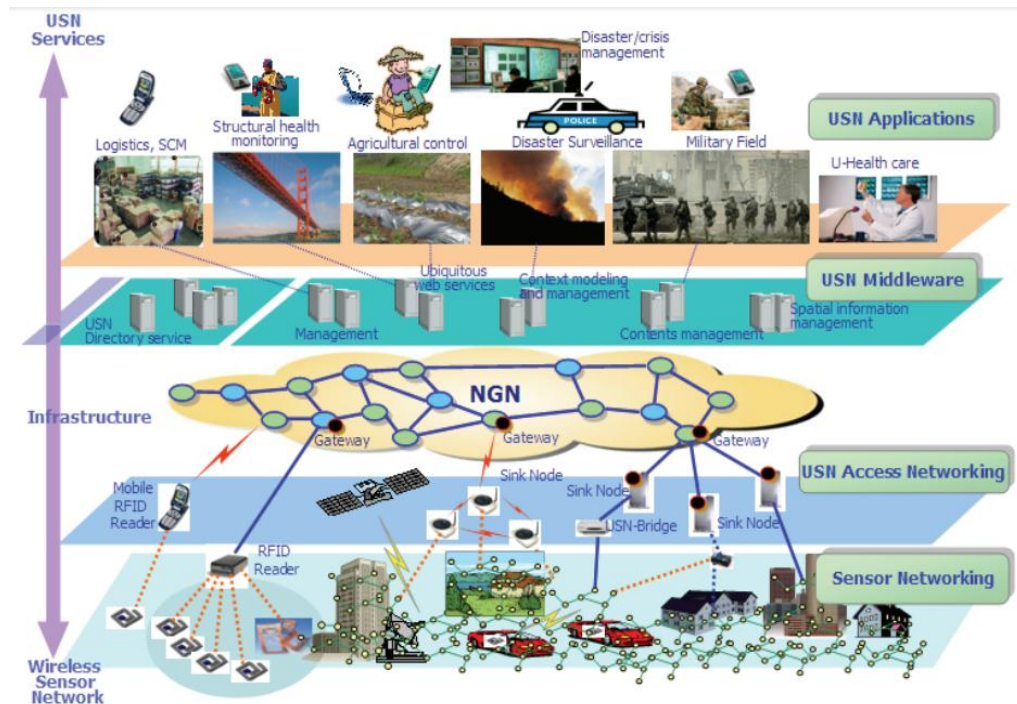
A sensor network comprises a group of small, powered devices and wireless or wired networked infrastructure. The sensor network connects the internet networks to transfer data for analysis use then the sensor network nodes will cooperatively sense and control the environment.

What is ubiquitous sensing?

Ubiquitous sensing, or ubiquitous 'geo'-sensing defines as devices that has wide variety of omnipresent technical, human sensors and geo-sensor networks with the ability to probe geographic phenomena even in real time.

USN definition by ITU Telecommunication Standardization Sector

“USN is used to describe networks of intelligent sensor nodes that could be deployed “anywhere, anytime, by anyone and anything”



Picture 5.11: Schematic Layers of a Ubiquitous Sensor Network

List out the characteristics of a USN?

- i. Small-scale sensor nodes;
- ii. Limited power requirements (e.g., solar power) or stored (e.g., battery);
- iii. Able to withstand harsh environmental conditions;
- iv. Fault tolerant and designed to cope with high possibility of node failures;
- v. Support for mobility;
- vi. Dynamic network topology;
- vii. Able to withstand communication failures;
- viii. Heterogeneity of nodes;
- ix. Large scale of deployment.

5.5.1 USN Applications

What are the applications of USN?

The USN applications can be assigned into three categories:

1. Detection
Using temperatures that passing a particular threshold of intruders or etc.
2. Tracking
Using the supply chain management, the vehicles with intelligent transport systems can track the chain of any product.
3. Monitoring.
Using medical devices parameter such patient's blood pressure the structural health of human or thing like plant and animal can be monitored.

Activities:

Explain briefly the definition of Ubiquitous Sensor Network (USN), the advantages and example of applications.

Ubiquitous Sensor Network (USN)	Details
Definition	
Advantages	
Applications	

5.6 Understand VPN Services in NGN

What is VPN?

VPN is a term for Virtual Private Network that describes the technology that can encapsulate and transmit network data such Internet Protocol data to other IP network.

How VPN works?

A VPN connection establishes a secure connection between the user and the internet. Using VPN, all the data traffic is routed through an encrypted virtual tunnel making its location invisible to everyone. A VPN connection is also secure against the external attacks.

Is a VPN free?

Very few VPNs offer a truly free option. Instead, many companies will offer time-limited trials or money-back guarantees.

How to use VPN?

VPNs can set up using desktops or laptops or using iPhone, iPad, or Android phone. VPN can hide user IP address and physical location while encrypting internet traffic so that no body know the status of the user connection.

Explain the advantages of VPN?

Advantages of using a VPN Connection;

- i. Anonymity
- ii. Security
- iii. Accessing geo-location blocked services (Netflix, Hulu, etc)

Explain the configuration of VPN?

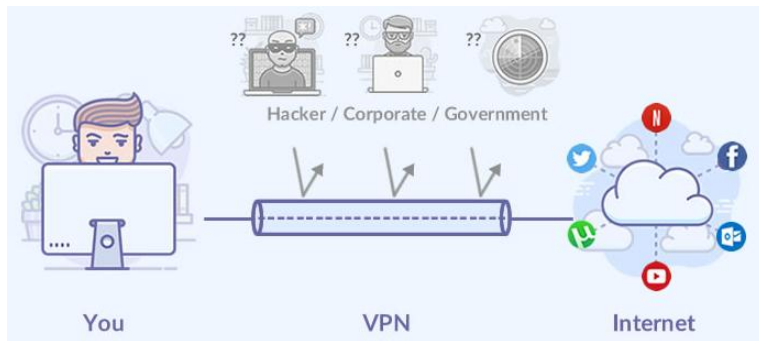
VPN configurations fall into 2 categories:

1. Remote access

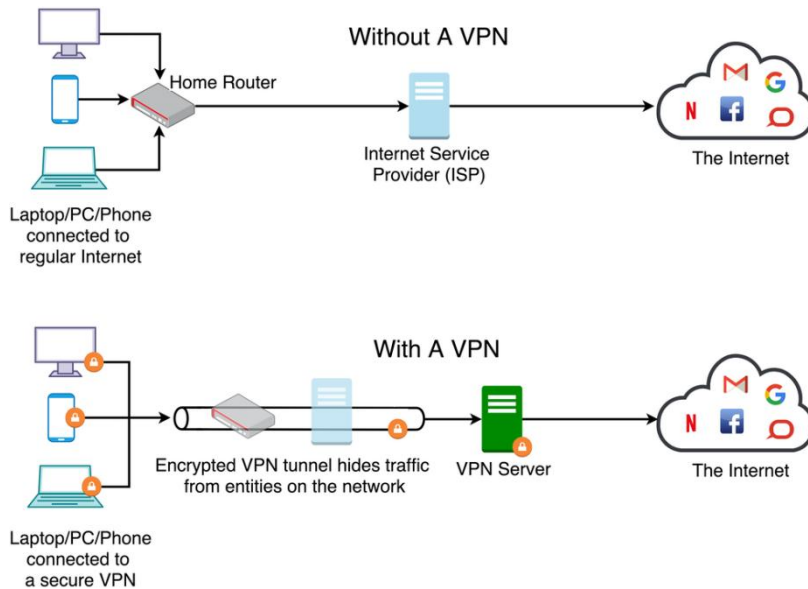
By simply plug the computer into a network, this configuration enables an individual to access an intranet as if they were physically connected to it. Such a configuration may be employed when a remote worker needs access to private resources exposing to the public internet.

2. Site-to-site

Site-to-site connections are refer to the connection of two routers. These routers then route traffic bound for other sites over the VPN and creating one seamless local area network that spans multiple physical locations. This configuration is of particular use for businesses and cloud computing platforms to seamlessly interconnect.



Picture 5.12: Example illustration of VPN connection



Picture 5.13: Differentiation of network with VPN and without VPN

Activities:

State TWO (2) advantages and disadvantages of Virtual Private Network (VPN);

VPN	Details
Advantages	
Disadvantages	

5.7 Understand Various Concepts in NGN

List out the various Concept in NGN?

- i. Internet of Things (IoT)
- ii. Web of Things (WoT)
- iii. Software-Defined Networking (SDN)
- iv. Network Functions Virtualization (NFV)

5.7.1 Internet of Things (IoT)

What is IoT?

The Internet of things (IoT) describes as a network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.

How IoT works?

IoT devices contain a sensors and mini-computer processors that act as data collector sensors via machine learning that collecting data from their surroundings.

What are examples of the Internet of things?

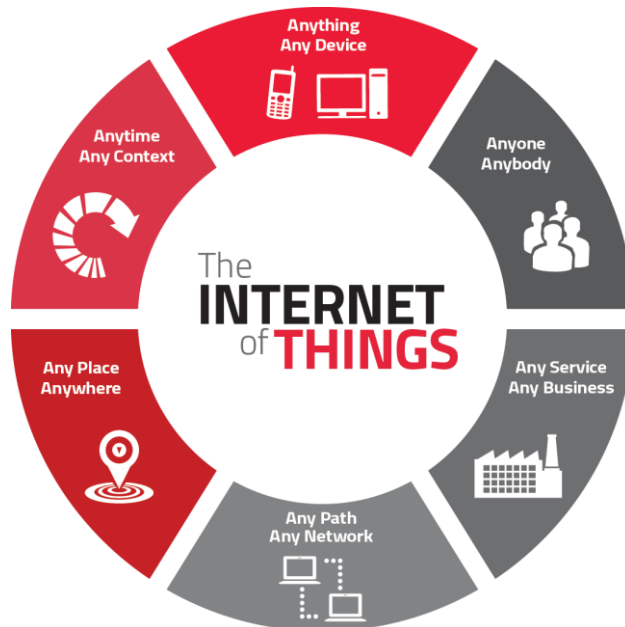
Top Internet-of-Things (IoT) examples to know;

- i. Connected appliances.
- ii. Smart home security systems.
- iii. Autonomous farming equipment.

- iv. Wearable health monitors.
- v. Smart factory equipment.
- vi. Wireless inventory trackers.
- vii. Ultra-high speed wireless internet.
- viii. Biometric cyber security scanners.

List out the crucial IoT characteristics?

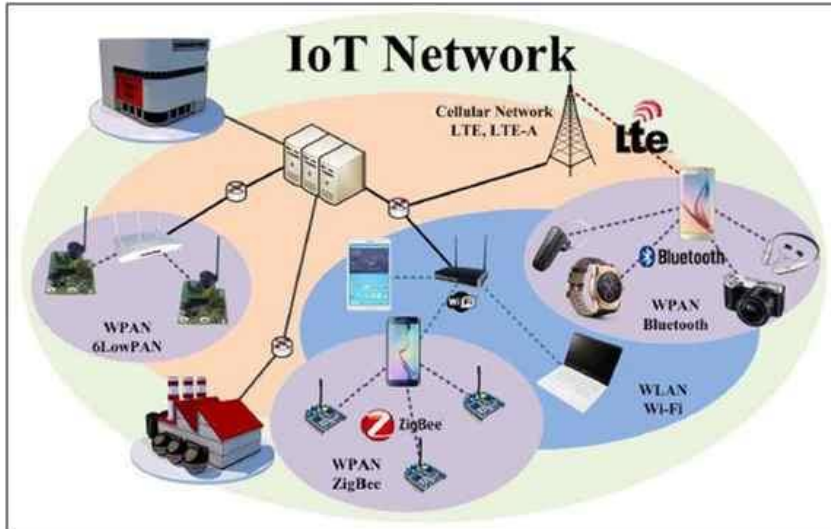
- i. Connectivity.
- ii. Things. Anything that can be tagged or connected
- iii. Data.
- iv. Communication.
- v. Intelligence.
- vi. Action.
- vii. Ecosystem



Picture 5.14: IoT focus of implementation

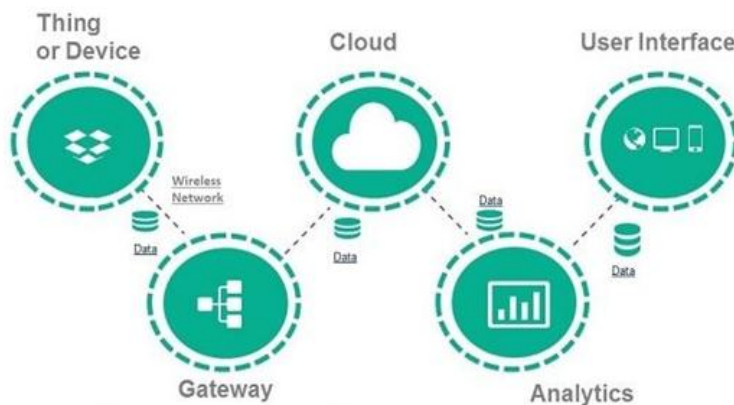
Can IoT work without Internet?

IoT systems also referred as a 'smart' and 'connected devices that can be without internet connection to be functional properly. But it mostly require a connection to other gadgets on for automate a certain tasks and allow to interact with it via direct commands or configuration.



Picture 5.15: Example of IoT Network

Where; WLAN = Wireless Local Area Network and WPAN = Wireless Personal Area Network.



Picture 5.16: Major components of IoT

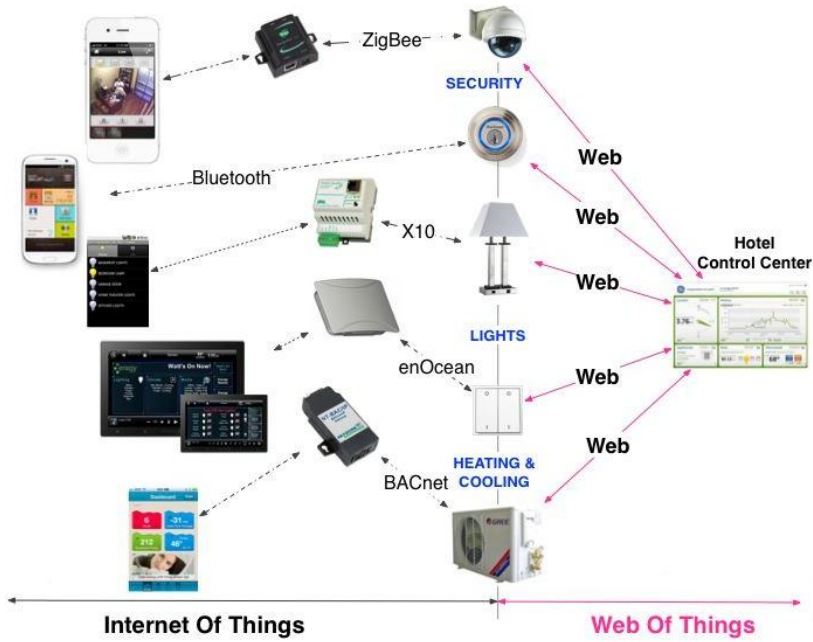
5.7.2 Web of Things (IoT)

What is Web of Thing?

Web of Things describes a set of standards by the W3E (World Wide Web for Education) for solving the interoperability issues of different Internet of Things platforms and application domains.

Is WoT related to IoT?

WoT is closely related to IoT; it's an additional application layer that added to IoT's network layer to maximize connectivity. WoT allows access and control over IoT applications using web technologies such as HTML, JavaScript.



Picture 5.17: Differences between IoT and WoT

Layer 4: Compose	Systems integration WoT-a-Mashup	IFTTT Physical mashups Node-RED	Web applications Automated UI generation	
Layer 3: Share	Social networks PKI Encryption	API tokens OAuth Social WoT	TLS JWT	DTLS Delegated authentication
Layer 2: Find	REST Crawler HATEOAS Link header	RDFa mDNS	Web Thing Model Search engines Schema.org	JSON-LD Semantic Web Linked Data
Layer 1: Access	HTML Webhooks URI/URL	JSON Gateway	Proxy WebSockets MQTT	REST API HTTP CoAP
Networked things	NFC QR	6LoWPAN Beacons	Thread Bluetooth	Ethernet ZigBee Wi-Fi 3/4/5 G

Picture 5.18: WoT layer architecture and example

What is the difference between Web of Things and Internet of things?

IoT is about creating a network of objects, things, people, systems and applications, while WoT tries to integrate them to the Website.

5.7.3 Software Defined Networking (SDN)

What is Software Defined Networking (SDN)?

Software-defined networking is a technology approach for network management to enables and improve the network performance while monitoring and making it more like cloud computing rather than traditional network management.

How SDN works?

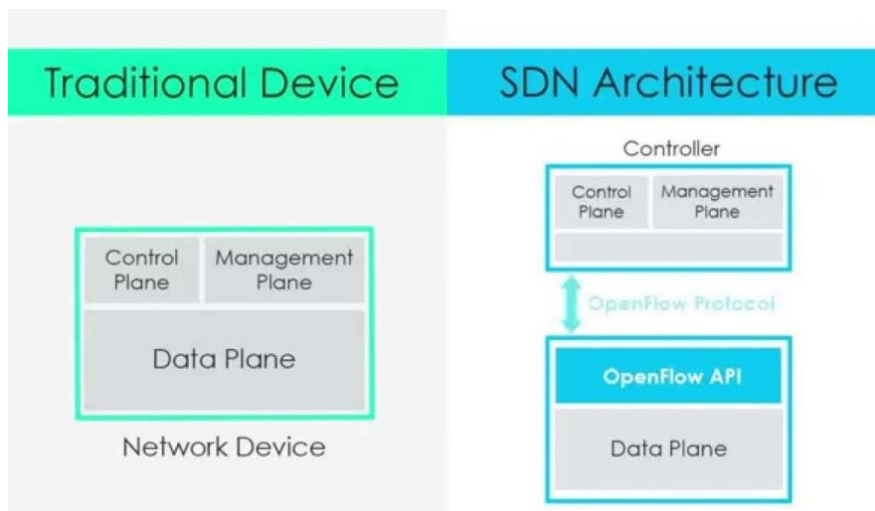
SDN is a networking approach that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.

What are the three SDN layers?

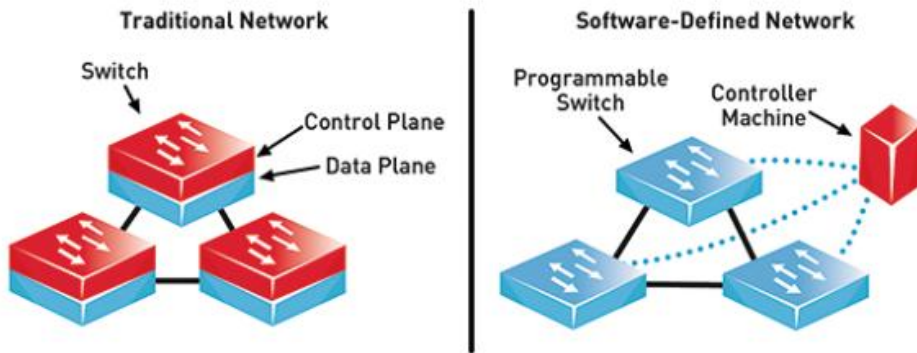
A layer of SDN architecture includes: the application layer, the control layer and the infrastructure layer. The SDN application layer, contains the network applications that functions like detection systems and firewalls.

Is SDN the future of networking?

SDN help the companies to enable virtualization of their networking infrastructure. It is an open-source technology which has centralized network monitoring system. In the coming future of SDN, the technology will be more responsive, fully automated, and highly secure.



Picture 5.19: SDN architecture versus traditional device



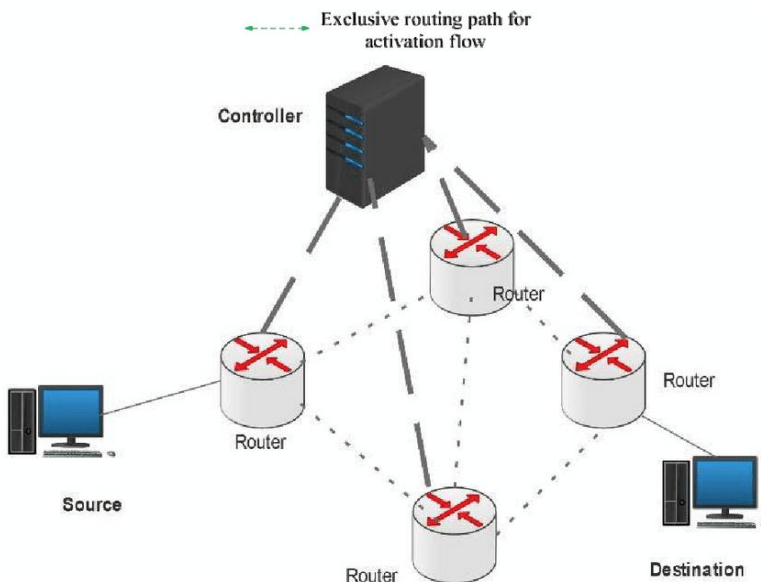
Picture 5.20: Differentiation between SDN and traditional network

How is SDN different from traditional networking?

The most difference between SDN and traditional networking is that SDN is software based while traditional networking is hardware-based. SDN is more flexible, allowing users greater control and ease for managing resources virtually throughout the control plane.

What are the disadvantages of SDN?

The disadvantages of a SDN network is that the eliminating use of the physical routers and switches that may compromise the security issues. Other is the remove features firewall control that can leave more vulnerable on the network.



Picture 5.21: Example of SDN network from source to destination

Explain the architectures of SDN?

SDN architectures can be explained onto these categories;

- i. Directly programmable,
Network control is directly programmable because it is decoupled from forwarding functions.
- ii. Agile (able to move quickly and easily),
Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.
- iii. Centrally managed,
Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch.
- iv. Programmatically configured
SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.
- v. Open standards-based and vendor-neutral,
When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.

5.7.4 Network Functions Virtualization (NFV)

What is NFV?

Network functions virtualization or NFV is a network architecture concept that uses the IT virtualization technologies to virtualize entire network node into building blocks that may connect, or chain together, to create communication services. NFV refers to the concept of framework running software-defined network functions

What is difference between SDN and NFV?

SDN roles to separate network control functions from network forwarding functions, while NFV roles to abstract network forwarding and other networking functions from the hardware. When SDN executes on a NFV infrastructure, SDN forwards data packets from one network device to another.

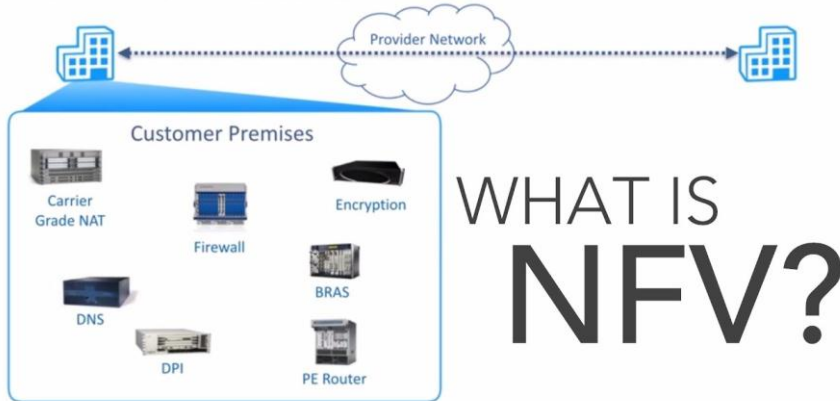
Explain the component of NFV?

The NFV framework consists of three main components:

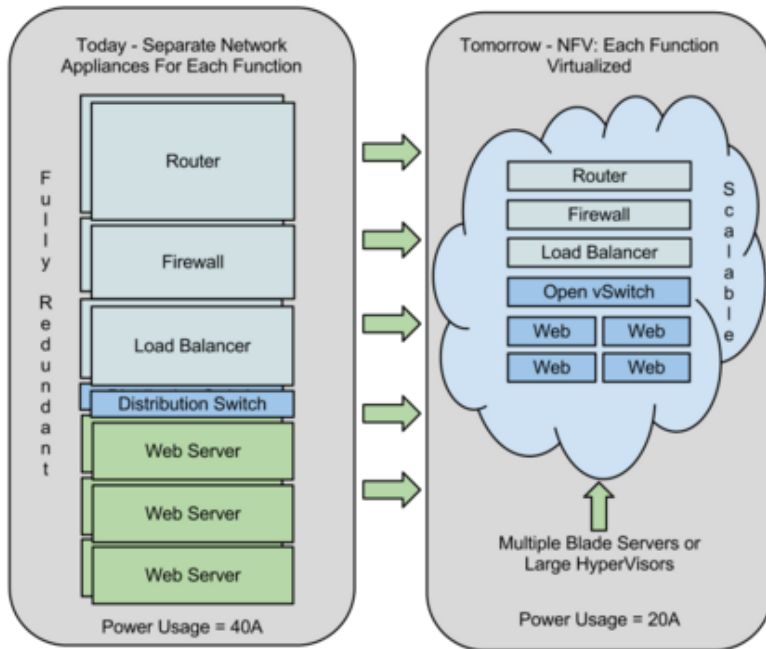
- i. Virtualized Network Functions (VNFs),
VNFs are software implementations of network functions that can be deployed on a Network Functions Virtualization Infrastructure (NFVI).
- ii. Network Functions Virtualization Infrastructure (NFVI),
NFVI is the totally the hardware and software components that build the environment where VNFs are deployed. The NFV infrastructure can span several locations. The network providing connectivity between these locations is considered as part of the NFV infrastructure.

- iii. Network Functions Virtualization Management and Orchestration Architectures Framework (NFV-MANO Architectural Framework),
 NFV-MANO Architectural Framework is the collection of all functional blocks, data repositories used by these blocks, and reference points and interfaces through which these functional blocks exchange information for the purpose of managing and orchestrating NFVI and VNFs.

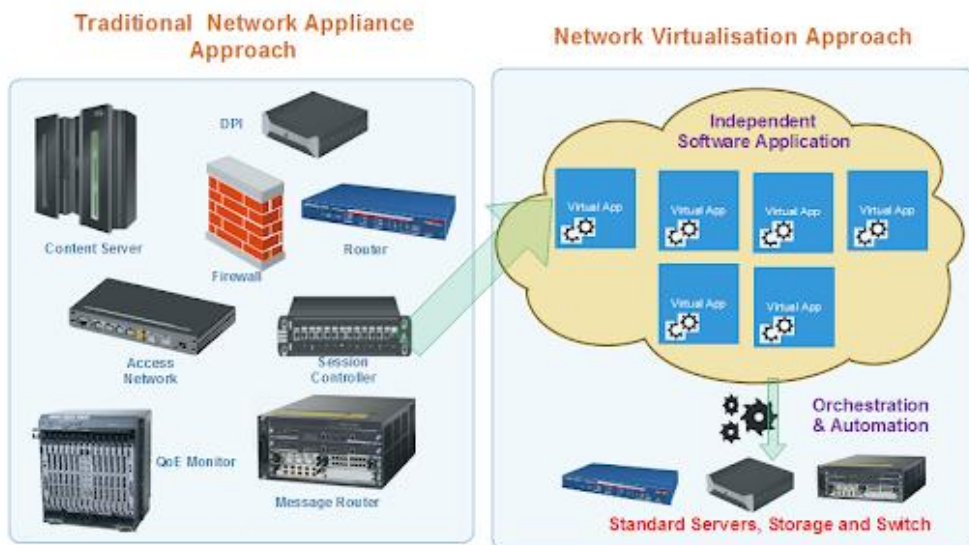
Network Functions



Picture 5.22: NFV is a chain network between nodes of provider



Picture 5.23: Differentiation between NFV system and traditional system



Picture 5.24: Differentiation between NFV approach and traditional network appliance approach

Activities:

Explain the various concept of NGN for IoT, WoT, SDN and NFV;

Technologies	Concept details
IoT	
WoT	
SDN	
NFV	

Practical Activities

Installation Tools in Ethernet LAN Network – Fixed and Mobile Broadband Internet Access – IPTV with VPN Services – VPN Services with IPv4 Addressing – IPV4 in VoIP Services – LED Control Using Web of Thing (WoT)

PRACTICAL ACTIVITIES A

TOPIC: INSTALLATION TOOLS IN ETHERNET LAN NETWORK

OBJECTIVES:

At the end of this practical activities, you should be able to;

1. Understand concept of Ethernet cable network.
2. Learn the installation of RJ45 at Ethernet cable network.
3. Test the functionality of Ethernet cable network using appropriate device.

EQUIPMENTS:

Below are the list of equipments used for the activities.

1. 1 unit Cable Crimper or flat-head screwdriver.
2. 1 unit Cable Tester
3. 1 unit 9VDC Battery
4. 1 unit Wire Stripper
5. Ethernet Cable
6. 1 unit Blade
7. 2 units of RJ45 Crystal Network Connector with Network Connector Protective Cover

SAFETY PRECAUTION:

Before performing a practical work, make sure that these instructions are read to be complied;

1. Items such as keys, aluminium foil, and steel wool should never be kept near 9VDC batteries. If one of these items touches both battery posts, there is an even greater risk of a fire starting. Batteries should be kept in original packaging until ready for use.
2. Wear cut resistant gloves and sleeves to protect your hands and arms when using blade.

THEORY:

There are many Ethernet cables that can be bought. Often these cables are supplied free with equipment that uses Ethernet connectivity in some way or another. There are several different varieties of Ethernet cable that can be obtained: speed variations, crossover cables, Cat 5, Cat 5e, Cat6, Cat 6a, Cat 7 and etc. Normally Ethernet cables will be bought and there is no major need to understand what is inside or on the connectors, although it can be both interesting and helpful on some occasions. Even so, an understanding of the different types of Ethernet cable and the maximum lengths that should be used is helpful.

The commonly used network cables: Cat 5, Cat 5e, Cat 6, Cat 6a, Cat 7 all have different levels of performance, and therefore it is necessary to buy or select the right cable for the

right application. These network cables are used for connecting a variety of network elements from Ethernet switches and Ethernet routers to computers, servers and other network items if there is an Ethernet interface, they can be connected using Ethernet cables. The Ethernet cables for connectivity in most office and home environments rely on twisted wire pairs within an overall cable - Cat 5, Cat 6 and Cat 7 all used this format. Twisting the wires together enables the currents to balance, i.e., in one wire the current is moving in one direction, and in the other wire of the pair the current is going in the other, enabling the overall fields around the twisted pair to cancel. In this way, data can be transmitted over considerable lengths without the need for undue precautions.

As several twisted pairs are contained within a particular network cable, the number of twisted per unit length is arranged to be different for each pair - the rate being based on prime numbers so that no two twists ever align. This reduces crosstalk within the cable. The Ethernet cables are available in a variety of lengths as patch cables, or the cable itself is available for incorporating into systems, buildings, etc. The terminations can then be made to the required connector using a crimp tool. These network cables are available in a variety of lengths - long Ethernet cables are available, some of the longest being up to 75 metres. Earlier network cables were unshielded, but later ones were shielded to improve the performance. For example an unshielded twisted pair (UTP) cable may be satisfactory for a short run between a computer and router, but a foil shielded cable, FTP, is best longer runs or where the cable passes through areas of high electrical noise.

CATEGORY	SHIELDING	MAX TRANSMISSION SPEED (AT 100 METERS)	MAX BANDWIDTH
Cat 3	Unshielded	10 Mbps	16 MHz
Cat 5	Unshielded	10/100 Mbps	100 MHz
Cat 5e	Unshielded	1000 Mbps / 1 Gbps	100 MHz
Cat 6	Shielded or Unshielded	1000 Mbps / 1 Gbps	>250 MHz
Cat 6a	Shielded	10000 Mbps / 10 Gbps	500 MHz
Cat 7	Shielded	10000 Mbps / 10 Gbps	600 MHz
Cat 8	Shielded	25 Gbps or 40Gbps *	2000 MHz

Figure A1: Ethernet cable performance summary



Figure A2: Flat Ethernet cable and connector

PROCEDURES:



Figure A3: Wire stripper

1. Strip the Ethernet cable back 1 inch (25 mm) from the end. Insert the cable into the stripper section of the tool and squeeze it tight. Then, rotate the crimping tool around the cable in a smooth and even motion to create a clean cut. Keep the tool clamped and pull away towards the end of the wire to remove the sheathing.

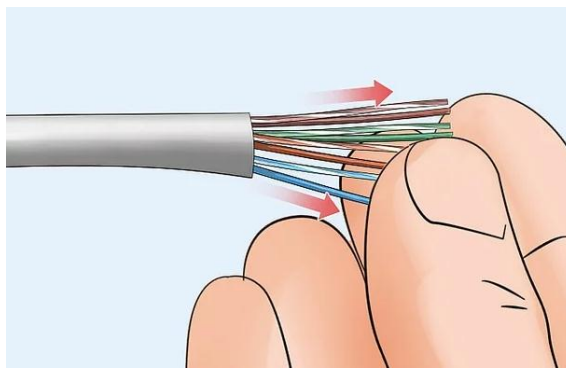


Figure A4: Untwist and straighten the wires

2. Untwist and straighten the wires inside of the cable. Inside of the cable you'll see a bunch of smaller wires twisted together. Separate the twisted wires and straighten them out so they're easier to sort into the right order.

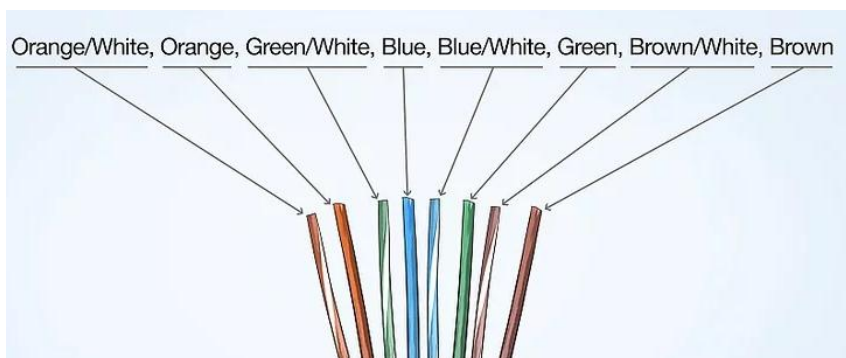


Figure A5: Wire colour arrangement of network cable for both side end of the cable

3. Arrange the wires into the right order. Use your fingers to put the wires in the correct order so they can be properly crimped. The proper sequence is as follows from left to right:
Orange/White, Orange, Green/White, Blue, Blue/White, Green, Brown/White, Brown

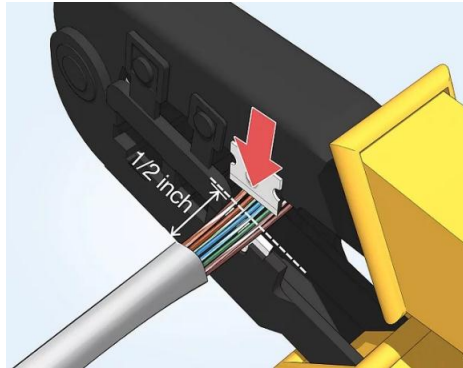


Figure A6: Cutting wire process into even line

4. Cut the wires into an even line 1/2 inch (13 mm) from sheathing. Hold the wires with your thumb and index finger to keep them in order. Then, use the cutting section of the crimping tool to cut them into an even line.

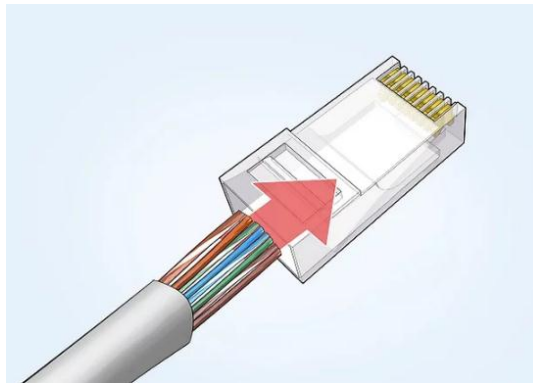


Figure A7: Wire insertion process into RJ45 connector

5. Insert the wires into the RJ-45 connector. Hold the RJ-45 connector so the clip is on the underside and the small metal pins are facing up. Insert the cable into the connector so that each of the small wires fits into the small grooves in the connector.

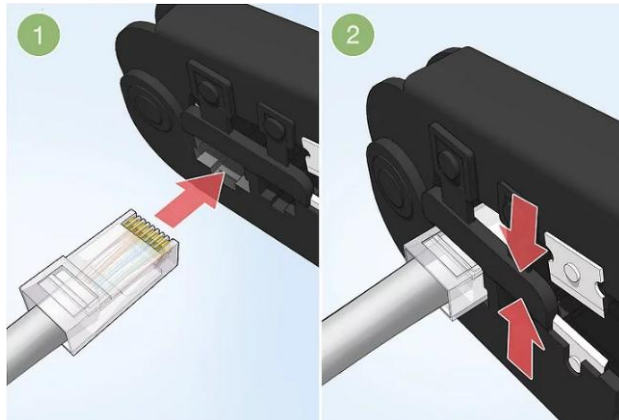


Figure A8: Crimping process using wire crimper

6. Stick the connector into the crimping part of the tool and squeeze twice. Insert the connector in the crimping section of the tool until it can't fit any further. Squeeze the handles to crimp the connector and secure the wires. Release the handles, and then squeeze the tool again to make sure all of the pins are pushed down.

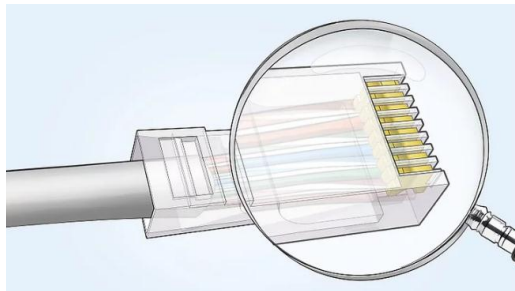


Figure A9: Checking process

7. Remove the cable from the tool and check that all of the pins are down. Take the connector out of the tool and look at the pins to see that they're all pushed down in an even line. Lightly tug at the connector to make sure it's attached to the cable.



Figure A10: Plug both Ethernet cable end into cable tester

- Now use the cable tester to check the functionality and detect any faulty of the cable. Make sure it has a battery in it and power it on. Plug both end of the Ethernet cable into the cable tester.

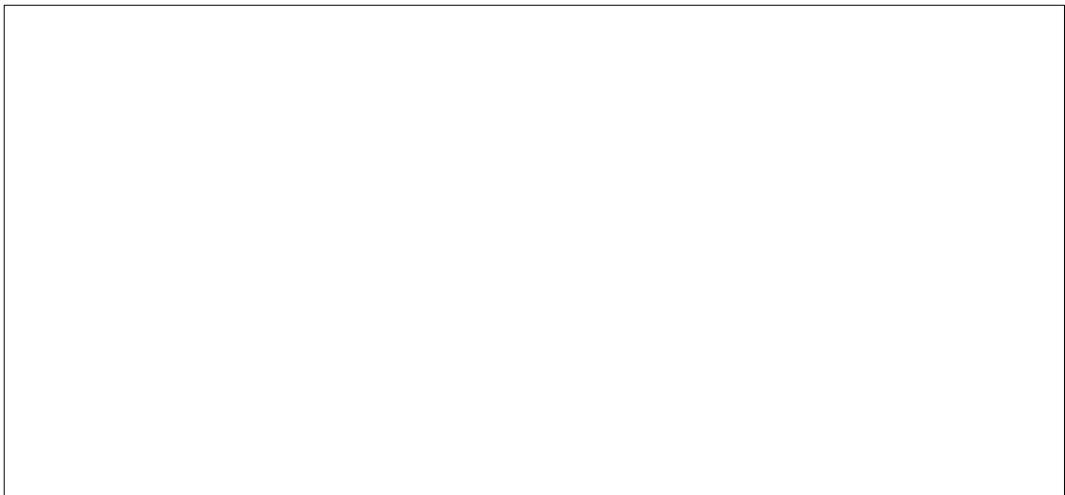


Figure A11: Sequence indicator correspond to 8 pins of wire Ethernet cable

- Check the lights on the cable tester. The testers have 2 sets of 8 LED lights that correspond to the 8 pins on the transmitting and receiving end of the Ethernet cable.

RESULTS:

Attach the picture of complete Ethernet cable with RJ45 done in practical work activities.



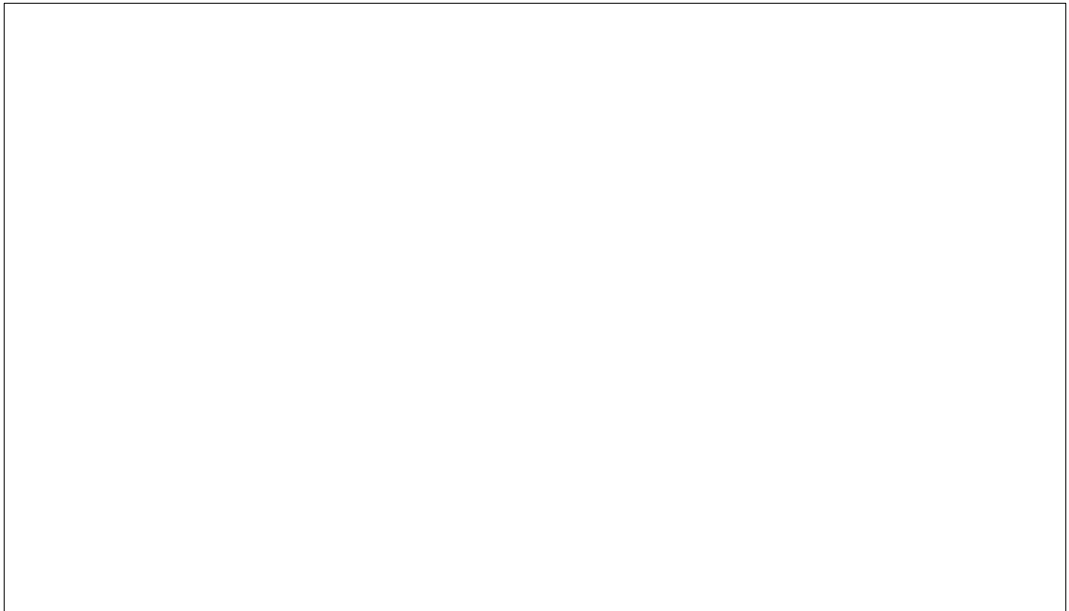
REFLECTION:

Discuss with your friends or lecturer or instructor, which one is better in term of speed data flow, either using Ethernet cable or wirelessly using WiFi.



DISCUSSION/CONCLUSION:

What are the advantages of using an Ethernet cable?



PRACTICAL ACTIVITIES B

TOPIC: FIXED AND MOBILE BROADBAND INTERNET ACCESS

OBJECTIVES:

At the end of this practical activities, you should be able to;

1. Understand concept of Signalling Network
2. Apply understanding of Transmission Systems
3. Differentiate the Internet Access Speed of Fixed and Mobile Broadband

EQUIPMENTS:

Below are the list of equipments used for the activities.

1. PC with Fixed Broadband Network.
 2. Smartphone with Mobile Broadband Network.
 3. Speedtest by Ookla an Android Application from Google Play Store.
 4. PC online Speed Test Network, e.g.;
- LINK 1: <http://speedtest.tm.com.my/>
LINK 2: <https://fast.com/>
LINK 3: <https://www.speedtest.net/>

SAFETY PRECAUTION:

Before performing a practical work, make sure that these instructions are read to be complied;

1. Do not plug in external devices (e.g. USB thumb drive) without scanning them for computer viruses.
2. Always back up all your important data files.

THEORY:

Fixed Broadband is an ultra-fast business internet connection that beams through radio signals. Fixed Broadband can give an internet speed of up to 1Gbps. Understanding the different types of internet connections is imperative for any business looking for the best solution for their needs. But with so many terms flying around, it's not surprising people are often confused by what's available. Fixed broadband encompasses any high-speed data transmission to a residence or a business – i.e. a fixed location – using a variety of technologies, including cable, DSL, fibre optics, and wireless. Essentially, it refers to high-speed internet connections that are “always on” in fixed locations. This particular term does not include mobile connections, i.e. the transmission of data via cellular networks to mobile devices. The type of fixed broadband connection you opt for will depend on various factors, including your location, the various packages available, and prices. The most common are Digital Subscriber Line (DSL), cable modem, fibre optic, fixed wireless, satellite and broadband over power lines (BPL).

Mobile broadband is the marketing term for wireless Internet access through a portable modem, USB wireless modem, or a tablet/smartphone or other mobile device. The first wireless Internet access became available in 1991 as part of the second generation (2G) of mobile phone technology. Higher speeds became available in 2001 and 2006 as part of the third (3G) and fourth (4G) generations. In 2011, 90% of the world's population lived in areas with 2G coverage, while 45% lived in areas with 2G and 3G coverage. Mobile broadband uses the spectrum of 225 MHz to 3700 MHz. The bit rates available with Mobile broadband devices support voice and video as well as other data access. Internet access subscriptions are usually sold separately from mobile service subscriptions.

Devices that provide mobile broadband to mobile computers include:

- i. PC cards, also known as PC data cards, and Express cards
- ii. Mini PCI (Peripheral Component Interconnect) and Mini PCI Express cards that are integrated into the laptop.
- iii. USB and mobile broadband modems, also known as connect cards
- iv. Portable devices with built-in support for mobile broadband, such as laptops, smartphones or tablets, PDAs and other mobile Internet devices.

MOBILE BROADBAND	FIXED BROADBAND
• 100% mobility/Portable	• Fixed at Homes and Offices
• Affordable communication service	
• Simple and free to set up	• Involves initial installation cost
• Coverage limitations	• Wider coverage and connection stability
• Mobile Device should be 4G compatible	• Device compatibility is unnecessary
• Maximum speed up to 100mbps dependent on the coverage area.	• On Normal Ethernet cable maximum speed is 100mbps and on Fibre Gigabyte speed is assured.
• Limited multiple usage	• Multiple usage
• Always have restrictive usage caps with high costs when you exceed them	• Guaranteed Unlimited data

Figure B1: Differences between mobile broadband and fixed broadband

PROCEDURES 1:

1. To run this procedure, you must have a fixed home internet access such streamyx or Unifi or Maxis Home Broadband or else at your home or computer laboratory.
2. By using PC or smartphones that connected to your fixed home or lab internet access, open the Online Speed Test Network page (refer LINK 1, LINK2 & LINK3) and run the application to find the speed of network as shown in Figure B2, B3 and B4.

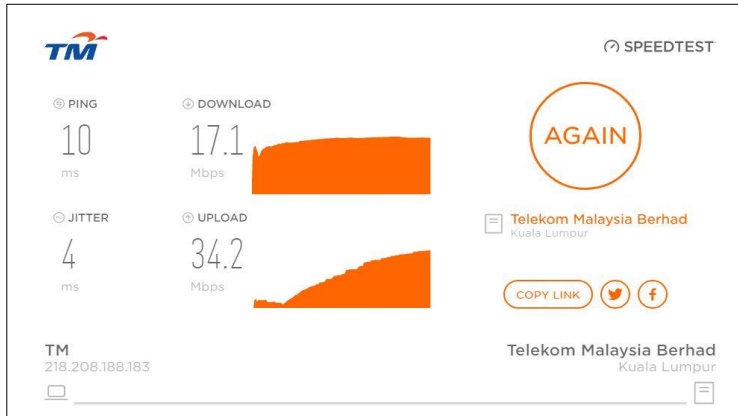


Figure B2: TM Speed Test Online page by Telekom Malaysia

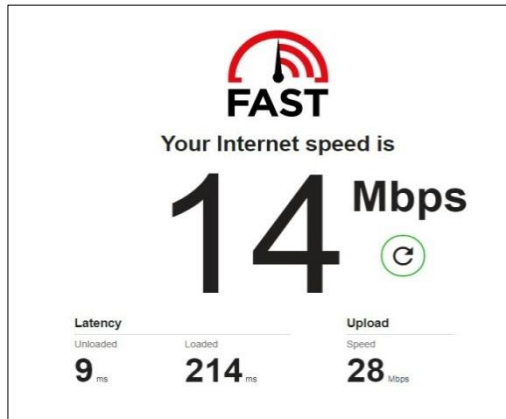


Figure B3: Internet Speed Test Online page by Fast.com

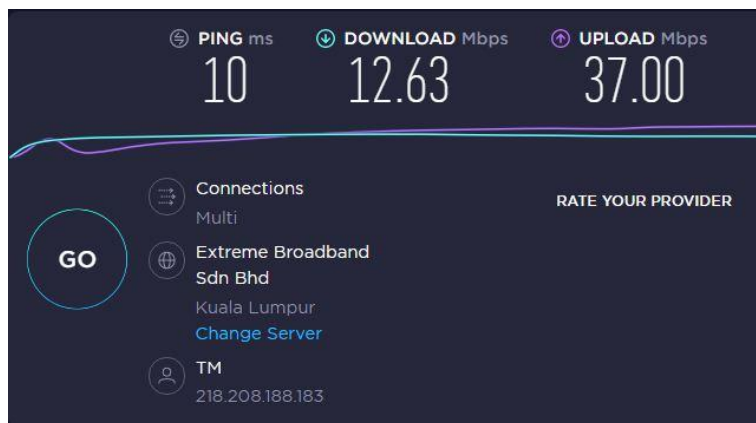


Figure B4: Speedtest Online page by Ookla - The Global Broadband Speed Test

RESULT PROCEDURES 1:

Name of the provider:

.....

Location of fixed home internet access:

.....

Table B1: Home internet speed test result

TM Speed Test Online page by Telekom Malaysia		Internet Speed Test Online page by Fast.com		Speedtest Online page by Ookla	
Download (Mbps)	Upload (Mbps)	Download (Mbps)	Upload (Mbps)	Download (Mbps)	Upload (Mbps)

PROCEDURES 2:

1. Now, to run these procedures, you must use a smartphone with Mobile Broadband Network subscription.
2. Make sure used your internet data from your Mobile Broadband provider such Maxis, Celcom, Digi and etc.
3. Then, install the Speedtest by Ookla Application from Google Play Store at your smartphone at shown in Figure B5.
4. Before start use the application, set the 3G network as a preferred network selection on your smartphone as shown in Figure B6. The selection setting may differ depend on the types of the smartphone.
5. After that, run the Speedtest by Ookla Application the find the speed of the network as shown in Figure B7 and write it on the results.
6. Now, set again the mobile data preferred network to 4G and then run the Speedtest by Ookla Application the find the speed of the network and write it on the results.

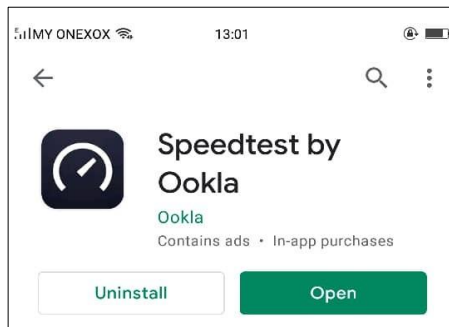


Figure B5: An Android Application of Speedtest by Ookla from Google Play Store

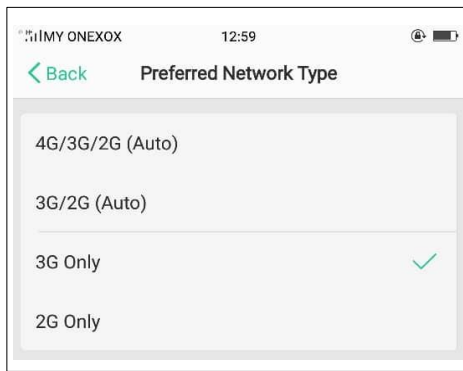


Figure B6: Mobile data preferred network selection of the smartphone

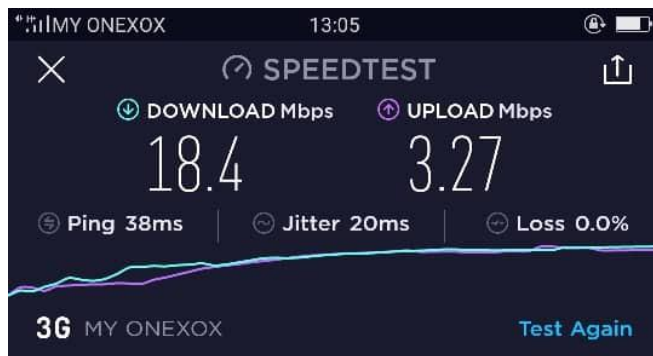


Figure B7: Example result of 3G MY ONEXOX network from Ookla Application

RESULT PROCEDURES 2:

Name of the provider:

.....

Location of Mobile Broadband internet access:

.....

Table B2: Mobile broadband speed test result

Detail	Your device available speed	
	Download Speed (Mbps)	Upload Speed (Mbps)
3G Network		
4G Network		

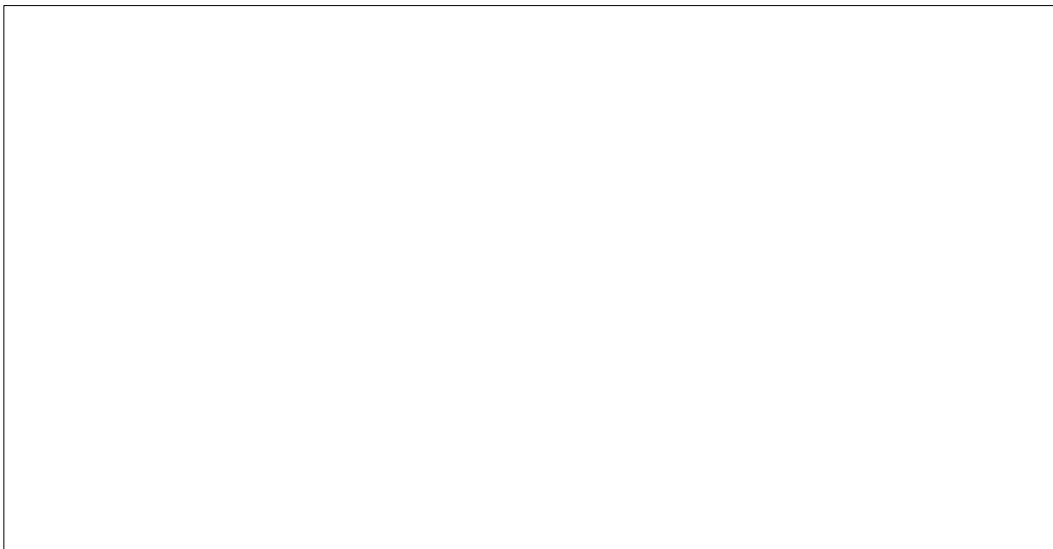
REFLECTION:

List down THREE (3) telecommunication provider for Mobile Broadband and Fixed Home Broadband that exist in Malaysia



DISCUSSION/CONCLUSION:

From results in Table B1 and Table B2, explain why there are a difference of speed rate occurs when referring the standard speed rate that offered by the networking provider.



PRACTICAL ACTIVITIES C

TOPIC: IPTV WITH VPN SERVICES

OBJECTIVES:

At the end of this practical activities, you should be able to;

1. Understand IPTV over NGN
2. Explain IPTV Functional Architecture
3. Learn the function of VPN on IPTV services

EQUIPMENTS:

Below are the list of equipments used for the activities.

1. Android smartphone.
2. Eth_Update_IPTV_2020.m3u file
3. Android applications:
 - i. iptv-pro in apk file
 - ii. MX Player application from Google Play Store
 - iii. Phone Guardian Mobile Security & VPN Protection from Google Play Store

SAFETY PRECAUTION:

Before performing a practical work, make sure that these instructions are read to be complied;

1. Do not plug in external devices (e.g. USB thumb drive) without scanning them for computer viruses.
2. Always back up all your important data files.

THEORY:

Internet Protocol television (IPTV) is the delivery of television content over Internet Protocol (IP) networks. This is in contrast to delivery through traditional terrestrial, satellite, and cable television formats. Unlike downloaded media, IPTV offers the ability to stream the source media continuously. As a result, a client media player can begin playing the content (such as a TV channel) almost immediately. This is known as streaming media.

Although IPTV uses the Internet protocol it is not limited to television streamed from the internet. IPTV is widely deployed in subscriber-based telecommunications networks with high-speed access channels into end-user premises via set-top boxes or other customer-premises equipment. IPTV also used for media delivery around corporate and private networks. IPTV in the telecommunications arena is notable for its on-going standardisation process (e.g., European Telecommunications Standards Institute). IPTV services may be classified into live television and live media, with or without related interactivity; time

shifting of media, e.g., catch-up TV (replays a TV show that was broadcast hours or days ago), start-over TV (replays the current TV show from its beginning); and video on demand (VOD) which involves browsing and viewing items of a media catalogue.

IPTV supports both live TV as well as stored video-on-demand. Playback requires a device connected to either a fixed or wireless IP network in the form of a standalone personal computer, smartphone, touch screen tablet, game console, connected TV or set-top box. Content is compressed by Video and audio codecs and then encapsulated in MPEG transport stream or Real Time Transport Protocol or other packets. IP multicasting allows for live data to be sent to multiple receivers using a single multicast group address. In standards-based IPTV systems, the primary underlying protocols used are:

- i. Service provider-based streaming.
- ii. Web-based unicast only live and VoD streaming:
 - a) Adobe Flash Player prefers RTMP over TCP with setup and control via either AMF or XML or JSON transactions.
 - b) Apple iOS uses HLS adaptive bitrate streaming over HTTP with setup and control via an embedded M3U playlist file.
 - c) Microsoft Silverlight uses smooth streaming (adaptive bitrate streaming) over HTTP.
- iii. Web-based multicast live and unicast VoD streaming: The Internet Engineering Task Force (IETF) recommends RTP over UDP or TCP transports with setup and control using RTSP over TCP.
- iv. Connected TVs, game consoles, set-top boxes and network personal video recorders:
 - a) Local network content uses UPnP AV for unicast via HTTP over TCP or for multicast live RTP over UDP.
 - b) Web-based content is provided through either inline Web plug-ins or a television broadcast-based application that uses a middleware language such as MHEG-5 that triggers an event such as loading an inline Web browser using an Adobe Flash Player plug-in.

A telecommunications company IPTV service is usually delivered over an investment-heavy walled garden network. Local IPTV, as used by businesses for audio visual AV distribution on their company networks is typically based on a mixture of conventional TV reception equipment with IPTV encoders and IPTV gateways that take broadcast MPEG channels and IP wrap them to create multicast streams.

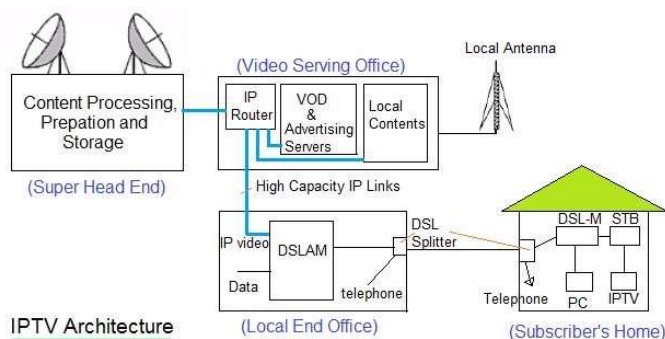


Figure C1: Example of IPTV architecture

PROCEDURES:

1. Firstly, download and install MX Player from Google Play Store.
2. Next get these two files (iptv-pro.apk and Eth_Update_IPTV_2020.m3u) from the internet and then download and save it at the android smartphone.
3. Now find the location of iptv-pro.apk on the smartphone and then install and run the application.
4. On the smartphone, there will be 2 icons of application which is Aptoide and IPTV Pro application as shown in Figure C2. Actually the IPTV Pro is an in-app purchases application but with using the given apk file, the student shall use an Aptoide apps to install IPTV Pro by free.

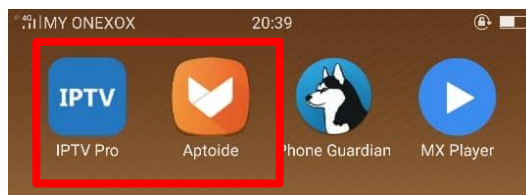


Figure C2: The application icon for Aptoide and IPTV Pro.

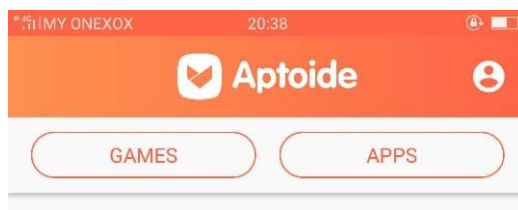


Figure C3: The front appearances of Aptoide application.

5. Make sure to *full update* the IPTV Pro application at Aptoide or otherwise the IPTV Pro won't work.
6. Now it's time to protect the network connection, by turning on the Virtual Private Network (VPN). Please download and install the Phone Guardian Mobile Security & VPN Protection from Google Play Store.
7. After install the Phone Guardian Mobile Security & VPN Protection, go to setting notification on the smartphone and enable (set 'ON') the notification for the application.

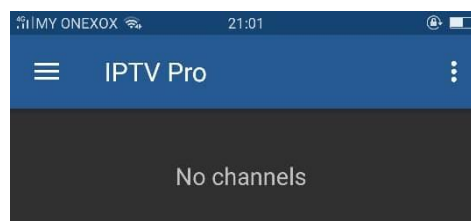


Figure C4: The first front appearances of IPTV Pro (*fully updated*) application without any added channel.



Figure C5: The MX Player application at Google Play Store



Figure C6: The Phone Guardian Mobile Security & VPN Protection at Google Play Store

8. Then, open the IPTV app and find button 'EDIT' and then click '+ Add playlist' icon as shown in Figure C7.
9. Next choose 'Select File' as shown in Figure C8 to add the Eth_Update_IPTV_2020.m3u file that refer to playlist most of frequent television watching channel at Malaysia or double click the file.
10. Lastly, make the IPTV Pro apps shall appear the list of channel as shown in Figure C8.
11. Now watch and observe the QoS for given channel and compare it with conventional DBVT2 similar television channel.

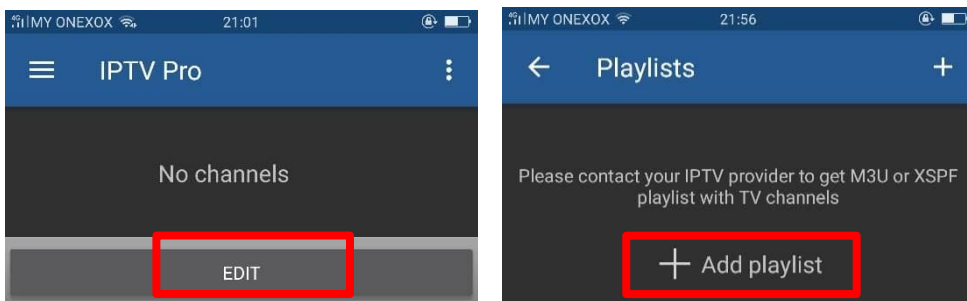


Figure C7: 'EDIT' and '+ Add playlist' icon at IPTV Pro apps.

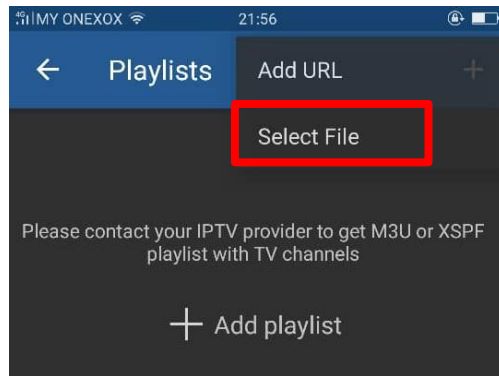


Figure C8: Option to add playlist m3u link file

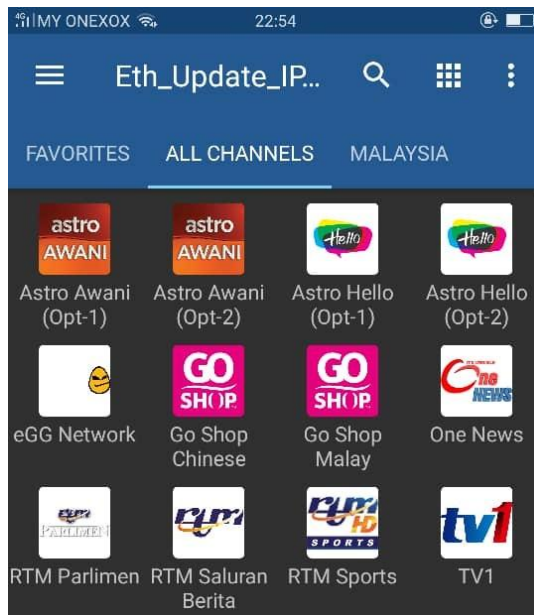


Figure C9: The list of channel at IPTV Pro.

RESULT:

From the practical works, what the average delays (in second) and the quality pictures of IPTV compare to conventional television (e.g. DBVT2) network?

Average delays:

Quality pictures:

List down at least TWO (2) differences IPTV compare with conventional television (e.g. DBVT2) network.

IPTV	Traditional TV

REFLECTION

List out FOUR (4) popular types of IPTV services

Explain the future and challenges if IPTV for the next decades.

DISCUSSION/CONCLUSION:

List down at least TWO (2) the advantages and disadvantages of IPTV

PRACTICAL ACTIVITIES D

TOPIC: VPN SERVICES WITH IPV4 ADDRESSING

OBJECTIVES:

At the end of this practical activities, you should be able to;

1. Understand VPN Services in NGN
2. Explain VPN Functional Architecture
3. Learn the function of VPN services

EQUIPMENTS:

Below are the list of equipments used for the activities.

1. Desktop computer or notebook with internet network.
2. CyberGhost software for windows.
https://www.cyberghostvpn.com/en_US/apps/windows-vpn/download-trial/latest

SAFETY PRECAUTION:

Before performing a practical work, make sure that these instructions are read to be complied;

1. Do not plug in external devices (e.g. USB thumb drive) without scanning them for computer viruses.
2. Always back up all your important data files.

THEORY:

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common, although not an inherent, part of a VPN connection. VPN technology was developed to provide access to corporate applications and resources to remote or mobile users, and to branch offices. For security, the private network connection may be established using an encrypted layered tunnelling protocol, and users may be required to pass various authentication methods to gain access to the VPN.

In other applications, Internet users may secure their connections with a VPN to circumvent geo-blocking and censorship or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet. Some websites, however, block access to known IP addresses used by VPNs to prevent the circumvention of their geo-restrictions, and many VPN providers have been developing strategies to get around these

blockades. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunnelling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely. Three broad categories of VPNs exist, namely remote access, intranet-based site-to-site, and extranet-based site-to-site. While individual users most frequently interact with remote access VPNs, businesses make use of site-to-site VPNs more often.

Early data networks allowed VPN-style connections to remote sites through dial-up modem or through leased line connections utilizing X.25, Frame Relay and Asynchronous Transfer Mode (ATM) virtual circuits provided through networks owned and operated by telecommunication carriers. These networks are not considered true VPNs because they passively secure the data being transmitted by the creation of logical data streams. They have been replaced by VPNs based on IP and IP/Multi-protocol Label Switching (MPLS) Networks, due to significant cost-reductions and increased bandwidth provided by new technologies such as digital subscriber line (DSL) and fiber-optic networks. VPNs can be characterized as host-to-network or remote access by connecting a single computer to a network or as site-to-site for connecting two networks. In a corporate setting, remote-access VPNs allow employees to access the company's intranet from outside the office. Site-to-site VPNs allow collaborators in geographically disparate offices to share the same virtual network. A VPN can also be used to interconnect two similar networks over a dissimilar intermediate network, such as two IPv6 networks connected over an IPv4 network.

A wide variety of (typically commercial) entities provide "VPNs" for all kinds of purposes, but depending on the provider and the application, they often do not create a true "private network" with anything meaningful on the local network. Nonetheless the term is increasingly prevalent. The general public has come to mainly use the term VPN service or just VPN specifically for a commercially marketed product or service that uses a VPN protocol to tunnel the user's internet traffic so an IP address of the service provider's server appears to the public to be the IP address of the user. Depending on the features properly implemented, the user's traffic, location and/or real IP may be hidden from the public, thereby providing the desired internet access features offered, such as Internet censorship circumvention, traffic anonymization, and geo-unblocking. They tunnel the user's internet traffic securely only between the public internet and the user's device and there is typically no way for a user's devices connected to the same "VPN" to see each other.

These VPNs can be based on typical VPN protocols or more camouflaged VPN implementations like SoftEther VPN, but proxy protocols like Shadowsocks are used as well. These VPNs are usually marketed as privacy protection services. On the client side, a common VPN setup is by design not a conventional VPN, but does typically use the operating system's VPN interfaces to capture a user's data to send through. This includes virtual network adapters on computer OSes and specialized "VPN" interfaces on mobile operating systems. A less common alternative is to provide a SOCKS proxy interface. Users must consider that when the transmitted content is not encrypted before entering a VPN, that data is visible at the receiving endpoint (usually the public VPN provider's site) regardless of whether the VPN tunnel wrapper itself is encrypted for the inter-node transport.

The only secure VPN is where the participants have oversight at both ends of the entire data path, or the content is encrypted before it enters the tunnel provider. As of March 2020 it is estimated that over 30% of Internet users around the world use a commercial VPN, with that number higher in the Middle East, Asia, and Africa.

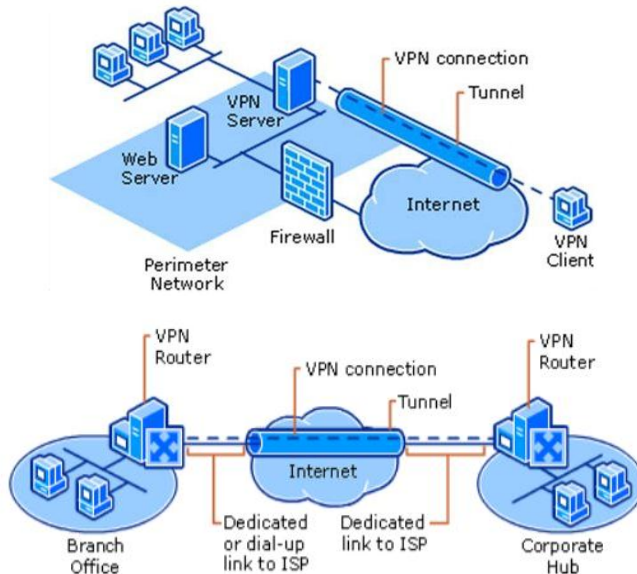


Figure D1: The basic example of VPN architecture

PROCEDURES:

1. First, go to Google browser and search 'my ip' as shown in Figure 4.2 to find the public IP address and fill it in the results.
2. Now download and run the CyberGhost software from the given link for a trial version. Make sure to uninstall the software after finish the practical work.

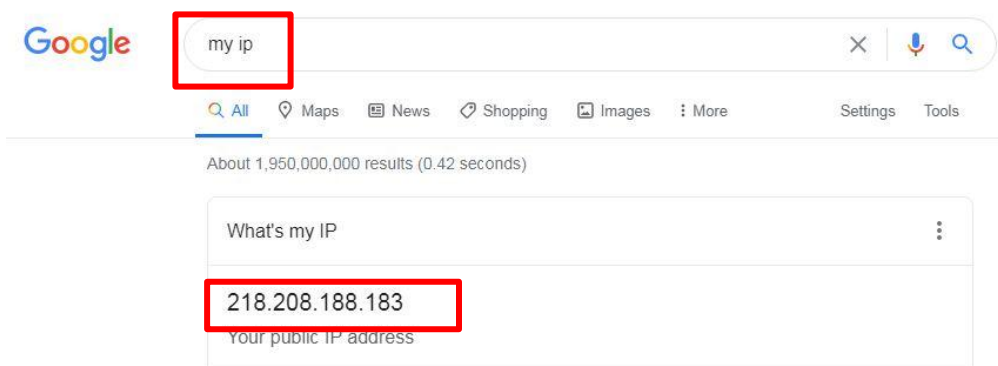


Figure D2: Determination of public IP address from Google browser.

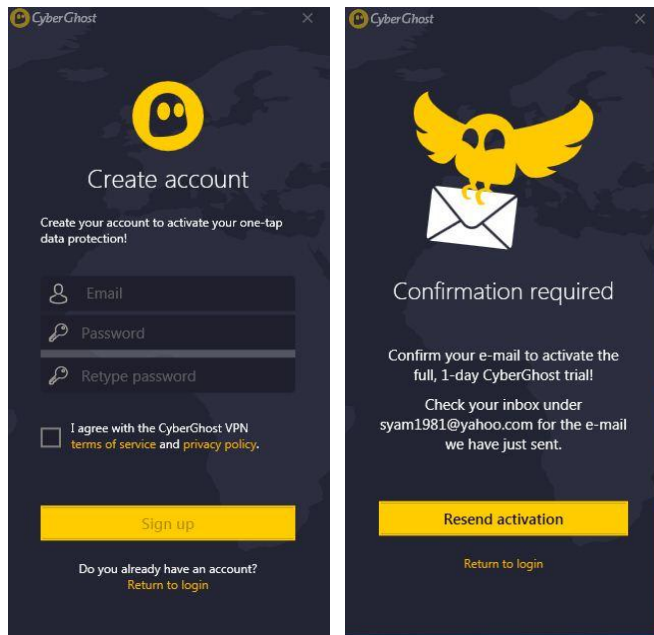


Figure D3: CyberGhost software sign-up account

3. Besides, open the <https://www.iplocation.net> and screen shot the 'IP Address Detail' as shown in Figure 4.4. Attach the screen shot in the given empty at results.
4. After verified the CyberGhost at email, open the software and connecting to any available VPN server as shown in Figure 4.5.
5. Now, go again to Google browser and search '*my ip*' as shown in Figure 4.2 to find the public IP address and fill it in the results.
6. Last, open again the <https://www.iplocation.net> and screen shot the 'IP Address Detail' as shown in Figure 4.6. Attach the screen shot in the given empty at results

IP Address Details

IP Address	218.208.188.183 Hide my IP with VPN
IP Location	Muar, Johor (MY) [Details]
ISP	Telekom Malaysia Berhad
Proxy	218.208.188.183, 192.230.115.2
Platform	Windows 7
Browser	Chrome 86.0.4240.193
User Agent	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36
Screen Size	1440px X 900px
Cookie	Enabled
Javascript	Enabled

Figure D4: Example of 'IP Address Detail' from <https://www.iplocation.net>.

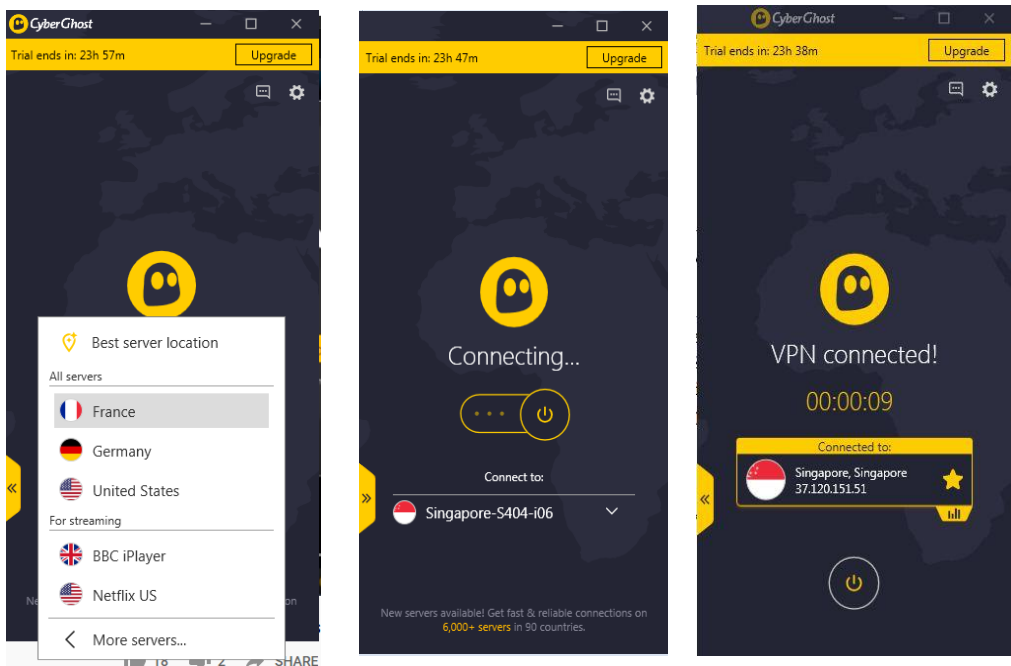


Figure D5: Server selection and connecting process of CyberGhost software.

IP Address Details

IP Address	37.120.151.51	Hide my IP with VPN
IP Location	Singapore, Singapore (SG) [Details]	
ISP	Secure Data Systems SRL	
Proxy	37.120.151.51, 198.143.39.16	
Platform	Windows 7	
Browser	Chrome 86.0.4240.193	
User Agent	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36	
Screen Size	1440px X 900px	
Cookie	Enabled	
Javascript	Enabled	

Figure D6: Example of connected VPN 'IP Address Detail' from <https://www.iplocation.net>.

RESULTS:

From the practical works, list out the results of Public IP address **before** connected to CyberGhost software with possible other addressing information.

Items	Details
Public IP Address	
IP Location	
IP Class	
Broadcast Address	
Host Address	
Subnet Mask	

From the practical works, list out the results of VPN IP address **after** successful connected to CyberGhost software.

Items	Details
VPN IP Address	
IP Location	
IP Class	
Broadcast Address	
Host Address	
Subnet Mask	

REFLECTION:

List out FOUR (4) most popular VPN services platform.

List out FIVE (5) advantages and disadvantages of VPN

DISCUSSION/CONCLUSION:

Explain the important of Virtual Private Network (VPN).

PRACTICAL ACTIVITIES E

TOPIC: IPV4 IN VoIP SERVICES

OBJECTIVES:

At the end of this practical activities, you should be able to;

1. Setting up a conversation using VoIP.
2. Differentiate between conventional telephony and VoIP telephony.
3. Learn use VoIP services.

EQUIPMENTS:

Below are the list of equipments used for the activities.

1. TWO android smartphone devices; Smartphone #1 and Smartphone #2.
2. Hotspot and WiFi capabilities on both smartphone.
3. IP call android apps by Rnet Software

SAFETY PRECAUTION:

Before performing a practical work, make sure that these instructions are read to be complied;

1. Do not plug in external devices (e.g. USB thumb drive) without scanning them for computer viruses.
2. Always back up all your important data files.

THEORY:

Voice over Internet Protocol (also voice over IP, VoIP or IP telephony) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN).

The steps and principals involved in originating VoIP telephone calls are similar to traditional digital telephony and involve signalling, channel setup, digitization of the analog voice signals, and encoding. Instead of being transmitted over a circuit-switched network, the digital information is packetized, and transmission occurs as IP packets over a packet-switched network. They transport media streams using special media delivery protocols that encode audio and video with audio codecs, and video codecs. Various codecs exist that optimize the media stream based on application requirements and network bandwidth; some implementations rely on narrowband and compressed speech, while others support high-fidelity stereo codecs.

Early providers of voice-over-IP services offered business models and technical solutions that mirrored the architecture of the legacy telephone network. Second-generation providers, such as Skype, built closed networks for private user bases, offering the benefit of free calls and convenience while potentially charging for access to other communication networks, such as the PSTN. This limited the freedom of users to mix-and-match third-party hardware and software. Third-generation providers, such as Google Talk, adopted the concept of federated VoIP—which is a departure from the architecture of the legacy networks. These solutions typically allow dynamic interconnection between users on any two domains on the Internet when a user wishes to place a call. In addition to VoIP phones, VoIP is also available on many personal computers and other Internet access devices. Calls and SMS text messages may be sent over mobile data or Wi-Fi. VoIP allows modern communications technologies (including telephones, smartphones, voice and video conferencing, email, and presence detection) to be consolidated using a single unified communications system.

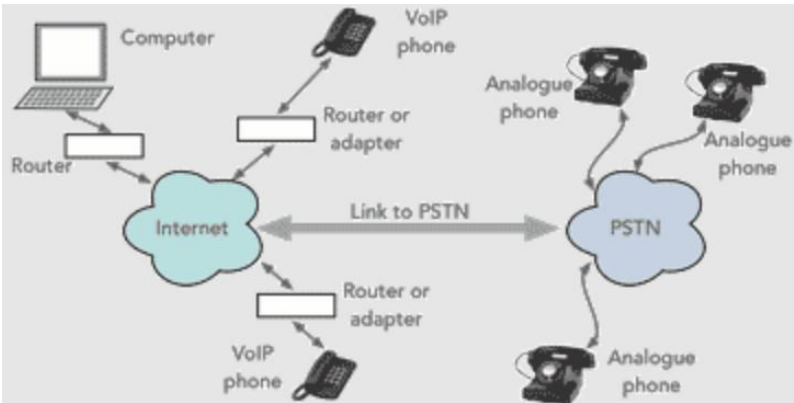


Figure E1: Block diagram connection network from VoIP to PSTN

PROCEDURES 1:

1. Install the application of IP call from Google play store to the both smartphones as shown in Figure E2.
2. Turn 'ON' the Mobile Data Network and then make sure to "Refresh IP" as shown in Figure E3 to find out your IP Address given by the Telco Provider.
3. Fill up the IP Address result in the table below and do the same step for others smartphone.



Figure E2: An application 'IP call' create by Rnet Softwares

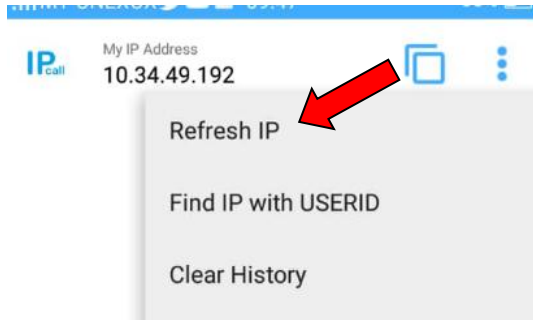


Figure E3: Column of "Refresh IP" setting at IP call application.

4. Make a VoIP call (from Smartphone #1 to #2) less than one minute using the IP address that obtain from Smartphone #2. Make sure both smartphone in same Telco provider and observe the QoS (Quality of Services) during call process.

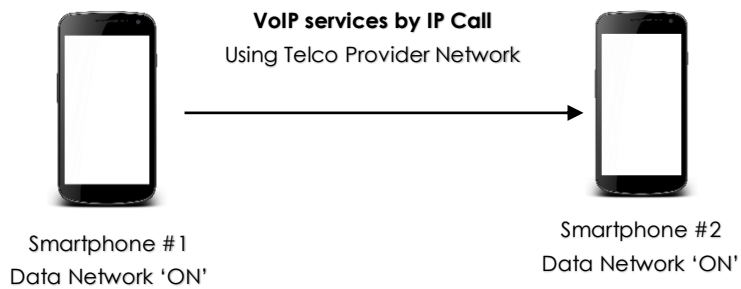
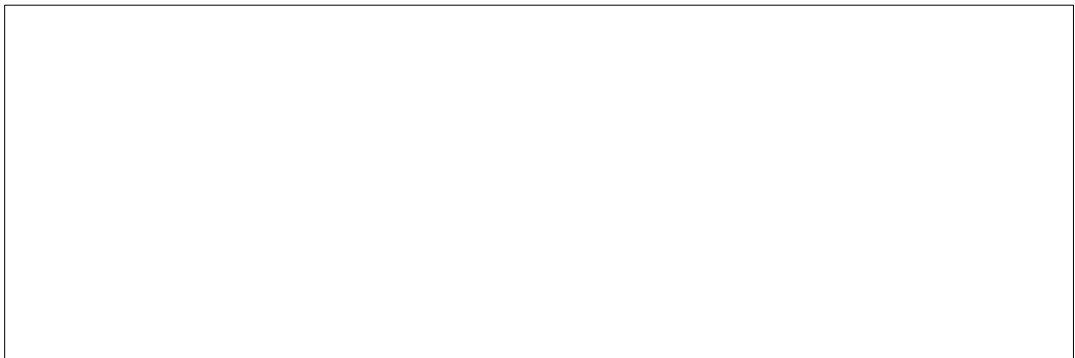


Figure E4: VoIP connection from Smartphone #1 to Smartphone #2 through mobile broadband network.

RESULT 1:

QoS observation:

**in term of clarity, noise interruption, delays or jitters, continuity (or intermittent) and else*



State the IP address of Smartphone #1 that obtain from IP Call application

Description	Detail
IP Address Smartphone #1	
Telco Provider of Smartphone #1	
Location	
IP Class Category	
Host Address	
Subnet Mask	

State the IP address of Smartphone #2 that obtain from IP Call application

Description	Detail
IP Address Smartphone #2	
Telco Provider of Smartphone #2	
Location	
IP Class Category	
Host Address	
Subnet Mask	

PROCEDURES 2:

1. Now turn "OFF" the Mobile Data Network and make your own network within the two smartphone using hotspot and WiFi.
2. Make a "Refresh IP" in IP Call to find out the IP Address that being set for the smartphone for Hotspot and WiFi standalone network.
3. Make a VoIP call using Smartphone #1 to Smartphone #2.
4. Observe the QoS (Quality of Services) and fill up the result below.

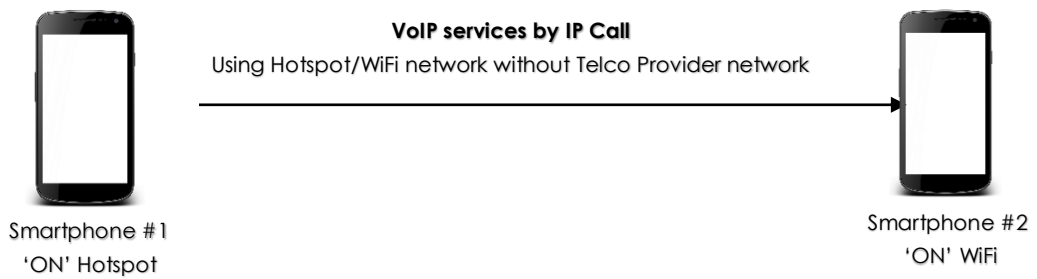


Figure E5: VoIP connection from Smartphone #1 to Smartphone #2 through Hotspot & WiFi network.

RESULT 2:

QoS observation:

**in term of clarity, noise interruption, delays or jitters, continuity (or intermittent) and else*

State the IP address of Smartphone #1 that obtain from IP Call application

Description	Detail
IP Address Smartphone #1	
Telco Provider of Smartphone #1	
Location	
IP Class Category	
Host Address	
Subnet Mask	

State the IP address of Smartphone #2 that obtain from IP Call application

Description	Detail
IP Address Smartphone #2	
Telco Provider of Smartphone #2	
Location	
IP Class Category	
Host Address	
Subnet Mask	

REFLECTION:

List out 4 (FOUR) software or smartphone applications that can be used for VoIP telephone services;

State 2 (TWO) advantages and disadvantages of VoIP;

DISCUSSION/CONCLUSION:

Discuss 3 (THREE) differences between VoIP services compare with traditional telephony using PSTN.



PRACTICAL ACTIVITIES F

TOPIC: LED CONTROL USING WEB OF THING (WoT)

OBJECTIVES:

At the end of this practical activities, you should be able to;

1. Learn to setup a WoT services.
2. Differentiate between IoT and WoT.
3. Know the advantages of WoT in NGN

EQUIPMENTS:

Below are the list of equipments used for the activities.

1. NodeMCU ESP8266 12E,
2. 220 ohms Resistor,
3. LED,
4. Breadboard and Jumper Wire.
5. Computer or laptop.

SAFETY PRECAUTION:

Before performing a practical work, make sure that these instructions are read to be complied;

1. Do not plug in external devices (e.g. USB thumb drive) without scanning them for computer viruses. Always back up all your important data files.
2. Electrically NodeMCU is very sensitive. Supply voltages should not exceed 5 volts through the USB and be within 7 to 12 volts. Do not exceed current drawn from each pin 40 mA.

THEORY:

As billions of devices connect to the Internet, a new Web of Things is emerging, with virtual representations of physical or abstract realities increasingly accessible via Web technologies. Achieving a new phase of exponential growth, comparable to the earliest days of the Web, will require open markets, open standards, and the vision to imagine the potential for this expanding WoT. The Web of Things (WoT) is a computing concept that describes a future where everyday objects are fully integrated with the Web. The prerequisite for WoT is for the "things" to have embedded computer systems that enable communication with the Web. Such smart devices would then be able to communicate with each other using existing Web standards.

Considered a subset of the Internet of Things (IoT), WoT focuses on software standards and frameworks such as REST, HTTP and URIs to create applications and services that combine

and interact with a variety of network devices. So, you could think of the Web of Things as everyday objects being able to access Web services. The key point is that this doesn't involve the reinvention of the means of communication because existing standards are used. Internet of Things is more often used in the context of radiofrequency identification (RFID) and how physical objects are tied to the Internet and can communicate with each other. Both terms are difficult to define precisely, although they are related in their general theme.

The Web of Things is simply the next stage in this evolution, using and adapting Web protocols to connect anything in the physical world and give it an existence on the World Wide Web. The WoT architecture is an effort to structure the galaxy of Web protocols and tools into an advantageous framework for connecting any object or device to the Web. The WoT architecture stack is not composed of layers in the rigid sense, but rather of levels that add extra functionality.

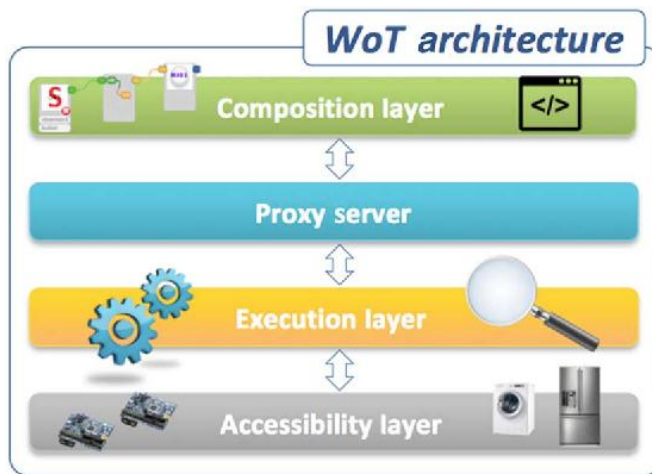


Figure F1: WoT architecture

PROCEDURES:

1. Install the ESP8266 NodeMCU, resistor, led and wire jumper on the breadboard as shown in Figure 6.2. Then connect USB 3.0 (data type) to the computer.

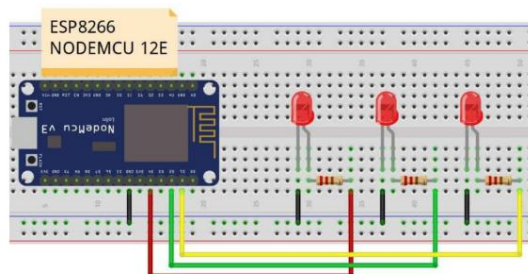


Figure F2: Diagram for controlling LED from ESP8266 Web Server

2. Install Arduino IDE on the computer and update ESP8266 on the software. You can do by go to File> Preferences to update by pasting the following link:

https://arduino.esp8266.com/stable/package_esp8266com_index.json

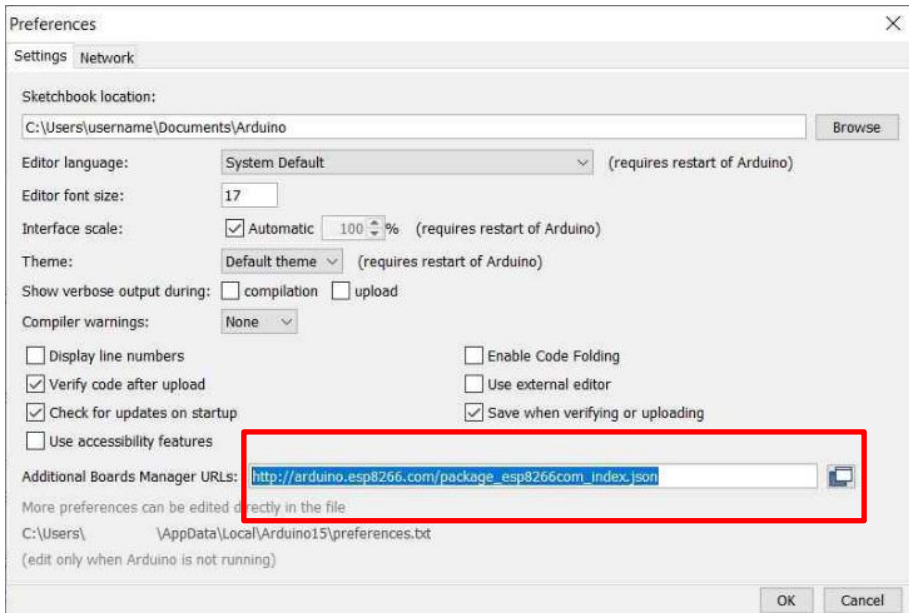


Figure F3: Update proses of software at Additional Board Manager



Figure F4: Update the esp8266 package by ESP8266 Community

- To double check the update process, go to Tools > Board > Boards Manager and type "ESP8266" in search bar. You will see ESP8266 by ESP8266 community. You can see it is showing "INSTALLED".
- Then go to "tools > Board > select Generic ESP8266 Module" and then then go to tools again and select the correct port. Restart the Arduino IDE. Now you are ready work with NodeMCU ESP8266 using Arduino IDE.

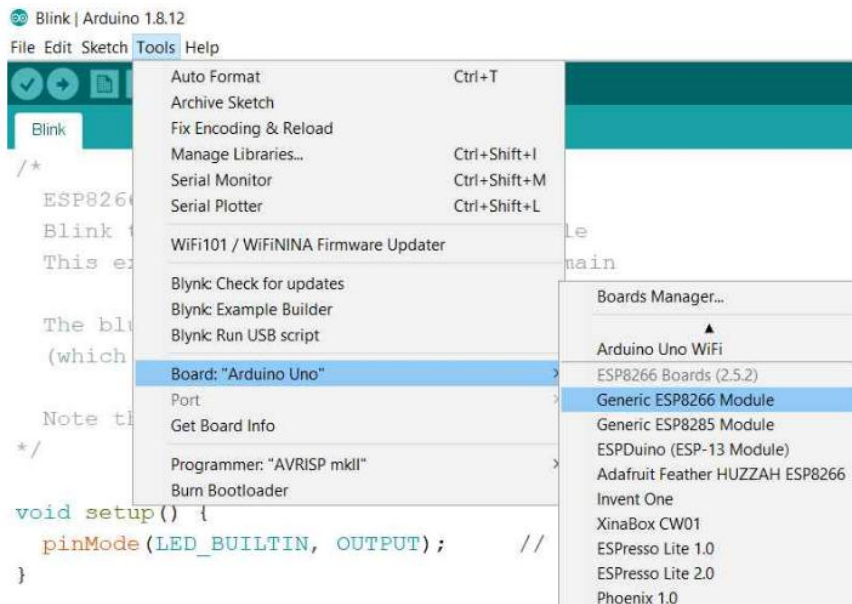


Figure F5: The selection of Generic ESP8266 Module for run the programme

- Now upload the code to Arduino IDE. Please set the SSID and Password. i.e., Wi-Fi network name and Password at the code. After uploading code go to serial monitor to see IP Address so that you can control your LED. If in serial monitor you can't see anything. Press reset button on NodeMCU ESP8266.
- Below are the three page code for controlling LED, you also can get the full code from your instructor. Run the code at Arduino IDE.

```

// Enter your wifi network name and Wifi Password
const char* ssid = "Your SSID";
const char* password = "Your Password";

// Set web server port number to 80
WiFiServer server(80);

// Variable to store the HTTP request
String header;

// These variables store current output state of LED
String outputRedState = "off";
String outputGreenState = "off";
String outputYellowState = "off";

// Assign output variables to GPIO pins
const int redLED = 2;
const int greenLED = 4;
const int yellowLED = 5;

// Current time
unsigned long currentTime = millis();
// Previous time
unsigned long previousTime = 0;
// Define timeout time in milliseconds (example: 2000ms = 2s)
const long timeoutTime = 2000;

void setup() {
  Serial.begin(115200);
  // Initialize the output variables as outputs
  pinMode(redLED, OUTPUT);
  pinMode(greenLED, OUTPUT);
  pinMode(yellowLED, OUTPUT);
  // Set outputs to LOW
  digitalWrite(redLED, LOW);
  digitalWrite(greenLED, LOW);
  digitalWrite(yellowLED, LOW);

  // Connect to Wi-Fi network with SSID and password
  Serial.print("Connecting to ");
  Serial.println(ssid);
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }

  // Print local IP address and start web server
  Serial.println("");
  Serial.println("WiFi connected.");
  Serial.println("IP address: ");
  Serial.println(WiFi.localIP());
  server.begin();
}
#include <ESP8266WiFi.h>

void loop(){
  WiFiClient client = server.available(); // Listen for incoming clients

  if (client) { // If a new client connects,
    Serial.println("New Client."); // print a message out in the serial port
    String currentLine = ""; // make a String to hold incoming data from the client
    currentTime = millis();
    previousTime = currentTime;
    while (client.connected() && currentTime - previousTime <= timeoutTime) { // loop while the client's connected
      currentTime = millis();
      if (client.available()) { // if there's bytes to read from the client,
        char c = client.read(); // read a byte, then
        Serial.write(c); // print it out the serial monitor
        header += c;
        if (c == '\n') { // if the byte is a newline character
          // if the current line is blank, you got two newline characters in a row.
          // that's the end of the client HTTP request, so send a response:
          if (currentLine.length() == 0) {
            // HTTP headers always start with a response code (e.g. HTTP/1.1 200 OK)
            // and a content-type so the client knows what's coming, then a blank line:
            client.println("HTTP/1.1 200 OK");
            client.println("Content-type:text/html");
            client.println("Connection: close");
            client.println();
          }
        }
      }
    }
  }
}

```

```

// turns the GPIOs on and off
if (header.indexOf("GET /2/on") >= 0) {
Serial.println("RED LED is on");
outputRedState = "on";
digitalWrite(redLED, HIGH);
} else if (header.indexOf("GET /2/off") >= 0) {
Serial.println("RED LED is off");
outputRedState = "off";
digitalWrite(redLED, LOW);
} else if (header.indexOf("GET /4/on") >= 0) {
Serial.println("Green LED is on");
outputGreenState = "on";
digitalWrite(greenLED, HIGH);
} else if (header.indexOf("GET /4/off") >= 0) {
Serial.println("Green LED is off");
outputGreenState = "off";
digitalWrite(greenLED, LOW);
} else if (header.indexOf("GET /5/on") >= 0) {
Serial.println("Yellow LED is on");
outputYellowState = "on";
digitalWrite(yellowLED, HIGH);
} else if (header.indexOf("GET /5/off") >= 0) {
Serial.println("Yellow LED is off");
outputYellowState = "off";
digitalWrite(yellowLED, LOW);
}

// Display the HTML web page
client.println("<DOCTYPE html><html>");
client.println("<head><meta name=\"viewport\" content=\"width=device-width, initial-scale=1\">");
client.println("<link rel=\"icon\" href=\"data:,\");");
// CSS to style the on/off buttons
client.println("<style>html { font-family: Helvetica; display: inline-block; margin: 0px auto; text-align: center;};");
client.println(".buttonRed { background-color: #ff0000; border: none; color: white; padding: 16px 40px; border-radius: 60%;");
client.println("text-decoration: none; font-size: 30px; margin: 2px; cursor: pointer;});");
client.println(".buttonGreen { background-color: #00ff00; border: none; color: white; padding: 16px 40px; border-radius: 60%;");
client.println("text-decoration: none; font-size: 30px; margin: 2px; cursor: pointer;});");
client.println(".buttonYellow { background-color: #feeb36; border: none; color: white; padding: 16px 40px; border-radius: 60%;");
client.println("text-decoration: none; font-size: 30px; margin: 2px; cursor: pointer;});");
client.println(".buttonOff { background-color: #77878A; border: none; color: white; padding: 16px 40px; border-radius: 70%;");
client.println("text-decoration: none; font-size: 30px; margin: 2px; cursor: pointer;};</style></head>");

// Web Page Heading
client.println("<body><h1>My LED Control Server</h1>");

// Display current state, and ON/OFF buttons for GPIO 2 Red LED
client.println("<p>Red LED is " + outputRedState + "</p>");
// If the outputRedState is off, it displays the OFF button
if (outputRedState=="off") {
client.println("<p><a href=\"/2/on\"><button class=\"button buttonOff\">OFF</button></a></p>");
} else {
client.println("<p><a href=\"/2/off\"><button class=\"button buttonRed\">ON</button></a></p>");
}
// Display current state, and ON/OFF buttons for GPIO 4 Green LED
client.println("<p>Green LED is " + outputGreenState + "</p>");
// If the outputGreenState is off, it displays the OFF button
if (outputGreenState=="off") {
client.println("<p><a href=\"/4/on\"><button class=\"button buttonOff\">OFF</button></a></p>");
} else {
client.println("<p><a href=\"/4/off\"><button class=\"button buttonGreen\">ON</button></a></p>");
}
client.println("</body></html>");

// Display current state, and ON/OFF buttons for GPIO 5 Yellow LED
client.println("<p>Yellow LED is " + outputYellowState + "</p>");
// If the outputYellowState is off, it displays the OFF button
if (outputYellowState=="off") {
client.println("<p><a href=\"/5/on\"><button class=\"button buttonOff\">OFF</button></a></p>");
} else {
client.println("<p><a href=\"/5/off\"><button class=\"button buttonYellow\">ON</button></a></p>");
}
client.println("</body></html>");

```

```

// The HTTP response ends with another blank line
client.println();
// Break out of the while loop
break;
} else { // if you got a newline, then clear currentLine
currentLine = "";
}
} else if (c != '\r') { // if you got anything else but a carriage return character,
currentLine += c; // add it to the end of the currentLine
}
}
// Clear the header variable
header = "";
// Close the connection
client.stop();
Serial.println("Client disconnected.");
Serial.println("");
}
}

```



Figure F6: Reset button at NodeMCU ESP8266 board

7. Then copy IP address at Serial Monitor and paste the IP address at any browser. Now you can control the LED via html or web.

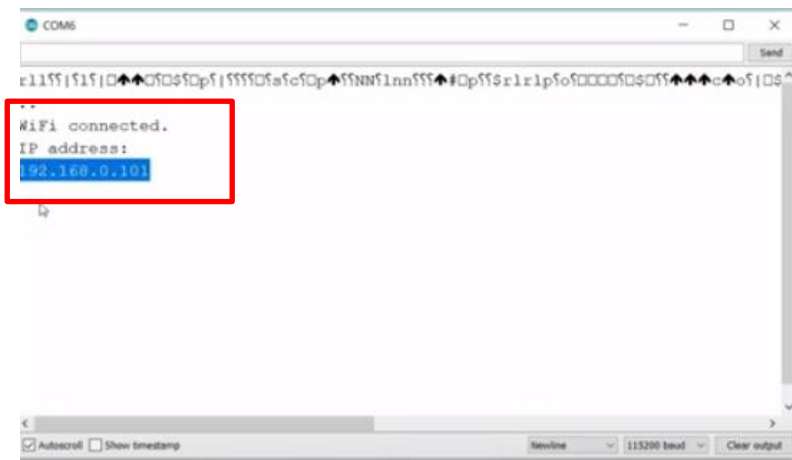


Figure F7: Serial Monitor display for IP Address

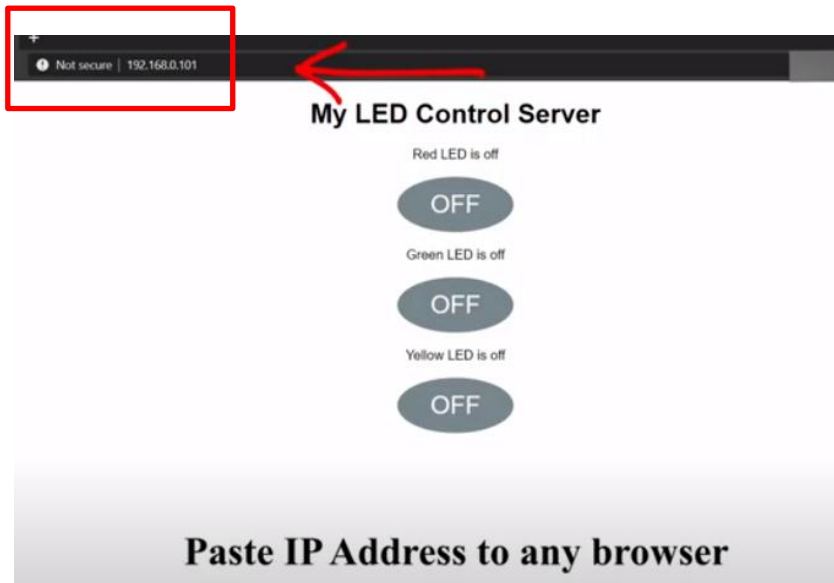


Figure F8: Paste the IP Address at any browser

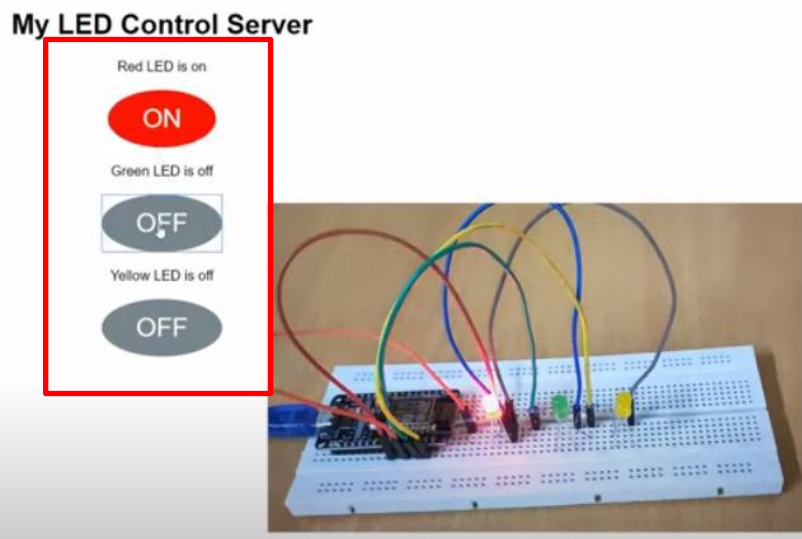


Figure F9: Control the LED using IP Address.

RESULTS:

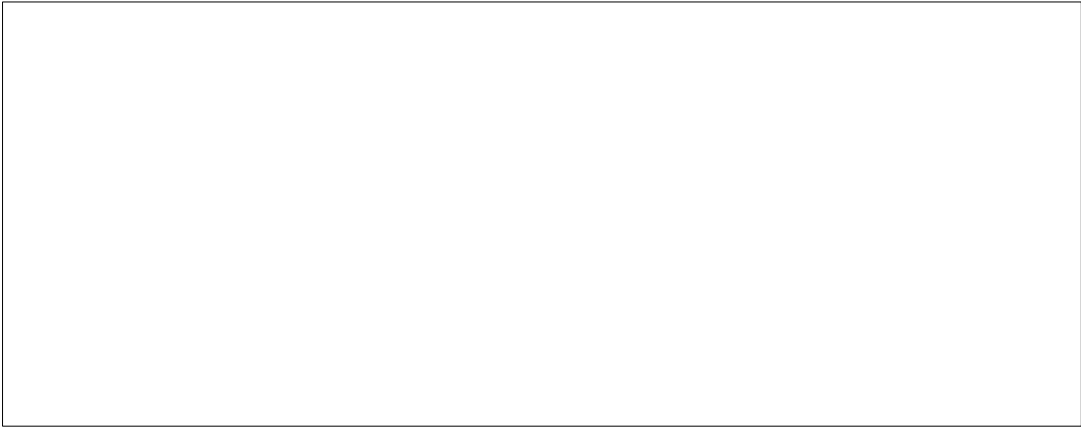
The IP address obtains from the Serial Monitor:

Sketch the wired connection from LED breadboard to NodeMCU board;



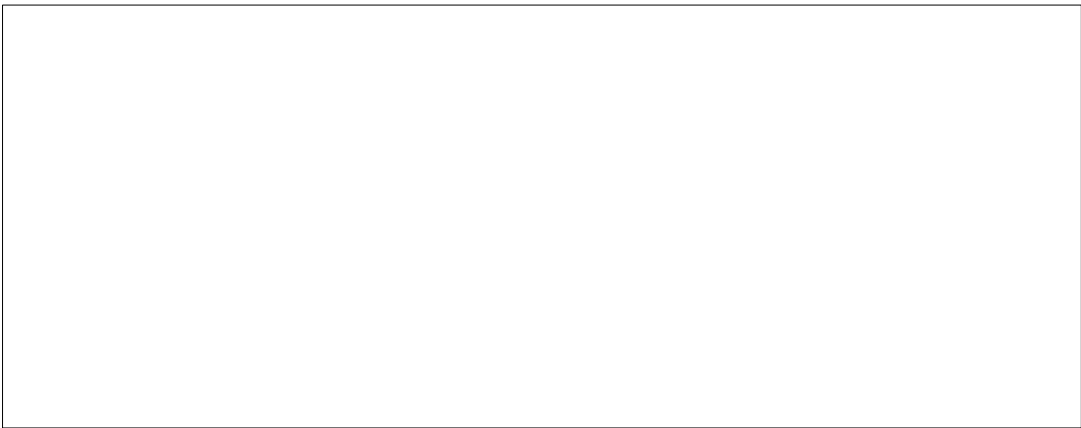
REFLECTION:

List out 2 advantages and disadvantages of WoT;



DISCUSSION/CONCLUSION:

Explain the differentiation of WoT and IoT;



ABBREVIATION

0-9

2G	Second Generation
3G	Third Generations
3GPP	3rd Generation Partnership Project
4G	Fourth Generations
5G	Fifth Generations

A

AAA	Authentication, Authorization, and Accounting
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AMC	Adaptive Modulation and Coding
AMPS	Advanced Mobile Phone System
ANSI	American National Standards Institute
APIs	Application Programming Interfaces
ARQ	Automatic Retransmission Requests
ATA	Analog Telephony Adaptor

B

BPL	Broadband over Power Lines
-----	----------------------------

C

CapEx	Capital Expenditures
CAS	Channel Associated Signaling
CCITT	Consultative Committee for International Telephony & Telegraphy
CCs	Component Carriers
CD	Compact Disc
CDM	Code Division Multiplexing
CDMA	Code-division multiple access
CDPD	Cellular Digital Packet Data
CO	Central Office
CoMP	Coordinated Multi Point
CSD	Circuit Switched Data

D

D/A	Digital/Analog
DC	Direct Current
DeNB	Donor eNB
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DMT	Discrete Multitone
DMUX	Demultiplexer
DNS	Domain Name Server

DP	Distribution Point
DSLAM	Digital Subscriber Line Access Multiplexer
DSL	Digital Subscriber Line
DSL-M	DSL Modem
E	
EDGE	Enhanced Data rates for GSM Evolution
ED-VO	Evolution-Data Optimized
ENUM	E.164 Number Mapping
ETSI	European Telecommunications Standards Institute
F	
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FMCA	Fixed-Mobile Convergence Alliance
FMC	Fixed-Mobile Convergence
FTP	Foil Shielded Cable
G	
GERAN	GSM EDGE Radio Access Network
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
H	
HDSL	High-Bit-Rate Digital Subscriber Line
HSPA	High Speed Packet Access
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I	
ICT	Information and Communications Technology
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Systems
IMT	International Mobile Telecommunications
IoT	Internet of Things
IP	Internet Protocol
IPTV	Internet Protocol television
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISUP	ISDN Services User Part
ITU	International Telecommunication Union

L

LAN	Local Area Network
LED	Light Emitting Diode
LTE	Long Term Evolution
LTE-A	Long Term Evolution - Advanced

M

MBWA	Mobile Broadband Wireless Access
MDF	Main Distribution Frame
MIMO	Multiple Input Multiple Output
MTP	Media Transfer Protocol
MUX	Multiplexing

N

nVoD	Near Video on Demand
NAT	Network Address Translation
NFV	Network Functions Virtualization
NFVI	Network Functions Virtualization Infrastructure
NFV-MANO	Network Functions Virtualization Management And Orchestration
NGN	Next Generation Network
NLOS	Non-line-of-sight
NMS	Network Management
NMT	Nordic Mobile Telephone
NOMA	Non-Orthogonal Multiple Access

O

OFDMA	Orthogonal Frequency Division Multiple Access
OMAP	Open Multimedia Applications Platform
OPEX	Operating Expenses
OSI	Open Systems Interconnection
OTT	Over-the-top

P

PAM	Pulse Amplitude Modulation
PBX	Private Branch Exchange
PC	Personal computer
PCM	Pulse Code Modulation
PDA	Personal Digital Assistant
PDH	Plesiochronous Digital Hierarchy
PHY	Physical Layer
PLMN	Public Land Mobile Network
POTS	Plain old telephone service
PSTN	Public Switched Telephone Network

Q

QoS Quality-of-service

R

RADIUS Remote Authentication Dial-In User Service
RAN Radio Access Network
RJ Register Jack
RN Relay Nodes
RTP Real-time Transport Protocol
RX Receive

S

SaaS Software as a Service
S/N Signal to Noise
SCCP Signalling Connection Control Part
SCP Signal Control Point
SCTP Stream Control Transmission Protocol
SDN Software-Defined Networking
SDSL Symmetric Digital Subscriber Line
SIDS Small Island Developing States
SIP Session Initiation Protocol
SMTP Simple Mail Transfer Protocol
SOAP Simple Object Access Protocol
SPC Store Programme Control
SS7 Signaling System No. 7
SSP Service Switching Point
STB Set-top box
STP Signal Transfer Point
SW Switching

T

TACS Total Access Communications System
TCAP Transaction Capabilities Application Part
TCP/IP Transmission Control Protocol/Internet Protocol
TDD Time-Division Duplexing
TDM Time Division Multiplexing
TDMA Time-Division Multiple Access
TLS Transport Layer Security
TUP Telephone User Part
TV Television
TVoD TV on Demand
TX Transmit

U

UDP	User Datagram Protocol
UE	User Equipment
UL	Uplink
UMTS	Universal Mobile Telecommunications Service
USB	Universal Serial Bus
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
UTRAN	UMTS Terrestrial Radio Access Network
UTP	Unshielded Twisted Pair
USN	Ubiquitous Sensor Network

V

VDSL	Very High-Speed Digital Subscriber Line
VoD	Video on demand
VoIP	Voice over Internet Protocol
VNFs	Virtualized Network Functions
VPN	Virtual Private Network

W

W3E	World Wide Web for Education
WCDMA	Wideband Code Division Multiple Access
WDM	Wavelength-Division Multiplexing
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WoT	Web of Things
WPAN	Wireless Personal Area Network
WRC	World Radiocommunication Conference
WS	Web Services
WSDL	Web Services Description Language

X

XML	Extensible Mark-up Language
-----	-----------------------------

REFERENCES

- i. Cohen, T. (2007). "Next Generation Networks (NGN) Regulation Overview". Independent Communications Authority of South Africa, 38.
- ii. Couch, L. W., Kulkarni, M., & Acharya, U. S. (2013). "Digital and Analog Communication Systems". Volume. 8, Upper Saddle River: Pearson.
- iii. Forouzan, A. B. (2007). "Data Communications and Networking". McGraw-Hill Education.
- iv. Jeffrey S. Beasley & Gary M. Miller. (2005). "Modern Electronic Communication". Pearson/Prentice Hall, 2005 - Technology & Engineering.
- v. International Telecommunication Union (2021, July 6). "Telecommunication Standardization Policy Division ITU Telecommunication Standardization Sector Ubiquitous Sensor Networks (USN) ITU-T Technology Watch Report". Printed in Switzerland Geneva, 4 February 2008. www.itu.int/itu-t/techwatch
- vi. Proakis, J. G., & Salehi, M. (2007). "Fundamentals of Communication Systems". Pearson Education India.
- vii. Rashmi Bhardwaj (2021, July 6). "DHCP (Dynamic Host Configuration Protocol): Explained". IPWITHEASE Pages. <https://ipwithease.com/dhcp-dynamic-host-configuration-protocol/>
- viii. Rezabeigi, K., Vafaei, A., & Movahhedinia, N. (2008). "A Web Services Based Architecture for NGN Services Delivery". World Academy of Science, Engineering and Technology, 43, 472-476.
- ix. Sen, J., Sayyad, M., & Hooli, B. (2010). "Convergence and Next Generation Networks". arXiv preprint arXiv:1012.2524.
- x. Sutherland, E. (2007). "Fixed-Mobile Convergence". Trends in Telecommunication Reform 2007, 87-100.
- xi. Wheeler, T. (2001). "Electronic Communications for Technicians". Prentice Hall.

This book is produced as a learning reference material in the field of electronic engineering (communications) related to telecommunication networks for the Next Generation Network (NGN). It is suitable for reference for students pursuing studies at the diploma and certificate level. It provides Q&A notes and exercises on each sub-topic. It also contains interesting and easy-to-understand graphic information with the list of abbreviations at the end of the chapter. In addition, there are 6 practical activities provided to students and readers for learning purposes and linked to the learning process by theoretically.



Syamsul Bahri Bin Mohamad is a Lecturer in the Department of Electrical Engineering, Politeknik Merlimau, Melaka (PMM). He holds a Master's Degree (Communication and Computer) from Universiti Kebangsaan Malaysia and a Master's Degree (Technical and Vocational Education) as well as a Bachelor's Degree (Electrical Engineering) from Kolej Universiti Teknologi Tun Hussein Onn (KUiTTHO) which is now Universiti Tun Hussein Onn (UTHM). He is an instructor for the Telecommunication Network course at Electrical Engineering Department, Politeknik Merlimau Melaka, which is one of the courses offered at the Malaysia polytechnic since 2019 until now.

e ISBN 978-967-2241-75-1

