SYLLABUS HIGHLIGHTS

Communication & Networking	-01
Components of communication	-02
Communication Media	-03
Copper cables	-04
Twisted Pair	-05
Shielded Twisted Pair	-05
Unshielded TP	-06
STP Vs UTP Comparison	06
Coaxial Cables	-09
Fiber Optic Cables	-13
Radio Waves	-20
Microwaves	-20
Infrared	-20
Visible light	-22
Properties of waves introduction	-24
Amplitude	-24
Wavelength	-25
Frequency	-25
Phase	-26
Waves vs Signals	-29
Analog Vs Digital Signals	-30
Need of Binary Systems	-31
Propagation Speed	-32
Bandwidth	-32
Latency	-34
Throughput	-37
Attenuation	-38
Distortion	-39
Noise	-40
Signal Encoding Schemes	-43
Voltage/Current/Binary	-44
Non-Return to zero	-45
Manchester Encoding	-47
Error Detection/Error Correction	-48
Parity Check/Odd/Even	-49
Hashing (needed later)	-51
Synchronization	-52
Clock Frequency/Timing	-53
Why we need Modulation	-54
Introduction to Modulation	-55
Types/Amplitude Modulation (AM)	-56
Frequency Modulation (FM)	-57
Phase Modulation (PM)	-58
Amplitude Shift Keying (ASK)	-59
Frequency Shift Keying (FSK)	-60
Phase Shift Keying (PSK)	-61
Pulse Code Modulation (PCM)	-62
Circuit Switching	-65
Public Switched Telephone Networks	-65
Packet Switching	-67
Simplex/Half-Duplex/Full-Duplex	-69
Unicasting/Multicasting/Broadcasting	-70
Client-Server Model	-72
Peer-to-Peer Model	-73
Network Interface Card	-75
Repeater	-78
Network Hub	-80
Bridge	-82
Network Switch	-83
Router	-85
Modem	-87
Firewall	-89
Access Point	-90
Gateway	-93
Simple topology	-95
Bus topology	-96
Ring topology	-98
Star topology	-100
Mesh topology	-101
Hybrid topologies	-103
Tree topology	-105
Internet Service Providers (ISP)	-109
Dial Up Internet	-110
DSL/ADSL Internet	-113
Network Address Translation (NAT)	-115
Proxy Servers	-116
Types of networks LAN/MAN/WAN	-119
Virtual Private Network (VPN)	-120
Networking Ports	-127
Hyper Text Transfer Protocol (HTTP)	-129
File Transfer Protocol (FTP)	-130
Domain Name System (DNS)	-132
Uniform Resource Locator (URL)	-132
Domain Name Hierarchy	-133
Dynamic Host Configuration Protocol	-135
Pure ALOHA	-137
Slotted ALOHA	-138
CSMA/CD	-139
Transmission Control Protocol (TCP)	-140
User Datagram Protocol (UDP)	-141

Introduction to Multiplexing -143
Time Division Multiplexing (TDM) -144
Frequency Division Multiplexing (FDM) -146
Wavelength division multiplexing (WDM) -147
Code division multiplexing (CDM) -149

Open Systems Interconnection (OSI) -151
Application layer -152
Presentation layer -153
Session layer -153
Transport layer -155
Network layer -156
Data link layer -156
Physical layer -157
Layer Summary -158
TCP/IP model -159
Encapsulation/Decapsulation -160
Frames -161
Packets -162
Best Effort Delivery -164
Internet Protocol (IP) -165

Confidentiality/Authentication -167
Encryption/Decryption -167
Symmetric Key Encryption -168
Asymmetric Key Encryption -168
Digital Signatures -170

Virus/Worms/Trojan Horses -174
Phishing -175
Antivirus -178

Network Addresses -179
Media Access Control Addresses (MAC) -179
Internet Protocol Addresses (IPv4) -180
Private/Public IP -181
Static/Dynamic IP -181
Internet Protocol Addresses (IPv6) -182
Classful Addressing -183
Network/Host part -183
Network/Broadcast Address -184
IP Classes A, B, C, D, E -184
Class A -184
Class B -187
Class C -188
Class D/Class E -190
Calculation Summary -191
Default Mask -192
Classless IP Addressing -193
Network Mask -194

Subnetting -195
Subnet Mask -196
VLSM/FLSM -197
Basic Questions & Answers -198
Short Questions & Answers -208

NOT IN SYLLABUS

Straight-through/Crossover cables -07
Categories of Twisted pair -08
Types of Coaxial -09
Twisted pair Vs Coaxial -10
Reflection/Refraction -11
Total Internal Refraction -12
Fiber optic types -14
Submarine cable map -16
Fiber Vs Copper -17
Introduction to Waves -18
Mechanical/Electromagnetic Waves -19
Electromagnetic Spectrum -20
Ultraviolet Rays -22
X-rays/Gamma rays -23
Period -26
Circular Motion to waves -27
Three phased/Single phased -28
Checksum -50
Cyclic Redundancy Check -51
Nyquist Theorem -62
Serial/Parallel Transmission -71
Bus-based tree topology -106
Star-based tree topology -107
Mobile Internet -110
Fiber Optic Internet -111
Satellite Internet -112
Basic Networking Commands -123
HTTPS -130
Simple Mail Transfer Protocol (SMTP) -131
Internet Message Access Protocol (IMAP) -131
Post Office Protocol (POP3) -131
Address Resolution Protocol -136
Ransomeware -175
DDoS/Botnets/MitM -175
Zero-Day Exploits/Insider Threats -176
Password Attacks/Spoofing -176
SQL injection/Vulnerabilities -177
Demilitarized Zone -214

Introduction to Networking
ජාලකරණය හැඳින්වීම

What is data communication?
දත්ත සන්නිවේදනය යනු කුමක්ද?

Data communication is the exchange of information between two or more devices/parties.
දත්ත සන්නිවේදනය යනු උපාංග / පාර්ශව දෙකක් හෝ වැඩි ගණනක් අතර තොරතුරු හුවමාරු කර ගැනීමයි.

Why Do Computers Need Communication
පරිගණකවලට සන්නිවේදනයේ අවශ්‍යතාව

A single, isolated computer can only use the resources stored inside it. Computers need to communicate with each other for the following reasons.
හුදකලා වූ තනි පරිගණකයකට භාවිත කළ හැක්කේ ඒ තුළ ගබඩා කර ඇති සම්පත් පමණි. පහත සඳහන් හේතු නිසා පරිගණක එකිනෙකා සමඟ සන්නිවේදනය කිරීමට අවශ්‍ය වේ.

Resource Sharing / සම්පත් බෙදාගැනීම
Sharing hardware resources like printers, scanners, and storage devices across multiple users, saving cost.
ප්‍රින්ටර්, ස්කෑනර් සහ ගබඩා උපාංග වැනි දෘඩාංග සම්පත් පරිශීලකයින් කිහිප දෙනෙකු අතර බෙදා ගැනීම, එමඟින් පිරිවැය ඉතිරි වේ.

Data/Information Sharing
දත්ත/තොරතුරු බෙදාගැනීම
Files, documents, and databases can be accessed and shared instantly between users in different locations.
විවිධ ස්ථානවල සිටින පරිශීලකයින් අතර ගොනු, ලේඛන සහ දත්ත සමුදායන් ක්ෂණිකව ප්‍රවේශ කිරීමට සහ බෙදා ගැනීමට හැකිය.

Remote Access & Collaboration
දුරස්ථ ප්‍රවේශය සහ එක්ව වැඩ කල හැකි වීම
Users can access another computer or server remotely (e.g., cloud storage, remote desktop) and work together on shared documents in real time.
පරිශීලකයින්ට වෙනත් පරිගණකයකට හෝ සේවාදායකයකට දුරස්ථව ප්‍රවේශ විය හැකි අතර (උදා: ක්ලවුඩ් ගබඩාව, රිමෝට් ඩෙස්ක්ටොප්) සහ හවුල් ලේඛන මත තථ්‍ය කාලීනව එකට වැඩ කළ හැකිය.

Communication Services
සන්නිවේදන සේවා
Enables email, video calls, instant messaging, and social media, connecting people across the globe.
ලොව පුරා සිටින පුද්ගලයින් සම්බන්ධ කරමින් විද්‍යුත් තැපෑල, වීඩියෝ ඇමතුම්, ක්ෂණික පණිවිඩ යැවීම සහ සමාජ මාධ්‍ය සඳහා ඉඩ සලසයි.

Centralized Data Management
මධ්‍යගත දත්ත කළමනාකරණය
Data can be stored on a central server, making it easier to back up, secure, and manage rather than keeping scattered copies on every machine.
සෑම පරිගණකයකම විසිරුණු පිටපත් තබා ගැනීමට වඩා, දත්ත මධ්‍යම සේවාදායකයක ගබඩා කළ හැකි අතර, එමඟින් ඒවා උපස්ථ කිරීම, සුරක්ෂිත කිරීම සහ කළමනාකරණය කිරීම පහසු කරයි.

Cost Reduction
පිරිවැය අඩු කිරීම
Sharing resources (like one internet connection or one printer) reduces the need to buy duplicate hardware/software for every computer.
සම්පත් බෙදාගැනීම (එක් අන්තර්ජාල සම්බන්ධතාවයක් හෝ එක් ප්‍රින්ටරයක් වැනි) සෑම පරිගණකයක් සඳහාම අනුපිටපත් දෘඩාංග/මෘදුකාංග මිලදී ගැනීමේ අවශ්‍යතාවය අඩු කරයි.

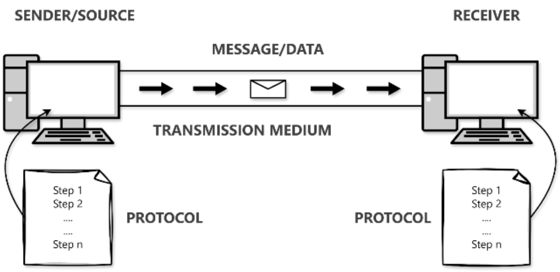
Scalability
පරිමාණය කිරීමේ හැකියාව
Networks make it easy to add new computers, users, or services as an organization grows.
සංවිධානයක් වර්ධනය වන විට නව පරිගණක, පරිශීලකයින් හෝ සේවාවන් එක් කිරීම ජාල මඟින් පහසු කරයි.

What is a Computer Network?
පරිගණක ජාලයක් යනු කුමක්ද?

A Computer Network is a collection of two or more interconnected computing devices (computers, servers, printers, mobile phones, etc.) linked together by a communication medium, allowing them to share data, resources, and services.
පරිගණක ජාලයක් යනු දත්ත, සම්පත්, සහ සේවාවන් එකිනෙකා අතර හුවමාරු කරගැනීම සඳහා සන්නිවේදන මාධ්‍යයක් මඟින් එකිනෙකට සම්බන්ධ කරන ලද පරිගණක උපාංග දෙකක් හෝ කිහිපයක (පරිගණක, සේවාදායකයන්, මුද්‍රණ යන්ත්‍ර, ජංගම දුරකථන ආදී) එකතුවකි.

Simple Example
සරල උදාහරණයක්
A home Wi-Fi setup where a laptop, smartphone, and smart TV are all connected to the same router, sharing one internet connection and able to send files to each other, is a basic computer network.
ලැප්ටොප් පරිගණකයක්, ස්මාර්ට් ජංගම දුරකථනයක් සහ ස්මාර්ට් රූපවාහිනියක් යන සියල්ලම එකම රවුටරයකට සම්බන්ධ වී, එක් අන්තර්ජාල සම්බන්ධතාවයක් බෙදා ගනිමින් එකිනෙකාට ගොනු යැවීමට හැකි නිවසේ පවතින Wi-Fi සැකසුම මූලික පරිගණක ජාලයකි.

Components of a Communication System
සන්නිවේදන පද්ධතියක ප්‍රධාන අංග



1. Sender (Source)
යවන්නා (මූලාශ්‍රය)

The device/object that originates the data is known as source.
දත්ත යැවීම සිදු කරන උපාංගය / වස්තුව මූලාශ්‍රය ලෙස හැඳින්වේ.

This could be a computer, phone tablet, sensor, or any other device or object that can create information.
මෙය පරිගණකයක්, දුරකථන ටැබ්ලටයක්, සංවේදකයක් හෝ තොරතුරු නිර්මාණය කළ හැකි වෙනත් උපාංගයක් හෝ වස්තුවක් විය හැකිය.

2. Data
දත්ත

The actual information being sent via a communication medium.
සන්නිවේදන මාධ්‍යයක් හරහා යවනු ලබන තොරතුරු වේ.

This can be text, images, audio, video, or any other format of data.
මෙය පෙළ, රූප, ශ්‍රව්‍ය, වීඩියෝ හෝ වෙනත් ඕනෑම දත්ත ආකෘතියක් විය හැකිය.

3. Receiver
ලබන්නා

The device/object that receives the data is known as receiver.
දත්ත ලබා ගන්නා උපාංගය/ වස්තුව ග්‍රාහකයා ලෙස හැඳින්වේ.

This could be another computer, phone, microphone, camera or any other device or object that can interpret information.
මෙය වෙනත් පරිගණකයක්, දුරකථනයක්, මයික්‍රෆෝනයක්, කැමරාවක් හෝ තොරතුරු අර්ථ නිරූපණය කළ හැකි වෙනත් උපාංගයක් හෝ වස්තුවක් විය හැකිය.

Human eye and ear can also be considered as receivers.
මිනිස් ඇස සහ කණ ද ග්‍රාහකයක් ලෙස සැලකිය හැකිය.

4. Protocols
නියමාවලි

The set of rules that governs how data is transmitted and received.
දත්ත සම්ප්‍රේෂණය හා ලැබෙන ආකාරය පාලනය කරන නීති මාලාව නියමලියක් නම් වේ.

Protocols ensure that devices can communicate with each other correctly and efficiently.
නියමාවලි මගින් උපාංග වලට එකිනෙකා සමඟ නිවැරදිව හා කාර්යක්ෂමව සන්නිවේදනය කළ හැකි බව සහතික කරයි

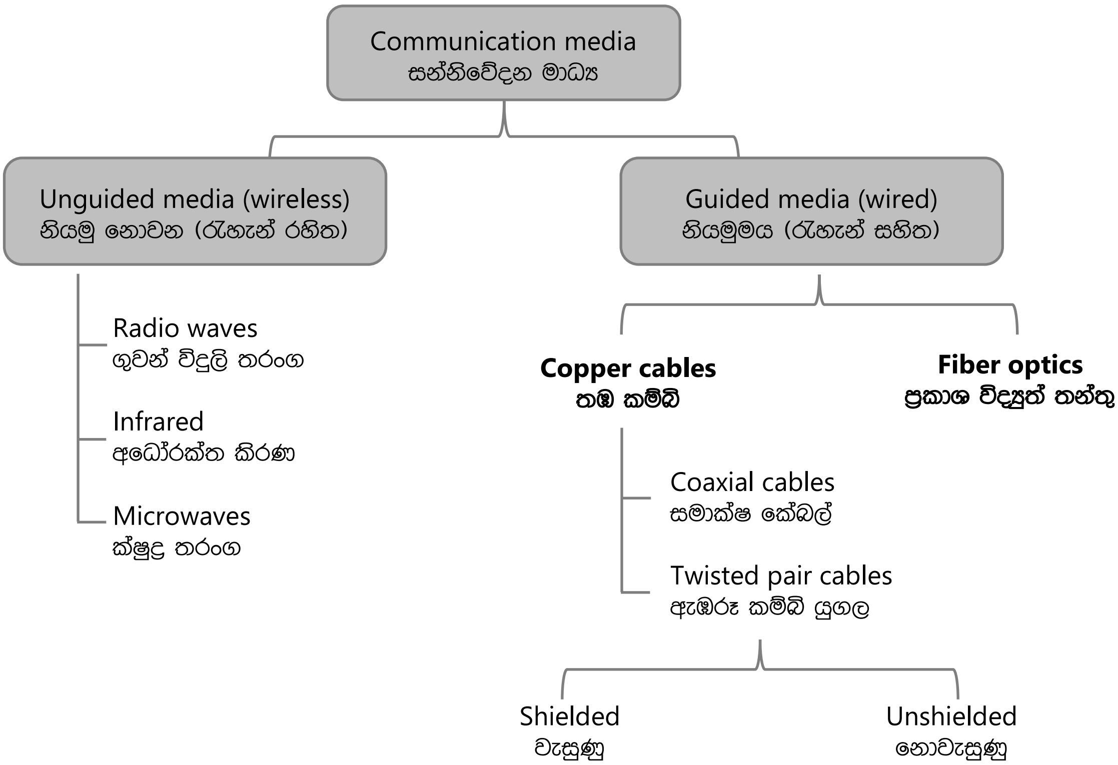
Ex. HTTP, SMTP, FTP, TCP, UDP

5. Transmission medium
සම්ප්‍රේෂණ මාධ්‍යය

The physical path over which the data travels from the source to the receiver.
දත්ත මූලාශ්‍රය සිට ග්‍රාහකයා දක්වා ගමන් කරන භෞතික මාර්ගය.

Ex. Fiber optics, Twisted pair cables, Coaxial cables

Communication media
සන්නිවේදන මාධ්‍යය



Feature	Guided Media	Unguided Media
Installation Cost ස්ථාපන පිරිවැය	Higher due to the need for physical cables and infrastructure. භෞතික කේබල් සහ යටිතල පහසුකම් සඳහා ඇති අවශ්‍යතාවය හේතුවෙන් ඉහළයි.	Lower as less physical infrastructure is required. භෞතික යටිතල පහසුකම් අවම වන බැවින් පහළය.
Mobility සංචලනය	Limited; devices need to be connected to physical cables. සීමා සහිතයි; උපාංග භෞතික කේබල් වලට සම්බන්ධ කළ යුතුය.	High; allows for wireless communication and greater flexibility. ඉහළයි; රැහැන් රහිත සන්නිවේදනය සහ වැඩි නම්‍යශීලීභාවය සඳහා ඉඩ ලබා දේ.
Bandwidth කලාප පළල	Generally high, especially with fiber optics. සාමාන්‍යයෙන් ඉහළයි, විශේෂයෙන්ම ප්‍රකාශ තන්තු සමඟ.	Varies; can be limited by interference and distance. වෙනස් වේ; බාධා කිරීම් සහ දුර ප්‍රමාණය සීමා කළ හැකිය.
Signal Range සංඥා පරාසය	Limited by cable length and type. කේබල් දිග සහ වර්ගය අනුව සීමා වේ.	Can cover large areas, especially with radio and microwave signals. විශේෂයෙන් රේඩියෝ සහ මයික්‍රෝවේව් සංඥා සමඟ විශාල ප්‍රදේශ ආවරණය කළ හැක.
Interference මැදිහත් වීම	Low; less affected by external factors. අඩුයි; බාහිර සාධක මගින් අඩු බලපෑමක් ඇති කරයි.	High; more prone to interference from environmental factors. ඉහළයි; පාරිසරික සාධක වලින් මැදිහත් වීමට වැඩි ප්‍රවණතාවක් ඇත.
Security ආරක්ෂාව	More secure as signals are confined to physical paths. සංඥා භෞතික මාර්ගවලට සීමා වී ඇති බැවින් වඩාත් ආරක්ෂිතයි.	Less secure; signals can be intercepted without direct access. අඩු ආරක්ෂිතයි; සෘජු ප්‍රවේශයකින් තොරව සංඥා වලට බාධා විය හැක.
Use Cases යෙදීම්	LANs, telephone networks, data centers. LANs, දුරකථන ජාල, දත්ත මධ්‍යස්ථාන.	Wi-Fi, cellular networks, satellite communication. Wi-Fi, සෙලියුලර් ජාල, චන්ද්‍රිකා සන්නිවේදනය.

ictfromabc.com

Unguided media
නියමු නොවන මාධ්‍යය

Unguided media, also known as wireless media, transmit signals without physical paths.
රැහැන් රහිත මාධ්‍ය ලෙසද හැඳින්වෙන නියමු නොවන මාධ්‍ය, භෞතික මාර්ග නොමැතිව සංඥා සම්ප්‍රේෂණය කරයි.

The data is sent through air, water, or space using electromagnetic waves.
විද්‍යුත් චුම්භක තරංග භාවිතයෙන් දත්ත, වාතය, ජලය හෝ අවකාශය හරහා යවනු ලැබේ.

Guided Media
නියමු මාධ්‍ය

Guided media, also known as wired media, use physical paths like cables or wires to transmit signals.
රැහැන්ගත මාධ්‍ය ලෙසද හැඳින්වෙන නියමු මාධ්‍ය, සංඥා සම්ප්‍රේෂණය කිරීමට කේබල් හෝ වයර් වැනි භෞතික මාර්ග භාවිතා කරයි.

The data travels along a specific path, controlled and confined by the medium.
දත්ත, මාධ්‍යයෙන් පාලනය වන සහ සීමා කරන ලද නිශ්චිත මාර්ගයක් ඔස්සේ ගමන් කරයි.

Copper cables
තඹ කම්බි

These are widely used in data transmission for several reasons:
තඹ කම්බි හේතු කිහිපයක් නිසා දත්ත සම්ප්‍රේෂණයේදී බහුලව භාවිතා වේ:

Mainly copper is a good electrical conductor, allowing signals to travel efficiently, reliably, and at low cost.
ප්‍රධාන වශයෙන් තඹ යනු හොඳ විද්‍යුත් සන්නායකයක් වන අතර, එමඟින් සංඥා කාර්යක්ෂමව, විශ්වසනීයව සහ අඩු පිරිවැයකින් ගමන් කිරීමට ඉඩ සලසයි.

Copper’s low electrical resistance reduces energy loss, ensuring more efficient signal transmission.
තඹවල අඩු විද්‍යුත් ප්‍රතිරෝධය බලශක්ති හානිය අඩු කරයි, වඩා කාර්යක්ෂම සංඥා සම්ප්‍රේෂණය සහතික කරයි.

Less expensive than other materials like fiber optics, making it an affordable choice for many applications.
ෆයිබර් ඔප්ටික් වැනි අනෙකුත් ද්‍රව්‍යවලට වඩා තඹ මිල අඩු වන අතර එය බොහෝ යෙදුම් සඳහා දැරිය හැකි තේරීමක් වෙයි.

More flexible, allowing easier bending and maneuvering during installation, especially in tight spaces.
වඩාත් නම්‍යශීලී වන අතර, ස්ථාපනය අතරතුර, විශේෂයෙන් තද අවකාශයන්හි පහසුවෙන් නැමීමට සහ උපාමාරු කිරීමට ඉඩ සලසයි.

Can carry both data and power (e.g., Power over Ethernet or PoE) through a single cable.
තනි කේබලයක් හරහා දත්ත සහ බලය යන දෙකම ගෙන යා හැකිය (උදා: ඊතර්නෙට් හෝ PoE).

Robust and can withstand various environmental conditions.
තඹ කේබල් ශක්තිමත් වන අතර විවිධ පාරිසරික තත්ත්වයන්ට ඔරොත්තු දිය හැකිය.

faults can be quickly identified, repaired, or replaced using simple tools and widely available materials.
සරල මෙවලම් සහ බහුලව ලබාගත හැකි ද්‍රව්‍ය භාවිතයෙන් දෝෂ ඉක්මනින් හඳුනා ගැනීමට, අලුත්වැඩියා කිරීමට හෝ ප්‍රතිස්ථාපනය කිරීමට හැකිය.

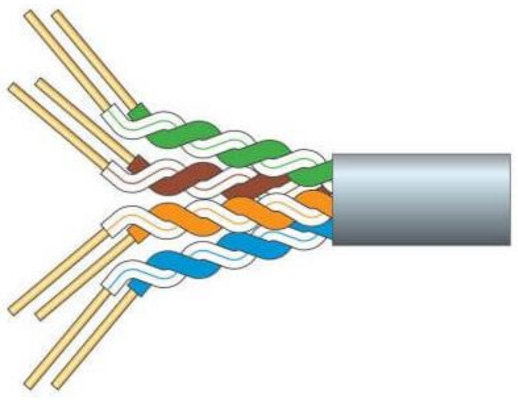
ictfromabc.com

There are two types of copper cables used in communication as a standard.
සම්මතයක් ලෙස දත්ත සන්නිවේදනය සඳහා භාවිතා කරන තඹ කේබල් වර්ග දෙකක් තිබේ

1. Twisted pair cables ඇඹරි යුගල
2. Coaxial cables සමාංශක රැහැන්

Twisted pair cables
ඇඹරි යුගල රැහැන්

The cable consists of pairs of insulated copper wires twisted together.
මෙම කේබලය සමන්විත වන්නේ එකට ඇඹරුණු පරිවරණය කරන ලද තඹ වයර් යුගල වලින්ය.



The twisting helps reduce electromagnetic interference (EMI) from external sources and crosstalk between the pairs.මෙම ඇඹරීම බාහිර මූලාශ්‍රවලින් විද්‍යුත් චුම්භක මැදිහත්වීම් (EMI) අඩු කිරීමට සහ යුගල අතර crosstalk එක අඩු කිරීමට උපකාරී වේ.

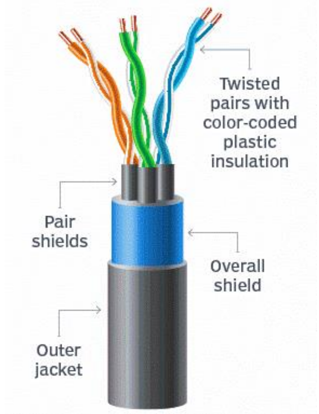
There are two types of twisted pair cables.
ඇඹරුණු යුගල කේබල් වර්ග දෙකක් තිබේ.

1. Shielded twisted pair (STP)
වැසුණු ඇඹරුණු යුගල

2. Unshielded twisted pair (UTP)
නොවැසුණු ඇඹරුණු යුගල

1. Shielded twisted pair (STP)
වැසුණු ඇඹරුණු යුගල

Shielded Twisted Pair (STP) cables include additional shielding, such as foil or a metallic braid, around the individual wire pairs or around the overall cable or around both.
වැසුණු ඇඹරුණු යුගල කේබල්වලට තනි වයර් යුගල වටා හෝ සමස්ත කේබලය වටා හෝ දෙකම වටා තීරු හෝ ලෝහමය ගෙත්තම් වැනි අමතර ආවරණ ඇතුළත් වේ.



This shielding reduces electromagnetic interference (EMI) and crosstalk.
මෙම ආවරණ මගින් විද්‍යුත් චුම්භක මැදිහත්වීම් (EMI) සහ එක අඩු කරයි.

Pair Shield

Individual shielding applied around each twisted pair of wires within the cable.
කේබලය තුළ එක් එක් ඇඹරුණු වයර් යුගල වටා තනි ආවරණයක් යොදනු ලැබේ.

Purpose is to protect the data signals in each pair from crosstalk and interference coming from other pairs within the same cable and external sources.
අරමුන වන්නේ එක් එක් යුගලයේ දත්ත සංඥා එකෙන් සහ එකම කේබලයේ සහ බාහිර ප්‍රභවයන් තුළ ඇති අනෙකුත් යුගල වලින් එන බාධා වලින් ආරක්ෂා කිරීමයි.

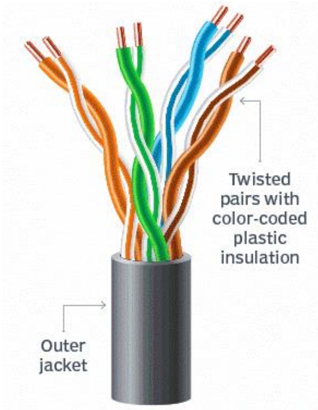
Overall Shield

Shielding that covers the entire bundle of twisted pairs within the cable.
කේබලය තුළ සම්පූර්ණ ඇඹරුණු යුගල කට්ටලය ආවරණය කරන පලිහයි.

Purpose is to provide additional protection against external electromagnetic interference (EMI) and to ensure that all the pairs are shielded from external noise.
අරමුණ වන්නේ බාහිර විද්‍යුත් චුම්භක මැදිහත්වීම් (EMI) වලට එරෙහිව අමතර ආරක්ෂාවක් සැපයීම සහ සියලුම යුගල බාහිර ඝෝෂාවෙන් ආරක්ෂා කර ඇති බව සහතික කිරීමයි.

2. Unshielded twisted pair (UTP)
නොවැසුණු ඇඹරුණු යුගල

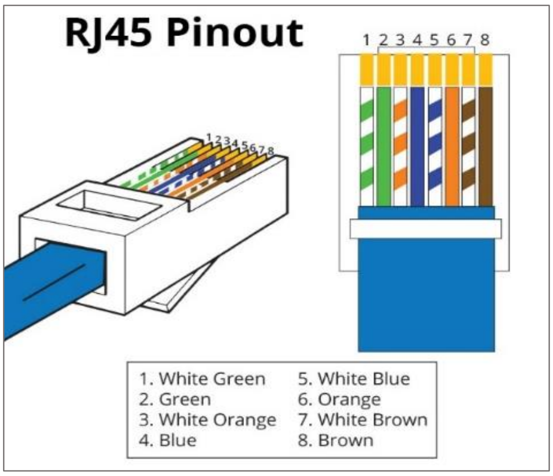
In unshielded Twisted Pair (UTP), pairs of insulated copper wires are twisted together without additional shielding.
නොවැසුණු ඇඹරුණු යුගල වලදී පරිවරණය කරන ලද තඹ වයර් යුගල අතිරේක ආවරණ නොමැතිව එකට අඹරා ඇත.



Generally cheaper and easier to install compared to shielded cables due to the absence of extra shielding layers.
අතිරේක ආවරණ ස්ථර නොමැති වීම නිසා වැසුණු කේබල් වලට සාපේක්ෂව සාමාන්‍යයෙන් ලාභදායී සහ ස්ථාපනය කිරීමට පහසුය.

Without additional shielding, UTP cables are more vulnerable to electromagnetic interference, which can impact signal quality.
අතිරේක ආවරණයක් නොමැතිව, UTP) කේබල් විද්‍යුත් චුම්භක මැදිහත්වීම් වලට වැඩි අවදානමට ලක් වේ, එය සංඥා ගුණාත්මක භාවයට බලපෑම් කළ හැකිය.

UTP cables have limitations on the distance they can effectively transmit data, especially at higher speeds.
UTP කේබල් වලට ඵලදායි ලෙස දත්ත සම්ප්‍රේෂණය කළ හැකි දුර සීමාවන් ඇත, විශේෂයෙන්ම වැඩි වේගයකින්.



Comparison (STP vs UTP)

Feature	STP	UTP
Interference සංඥා බාධා	Low අඩු	High වැඩි
Cost පිරිවැය	Higher වැඩි	Lower අඩු
Flexibility නම්‍යශීලීභාවය	Less අඩු	More වැඩි
Installation ස්ථාපනය	Harder වඩා අපහසු	Easier වඩා පහසු
Performance කාර්යසාධනය	Better වඩා හොඳ	Good හොඳ
Durability කල්පැවැත්ම	Higher වැඩි	Lower අඩු
Usage භාවිතය	Industrial කාර්මික	Common පොදු
Data Rate දත්ත හුවමාරු	Higher වේගය වැඩි	Moderate මධ්‍යස්ථ
Environment පරිසරය	Noisy ශබ්ද බහුල	Less noisy ශබ්ද අඩු

1. Orange
2. White and Orange
3. Green
4. White and Green
5. Blue
6. White/Blue
7. Brown
8. White/Brown

These colors are used for the eight individual wires within the UTP and STP cables.
යුගල වශයෙන් එකට ඇඹරී ඇති තනි රැහැන් අට සඳහා මෙම වර්ණ භාවිතා වේ.

The color-coding helps ensure consistency and accuracy when terminating the cables into connectors or sockets.
සම්බන්ධක හෝ සොකට් ලෙස අවසන් කිරීමේදී වර්ණ-කේතනය එක් එක් රැහැන හඳුනාගැනීමට සහ නිරවද්‍යතාවය සහතික කිරීමට උපකාරී වේ.

Twisted pair cables use various types of connectors or sockets to establish connections.
ඇඹරුණු යුගල කේබල් සම්බන්ධතා ස්ථාපනය කිරීම සඳහා විවිධ ආකාරයේ සම්බන්ධක හෝ කෙවෙනි භාවිතා කරයි.

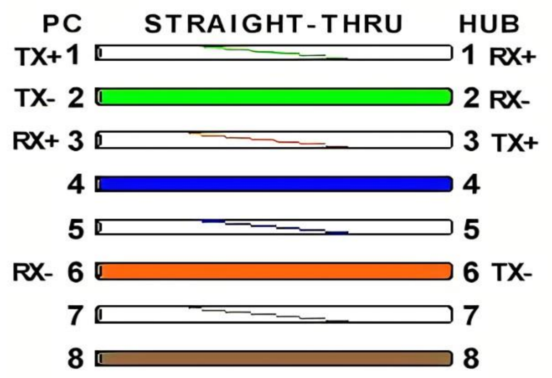
Note: (Legacy)

Straight-through and Crossover Cables

They differ in how the wires within the cable are connected to the connectors at each end.
කේබලය තුළ ඇති වයර් එක් එක් කෙළවරේ සම්බන්ධකවලට සම්බන්ධ වන ආකාරය අනුව ඒවා වෙනස් වේ.

Straight-through cables

In a straight-through cable, the wiring configuration at one end of the cable is identical to the wiring configuration at the other end.
Straight-through කේබල් එකක, කේබලයේ එක් කෙළවරක රැහැන් වින්‍යාසය අනෙක් කෙළවරේ රැහැන් වින්‍යාසයට සමාන වේ.



Used to connect different types of devices.
විවිධ වර්ගයේ උපාංග සම්බන්ධ කිරීමට භාවිතා කරයි.

Computer to switch
Router to switch
Computer to router

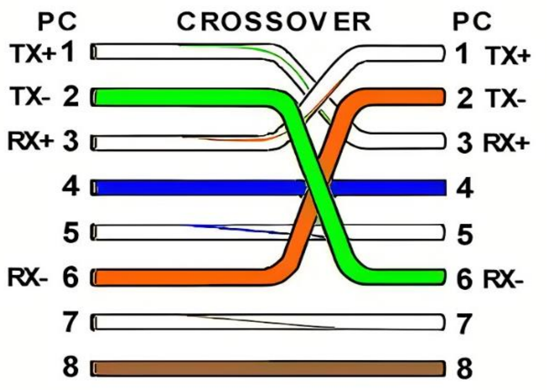
The most common use of straight-through cables is to connect a computer or network device to a network switch or router.
Straight-through කේබල් වල වඩාත් සුලභ භාවිතය වන්නේ පරිගණකයක් හෝ ජාල උපාංගයක් ජාල ස්විචයකට හෝ රවුටරයකට සම්බන්ධ කිරීමේදීය.

It is used to connect devices that operate on different layers of the OSI model (like a computer nd a switch).
OSI ආකෘතියේ විවිධ ස්ථරවල (පරිගණකයක් සහ ස්විචයක් වැනි) ක්‍රියා කරන උපාංග සම්බන්ධ කිරීමට එය භාවිතා කරයි.

For example, a switch receives data on the pins where a computer transmits.
උදාහරණයක් ලෙස, ස්විචයක් මගින් පරිගණකයක් විසින් සම්ප්‍රේෂණය කරීමට භාවිතා කරන පින් එකෙන් දත්ත ග්‍රහණය ගනී.

Crossover cables

The wiring sequence is different at each end.
එක් එක් කෙළවරේ රැහැන් අනුපිළිවෙල වෙනස් වේ.



Specifically, the transmit (TX) pins at one end are connected to the receive (RX) pins at the other end, and vice versa.
විශේෂයෙන්, එක් කෙළවරක සම්ප්‍රේෂණ (TX) පින් අනෙක් කෙළවරේ ග්‍රාහක (RX) පින් වලට සම්බන්ධ වන අතර එය ප්‍රතිවිරුද්ධ අතටද සිදුවේ.

Used to connect similar types of devices directly.
සමාන ආකාරයේ උපාංග සෘජුවම සම්බන්ධ කිරීමට භාවිතා කරයි.

Computer to computer
Switch to switch
Router to router

The crossover cable swaps the transmit and receive pins, allowing the devices to communicate directly.
Crossover කේබලය මගින් සම්ප්‍රේෂණ සහ ග්‍රාහක අග්‍ර මාරු කරමින් උපාංගවලට සෘජුවම සන්නිවේදනය කිරීමට ඉඩ සලසයි.

For example, it switches the Tx pins of one device to the Rx pins of the other device.
උදාහරණයක් ලෙස, එමගින් එක් උපාංගයක Tx අග්‍රය අනෙක් උපාංගයේ Rx අග්‍රය වෙත මාරු කරයි.

NOTE:

Very old switches and hubs may need them
ඉතා පැරණි හබ් සහ ස්විච් සඳහා මේවා අවශ්‍ය විය හැක

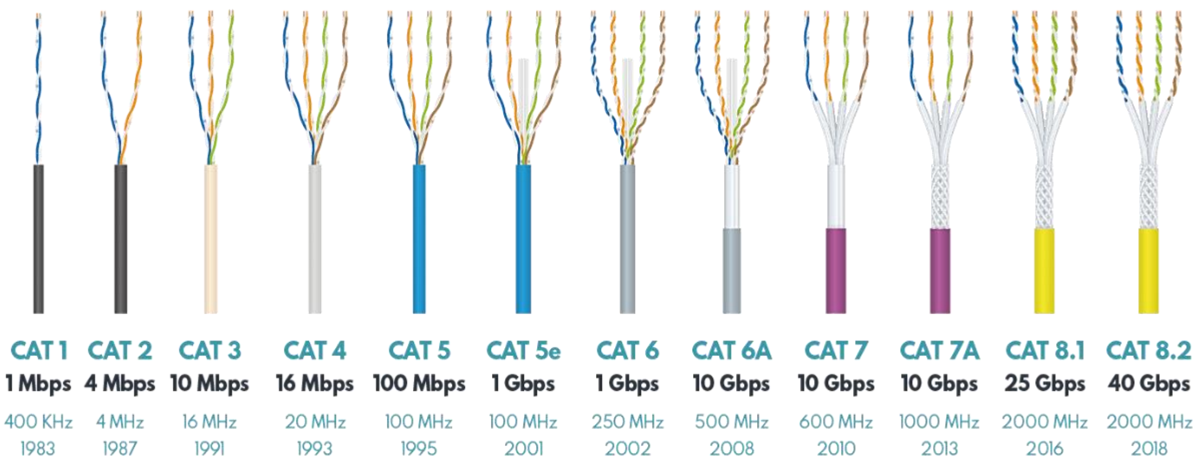
Good for troubleshooting old networks
පැරණි ජාලයන්හි දෝෂ සෙවීම සඳහා සුදුසු වීම

Taught and used in some networking labs and certification exams
සමහර ජාලකරණ විද්‍යාගාර සහ සහතික කිරීමේ විභාග

Twisted pair cables are categorized based on their performance characteristics, primarily their bandwidth and frequency response. ඇඹරි යුගල කේබල් ඒවායේ කාර්ය සාධන ලක්ෂණ, මූලික වශයෙන් ඒවායේ කලාප පළල සහ සංඛ්‍යාත ප්‍රතිචාරය මත පදනම්ව වර්ගීකරණය කර ඇත.

NOTE:
The higher the category number, the greater the bandwidth and frequency response of the cable.
කාණ්ඩ අංකය වැඩි වන තරමට කේබලයේ කලාප පළල සහ සංඛ්‍යාත ප්‍රතිචාරය වැඩි වේ.

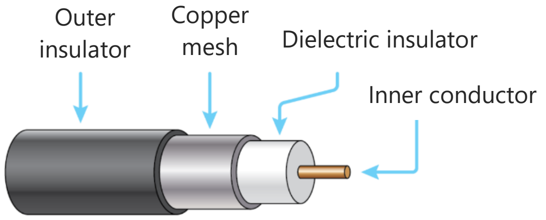
Category **කාණ්ඩය**	**Bandwidth** **කලාප පළල**	**Uses** **භාවිතයන්**
Cat 1	Less than 1 Mbps	Primarily for telephone lines ප්‍රධාන වශයෙන් දුරකථන රැහැන් සඳහා
Cat 2	4 Mbps	Early Ethernet networks මුල්කාලීන Ethernet ජාල සඳහා
Cat 3	10 Mbps	Ethernet networks, mainly 10BASE-T Ethernet ජාල සඳහා, ප්‍රධාන වශයෙන් 10BASE-T තාක්ෂණය
Cat 4	16 Mbps	Token Ring networks Token Ring ජාල සඳහා
Cat 5	100 Mbps	Ethernet networks, mainly 100BASE-TX Ethernet ජාල සඳහා, ප්‍රධාන වශයෙන් 100BASE-TX තාක්ෂණය
Cat 5e	1000 Mbps	Modern Ethernet networks / Gigabit Ethernet නවීන Ethernet ජාල / ගිගාබිට් Ethernet සඳහා
Cat 6	1000 Mbps	Higher-performance networks, especially for longer distances ඉහළ කාර්යසාධනයක් සහිත ජාල, දිගු දුර සන්නිවේදනය සඳහා
Cat 6A	10,000 Mbps	High-speed data centers and demanding applications අධිවේගී දත්ත මධ්‍යස්ථාන සහ ඉහළ ධාරිතාවක් අවශ්‍ය වන යෙදුම් සඳහා
Cat 7	10,000 Mbps	Data centers and high-performance environments දත්ත මධ්‍යස්ථාන සහ ඉහළ කාර්යසාධනයක් සහිත පරිසරයන් සඳහා
Cat 8	25,000 Mbps and 40,000 Mbps	High-speed data centers and demanding applications අධිවේගී දත්ත මධ්‍යස්ථාන සහ ඉහළ ධාරිතාවක් අවශ්‍ය වන යෙදුම් සඳහා



Coaxial cables
සමාංශක රැහැන්

Coaxial cables are a type of electrical cable used for transmitting data, video, and radio frequency signals.
සමාංශක රැහැන් යනු දත්ත, වීඩියෝ සහ රේඩියෝ සංඛ්‍යාත සංඥා සම්ප්‍රේෂණය කිරීම සඳහා භාවිතා කරන විද්‍යුත් කේබල් වර්ගයකි.

They consist of four layers: a central conductor, an insulating layer (Dielectric insulator), a metallic shield (Copper mesh), and an outer insulating jacket.
ඒවා ස්ථර හතරකින් සමන්විත වේ: එනම් මධ්‍ය සන්නායකයක්, පරිවාරක ස්ථරයක්, ලෝහමය පලිහක් (Copper mesh) සහ පිටත පරිවාරක ජැකට්ටුවක් වශයෙනි.



Inner Conductor
The core wire (usually copper) that carries the data signals.
දත්ත සංඥා රැගෙන යන මූලික වයරය (සාමාන්‍යයෙන් තඹ).

Dielectric insulator
Surrounds the inner conductor to separate it from the outer layers.
පිටත ස්ථර වලින් වෙන් කිරීම සඳහා අභ්‍යන්තර සන්නායකය වට කරයි.

Metallic Shield (Copper mesh)
A woven copper or aluminum braid that blocks external electromagnetic interference (EMI).
බාහිර විද්‍යුත් චුම්භක බාධා කිරීම් ((ඊඑම්)) අවහිර කරන වියන ලද තඹ හෝ ඇලුමිනියම් වියනකි.

Outer Jacket
The final protective layer, typically made of plastic, which encases the entire cable.
අවසාන ආරක්ෂිත තට්ටුවයි, සමාන්‍යයෙන් ප්ලාස්ටික් වලින් සාදා ඇති අතර, එය සම්පූර්ණ කේබලයම ආවරණය කරයි.

Types of Coaxial Cables

RG-6: Commonly used for cable television, satellite connections, and internet.

RG-59: Used for older analog video and CCTV systems.

RG-11: Used for long-distance connections due to its thicker conductor.

Coaxial cables are versatile and have been used in various applications due to their ability to transmit high-frequency signals with low interference.
සමාංශක රැහැන් බහුකාර්ය වන අතර අඩු මැදිහත්වීම් සහිත අධි-සංඛ්‍යාත සංඥා සම්ප්‍රේෂණය කිරීමේ හැකියාව හේතුවෙන් විවිධ යෙදුම්වල භාවිතා කර ඇත.

Applications of Coaxial Cables
සමාංශක රැහැන්වල භාවිතයන්

1. Ethernet Networking (Older Systems)
Before twisted pair cables became the standard, coaxial cables were used in LANs to connect computers and networking devices.
ඇඹරි යුගල කේබල් සම්මත වීමට පෙර, පරිගණක සහ ජාල උපාංග සම්බන්ධ කිරීම සඳහා LAN වල සමාංශක රැහැන් භාවිතා කරන ලදී.

2. Internet and Broadband Connections

In the past, internet Service Providers (ISPs) used coaxial cables to deliver broadband internet to customers.
අතීතයේදී, අන්තර්ජාල සේවා සපයන්නන් (ISPs) පාරිභෝගිකයින්ට බ්‍රෝඩ්බෑන්ඩ් අන්තර්ජාලය ලබා දීමට සමාංශක රැහැන් භාවිතා කළේය.

3. Cable Television (CATV)

Coaxial cables are widely used by cable television companies to deliver TV signals to homes and businesses.
නිවෙස් සහ ව්‍යාපාර වෙත රූපවාහිනී සංඥා ලබා දීම සඳහා කේබල් රූපවාහිනී සමාගම් විසින් සමාංශක රැහැන් බහුලව භාවිතා කරයි.

4. CCTV and Video Surveillance
Coaxial cables are commonly used in Closed-Circuit Television (CCTV) systems for transmitting video signals.
වීඩියෝ සංඥා සම්ප්‍රේෂණය කිරීම සඳහා සංවෘත පරිපථ රූපවාහිනී (CCTV) පද්ධතිවල සමාංශක රැහැන් බහුලව භාවිතා වේ.

5. Telephone Networks
Historically, coaxial cables were used for long-distance telephone connections, especially in trunk lines.
සමාංශක රැහැන් දිගු දුර දුරකථන සම්බන්ධතා සඳහා, විශේෂයෙන් trunk lines වල භාවිතා කරන ලදී.

6. Radio Frequency (RF) Transmission
Coaxial cables are used in radio transmitters, receivers, and antenna systems.
රේඩියෝ සම්ප්‍රේෂක, ග්‍රාහක සහ ඇන්ටෙනා පද්ධතිවල සමාංශක රැහැන් භාවිතා වේ.

Twisted pair cables vs. Coaxial cables

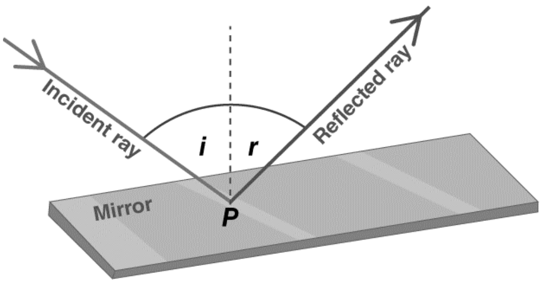
Feature	**Twisted Pair Cable**	**Coaxial Cable**
Structure ව්‍යුහය	Two twisted copper wires ඇඹරුණු තඹ රැහැන් දෙකකි	Single copper core with shielding ආවරණ සහිත තනි තඹ හරයකි
Shielding පලිහ	Minimal (STP) or None (UTP) අවම (STP) හෝ කිසිවක් නැත (UTP)	Metallic braid and foil shielding ලෝහමය දැලක් සහ තීරු ආවරණ
Interference මැදිහත්වීම්	Moderate (in STP) මධ්‍යස්ථයි (STP වලින්)	Low due to effective shielding ඵලදායී පලිහක් හේතුවෙන් පහළයි
Bandwidth කලාප පළල	Suitable for moderate speeds මධ්‍යස්ථ වේගයන් සඳහා සුදුසු වේ	Higher speeds and frequencies ඉහළ වේගයන් සහ සංඛ්‍යාත
Cost පිරිවැය	Generally low and affordable සමාන්‍යයෙන් අඩු සහ දැරිය හැකි මිලකි	Higher due to more materials වැඩි අමුද්‍රව්‍ය නිසා ඉහළයි
Flexibility නම්‍යශීලී බව	Highly flexible and easy to bend ඉතා නම්‍යශීලී සහ නැමීමට පහසුය	Less flexible, slightly rigid අඩු නම්‍යශීලීය, තරමක් දෘඪයි
Installation ස්ථාපනය	Easy to install and handle ස්ථාපනය සහ හැසිරවීමට පහසුය	Slightly complex due to rigidity දෘඪතාව නිසා තරමක් සංකීර්ණයි
Distance දුර	Effective over short distances කෙටි දුර සඳහා ඵලදායී වේ	Effective over longer distances දිගු දුරක් සඳහා ඵලදායී වේ
Applications යෙදුම්	LAN, telephones, basic networking LAN, දුරකථන, මූලික ජාලකරණය	Cable TV, broadband, CCTV
Noise Resistance ශබ්ද ප්‍රතිරෝධය	Lower, susceptible to noise අඩුය, ඝෝෂාවට ගොදුරු වේ	High resistance to noise and EMI ඝෝෂාව සහ (EMI) වලට ඉහළ ප්‍රතිරෝධයක්

Fiber optics cables
ප්‍රකාශ විද්‍යුත් තන්තු

Fundamentals
මූලික කරුණු

Reflection
පරාවර්තනය
When a ray of light approaches a smooth polished surface and the light ray bounces back, it is called the reflection of light.
ආලෝක කිරණ සුමට ඔප දැමූ මතුපිටක් වෙත ළඟා වී ආපසු bounce වී පැමිණෙන විට එය ආලෝකයේ පරාවර්තනය ලෙස හැඳින්වේ.

Laws of reflection
පරාවර්තන නීති
- The incident ray and the reflected ray lie in the same plane.
  පතන කිරණය සහ පරාවර්තිත කිරණය එකම තලයක පවතී.
- The angle of incidence is equal to the angle of reflection
  පතන කෝණය පරාවර්තිත කෝණයට සමාන වේ



Here, i = r

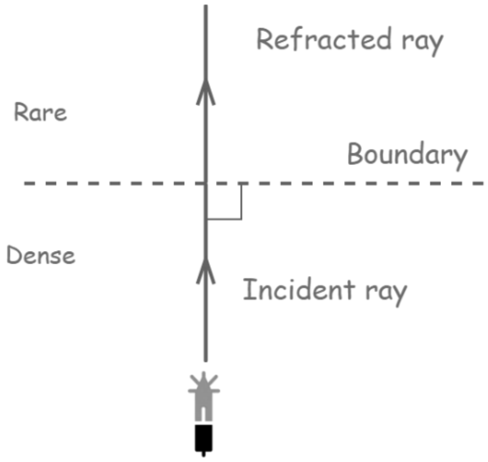
Refraction
වර්තනය
Refraction is the change in direction of a wave when passing from one medium to another caused by its change in speed.
වර්තනය යනු තරංගයක වේගය වෙනස් වීම නිසා එක් මාධ්‍යයක සිට තවත් මාධ්‍යයකට ගමන් කරන විට එහි දිශාව වෙනස් වීමයි.

Rare Media
විරල මාධ්‍ය
A medium in which light (or any other wave) travels faster compared to a denser medium.
ගහන මාධ්‍යයකට සාපේක්ෂව ආලෝකය (හෝ වෙනත් ඕනෑම තරංගයක්) වඩා වේගයෙන් ගමන් කරන මාධ්‍යයකි.

Dense Media
ගහන මාධ්‍ය
A medium in which light (or any other wave) travels slower compared to a rarer medium.
විරල මාධ්‍යයකට සාපේක්ෂව ආලෝකය (හෝ වෙනත් ඕනෑම තරංගයක්) මන්දගාමීව ගමන් කරන මාධ්‍යයකි.

Laws of Refraction
වර්තන නීති
- The angle of incidence, the tangent to the boundary at the point of incidence, and the refracted ray lie in the same plane.
  පතන කෝණයත්, පතන ලක්ෂ්‍යයේ මායිමට ඇඳි අභිලම්බයත්, වර්තන කිරණයත් එකම තලයක පිහිටයි
- The ratio of the sine of the angle of incidence to the sine of the angle of refraction is constant for two considered media.
  සලකන මාධ්‍ය දෙකක් සඳහා පතන කෝණයේ සයින් අගයට වර්තන කෝණයේ සයින් අගය දක්වන අනුපාතය නියත වේ.

1. First instance

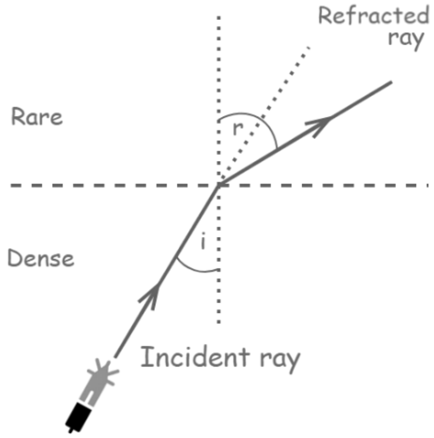


Incident Angle: 0° (perpendicular to the boundary).

Behavior: When light strikes the boundary perpendicularly, it passes straight through without changing direction.
ආලෝකය මායිමට ලම්බකව පතිත වන විට, එය දිශාව වෙනස් නොකර කෙලින්ම ගමන් කරයි.

Explanation: Since the light is not at an angle, it doesn't bend; it simply slows down because it's moving from a dense to a rare medium.
ආලෝක කිරණය කෝණයකින් නොමැති බැවින්, එය නැමෙන්නේ නැත; එය ගහන මාධ්‍යයෙන් විරල මාධ්‍යයකට ගමන් කරන නිසා සරලව එහි වේගය අඩු වී මන්දගාමී වේ.

2. Second instance



i - Incident angle (i > 0 < C)

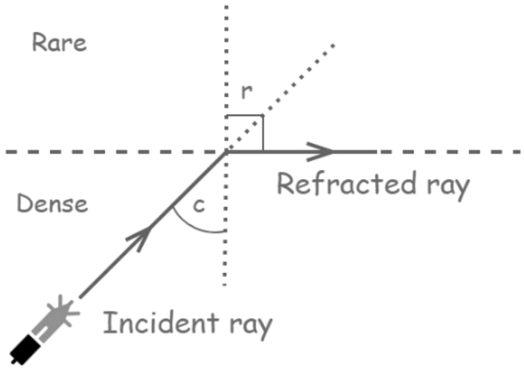
r - Refracted angle

Incident Angle: Less than the critical angle (but not 0°).
පතන කෝණය අවධි කෝණයට වඩා අඩුය (නමුත් 0° නොවේ).

Explanation: When the light enters the rare medium at an angle, it speeds up, causing the ray to bend away from the normal (the imaginary line perpendicular to the boundary).
ආලෝකය කෝණයකින් විරල මාධ්‍යයට ඇතුළු වූ විට, එය වේගවත් වන අතර, කිරණ අභිලම්බයේ (මායිමට ලම්බක වූ මනඃකල්පිත රේඛාව) සිට නැමීමට හේතු වේ.

This bending is refraction. The greater the angle of incidence (up to the critical angle), the more the light will bend away from the normal.
මෙම නැමීම වර්තනයකි. පතන කෝණය වැඩි වන තරමට (අවධි කෝණය දක්වා), ආලෝකය අභිලම්බයෙන් ඉවතට නැමෙන ප්‍රමාණය වැඩි වේ.

3. Third instance



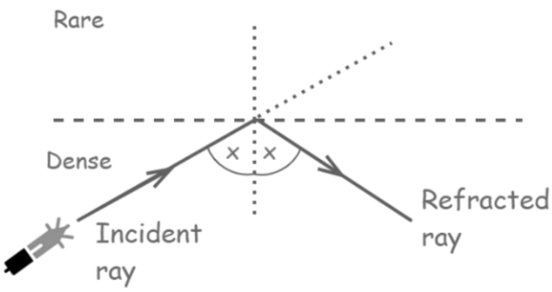
c - Critical angle

Incident Angle: Equal to the critical angle.
පතන කෝණය අවධි කෝණයට සමාන වේ.

Explanation: The critical angle is the angle of incidence at which the refracted ray just skims the boundary between the two media.
අවධි කෝණය යනු වර්තන කිරණ මාධ්‍ය දෙක අතර මායිම මතින් ගමන් කරන පතන කෝණයයි.

At this angle, the light does not enter the rarer medium; instead, it moves along the interface between the two media.
මෙම කෝණයෙන් ආලෝකය විරල මාධ්‍යයට ඇතුල් නොවේ; ඒ වෙනුවට, එය මාධ්‍ය දෙක අතර අතුරු මුහුණත ඔස්සේ ගමන් කරයි.

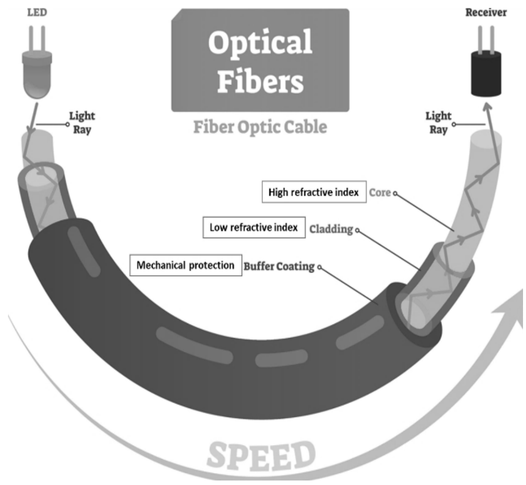
4. Fourth instance



Incident Angle: Greater than the critical angle.
පතන කෝණය අවධි කෝණයට වඩා විශාලය.

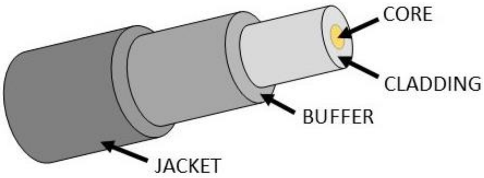
Explanation: When the angle of incidence exceeds the critical angle, the light cannot pass into the rarer medium. Instead, it is entirely reflected back into the denser medium.
පතන කෝණයා අවධි කෝණය ඉක්මවා ගිය විට, ආලෝකයට විරල මාධ්‍යයට ගමන් කළ නොහැක. ඒ වෙනුවට, එය සම්පූර්ණයෙන්ම ඝනන මාධ්‍යයට නැවත පරාවර්තනය වේ.

This phenomenon is known as **total internal reflection**.
මෙම සංසිද්ධිය පූර්ණ අභ්‍යන්තර පරාවර්තනය ලෙස හැඳින්වේ



Fiber optic cables
ප්‍රකාශ තන්තු රැහැන්

Fiber optic cables use thin strands of glass or plastic fibers to transmit data as light pulses.
ප්‍රකාශ තන්තු මගින් ආලෝක ස්පන්දන ලෙස දත්ත සම්ප්‍රේෂණය කිරීමට තුනී වීදුරු හෝ ප්ලාස්ටික් තන්තු භාවිතා කරයි.



Core
The core is the central part of the optical fiber where light is transmitted.
Core එක යනු ආලෝකය සම්ප්‍රේෂණය වන ප්‍රකාශ තන්තු වල මධ්‍යම කොටසයි.

It is usually made of high-purity glass or plastic.
එය සමාන්‍යයෙන් ඉහළ පිරිසිදු වීදුරු හෝ ප්ලාස්ටික් වලින් සාදා ඇත.

The size of the core determines how the light travels and the amount of data that can be transmitted.
Core එකෙහි ප්‍රමාණය ආලෝකය ගමන් කරන ආකාරය සහ සම්ප්‍රේෂණය කළ හැකි දත්ත ප්‍රමාණය තීරණය කරයි.

Cladding

The cladding is the layer that surrounds the core of the optical fiber.
Cladding එක යනු ප්‍රකාශ තන්තු වල core එක වටා ඇති ස්ථරයයි.

It is also made of glass or plastic, but with a lower refractive index than the core.
එය ද වීදුරු හෝ ප්ලාස්ටික් වලින් සාදා ඇත, නමුත් core එකට වඩා අඩු වර්තන දර්ශකයක් ඇත.

The cladding’s primary role is to reflect light back into the core using **total internal reflection**.
Cladding එකෙහි මූලික කාර්යභාරය වනුයේ පූර්ණ අභ්‍යන්තර පරාවර්තනය භාවිතා කර නැවත core එකට ආලෝකය පරාවර්තනය කිරීමයි.

How fiber optics work
ප්‍රකාශ තන්තු ක්‍රියා කරන ආකාරය

The process begins with an electrical signal that needs to be transmitted.
මෙම ක්‍රියාවලිය සම්ප්රේෂණය කළ යුතු විද්‍යුත් සංඥාවකින් ආරම්භ වේ.

The electrical signal is sent to an optical transmitter, which contains a light source, typically a laser diode or a light-emitting diode (LED).
විද්‍යුත් සංඥාව ආලෝක ප්‍රභවයකට, සාමාන්‍යයෙන් ලේසර් ඩයෝඩයක් හෝ ආලෝක විමෝචක ඩයෝඩයක් LED අඩංගු දෘශ්‍ය සම්ප්‍රේෂකයකට යවනු ලැබේ.

The transmitter converts the electrical signals into light pulses.
සම්ප්‍රේෂකය විදුලි සංඥා ආලෝක ස්පන්දන බවට පරිවර්තනය කරයි.

The light pulses are modulated to represent the binary data (0s and 1s) of the electrical signal.
විදුලි සංඥාවේ ද්විමය දත්ත (0 සහ 1) නියෝජනය කිරීම සඳහා ආලෝක ස්පන්දන මුහුර්ජණය කර ඇත.

A light pulse might represent a 1, and the absence of a pulse might represent a 0.
ආලෝක ස්පන්දනයක් 1 නියෝජනය කළ හැකි අතර ස්පන්දනයක් නොමැති වීම 0 නියෝජනය කළ හැකිය.

The light pulses are transmitted through the core of the optical fiber
ආලෝක ස්පන්දන ප්‍රකාශ තන්තු හරය හරහා සම්ප්‍රේෂණය වේ

Over long distances, the light signal may weaken due to attenuation.
දිගු දුර වලදී, attenuation හේතුවෙන් ආලෝක සංඥාව දුර්වල විය හැක.

To maintain signal strength, optical amplifiers are placed at intervals along the fiber.
සංඥාවේ ශක්තිය පවත්වා ගැනීම සඳහා, ප්‍රකාශ වර්ධක තන්තු දිගේ පරතරයන්ගෙන් තබා ඇත.

At the receiving end, the light pulses reach an optical receiver.
ග්‍රහන අන්තයේදී, ආලෝක ස්පන්දන ප්‍රකාශ ග්‍රාහකය වෙත ළඟා වේ.

This device contains a photodetector, typically a photodiode, which converts the light pulses back into electrical signals.
මෙම උපාංගයේ photodetector එකක් අඩංගු වේ, සාමාන්‍යයෙන් එය ප්‍රකාශ දියෝඩයක් වන අතර එමඟින් ආලෝක ස්පන්දන නැවත විද්‍යුත් සංඥා බවට පරිවර්තනය කරයි.

The electrical signals are then processed and converted back into the original data format.
එවිට විද්‍යුත් සංඥා සකස් කර නැවත මුල් දත්ත ආකෘතියට පරිවර්තනය වේ.

ictfromabc.com

Types of fiber optics
ෆයිබර් ඔප්ටික් වර්ග

Fiber Optic Technology

- **Optical Fiber**
  - Single-mode Fiber(SMF)
  - Multi-mode Fiber(MMF)
- **Fiber Optic Cable**
  - Indoor Cables
  - Outdoor Cables
  - Special Purpose Cables

Optical Fiber (Glass fiber)

A thin, flexible strand of glass that transmits data as pulses of light.
දත්ත ආලෝක ස්පන්ද ලෙස සම්ප්‍රේෂණය කරන වීදුරුවලින් තැනූ තුනී, නැමිය හැකි තන්තුවකි.

Optical fibers are classified into two main types based on the number of light paths (modes) they support.
ඔප්ටිකල් ෆයිබර් ඒවා මගින් ආධාර කරන ආලෝක පථ ගණන මත පදනම්ව ප්‍රධාන වර්ග දෙකකට වර්ගීකරණය කෙරේ.

1.Single-mode Fiber (SMF) / තනි ප්‍රකාශ තන්තු

It allows only one light path (mode) to travel through the fiber, reducing signal distortion and attenuation.
සංඥා විකෘති වීම සහ හායනය අවම කරමින්, තන්තුව හරහා ගමන් කිරීමට ඉඩ සලසන්නේ එක් ආලෝක පථයකට පමණි.

Used for long-distance communication.
දිගු දුර සන්නිවේදනය සඳහා භාවිත වේ.

Provides high bandwidth with low signal loss.
අඩු සංඥා හානියක් සමඟ ඉහළ කලාප පළලක් සපයයි.

Commonly uses Laser Diodes (LD)
සාමාන්‍යයෙන් ලේසර් ඩයෝඩ භාවිත කරයි.

Core Diameter :8–10 μm (Typically 9 μm)
මධ්‍යයෙහි විෂ්කම්භය :8–10 μm(සාමාන්‍යයෙන් 9μm)

Cladding Diameter : 125 μm.
වැස්මෙහි විෂ්කම්භය : 125 μm

2. Multi-mode Fiber (MMF) / බහු ප්‍රකාශ තන්තු

It allows multiple light paths (modes) to travel through the fiber simultaneously.
එකවර ආලෝක පථ කිහිපයකට තන්තුව හරහා ගමන් කිරීමට ඉඩ සලසයි.

Used for short-distance communication.
කෙටි දුර සන්නිවේදනය සඳහා භාවිත වේ.

Lower bandwidth than SMF.
SMF වලට වඩා අඩු කලාප පළලක් ඇත.

Commonly uses LEDs as the light source.
සාමාන්‍යයෙන් ආලෝක ප්‍රභවය ලෙස LED භාවිත කරයි.

Core Diameter : 50 μm or 62.5 μm
මධ්‍යයෙහි විෂ්කම්භය : 50 μm හෝ 62.5 μm

Cladding Diameter : 125 μm
වැස්මෙහි විෂ්කම්භය : 125 μm

Fiber Optic Cables

A protective cable assembly that contains one or more optical fibers used to transmit data.
දත්ත සම්ප්‍රේෂණය සඳහා භාවිත කරන, ඔප්ටිකල් ෆයිබර් එකක් හෝ කිහිපයක් අඩංගු ආරක්ෂිත කේබල් පද්ධතියකි.

Fiber optic cables are classified according to their installation environment and application.
ෆයිබර් ඔප්ටික් කේබල් ඒවා ස්ථාපනය කරන පරිසරය සහ යෙදවුම් අනුව වර්ගීකරණය කෙරේ.

1.Indoor Cable
Designed for use inside buildings where they are protected from harsh environmental conditions.
දරුණු පාරිසරික තත්ත්වයන්ගෙන් ආරක්ෂා වී ඇති ගොඩනැගිලි තුළ භාවිතය සඳහා නිර්මාණය කර ඇත.

Types / වර්ග:

- **Simplex** -One fiber for one-way communication.
  එක් දිශාවකට පමණක් සිදු කෙරෙන සන්නිවේදනය සඳහා එක් ෆයිබර් තන්තුවක් පවතින කේබල්.
- **Duplex** – Two fibers for simultaneous two-way communication.
  එකවර දෙදිශාවටම සිදු කෙරෙන සන්නිවේදනය සඳහා ෆයිබර් තන්තු දෙකක් පවතින කේබල්.
- **Distribution** – Multiple fibers bundled for indoor installations.
  ගොඩනැගිලි අභ්‍යන්තර ස්ථාපනයන් සඳහා ෆයිබර් තන්තු කිහිපයක් එකට මිටි කර ඇති කේබල්.
- **Breakout** – Each fiber is individually protected for direct connection.
  සෘජු සන්නිවේදන සම්බන්ධතා ලබා දීම සඳහා සෑම ෆයිබර් තන්තුවක්ම වෙන් වෙන් වශයෙන් ආරක්ෂා කර ඇති කේබල්.

2. Outdoor Cables

Designed to withstand moisture, temperature changes, and physical stress.
තෙතමනය, උෂ්ණත්ව වෙනස්වීම් සහ භෞතික බලපෑම්වලට ඔරොත්තු දෙන පරිදි නිර්මාණය කර ඇත.

Types / වර්ග:

- **Loose-tube** – Protects fibers from moisture and temperature changes.
  තෙතමනය සහ උෂ්ණත්ව වෙනස්වීම්වලින් තන්තු ආරක්ෂා කරයි.
- **Tight-buffered** – Fibers are tightly coated for easier handling.
  පහසුවෙන් හැසිරවීම සඳහා තන්තු තදින් ආවරණය කර ඇත.
- **Armored** – Includes a protective metal layer for harsh environments.
  රළු පරිසරයන් සඳහා ලෝහමය ආරක්ෂිත ස්ථරයක් අඩංගු වේ.

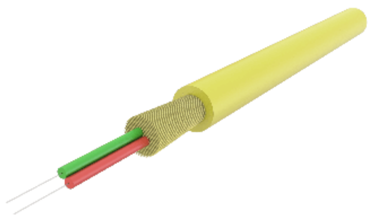
3. Special-purpose Cables

Designed for specific installation environments and specialized applications.
විශේෂිත ස්ථාපන පරිසරයන් සහ සුවිශේෂී යෙදවුම් සඳහා නිර්මාණය කර ඇත.

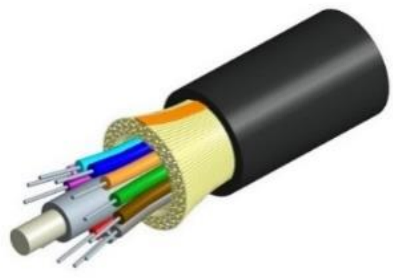
Types / වර්ග:

- **Submarine Cable** – Used for undersea communication.
  මුහුදු පතුල හරහා සිදුකෙරෙන සන්නිවේදනය සඳහා භාවිත වේ.
- **Aerial Cable** – Suspended between utility poles.
  විදුලි පණිවුඩ හෝ උපයෝගිතා කණුවල එල්ලා තබනු ලබයි.
- **Direct-burial Cable** – Installed directly underground.
  සෘජුවම පොළොව යට වළලනු ලබයි.
- **ADSS** – Installed on power lines without requiring a metal support wire.
  ලෝහමය ආධාරක රැහැනක් අවශ්‍ය නොවන පරිදි, විදුලි රැහැන් මත ස්ථාපනය කරනු ලබයි.

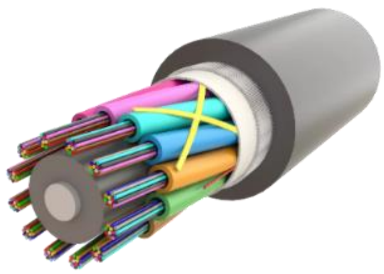
Indoor Simplex/Duplex Fiber



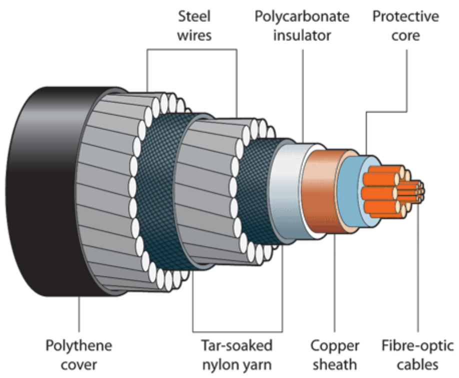
Distribution Fiber, Breakout Fiber



Loose-Tube Fiber, Armored Fiber



Submarine Fiber Optic Cable



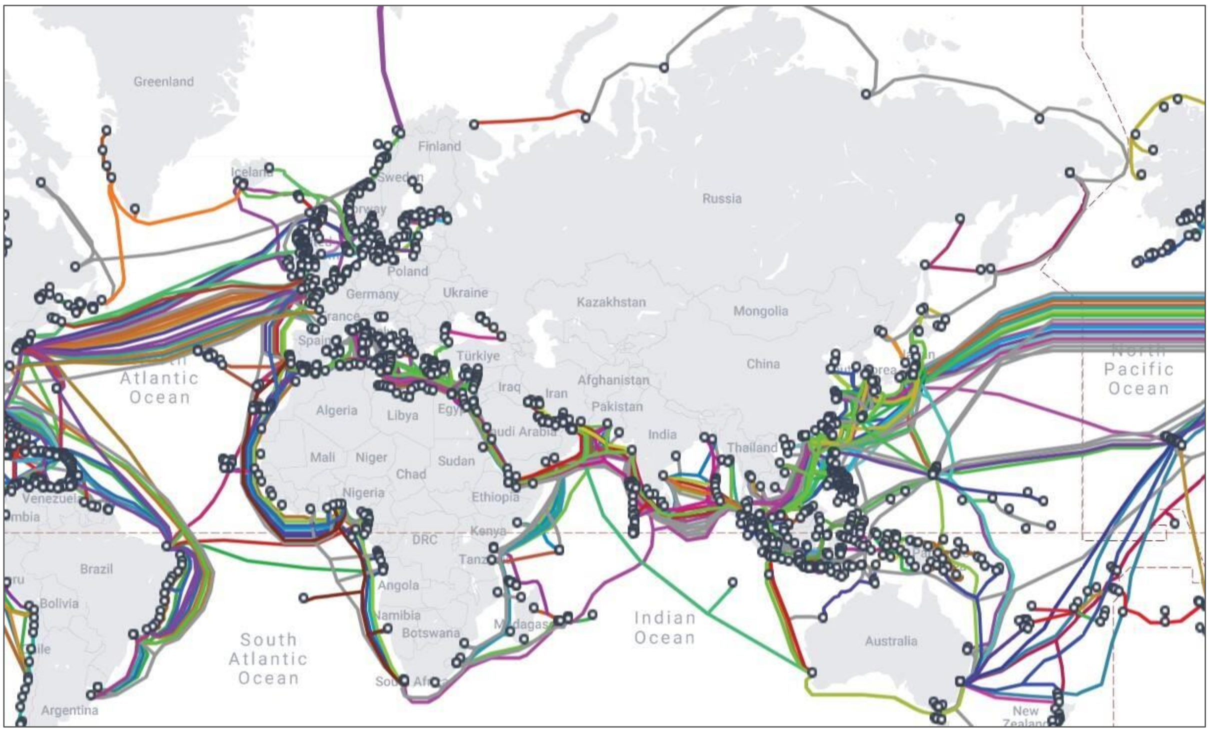
ictfromabc.com

Submarine cable map
සබ්මැරීන් කේබල් සිතියම

This map shows the undersea fiber-optic cables that connect countries and continents. These cables carry most international internet, phone, and data traffic. The map helps users understand how global communication networks are connected.
මෙම සිතියම රටවල් සහ මහාද්වීප එකිනෙකාට සම්බන්ධ කරන මුහුදු පතුලේ ඇති ප්‍රකාශ තන්තු රැහැන් පෙන්වනු ලබයි. ජාත්‍යන්තර අන්තර්ජාල, දුරකථන සහ දත්ත ගමනාගමනයෙන් වැඩි ප්‍රමාණයක් රැගෙන යන්නේ මෙම කේබල් මඟිනි.මෙම සිතියම මඟින් ගෝලීය සන්නිවේදන ජාලයන් එකිනෙකට සම්බන්ධ වී ඇති ආකාරය තේරුම් ගැනීමට පරිශීලකයින්ට උපකාර කරයි.

In the past, submarine cables used copper wires and were mainly used for telegraph messages.
අතීතයේදී, සබ්මැරීන් කේබල් සඳහා තඹ කම්බි භාවිත වූ අතර ඒවා ප්‍රධාන වශයෙන්ම යොදාගනු ලැබුවේ ටෙලිග්‍රාෆ් හුවමාරුව සඳහාය.

Modern submarine cables use fiber-optic strands made of glass, protected by layers of plastic, steel wires, copper/aluminum, and waterproof insulation.
නමුත් නවීන ප්‍රකාශ තන්තු රැහැන් සඳහා වීදුරුවලින් තැනූ ප්‍රකාශ තන්තු කෙඳි භාවිත වන අතර, ඒවා ප්ලාස්ටික් ස්ථර, වානේ කම්බි, තඹ හෝ ඇලුමිනියම් සහ ජලයට ඔරොත්තු දෙන පරිවාරක මඟින් ආරක්ෂා කර ඇත



Advantages

- Has higher bandwidth and can transmit large amounts of data at very high speeds
  ඉහළ කලාප පළලක් ඇති අතර ඉතා ඉහළ වේගයකින් විශාල දත්ත ප්‍රමාණයක් සම්ප්‍රේෂණය කළ හැකිය
- Experiences very low signal loss, allowing data to be transmitted over long distances
  ඉතා අඩු සංඥා අලාභයක් අත්විඳින අතර, දිගු දුරක් හරහා දත්ත සම්ප්රේෂණය කිරීමට ඉඩ සලයසි
- Immune to electromagnetic interference
  විද්‍යුත් චුම්භක මැදිහත්වීම් වලින් බාධා නොවේ
- Difficult to intercept without being detected.
  අනාවරණය නොවී දත්ත හොරා ගැනීම අපහසුය.
- More resistant to environmental factors like moisture, temperature changes, and corrosive elements.
  තෙතමනය, උෂ්ණත්ව වෙනස්වීම් සහ විඛාදන මූලද්‍රව්‍ය වැනි පාරිසරික සාධකවලට වඩා ප්‍රතිරෝධී වේ.

Disadvantages

- The initial installation cost can be high
  මූලික ස්ථාපන පිරිවැය ඉහළ විය හැක
- More fragile and can be easily damaged during installation
  වඩාත් බිඳෙනසුලු වන අතර ස්ථාපනය අතරතුර පහසුවෙන් හානි විය හැක
- Installing and maintenance requires specialized skills and equipment
  ස්ථාපනය සහ නඩත්තුව සඳහා විශේෂ කුසලතා සහ උපකරණ අවශ්‍ය වේ
- Sensitive to bending and can suffer signal loss or damage if bent beyond their specified radius
  නැමීමට සංවේදී වන අතර ඒවායේ නිශ්චිත අරයෙන් ඔබ්බට නැමුවහොත් සංඥා නැතිවීම හෝ හානි සිදුවිය හැක
- In some regions, fiber optic infrastructure may not be as widely available
  සමහර කලාපවල, ප්‍රකාශ තන්තු යටිතල පහසුකම් එතරම් පුළුල් ලෙස නොතිබිය

Aspect	**Fiber Optics**	**Copper Cables**
Bandwidth කලාප පළල	Extremely high, supporting Gbps+ ඉතා ඉහළයි, Gbps¬ සඳහා සහය දක්වයි	Moderate, supporting up to Mbps මධ්‍යස්ථයි, Mbps දක්වා සහය දක්වයි
Transmission Distance සම්ප්‍රේෂණ දුර	Long distances without repeaters වර්ධක නොමැතිව දිගු දුරක්	Shorter distances, frequent repeaters needed කෙටි දුර, නිතර වර්ධක අවශ්‍යයි
Signal Loss සංඥා හානිය	Minimal attenuation over long distances දිගු දුර වලදී අවම විකෘති වීම	Higher attenuation, especially over long distances විශේෂයෙන් දිගු දුර වලදී, වැඩි විකෘති වීම
Interference මැදිහත් වීම	Immune to electromagnetic interference (EMI) විද්‍යුත් චුම්භක මැදිහත්වීම් වලට ප්‍රතිරෝධීය (EMI)	Susceptible to EMI and radio frequency interference (RFI) EMI සහ ගුවන්විදුලි සංඛ්‍යාත මැදිහත්වීම් (RFI) වලට ගොදුරු වේ
Security ආරක්ෂාව	Very secure, difficult to tap without detection ඉතා ආරක්ෂිතයි, අනාවරණයකින් තොරව තට්ටු කිරීමට අපහසුය	Easier to tap, less secure තට්ටු කිරීමට පහසුයි, අඩු ආරක්ෂිතයි
Durability කල්පැවැත්ම	Resistant to moisture, temperature changes, and corrosion තෙතමනය, උෂ්ණත්ව වෙනස්වීම් සහ විඛාදනයට පරතිරෝධී වේ	Prone to corrosion, affected by environmental factors පාරිසරික සාධක මගින් බලපෑමට ලක් වූ විඛාදනයට ගොදුරු වේ
Installation Cost ස්ථාපන පිරිවැය	Higher initial cost due to specialized equipment විශේෂිත උපකරණ හේතුවෙන් ඉහළ ආරම්භක පිරිවැය	Lower cost, commonly used infrastructure අඩු පිරිවැය, බහුලව භාවිතා වන යටිතල පහසුකම්
Flexibility නම්‍යශීලී බව	Limited bending capability, sensitive to sharp bends සීමිත නැමීමේ හැකියාව, තියුණු නැමීම් වලට සංවේදී වේ	More flexible, easier to install in tight spaces වඩාත් නම්‍යශීලී, තද අවකාශයන් තුළ ස්ථාපනය කිරීමට පහසුය
Weight බර	Lightweight and thinner, easy to handle in bulk සැහැල්ලු හා සිහින්, තොග වශයෙන් හැසිරවීමට පහසුය	Heavier, bulkier, and requires more space වැඩි බර, විශාල, සහ වැඩි ඉඩක් ආවශ්‍ය වේ
Installation Complexity ස්ථාපන සංකීර්ණත්වය	Requires specialized skills and equipment විශේෂිත කුසලතා සහ උපකරණ අවශ්‍ය වේ	Easier to install with general skills and tools සාමාන්‍ය කුසලතා සහ මෙවලම් සමඟ ස්ථාපනය කිරීම පහසුය

Waves
තරංග

A wave is a disturbance that travels through a medium, transferring energy from one place to another without transporting matter.
තරංගයක් යනු පදාර්ථය හුවමාරු නොකර එක් ස්ථානයක සිට තවත් ස්ථානයකට ශක්තිය හුවමාරු කරමින් මාධ්‍යයක් හරහා ගමන් කරන කැළඹීමකි.

Waves can be classified based on different criteria.
විවිධ නිර්ණායක මත පදනම්ව තරංග වර්ගීකරණය කළ හැකිය.

1. Based on the Requirement of a Medium
මාධ්‍යයක අවශ්‍යතාවය මත පදනම්ව

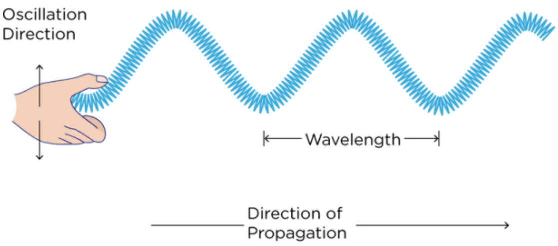
Mechanical Waves
Electromagnetic Waves

2. Based on the Direction of Particle Movement relative to wave propagation
තරංග ප්‍රචාරණයට සාපේක්ෂව අංශු වල චලන දිශාව මත පදනම්ව

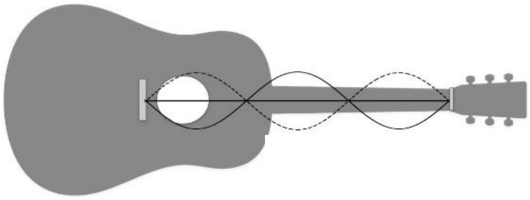
Transverse Waves
Longitudinal Waves
Surface Waves

Transverse Waves
තීර්යක් තරංග

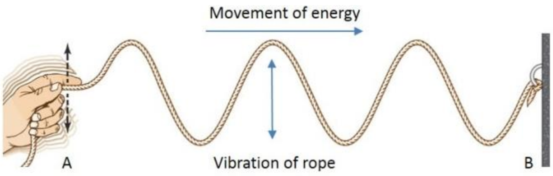
In transverse waves, the particles of the medium move perpendicular (at right angles) to the direction of wave propagation.
තීර්යක් තරංගවලදී, මාධ්‍යයේ අංශු තරංග ප්‍රචාරණ දිශාවට ලම්බකව (සෘජු කෝණවලින්) ගමන් කරයි.



Ex.
Light waves, Waves on a String
When you move one end of a string up and down, transverse waves travel along the string.
තන්තුවක එක් කෙළවරක් ඉහළට සහ පහළට ගෙන යන විට, තීර්යක් තරංග තන්තුව දිගේ ගමන් කරයි.

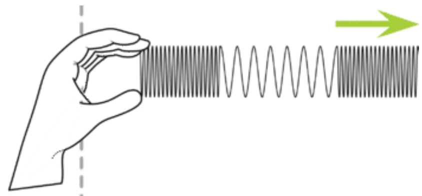


When you shake a rope, the same thing happens.
කඹයක් සොලවන විටද, එකම දෙය සිදු වේ.



Longitudinal Waves
අන්වායාම තරංග

In longitudinal waves, the particles of the medium move parallel (in the same direction) to the direction of wave propagation.
අන්වායාම තරංගවලදී, මාධ්‍යයේ අංශු තරංග ප්‍රචාරණ දිශාවට සමාන්තරව (එකම දිශාවටම) ගමන් කරයි.



Longitudinal waves require a medium (solid, liquid, or gas) to propagate. They cannot travel through a vacuum.
අන්වායාම තරංග වලට ප්‍රචාරණය සඳහා මාධ්‍යයක් (ඝන, ද්‍රව හෝ වායු) අවශ්‍ය වේ. ඒවාට රික්තයක් හරහා ගමන් කළ නොහැක.

Ex.
Sound Waves: Travel through air, water, and solids, involving compressions and rarefactions of particles.
අංශුවල සම්පීඩන සහ විරලන ක්‍රියාකාරකම් ඇතුළත් වෙමින් වාතය, ජලය සහ ඝන ද්‍රව්‍ය හරහා ගමන් කරයි.

Mechanical Waves
යාන්ත්‍රික තරංග

Mechanical waves are waves that require a medium (solid, liquid, or gas) to travel through.
යාන්ත්‍රික තරංග යනු ගමන් කිරීමට මාධ්‍යයක් (ඝන, ද්‍රව හෝ වායු) අවශ්‍ය වන තරංග වේ.

The energy of a mechanical wave is transferred from one particle to another within the medium, causing the wave to propagate.
යාන්ත්‍රික තරංගයක ශක්තිය මාධ්‍යය තුළ එක් අංශුවකින් තවත් අංශුවකට මාරු වන අතර එමඟින් තරංගය ප්‍රචාරණය වේ.

Speed directly depends on the medium's properties.
වේගය සෘජුව ම මාධ්‍යයේ ගුණාංග මත රඳා පවතී.

Ex: sound is faster in water than in air
වාතයට වඩා ජලයේදී ශබ්දය වේගවත් වේ.

Types of Mechanical Waves
යාන්ත්‍රික තරංග වර්ග

Transverse Waves (තීර්යක් තරංග)
Longitudinal Waves (අන්වායාම තරංග)
Surface Waves (මතුපිට තරංග)

Ex.
Sound Waves, Water Waves

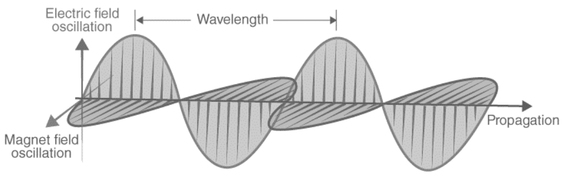
Electromagnetic Waves
විද්‍යුත් චුම්භක තරංග

Electromagnetic (EM) waves are formed through the synchronized vibrations of electric and magnetic fields.
විද්‍යුත් සහ චුම්භක ක්ෂේත්‍රවල සමමුහුර්ත කම්පන හරහා විද්‍යුත් චුම්භක (EM) තරංග සෑදෙයි.

Electric and magnetic fields are perpendicular to each other, forming a right angle, with the wave traveling in the direction perpendicular to both fields.
විද්‍යුත් සහ චුම්බක ක්ෂේත්‍ර එකිනෙකට ලම්බකව සෘජු කෝණයක් සාදයි, තරංගය ක්ෂේත්‍ර දෙකටම ලම්බක දිශාවකට ගමන් කරයි.

Electromagnetic waves are almost always transverse, meaning the oscillations of the electric and magnetic fields are perpendicular to the direction of wave propagation.
විද්‍යුත් චුම්භක තරංග සෑම විටම පාහේ තීර්යක් තරංග වේ, එනම් විද්‍යුත් සහ චුම්බක ක්ෂේත්‍රවල දෝලනය තරංග ප්‍රචාරණ දිශාවට ලම්බක වේ.

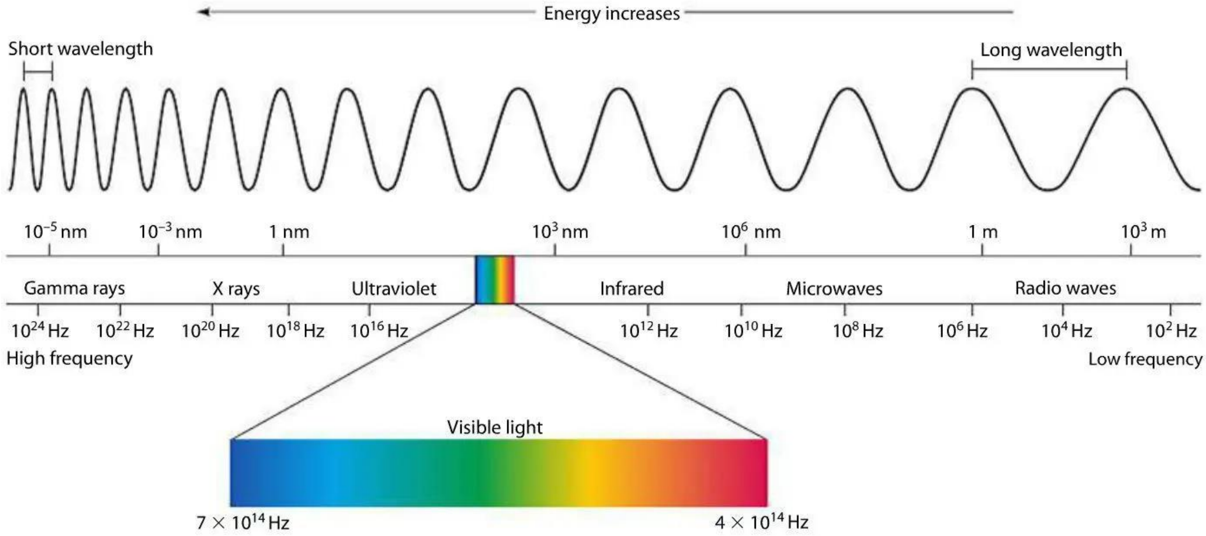
In a vacuum, all electromagnetic waves travel at the speed of light, which is approximately **299,792 kilometers per second** (km/s).
රික්තයක් තුළ, සියලුම විද්‍යුත් චුම්භක තරංග ආලෝකයේ වේගයෙන් ගමන් කරයි, එය ආසන්න වශයෙන් තත්පරයට කිලෝමීටර් 299,792 වේ.



Electromagnetic waves can also be described as streams of particles called photons, which carry energy proportional to the wave's frequency.
තරංගයේ සංඛ්‍යාතයට සමානුපාතිකව ශක්තිය රැගෙන යන ෆෝටෝන නම් අංශු ධාරා ලෙසද විද්‍යුත් චුම්භක තරංග විස්තර කළ හැක.

Higher frequency waves (like gamma rays) carry more energy than lower frequency waves (like radio waves).
ඉහළ සංඛ්‍යාත තරංග (ගැමා කිරණ වැනි) අඩු සංඛ්‍යාත තරංගවලට (රේඩියෝ තරංග වැනි) වඩා වැඩි ශක්තියක් රැගෙන යයි.

Electromagnetic Spectrum
විද්‍යුත් චුම්භක වර්ණාවලිය



Radio waves (1cm – 100km | 3 kHz – 1 GHz)
රේඩියෝ තරංග

Used to transmit data wirelessly over short and long distances.
කෙටි සහ දිගු දුර ප්‍රමාණ හරහා රැහැන් රහිතව දත්ත සම්ප්‍රේෂණය කිරීමට භාවිත කරයි.

Radio waves propagate in all directions from the transmitting antenna and do not require a direct line of sight between the transmitter and receiver.
රේඩියෝ තරංග ප්‍රේරක ඇන්ටනාවේ සිට සියලුම දිශාවලට ප්‍රචාරණය වන අතර, සම්ප්‍රේෂකයා සහ ග්‍රාහකයා අතර සෘජු දෘෂ්ටි රේඛාවක් තිබීම අවශ්‍ය නොවේ.

Advantages / වාසි

- Provides wide wireless coverage.
  පුළුල් රැහැන් රහිත ආවරණ කලාපයක් ලබා දෙයි.
- Can penetrate obstacles such as walls and buildings.
  බිත්ති සහ ගොඩනැගිලි වැනි බාධක හරහා ගමන් කිරීමට හැකියාව පවතී.
- Suitable for both indoor and outdoor communication.
  ගෘහස්ථ මෙන්ම එළිමහන් සන්නිවේදනය සඳහා ද සුදුසු වේ.
- Supports mobile communication over long distances.
  දිගු දුරක් පුරා සිදුවන ජංගම සන්නිවේදන කටයුතු සඳහා සහාය දක්වයි.

Disadvantages / අවාසි

- Susceptible to interference from other radio signals and electrical devices.
  වෙනත් රේඩියෝ සංඥා සහ විදුලි උපකරණ මඟින් ඇතිවන බාධා කිරීම්වලට ලක්වීමේ ප්‍රවණතාවක් පවතී.
- Provides lower bandwidth than microwaves and optical communication.
  ක්ෂුද්‍ර තරංග සහ දෘශ්‍ය සන්නිවේදනයට වඩා අඩු කලාප පළලක් ලබා දෙයි.
- Signals may weaken over long distances.
  දිගු දුරක් ගමන් කිරීමේදී සංඥා දුර්වල විය හැක.
- Communication can be affected by environmental conditions.
  පාරිසරික තත්ත්වයන් හේතුවෙන් සන්නිවේදනයට බලපෑම් එල්ල විය හැක.

Applications / භාවිතයන්

- AM and FM radio broadcasting.
  AM සහ FM ගුවන්විදුලි විකාශනය.
- Television broadcasting.
  රූපවාහිනී විකාශනය.
- Cellular communication.
  ජංගම දුරකථන සන්නිවේදනය.
- Walkie-talkies and two-way radio systems.
  වෝකි-ටෝකි සහ ද්විත්ව මාර්ග ගුවන්විදුලි පද්ධති.
- WiFi and Bluetooth

Microwaves (1mm – 100mm | 1 GHz – 300 GHz)
ක්ෂුද්‍ර තරංග

Used to transmit data wirelessly over long distances at high frequencies.
ඉහළ සංඛ්‍යාත භාවිත කරමින් දිගු දුරක් පුරා රැහැන් රහිතව දත්ත සම්ප්‍රේෂණය කිරීමට භාවිත කරයි.

Signals travel in a straight line and require a clear line of sight (LOS) between the transmitting and receiving antennas.
සංඥා සෘජු රේඛාවක ගමන් කරන බැවින්, ප්‍රේරක සහ ග්‍රාහක ඇන්ටනා අතර පැහැදිලි සෘජු දෘෂ්ටි රේඛාවක් තිබීම අනිවාර්ය වේ.

Advantages / වාසි

- Provides higher bandwidth than radio waves.
  රේඩියෝ තරංගවලට වඩා වැඩි කලාප පළලක් ලබා දෙයි.
- Less susceptible to interference than radio waves.
  රේඩියෝ තරංගවලට වඩා බාධා කිරීම්වලට ලක්වීමේ ප්‍රවණතාව අඩුය.
- Pass through the atmosphere to outer space without reflection.
  පරාවර්තනයකින් තොරව වායුගෝලයේ හරහා අභ්‍යවකාශය දක්වා ගමන් කරයි.
- Can penetrate through atmospheric conditions such as clouds, rain, and fog,
  වලාකුළු, වැසි සහ මීදුම වැනි වායුගෝලීය තත්වයන් හරහා විනිවිද යා හැක.

Disadvantages / අවාසි

- Communication can be interrupted by solid obstacles.
  ඝන පදාර්තමය බාධක හේතුවෙන් සන්නිවේදනයට බාධා ඇති විය හැක.
- Heavy rain, fog, and atmospheric conditions can weaken the signal.
  තද වැසි, මීදුම සහ වායුගෝලීය තත්ත්වයන් හේතුවෙන් සංඥාව දුර්වල විය හැක.
- Installation cost is higher due to antennas and towers.
  ඇන්ටනා සහ කුළුණු අවශ්‍ය වන බැවින් ස්ථාපන පිරිවැය ඉහළ අගයක් ගනී.
- Reflected by metallic surfaces.
  ලෝහමය පෘෂ්ඨ මගින් පරාවර්තනය වේ

Applications / භාවිතයන්

- Point-to-point wireless communication.
  Point-to-point සිදු කෙරෙන රැහැන් රහිත සන්නිවේදනය.
- Satellite and radar communication.
  චන්ද්‍රිකා සහ රේඩාර් සන්නිවේදනය.
- Wireless Internet Service Providers (Ex-Starlink)
  රැහැන් රහිත අන්තර්ජාල සේවා සපයන්නන් (උදා: Starlink).

Infrared (IR) (700nm – 1mm | 300 GHz – 400 THz)
අධෝරක්ත කිරණ

Used for short-range wireless communication between devices.
උපාංග අතර කෙටි දුර රැහැන් රහිත සන්නිවේදනය සඳහා භාවිත කරයි.

Cannot penetrate walls or other solid objects, communication is limited to devices within the open space.
බිත්ති හෝ වෙනත් ඝන වස්තූන් හරහා ගමන් කළ නොහැකි බැවින්, සන්නිවේදනය විවෘත අවකාශයක් තුළ ඇති උපාංග සඳහා පමණක් සීමා වේ.

Wavelength is longer than visible light but shorter than microwaves.
තරංග ආයාමය දෘශ්‍ය ආලෝකයට වඩා දිගු නමුත් ක්ෂුද්‍ර තරංග වලට වඩා කෙටි වේ.

Advantages / වාසි

- Is less affected by radio frequency interference.
  ගුවන්විදුලි සංඛ්‍යාත බාධා කිරීම් මඟින් එල්ල වන බලපෑම අවම වේ.
- Is inexpensive and easy to implement.
  පිරිවැය අඩු වන අතර ක්‍රියාත්මක කිරීමට පහසු වේ.

Disadvantages / අවාසි

- Requires a clear line of sight between devices.
  උපාංග අතර පැහැදිලි සෘජු දෘෂ්ටි රේඛාවක් තිබීම අනිවාර්ය වේ.
- Has a limited communication range.
  සීමිත සන්නිවේදන පරාසයක් පවතී.
- Performance can be affected by sunlight and strong ambient light.
  සූර්යාලෝකය සහ දැඩි පරිසර ආලෝකය හේතුවෙන් ක්‍රියාකාරීත්වයට බලපෑම් ඇති විය හැක.

Applications / භාවිතයන්

- Infrared data transfer between devices.
  උපාංග අතර අධෝරක්ත දත්ත හුවමාරුව.
- Remote control systems.
  දුරස්ථ පාලක පද්ධති.
- Heat radiation and thermal imaging.
  තාප විකිරණ සහ තාප රූපකරණය

Visible Light (400nm – 700nm | 400 THz – 790 THz)
දෘශ්‍ය ආලෝකය

In guided communication, light travels through optical fiber cables to provide high-speed, long-distance data transmission.
නියමු සන්නිවේදනයේදී , ඉහළ වේගයකින් යුත් දිගු දුර දත්ත සම්ප්‍රේෂණයක් ලබා දීම සඳහා ආලෝකය දෘශ්‍ය තන්තු කේබල් හරහා ගමන් කරයි.

In unguided communication, visible light is used in Light Fidelity (Li-Fi) systems, where LED lights transmit data wirelessly over short distances.
නියමු නොවන සන්නිවේදනයේදී, කෙටි දුරක් තුළ රැහැන් රහිතව දත්ත සම්ප්‍රේෂණය කිරීම සඳහා Li-Fi (Light Fidelity) පද්ධති මඟින් දෘශ්‍ය ආලෝකය භාවිත කරනු ලබයි.

The only part of the electromagnetic spectrum that humans can see.
මිනිසුන්ට දැකිය හැකි විද්‍යුත් චුම්භක වර්ණාවලියේ එකම කොටසයි.

The different wavelengths of visible light correspond to different colors, from red to violet (Colors of the rainbow).
දෘශ්‍ය ආලෝකයේ විවිධ තරංග ආයාම රතු සිට වයලට් දක්වා (දේදුන්නෙහි වර්ණ) විවිධ වර්ණවලට අනුරූප වේ.

Advantages / වාසි

- Does not cause radio frequency interference.
  ගුවන්විදුලි සංඛ්‍යාත බාධා කිරීම් ඇති නොකරයි.
- Provides secure communication because light cannot pass through walls.
  ආලෝකයට බිත්ති හරහා ගමන් කළ නොහැකි බැවින් ආරක්ෂිත සන්නිවේදනයක් ලබා දෙයි.
- Offers a large available bandwidth.
  විශාල කලාප පළලක් ලබා දෙයි.

Disadvantages / අවාසි

- Requires a clear line of sight between the transmitter and receiver.
  සම්ප්‍රේෂකයා සහ ග්‍රාහකයා අතර පැහැදිලි සෘජු දෘෂ්ටි රේඛාවක් තිබීම අනිවාර්ය වේ.
- Performance can be affected by strong ambient light or sunlight.
  දැඩි පරිසර ආලෝකය හෝ සූර්යාලෝකය හේතුවෙන් ක්‍රියාකාරීත්වයට බලපෑම් ඇති විය හැක.

Applications / භාවිතයන්
- Li-Fi communication.
- Optical Fiber

NOTE:
The following types of electromagnetic waves are not used for communication because they are harmful to human beings.
පහත දැක්වෙන ආකාරයේ විද්‍යුත් චුම්භක තරංග මිනිසුන්ට හානිකර බැවින් සන්නිවේදනය සඳහා භාවිතා නොකෙරේ.

Ultraviolet (10nm – 380nm | 790 THz – 30 PHz)
පාරජම්බුල කිරණ

Produced when energized patterns lose energy and come to lower energy levels.
ශක්තිජනක පරමාණු ශක්තිය නැති වී පහළ ශක්ති මට්ටම් කරා ළඟා වූ විට නිපදවනු ලැබේ.

May be harmful to living tissues with prolonged exposure
දිගු වේලාවක් නිරාවරණය වීමෙන් ජීවී පටක වලට හානිකර විය හැක.

Is partially absorbed by the Earth's atmosphere.
පෘථිවි වායුගෝලය මඟින් කොටසක් (කාණ්ඩ වශයෙන්) අවශෝෂණය කරගනු ලබයි.

Applications / භාවිතයන්

- Sterilization of medical equipment.
  වෛද්‍ය උපකරණ විෂබීජහරණය කිරීම.
- Water and air purification.
  ජලය සහ වාතය පිරිපහදු කිරීම.
- Forensic analysis.
  අධිකරණ වෛද්‍ය විද්‍යාත්මක විශ්ලේෂණ.
- Medical treatments.
  වෛද්‍ය ප්‍රතිකාර.
- UV curing in industrial processes.
  කාර්මික ක්‍රියාවලීන්හිදී UV කිරණ මඟින් (ද්‍රව්‍ය) වියළීම හෝ දැඩි කිරීම.
- Detection of fluorescent inks on currency, passports.
  මුදල් නෝට්ටු, විදේශ ගමන් බලපත්‍ර ඇති ප්‍රතිදීප්ත තීන්ත හඳුනා ගැනීම.

X-rays (0.01nm – 10nm | 30 PHz – 30 EHz)
X-කිරණ

Produced when high-energy electrons collide with a target material, such as tungsten.
අධි ශක්ති ඉලෙක්ට්‍රෝන ටංස්ටන් වැනි ද්‍රව්‍යයක් සමඟ ගැටෙන විට නිෂ්පාදනය වේ.

High frequency electromagnetic waves capable of penetrating many materials.
බොහෝ ද්‍රව්‍ය හරහා ගමන් කිරීමේ හැකියාව ඇති ඉහළ සංඛ්‍යාත සහිත විද්‍යුත් චුම්බක තරංග වේ.

Has very high energy and short wavelength.
ඉතා ඉහළ ශක්තියක් සහ කෙටි තරංග ආයාමයක් පවතී.

Applications / භාවිතයන්

- Medical X-ray imaging.
  වෛද්‍ය X-කිරණ ප්‍රතිරූපණය
- CT (Computed Tomography) scanning.
  CT (පරිගණකගත ටොමොග්‍රැෆි) ස්කෑන් කිරීම.
- Airport baggage scanners.
  ගුවන්තොටුපල ගමන් මලු පරීක්ෂා කරන යන්ත්‍ර
- Industrial non-destructive testing.
  කාර්මික විනාශකාරී නොවන පරීක්ෂණ
- Scientific and laboratory research.
  විද්‍යාත්මක සහ රසායනාගාර පර්යේෂණ.

Gamma Rays (<0.01nm | >30 EHz)
ගැමා කිරණ

Emitted from the nucleus of an atom during radioactive decay or nuclear reactions.
විකිරණශීලී ක්ෂය වීම හෝ න්‍යෂ්ටික ප්‍රතික්‍රියා වලදී පරමාණුවක න්‍යෂ්ටියෙන් විමෝචනය වේ.

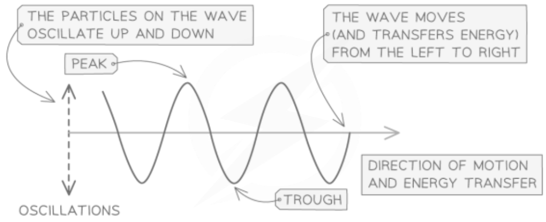
Highest frequency, shortest wavelength and highest energy electromagnetic waves.
ඉහළම සංඛ්‍යාතය, කෙටිම තරංග ආයාමය සහ ඉහළම ශක්තිය සහිත විද්‍යුත් චුම්බක තරංග වේ.

Primarily used in medicine, scientific research, and industrial applications rather than for conventional data communication.
සාමාන්‍ය දත්ත සන්නිවේදනය සඳහා භාවිත කරනවා වෙනුවට, මූලික වශයෙන් වෛද්‍ය විද්‍යාව, විද්‍යාත්මක පර්යේෂණ සහ කාර්මික යෙදවුම් සඳහා භාවිත වේ.

Applications / භාවිතයන්

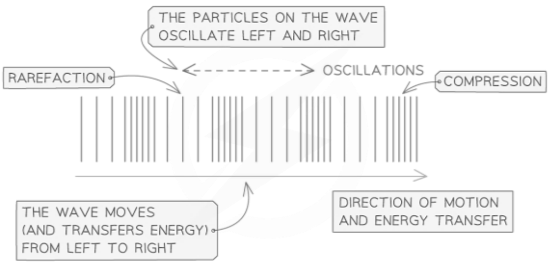
- Cancer treatment (Radiotherapy).
  පිළිකා ප්‍රතිකාර (විකිරණ ප්‍රතිකාර).
- Sterilization of medical equipment.
  වෛද්‍ය උපකරණ විෂබීජහරණය කිරීම.
- Food irradiation.
  ආහාර විකිරණකරණය
- Industrial radiography.
  කාර්මික රේඩියෝග්‍රැෆිය
- Scientific and nuclear research.
  විද්‍යාත්මක සහ න්‍යෂ්ටික පර්යේෂණ.

Properties of waves
තරංග වල ලක්ෂණ



Crest (Peak)
The highest point of a wave
තරංගයක උසම ස්ථානය

Trough
The lowest point of a wave
තරංගයක පහළම ස්ථානය



Compressions
සම්පීඩන

A compression is a region in a longitudinal wave where the particles of the medium are pushed closer together, resulting in increased density and pressure.
සම්පීඩන යනු අනවායාම තරංගයක මාධ්‍යයේ අංශු එකට සමීප වන කලාපයක් වන අතර එහි ඝනත්වය සහ පීඩනය වැඩිය.

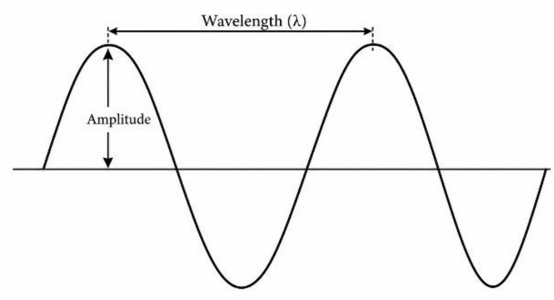
Rarefactions
විරලන

Rarefaction is a region in a longitudinal wave where the particles of the medium are spread farther apart, resulting in decreased density and pressure.
විරලන යනු අන්වායාම තරංගයක මාධ්‍යයේ අංශු දුරින් පැතිරී ඇති කලාපයක් වන අතර එහි ඝනත්වය සහ පීඩනය අඩුය.

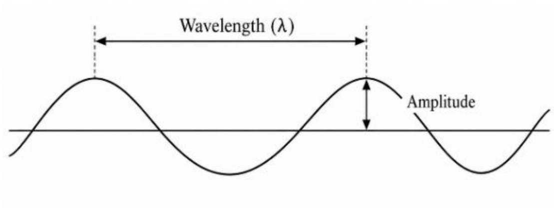
Amplitude
විස්තාරය

Amplitude is the maximum displacement point on the wave from its rest position. A crest or a Trough.
විස්තාරය යනු තරංගයේ නිශ්චල ස්ථානයේ සිට තරංගයේ උපරිම විස්ථාපන ලක්ෂ්‍යය වේ.

Amplitude relates to the wave's power intensity. More amplitude, more intense.
විස්තාරය තරංගයේ බල තීව්‍රතාවයට සම්බන්ධ වේ. වැඩි විස්තාරය, වඩා තීව්‍ර වේ.



A high amplitude wave has taller crests and deeper troughs, so it carries more energy when frequency and wavelength remain constant.
සංඛ්‍යාතය සහ තරංග ආයාමය නියතව පවතින විට, ඉහළ විස්තාරයක් සහිත තරංගයකට උස් වූ ශීර්ෂ සහ ගැඹුරු නිම්න පවතින බැවින්, එය වැඩි ශක්තියක් රැගෙන යයි.



A low amplitude wave has shorter crests and shallower troughs, so it carries less energy when frequency and wavelength remain constant.
විස්තාරයක් සහිත තරංගයකට කෙටි වූ ශීර්ෂ සහ නොගැඹුරු නිම්න පවතින බැවින්, එය රැගෙන යන්නේ අඩුශක්තියකි.

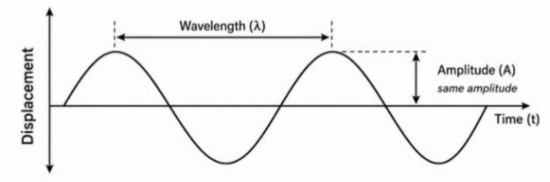
Ex: in Sea Waves, energy, in sound waves, loudness.

Note : Here, frequency & wavelength are held constant when amplitude changes.
මෙහිදී විස්තාරය වෙනස් වන විට සංඛ්‍යාතය සහ තරංග ආයාමය ස්ථාවරව පවත්වා ගෙන යයි.

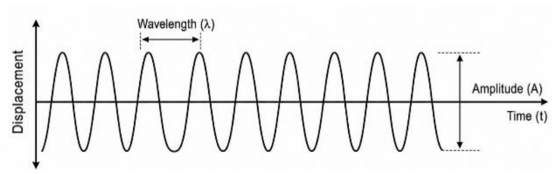
Wavelength (λ)
තරංග ආයාමය

Wavelength is the distance between two identical points in a wave pattern.
තරංග ආයාමය යනු තරංග රටාවක සමාන ලක්ෂ්‍ය දෙකක් අතර දුර වේ
(can be two consecutive crests or troughs)

It is inversely proportional to frequency.
එය සංඛ්‍යාතයට ප්‍රතිලෝමව සමානුපාතික වේ.



A long wavelength wave has crests that are farther apart, so fewer waves pass a point in a given time when amplitude and wave speed remain constant.
විස්තාරය සහ තරංග ප්‍රවේගය නියතව පවතින විට, දිගු තරංග ආයාමයක් සහිත තරංගයක ශීර්ෂයන් එකිනෙකට බොහෝ ඈතින් පිහිටයි. එබැවින් දී ඇති නිශ්චිත කාලයක් තුළදී ලක්ෂ්‍යයක් හරහා ගමන් කරන්නේ අඩු තරංග ප්‍රමාණයක් පමණි.



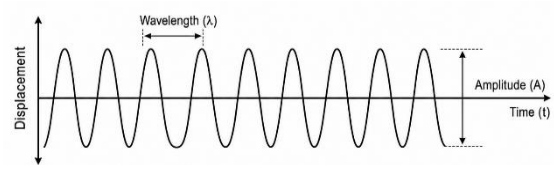
A short wavelength wave has crests that are closer together, so more waves pass a point in a given time when amplitude and wave speed remain constant.
විස්තාරය සහ තරංග ප්‍රවේගය නියතව පවතින විට, කෙටි තරංග ආයාමයක් සහිත තරංගයක ශීර්ෂයන් එකිනෙකට ඉතා සමීපව පිහිටයි. එබැවින් දී ඇති නිශ්චිත කාලයක් තුළදී ලක්ෂ්‍යයක් හරහා වැඩි තරංග ප්‍රමාණයක් ගමන් කරයි.

Note : Here amplitude is held constant when wave length changes.
මෙහිදී තරංග ආයාමය වෙනස් වන විට විස්තාරය ස්ථාවරව පවත්වා ගෙන යයි.

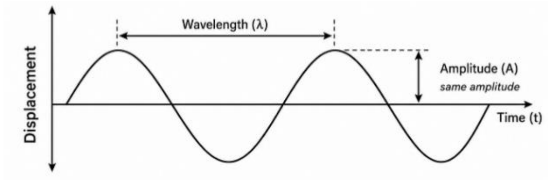
Frequency (f)
සංඛ්‍යාතය

Frequency is the number of wavelengths that pass a fixed point in one second.
සංඛ්‍යාතය යනු තත්පරයක් තුළ ස්ථාවර ලක්ෂ්‍යයක් පසුකර යන තරංග ආයාම ගණනයි.

It is measured in hertz (Hz). It means oscillations per unit time.
එය හර්ට්ස් වලින් මනිනු ලැබේ. එහි තේරුම ඒකක කාලයකට දෝලන ගණන යන්නයි.



A high frequency wave has more cycles passing a point in a given time, so the compressions and rarefactions are closer together.
ඉහළ සංඛ්‍යාත තරංගයකදී දී ඇති නිශ්චිත කාලයක් තුළ ලක්ෂ්‍යයක් හරහා වැඩි චක්‍ර ප්‍රමාණයක් ගමන් කරයි, එබැවින් එහි සම්පීඩන සහ විරලන එකිනෙකට ඉතා සමීපව පිහිටයි.



A low frequency wave has fewer cycles passing a point in a given time, so the compressions and rarefactions are farther apart.
අඩු සංඛ්‍යාත තරංගයකදී දී ඇති නිශ්චිත කාලයක් තුළ ලක්ෂ්‍යයක් හරහා ගමන් කරන්නේ අඩු චක්‍ර ප්‍රමාණයක් පමණි, එබැවින් එහි සම්පීඩන සහ විරලන එකිනෙකට බොහෝ ඈතින් පිහිටයි.

Note : Here amplitude is held constant when frequency changes.
මෙහිදී සංඛ්‍යාතය වෙනස් වන විට විස්තාරය ස්ථාවරව පවත්වා ගෙන යයි.

Period (T)
කාලාවර්තය

Period is the time taken for one complete wave cycle to pass a point.
කාලාවර්තය යනු එක් සම්පූර්ණ තරංග චක්‍රයක් සඳහා ලක්ෂ්‍යයක් පසු කිරීමට ගතවන කාලයයි.

It's the inverse of frequency.
එය සංඛ්‍යාතයේ ප්‍රතිලෝමය වේ.

T = 1/f
T - Period
F - Frequency

Period and frequency are opposites: when the period increases, the frequency decreases; when the period decreases, the frequency increases.
ආවර්ත කාලය සහ සංඛ්‍යාතය යනු එකිනෙකට ප්‍රතිලෝම සාධක වේ: ආවර්ත කාලය වැඩි වන විට සංඛ්‍යාතය අඩු වේ; ආවර්ත කාලය අඩු වන විට සංඛ්‍යාතය වැඩි වේ.

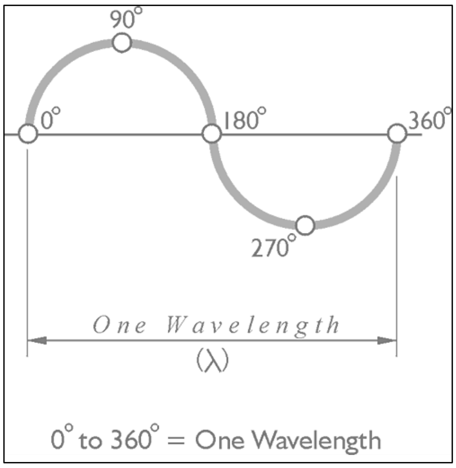
If one wave cycle takes 2 seconds, the period is 2 s, so the frequency is low. If one wave cycle takes 0.5 seconds, the period is 0.5 s, so the frequency is high.
යම් තරංග චක්‍රයක් සඳහා තත්පර 2 ක් ගතවන්නේ නම්, එහි ආවර්ත කාලය තත්පර 2 කි (T = 2s). එවිට එහි සංඛ්‍යාතය අඩුය. යම් තරංග චක්‍රයක් සඳහා තත්පර 0.5ක් ගතවන්නේ නම්, එහි ආවර්ත කාලය තත්පර 0.5 කි (T = 0.5s). එවිට එහි සංඛ්‍යාතය ඉහළය.

Phase
කලාව

Phase is the position of a point within a wave cycle relative to a reference point. කලාව යනු සමුද්දේශ ලක්ෂ්‍යයකට සාපේක්ෂව තරංග චක්‍රයක් තුළ ලක්ෂ්‍යයක පිහිටීමයි.

Waves that are in same phase with each other have crests (and troughs) that align, while waves out of phase do not align perfectly.
එකිනෙක සමග එකම කලාවක ඇති තරංගවල crests (and troughs) සම්පාත වන අතර කලාවෙන් පිටත තරංග එක්කාරව පෙලගැසෙන්නේ නැත.

Phase Angle: The phase angle indicates the current position within the wave cycle. For example, a phase of 0 degrees or 0 radians represents the start of the cycle, while 180 degrees or π radians represents the midpoint.
කලා කෝණය තරංග චක්‍රය තුළ වත්මන් තත්ත්වය පෙන්නුම් කරයි. උදාහරණයක් ලෙස, අංශක 0 හෝ රේඩියන 0 ක කලාව චක්‍රයේ ආරම්භය නියෝජනය කරන අතර අංශක 180 හෝ π රේඩියන මධ්‍ය ලක්ෂ්‍යය නියෝජනය කරයි.



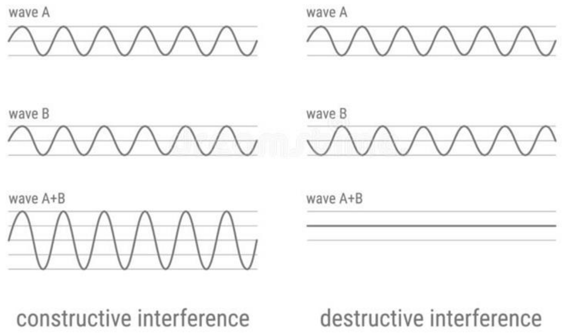
In-Phase Waves: When two waves have the same phase, their peaks and troughs align, resulting in **constructive interference**, where the amplitude is increased.
තරංග දෙකකට එකම කලාවක් ඇති විට, ඒවායේ ශීර්ෂ සහ නිම්න සම්පාත වන අතර, එහි ප්‍රතිඵලයක් ලෙස constructive interference ඇති වේ, එහිදී විස්තාරය වැඩි වේ.

Example:
When two speakers emit identical sound waves in phase, their peaks add together to create increased amplitude and louder volume.
Speakers දෙකක් කලාවෙන් සමාන ශබ්ද තරංග නිකුත් කරන විට, ඒවායේ ශීර්ෂ එකට එකතු වී වැඩි විස්තාරයක් සහ ශබ්දයක් ඇති කරයි.

Out-of-Phase Waves: When two waves are out of phase, their peaks and troughs do not align, leading to **destructive interference**, where the amplitude may be reduced or even canceled out.
තරංග දෙකක කලාව වෙනස් වූ විට, ඒවායේ ශීර්ෂ සහ නිම්න නොගැලපෙන අතර, එය destructive interference වලට තුඩු දෙයි, එහිදී විස්තාරය අඩු වීමට හෝ එවා එකිනෙක අහෝසි වීමට පවා ඉඩ ඇත.

Destructive interference is the basic principle used in Active Noise Cancellation (ANC), where an opposite sound wave is produced to reduce unwanted noise.
සක්‍රීය ශබ්ද අවලංගු කිරීමේ (ANC) තාක්ෂණයේදී භාවිත වන මූලික න්‍යාය වන්නේ Destructive interference. එහිදී අනවශ්‍ය ශබ්ද අවම කිරීම සඳහා ඊට ප්‍රතිවිරුද්ධ ශබ්ද තරංගයක් නිපදවනු ලබයි.

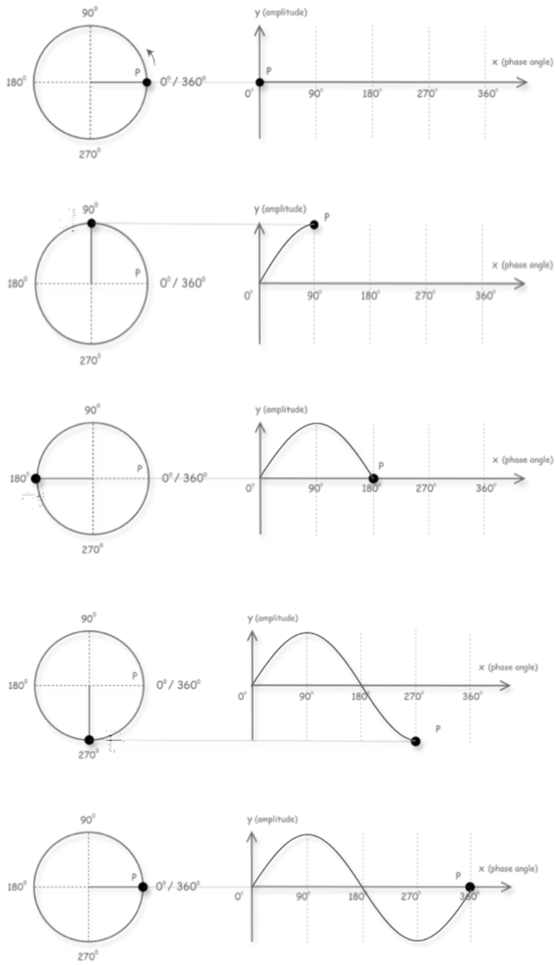
Example:
Microphones detect ambient noise and electronics generate inverted sound waves 180° out of phase, causing peaks and troughs to cancel each other out and eliminate unwanted sound.
මයික්‍රොෆෝන මගින් අවට ඝෝෂාව හඳුනා ගන්නා අතර ඉලෙක්ට්‍රොනික උපකරණය මඟින් (180°) ක කලාවකින් ප්‍රතිලෝම ශබ්ද තරංග ජනනය කර ශීර්ෂ සහ නිම්න එකිනෙක අහෝසි කර අනවශ්‍ය ඝෝෂාව ඉවත් කරයි.



Circular Motion to Waveform
වෘත්ත චලිතයෙන් තරංග ආකාරයක් සාදා ගැනීම

Consider a point moving around a circle with a constant angular velocity.
නියත කෝණික ප්‍රවේගයකින් වෘත්තයක් වටා ගමන් කරන ලක්ෂ්‍යයක් සලකා බලන්න.

As it moves, its position can be described by two components: one along the x-axis (horizontal) and one along the y-axis (vertical).
එය චලනය වන විට, එහි පිහිටීම සංරචක දෙකකින් විස්තර කළ හැකිය: එකක් x-අක්ෂය ඔස්සේ (තිරස්) සහ අනෙක y-අක්ෂය (සිරස්) ඔස්සේ.



If we project the position of this point onto the x-axis, the vertical displacement (y-component) of the point over time forms a sine wave.
මෙම ලක්ෂ්‍යයේ පිහිටීම x-අක්ෂයට ප්‍රක්ෂේපණය කරහොත්, කාලයත් සමඟ ලක්ෂ්‍යයේ සිරස් විස්ථාපනය (y-සංරචකය) සයිනාකාර තරංගයක් සාදයි.

The horizontal displacement corresponds to time, and the vertical displacement corresponds to the wave's amplitude.
තිරස් විස්ථාපනය කාලයට අනුරූප වන අතර සිරස් විස්ථාපනය තරංගයේ විස්තාරයට අනුරූප වේ.

The angle of the point in the circular motion corresponds to the phase of the wave.
වෘත්ත චලිතයේ යෙදෙන ලක්ෂ්‍යයේ කෝණය තරංගයේ කලාවට අනුරූප වේ.

Three Phases
තෙකලා

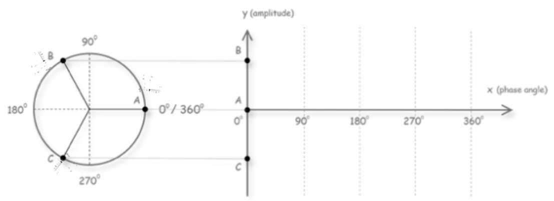
When considering three-phase systems, each phase can be visualized as originating from three points equally spaced around a circle (i.e., separated by 120 degrees or 2π/3 radians).
තෙකලා පද්ධති සලකා බැලීමේදී, සෑම කලාවක්ම වෘත්තයක් වටා සමාන පරතරයකින් (එනම් අංශක 120 කින් හෝ රේඩියන 2 π/3 කින් වෙන් කර ඇති) ලක්ෂ්‍ය තුනකින් ආරම්භ වන බව සිතිය හැක.

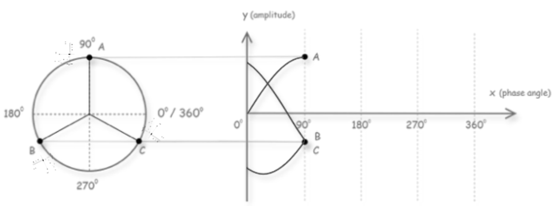
Imagine three points moving around the same circle but starting at different positions, 120 degrees apart.
අංශක 120ක් දුරින් විවිධ ස්ථානවලින් ආරම්භ වන නමුත් එකම වෘත්තය වටා ගමන් කරන ලක්ෂ්‍ය තුනක් සිතන්න.

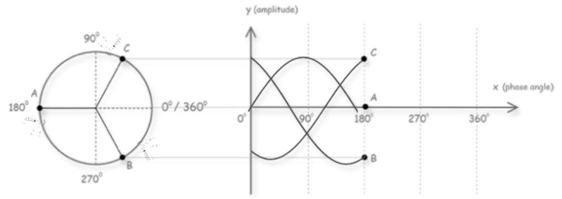
Each point represents a different phase of the wave (Phase A, Phase B, and Phase C).
සෑම ලක්ෂයක්ම තරංගයේ වෙනස් කලාවක් නියෝජනය කරයි (A කලාව, B කලාව සහ C කලාව).

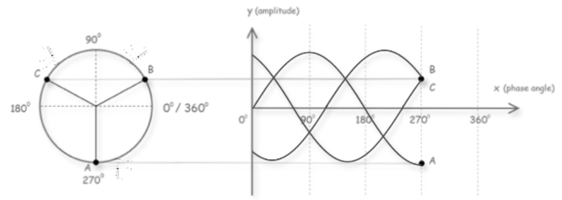
Projecting each of these points onto the x-axis will produce three sine waves, each with the same amplitude and frequency but with a phase shift of 120 degrees relative to each other.
මෙම සෑම ලක්ෂ්‍යයක්ම x-අක්ෂයට ප්‍රක්ෂේපණය කිරීමෙන් සයිනාකාර තරංග තුනක් නිපදවෙනු ඇත, ඒ සෑම තරංගයකම එකම විස්තාරය සහ සංඛ්‍යාතය ඇති නමුත් එකිනෙකට සාපේක්ෂව අංශක 120 ක කලා වෙනසක් ඇත.

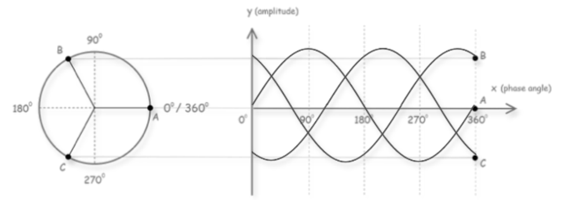
These three sine waves are often described as Phase A, Phase B, and Phase C in electrical systems, where they represent the voltages or currents in a three-phase power system.
මෙම සයිනාකාර තරංග තුන බොහෝ විට විද්‍යුත් පද්ධතිවල A, B සහ C කලාව ලෙස විස්තර කෙරෙන අතර එහිදී ඒවා තෙකලා බල පද්ධතියක වෝල්ටීයතා හෝ ධාරා නියෝජනය කරයි.











The three waves are out of phase with each other, but they combine to create a balanced, constant power output over time.
තරංග තුන එකිනෙකින් කලාවෙන් බැහැරව ඇත, නමුත් කාලයත් සමඟ සමතුලිත, නියත බල නිමැවුමක් නිර්මාණය කිරීමට ඒවා ඒකාබද්ධ වේ.

Why we need three phase systems
තෙකලා පද්ධති අවශ්‍ය වීමට හේතුව

Single-Phase Power
එකලා බලය

In a single-phase system, the voltage waveform follows a sine wave pattern.
එකලා පද්ධතියක, වෝල්ටීයතා තරංග ආකෘතිය සයිනාකාර තරංග රටාවක් අනුගමනය කරයි.

At 50Hz, the voltage crosses zero twice in each cycle (once every 10 milliseconds).
50Hz දී, වෝල්ටීයතාව සෑම චක්‍රයකටම දෙවරක් බිංදුවට පැමිණේ (සෑම මිලි තත්පර 10 කට වරක්).

During these zero-crossing points, no power is delivered because the voltage and current are both zero.
මෙම ශුන්‍ය හරස් ලක්ෂ්‍ය වලදී, වෝල්ටීයතාවය සහ ධාරාව යන දෙකම ශුන්‍ය වන බැවින් බලය ලබා නොදේ.

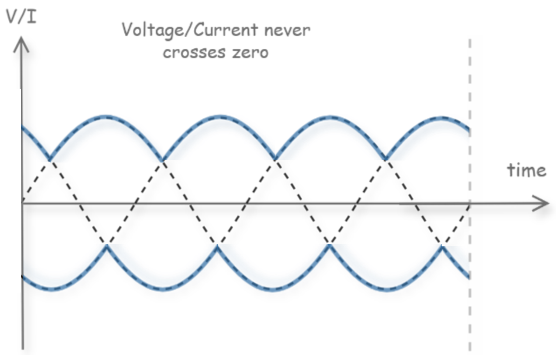
This results in pulsating power delivery, where power flow momentarily drops to zero twice per cycle.
මෙහි ප්‍රතිඵලයක් ලෙස ස්පන්දන බලය බෙදා හැරීම සිදුවේ, එහිදී බල ප්‍රවාහය මොහොතකට චක්‍රයකට දෙවරක් බිංදුව දක්වා පහත වැටේ.

Three-Phase Power
තෙකලා බලය

In a three-phase system, there are three sine waves (each phase) offset by 120 degrees from each other.
තෙකලා පද්ධතියක, සයිනාකාර තරංග තුනක් (එක් එක් කලාව) එකිනෙකින් අංශක (120) කින් විස්ථාපනය වේ.

Because of this phase offset, at least one phase is always at or near its peak voltage while the others are crossing zero.
මෙම කලා වෙනස නිසා, අවම වශයෙන් එක් කලාවක්වත් අනෙක් කලාවන් බිංදුවට පැමිණේමීදී සෑම විටම එහි උපරිම වෝල්ටීයතාවයේ හෝ ඊට ආසන්නයේ පවතී.

This ensures that power delivery is constant, with no momentary drops to zero, leading to smoother and more consistent energy supply.
මෙමගින් ශුන්‍යයට ක්ෂණික පහත වැටීම් නොමැතිව බල සැපයුම නියත බව සහතික කරයි, එමගින් සුමට හා වඩා ස්ථාවර බලශක්ති සැපයුමකට මග පාදයි.



The difference between signals and waves
සංඥා සහ තරංග අතර වෙනස

Waves
A wave is simply a physical phenomenon that exists around us all the time.
තරංගයක් යනු සරලවම අප වටා සෑම විටම පවතින භෞතික සංසිද්ධියකි.

Waves can be found everywhere in nature, such as light waves from the sun, sound waves in the air, or ocean waves. However, not all waves carry information or have a meaning, they just exist.
සූර්යයාගේ සිට ආලෝක තරංග, වාතයේ ඇති ශබ්ද තරංග හෝ සාගර තරංග වැනි ස්වභාවධර්මයේ සෑම තැනකම තරංග සොයාගත හැකිය. කෙසේ වෙතත්, සෑම තරංගයක්ම තොරතුරු රැගෙන යන්නේ හෝ ඒවාට අර්ථයක් හෝ නැත, ඒවා ස්වභාවිකව පවතී.

Signals
A signal is an electronic voltage or current, which varies with time.
සංඥාවක් යනු ඉලෙක්ට්‍රොනික වෝල්ටීයතාවයක් හෝ ධාරාවක් වන අතර එය කාලයත් සමඟ වෙනස් වේ.

Signals are used to communicate or convey data from one place to another.
එක් ස්ථානයක සිට තවත් ස්ථානයකට දත්ත සන්නිවේදනය කිරීමට හෝ සම්ප්‍රේෂණය කිරීමට සංඥා භාවිතා කරයි.

Note:
Not all waves are signals.
සියලුම තරංග සංඥා නොවේ.

Waves can exist without carrying any information, but when a wave is used to transfer information, it becomes a signal.
කිසිදු තොරතුරක් රැගෙන යාමකින් තොරව තරංග පැවතිය හැකි නමුත් තොරතුරු හුවමාරු කිරීමට තරංගයක් භාවිතා කරන විට එය සංඥාවක් බවට පත් වේ.

Types of signals
සංඥා වර්ග

There are two types of signals
සංඥා වර්ග දෙකකි

Analog signals ප්‍රතිසම සංඥා
Digital signals අංකිත සංඥා

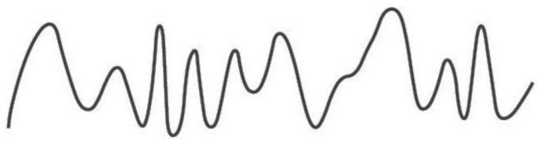
1. Analog signals
ප්‍රතිසම සංඥා

Analog signals continuously vary over time and can take any value within a range up to infinite.
ප්‍රතිසම සංඥා කාලයත් සමග සන්තතිකව වෙනස් වන අතර අනන්තය දක්වා පරාසයක් තුළ ඕනෑම අගයක් ගත හැක.

This means that there can be an infinite number of energy levels in an analog signal, allowing it to vary smoothly over time.
මෙයින් අදහස් කරන්නේ ප්‍රතිසම සංඥාවක ශක්ති මට්ටම් අසීමිත සංඛ්‍යාවක් පැවතිය හැකි අතර එය කාලයත් සමඟ සුමට ලෙස වෙනස් වීමට ඉඩ සලසන බවයි.

This continuous nature is why analog signals are well-suited to represent natural phenomena like sound, light, and temperature, which also vary in a smooth and uninterrupted manner.
මෙම අඛණ්ඩ ස්වභාවය නිසා ප්‍රතිසම සංඥා සුමට හා බාධාවකින් තොරව වෙනස් වන ශබ්දය, ආලෝකය සහ උෂ්ණත්වය වැනි ස්වභාවික සංසිද්ධි නියෝජනය කිරීමට හොඳින් ගැලපේ.

Random Analog Wave



Analog Sine Wave

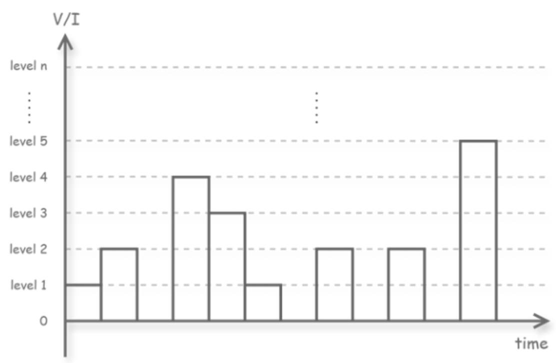
2. Digital signals
අංකිත සංඥා

Digital signals vary discretely within a specific range of energy levels, meaning they take on certain fixed values.
අංකිත සංඥා නිශ්චිත ශක්ති මට්ටම් පරාසයක් තුළ විවික්තව වෙනස් වේ, එයින් අදහස් වන්නේ ඒවා නිශ්චිත ස්ථාවර අගයන් ගන්නා බවයි.

In digital systems, signals can theoretically utilize a range of energy levels, not just two.
අංකිත පද්ධති තුළ, සංඥාවලට න්‍යායාත්මකව ශක්ති මට්ටම් දෙකක් පමණක් නොව ශක්ති මට්ටම් පරාසයක් භාවිතා කළ හැක.

For instance, a system might use ten different voltage levels to represent different values, allowing for a more compact representation of data.
උදාහරණයක් ලෙස, පද්ධතියක් විවිධ අගයන් නියෝජනය කිරීම සඳහා විවිධ වෝල්ටීයතා මට්ටම් දහයක් භාවිතා කළ හැකි අතර, දත්ත වඩාත් සංයුක්තව නිරූපණය කිරීමට එමගින් ඉඩ සලසයි.

However, practical constraints and limitations in technology often make it challenging to implement such systems.
කෙසේ වෙතත්, තාක්ෂණයේ ඇති ප්‍රායෝගික බාධාවන් සහ සීමාවන් බොහෝ විට එවැනි පද්ධති ක්‍රියාත්මක කිරීම අභියෝගාත්මක කරයි.



Challenges and Practical Limitations
අභියෝග සහ ප්‍රායෝගික සීමාවන්

To effectively use multiple energy levels, the equipment must be extremely precise in distinguishing between these levels.
බහු ශක්ති මට්ටම් ඵලදායී ලෙස භාවිතා කිරීම සඳහා, මෙම මට්ටම් අතර වෙනස හඳුනාගැනීමේදී උපකරණ අතිශයින් නිරවද්‍ය විය යුතුය.

Managing and transmitting signals with many levels adds complexity to both the hardware and software.
බොහෝ මට්ටම් සමඟ සංඥා කළමනාකරණය කිරීම සහ සම්ප්‍රේෂණය කිරීම දෘඩාංග සහ මෘදුකාංග යන දෙකටම සංකීර්ණත්වයක් එක් කරයි.

This complexity can lead to increased costs and more robust requirements for equipment calibration and maintenance.
මෙම සංකීර්ණත්වය මගින් වැඩි පිරිවැයක් හා උපකරණ ක්‍රමාංකනය සහ නඩත්තු කිරීම සඳහා වඩාත් දැඩි අවශ්‍යතා ඇති විය හැක.

Binary systems
ද්වීමය පද්ධති

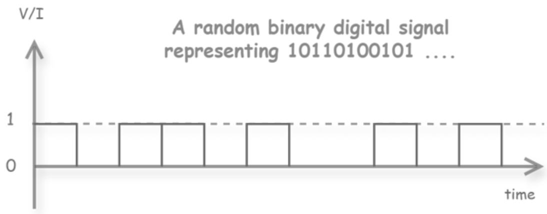
Due to these challenges, most digital systems use only two energy levels, one representing a current (or high voltage) and one representing no current (or low voltage).
මෙම අභියෝග හේතුවෙන්, බොහෝ අංකිත පද්ධති ශක්ති මට්ටම් දෙකක් පමණක් භාවිතා කරයි, එක් මට්ටමක් ධාරාවක් ඇති (හෝ අධි වෝල්ටීයතාවයක්) සහ අනෙක ධාරාවක් නොමැති (හෝ අඩු වෝල්ටීයතාවයක්) ලෙසින් නියෝජනය කරයි.

This binary system simplifies the design and operation of digital systems, making them more reliable and easier to implement.
මෙම ද්වීමය පද්ධතිය අංකිත පද්ධති සැලසුම් කිරීම සහ ක්‍රියාත්මක කිරීම සරල කරයි, ඒවා වඩාත් විශ්වාසදායක සහ ක්‍රියාත්මක කිරීමට පහසු කරයි.

But it may result in longer data transmission times due to the need for more bits to represent information.
නමුත් තොරතුරු නිරූපනය කිරීමට වැඩි බිටු ගණනක් අවශ්‍ය වීම නිසා එය දිගු දත්ත සම්ප්‍රේෂණ කාලයකට හේතු විය හැක.

Energy Efficiency
බල කාර්යක්ෂමතාව

Using only two levels reduces the energy consumption required to transmit and process data.
මට්ටම් දෙකක් පමණක් භාවිතා කිරීමෙන් දත්ත සම්ප්‍රේෂණය කිරීමට සහ සැකසීමට අවශ්‍ය බලශක්ති පරිභෝජනය අඩු වේ.



For instance, a small voltage level like 0.1 volts can effectively represent a binary 1 leading to low power consumption.
උදාහරණයක් ලෙස, වෝල්ට් 0.1 ක් වැනි කුඩා වෝල්ටීයතා මට්ටමක් මගින් ද්වීමය 1 ඵලදායි ලෙස නිරූපණය කළ හැකිය. එය අඩු බල පරිභෝජනයකට තුඩු දෙයි.

If computers could reliably handle multiple energy levels, the time to transmit data could be reduced. This is because each signal could carry more information at once, potentially speeding up data transfer.
පරිගණකවලට විශ්වාසදායක ලෙස බහු ශක්ති මට්ටම් හැසිරවිය හැකි නම්, දත්ත සම්ප්‍රේෂණය කිරීමට ගතවන කාලය අඩු කළ හැක. මන්ද, සෑම සංඥාවකටම එකවර වැඩි තොරතුරු ප්‍රමාණයක් රැගෙන යා හැකි අතර, දත්ත හුවමාරුව වේගවත් කළ හැකි බැවිනි.

The energy required to maintain and differentiate these levels would be higher compared to binary systems.
මෙම මට්ටම් පවත්වා ගැනීමට සහ වෙනස් කිරීමට අවශ්‍ය ශක්තිය ද්වීමය පද්ධති හා සසඳන විට වැඩි වේ.

Propagation Speed (v)
මාධ්‍යයක ප්‍රචාරණ වේගය

Propagation Speed is how fast the wave travels through a medium.
ප්‍රචාරණ වේගය යනු තරංගය මාධ්‍යයක් හරහා ගමන් කරන වේගයයි.

It's calculated by the product of frequency and wavelength.
එය සංඛ්‍යාතයේ සහ
තරංග ආයාමයේ ගුණිතයෙන් ගණනය කෙරේ.

v = fλ

v - speed
f - frequency
λ - wavelength

Electromagnetic waves, like light, travel at the speed of light, which is approximately 299,792 kilometers per second (km/s) or about 186,282 miles per second.
ආලෝකය වැනි විද්‍යුත් චුම්භක තරංග ආලෝකයේ වේගයෙන් ගමන් කරයි, එය ආසන්න වශයෙන් තත්පරයට කිලෝමීටර් (299,792 කි.මී./තත්පර) හෝ තත්පරයට සැතපුම් 186,282ක් පමණ වේ.

The propagation speed can vary depending on the type of wave and the properties of the medium it is traveling through.
තරංග වර්ගය සහ එය ගමන් කරන මාධ්‍යයේ ගුණ අනුව ප්‍රචාරණ වේගය වෙනස් විය හැක.

Bandwidth
කලාප පළල

Represents the capacity of the communication medium.
සන්නිවේදන මාධ්‍යයේ ධාරිතාව නිරූපණය කරයි.

It can be defined as the difference between the highest and lowest frequencies that a signal can have.
සංඥාවකට තිබිය හැකි ඉහළම සහ පහළම සංඛ්‍යාත අතර වෙනස ලෙස කලාප පළල අර්ථ දැක්විය හැක.

Bandwidth in Hertz

For example, if a signal ranges from 1 kHz to 3 kHz, its bandwidth is 2 kHz (3 kHz - 1 kHz).
උදාහරණයක් ලෙස, සංඥාවක් 1 kHz සිට 3 kHz දක්වා පරාසයක පවතී නම්, එහි කලාප පළල 2 kHz (3 kHz - 1 kHz) වේ.

It means that the signals transmitted within this channel are confined to a 2kHz frequency range and you can only fit signals within that 2 kHz range.
එයින් අදහස් වන්නේ මෙම නාලිකාව තුළ සම්ප්‍රේෂණය වන සංඥා 2kHz සංඛ්‍යාත පරාසයකට සීමා වී ඇති අතර එම 2 න්‍යු' පරාසය තුළ පමණක් සංඥා එය තුළ පැවතිය හැකි බවයි.

Narrower bandwidth
පටු කලාප පළල
A narrower bandwidth (Ex. 2 kHz) is often sufficient for transmitting basic audio signals like voice, but it might not support high-quality data or video signals.
කටහඬ වැනි මූලික ශ්‍රව්‍ය සංඥා සම්ප්‍රේෂණය කිරීම සඳහා පටු කලාප පළලක් (උදා: 2 kHz) ප්‍රමාණවත් වේ, නමුත් එය උසස් තත්ත්වයේ දත්ත හෝ වීඩියෝ සංඥා සඳහා සහාය නොදක්වයි.

Wider bandwidth
පුළුල් කලාප පළල
A wider bandwidth (Ex. 100 kHz or 1 MHz) allows you to transmit more complex information, like high-quality video or high-speed internet.
පුළුල් කලාප පළලක් (උදා: 100 kHz හෝ 1MHz) උසස් තත්ත්වයේ වීඩියෝ හෝ අධිවේගී අන්තර්ජාලය වැනි වඩාත් සංකීර්ණ තොරතුරු සම්ප්‍රේෂණය කිරීමට ඉඩ සලසයි.

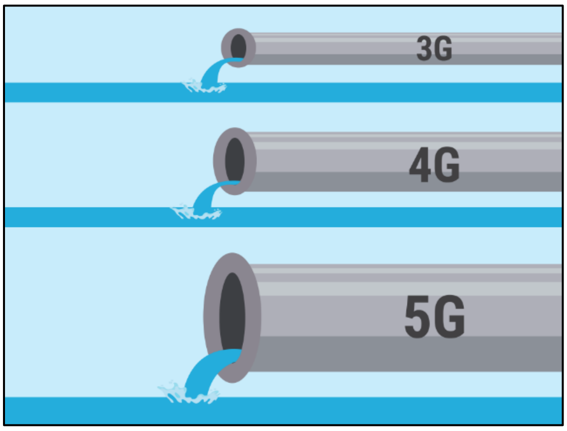
Higher the bandwidth, more data can be transmitted every second. Connection speed depends on this, not propagation speed if the medium is kept constant.
කලාප පළල වැඩි වන තරමට, සෑම තත්පරයකදීම වැඩි දත්ත ප්‍රමාණයක් සම්ප්‍රේෂණය කළ හැක. සන්නිවේදන මාධ්‍යය වෙනස් නොකර එකම මට්ටමක පවත්වා ගන්නේ නම්, සබැඳි වේගය රඳා පවතින්නේ මේ මත මිස ප්‍රචාරණ වේගය මත නොවේ.

Explanation of Bandwidth
කලාප පළල පැහැදිලි කිරීම

As an analogy, we can use an illustration of water flowing through two pipes.
උදාහරණයක් ලෙස, නළ දෙකක් හරහා ගලා යන ජලය පිළිබඳ නිදර්ශනයක් භාවිතා කළ හැකිය.

The diameter of the pipes will directly affect how much water can flow through the pipes.
නළවල විෂ්කම්භය නළ හරහා ජලය කොපමණ ප්‍රමාණයක් ගලා යා හැකිද යන්නට සෘජුවම බලපානු ඇත.

Let's assume that water flow at the same rate (speed) in both the pipes.
නළ දෙකෙහිම එකම අනුපාතයකින් (වේගයෙන්) ජලය ගලා යන්නෙ යැයි සිතමු.



But since the bottom pipe is wider than the top one, it is able to flow a lot more water at the same time, more than the top pipe.
නමුත් පහළ නළය ඉහළ නළයට වඩා පළල බැවින්, ඉහළ නළයට වඩා වැඩි ජල ප්‍රමාණයක් එකවර ගලා යාමට එයට හැකියාව ඇත.

So, the wider pipe will fill up the container a lot faster than the smaller pipe.
එබැවින්, පුළුල් නළය කුඩා නළයට වඩා වැඩි වේගයෙන් භාජනය පුරවනු ඇත.

Example – bandwidth in bits per second.

Let's say you were to download a video with a size of 4GB using two internet connections, one with 100Mbps and the other with 500Mbps but with the same speed.
ඔබ විසින් 100Mbps සහ 500Mbps සහිත නමුත් එකම වේගයකින් යුතු අන්තර්ජාල සම්බන්ධතා දෙකක් භාවිතා කරමින් 4GB ප්‍රමාණයේ වීඩියෝවක් බාගත කිරීමට යන බව සිතමු.

To calculate the amount of time it takes to download the video, we first need to convert the bandwidth and the video size into one unit.
වීඩියෝව බාගත කිරීමට ගතවන කාලය ගණනය කිරීම සඳහා, මුලින්ම කලාප පළල සහ වීඩියෝ පටයේ ප්‍රමාණය එක් ඒකකයකට පරිවර්තනය කළ යුතුය.

100Mbps / 8 = 12.5MBps
500Mbps / 8 = 62.5MBps

4GB = 4096MB

$T_{100mbps}$ = 4096MB / 12.5MBps
$T_{100mbps}$ = 4096~~MB~~ / 12.5~~MB~~ps
$T_{100mbps}$ = 327.68 seconds
$T_{100mbps}$ = 327.68 seconds / 60
$T_{100mbps}$ = <u>5.46 minutes</u>

$T_{500mbps}$ = 4096MB / 62.5MBps
$T_{500mbps}$ = 4096~~MB~~ / 62.5~~MB~~ps
$T_{500mbps}$ = 65.536 seconds
$T_{500mbps}$ = 65.536 seconds / 60
$T_{500mbps}$ = <u>1.09 minutes</u>

So, bandwidth increases the amount of data that can be sent per second. A higher bandwidth connection (500 Mbps) allows more bits to be transmitted simultaneously compared to a lower bandwidth connection (100 Mbps).
එබැවින්, කලාප පළල මගින් තත්පරයකට යැවිය හැකි දත්ත ප්‍රමාණය වැඩි කරයි. ඉහළ කලාප පළල සම්බන්ධතාවයක් මගින් (500 Mbps) අඩු කලාප පළලක් (100 Mbps) සමඟ සසඳන විට එකවර වැඩි බිටු සම්ප්‍රේෂණය කිරීමට ඉඩ සලසයි.

The frequency stays the same, but sending more bits in the same time boosts the data rate, making the connection seem faster.
සංඛ්‍යාතය එලෙසම පවතී. නමුත් එකවර බිටු වැඩි ප්‍රමාණයක් යැවීම දත්ත වේගය වැඩි කරන අතර එමගින් සම්බන්ධතාවය වේගවත් යැයි පෙනේ.

Factors Affecting Bandwidth
කලාප පළල කෙරෙහි බලපාන සාධක

- Communication medium
  සන්නිවේදන මාධ්‍යය
  - Fiber optic → Very high
    ප්‍රකාශ තන්තු → ඉතා ඉහළයි
  - Copper cable → Moderate
    තඹ කේබල් → මධ්‍යස්ථයි
  - Wireless → Depends on technology
    රැහැන් රහිත → තාක්ෂණය මත රඳා පවතී
- Channel width (frequency spectrum)
  මාධ්‍යය පළල (සංඛ්‍යාත වර්ණාවලිය)
- Network equipment
  ජාල උපකරණ
- Communication technology
  සන්නිවේදන තාක්ෂණය

Advantages of High Bandwidth
ඉහළ කලාප පළලක ඇති වාසි

- Faster downloads
  වේගවත් භාගත කිරීම්
- Better video streaming
  වඩා හොඳ වීඩියෝ ප්‍රවාහය
- Supports many users simultaneously
  එකවර පරිශීලකයින් විශාල සංඛ්‍යාවකට සහය දැක්වීම
- Faster file transfers
  වේගවත් ගොනු හුවමාරුව
- Better cloud services
  වඩා හොඳ වලාකුළු සේවා

Disadvantages of High Bandwidth
ඉහළ කලාප පළලක ඇති අවාසි

- Higher installation cost
  ඉහළ ස්ථාපන පිරිවැය
- More expensive networking equipment
  වඩා මිල අධික ජාල උපකරණ
- Greater infrastructure requirements
  වැඩි යටිතල පහසුකම් අවශ්‍යතා

Latency
ගුප්තතාවය

Data does not appear from the destination as soon as it is transmitted from the source. It takes time.
ප්‍රභවයේ සිට දත්ත සම්ප්‍රේෂණය කළ සැනින්ම එය ගමනාන්තය වෙත ළඟා නොවේ. ඒ සඳහා යම් කාලයක් ගත වේ.

Latency refers to the delay or time it takes for data to travel from the source to the destination across a network.
ගුප්තතාවය යනු ජාලයක් හරහා මූලාශ්‍රයේ සිට ගමනාන්තය දක්වා දත්ත ගමන් කිරීමට ගතවන ගුප්තතාවය හෝ කාලයයි.

It's typically measured in milliseconds (ms) and represents how quickly a system responds to a data request or action.
එය සාමාන්‍යයෙන් මිනිනු ලබන්නේ මිලි තත්පර (ms) වලින් වන අතර දත්ත ඉල්ලීමකට හෝ ක්‍රියාවකට පද්ධතියක් කෙතරම් ඉක්මනින් ප්‍රතිචාර දක්වයිද යන්න නිරූපණය කරයි.

Ways to measure latency
ගුප්තතාවය මැනීමේ ක්‍රම

Round-Trip Time (RTT)
වට-සංචාර කාලය

This is a common way to measure latency, which includes the time it takes for a signal to travel from the sender to the receiver and back again.
මෙය ගුප්තතාවය මැනීමේ පොදු ක්‍රමයකි, සංඥාවක් යවන්නාගේ සිට ග්‍රාහකයා වෙත ගමන් කිරීමට සහ නැවත ආපසු යාමට ගතවන කාලය මෙයට ඇතුළත් වේ.

One-Way Delay
Sometimes latency refers to the time it takes for data to travel from the sender to the receiver in one direction only.
සමහර අවස්ථාවලදී ගුප්තතාවය යන්නෙන් අදහස් කරන්නේ දත්ත යවන්නාගේ සිට ග්‍රාහකයා වෙත එක් දිශාවකට පමණක් ගමන් කිරීමට ගතවන කාලයයි.

Types of Latency
ගුප්තතාවයේ වර්ග

Propagation Delay
ප්‍රචාරණ ගුප්තතාවය

The time it takes for a signal to travel through the physical medium (like cables or air) from one point to another. It depends on the distance between the two points and the speed of the signal.
සංඥාවක් භෞතික මාධ්‍යය හරහා (රැහැන් හෝ වාතය වැනි) එක් ස්ථානයක සිට තවත් ස්ථානයකට ගමන් කිරීමට ගතවන කාලයයි. එය අන්ත දෙක අතර දුර සහ සංඥාවේ වේගය මත රඳා පවතී.

Transmission Delay
සම්ප්‍රේෂණ ගුප්තතාවය

The time it takes for the system to transmit all the bits of a message on to the communication channel. It depends on the size of the data and the bandwidth of the communication link.
පද්ධතියට පණිවිඩයක සියලුම බිටු සන්නිවේදන මාධ්‍යයට සම්ප්‍රේෂණය කිරීමට ගතවන කාලයයි. එය දත්තවල විශාලත්වය සහ සන්නිවේදන සම්බන්ධතාවයේ කලාප පළල මත රඳා පවතී.

Transmission delay = Data size/ Bandwidth

Uploading a 10MB video to Google Drive over a 2MBps connection has a transmission delay of 5 seconds.
2MBps සම්බන්ධතාවයක් හරහා Google Drive වෙත 10MB ක වීඩියෝවක් උඩුගත කිරීමේදී තත්පර 5ක සම්ප්‍රේෂණ ගුප්තතාවයක් ඇත.

Uploading that same file over a 10MBps connection has a transmission delay of 1 second.
එම ගොනුවම 10MBps සම්බන්ධතාවක් හරහා උඩුගත කිරීමේදී තප්පර 1ක සම්ප්‍රේෂණ ගුප්තතාවයක් ඇත.

Processing Delay
සැකසුම් ගුප්තතාවය

The time it takes for the network devices (like routers or switches) to process the data before forwarding it to the next node. This cause because of the error checking, routing and switching.
ජාල උපාංග වලට (රවුටර හෝ ස්විච වැනි) ඊළඟ නෝඩය වෙත දත්ත යොමු කිරීමට පෙර ඒවා සැකසීමට ගතවන කාලයයි. මෙය සිදුවන්නේ දෝෂ පරීක්ෂාව, මාර්ගගත කිරීම සහ මාරුකිරීම හේතුවෙනි.

Queuing Delay
පෝලිමේ ගුප්තතාවය

The time data packets spend waiting in queues (buffers) before they can be transmitted, especially when the network is congested.
දත්ත පැකට්ටු විශේෂයෙන්ම ජාලය තදබදයක් ඇති වී සම්ප්‍රේෂණය වීමට පෙර පෝලිම්වල (බෆර) රැඳී සිටින කාලයයි.

Simple analogy

Sending a parce / පාර්සලයක් යැවීම :

Propagation Delay / ප්‍රචාරණ ගුප්තතාවය
Time the truck spends driving to the destination.
ට්‍රක් රථය ගමනාන්තය වෙත ධාවනය කිරීමට ගතවන කාලය.

Transmission Delay / සම්ප්‍රේෂණ ගුප්තතාවය
Time taken to load all the parcels onto the truck.
සියලුම පාර්සල් ට්‍රක් රථයට පැටවීමට ගතවන කාලය.

Processing Delay / සැකසුම් ගුප්තතාවය
Time taken at checkpoints to inspect the parcel.
පාර්සලය පරීක්ෂා කිරීම සඳහා පරීක්ෂණ ස්ථානවලදී ගතවන කාලය.

Queuing Delay / පෝලිමේ ගුප්තතාවය
Time the truck waits in traffic.
ට්‍රක් රථය මාර්ග තදබදයට හසුවී රැඳී සිටින කාලය.

Factors Affecting Latency
ගුප්තතාවයට බලපාන සාධක

Distance
The further the data has to travel (e.g., from one country to another), the higher the latency due to the time it takes for the signal to propagate.
දත්තවලට ගමන් කිරීමට සිදුවන දුර වැඩි වන තරමට (උදා: එක් රටක සිට තවත් රටකට), සංඥාව ප්‍රචාරණය වීමට ගතවන කාලය හේතුවෙන් ගුප්තතාවයද වැඩි වේ.

Network Congestion
ජාල තදබදය

When a network is heavily used, data packets may get delayed in queues, increasing latency.
ජාලයක් දැඩි ලෙස භාවිතා කරන විට, දත්ත පැකට්ටු පෝලිම්වල ප්‍රමාද විය හැක,එමගින් ගුප්තතාවය වැඩි කරයි.

Routing and Switching

Each router or switch along the path takes a small processing delay, which can add up across many devices.

දත්ත ගමන් කරන මාර්ගය ඔස්සේ ඇති සෑම රවුටරයක්ම හෝ ස්විචයක්ම කුඩා සැකසුම් ගුප්තතාවයක් ලබා ගනියි, එය බොහෝ උපාංග හරහා එකතු විය හැක.

Signal Interference (in wireless networks)
සංඥා බාධා (රැහැන් රහිත ජාල වල)

Environmental factors like obstacles or other signals can cause retransmissions, increasing latency.

බාධක හෝ වෙනත් සංඥා වැනි පාරිසරික සාධක ගුප්තතාවය වැඩි කරමින් නැවත සම්ප්‍රේෂණයට හේතු විය හැක.

NOTE:

Latency is not a static value and can fluctuate over time depending on the current conditions of the network.

ගුප්තතාවය ස්ථිතික අගයක් නොවන අතර ජාලයේ වත්මන් තත්ත්වයන් අනුව කාලයත් සමඟ උච්චාවචනය විය හැක.

Advantages of Low Latency
අඩු ගුප්තතාවයකදී ඇති වාසි

- Faster web browsing
  වේගවත් වෙබ් අඩවි පිරික්සීම
- Better online gaming
  වඩා හොඳින් පරිගණක ක්‍රීඩා කිරීම
- Smooth video calls
  බාධාවකින් තොර වීඩියෝ ඇමතුම්
- Faster cloud applications
  වේගවත් වලාකුළු යෙදුම්
- Better remote desktop performance
  වඩා හොඳ දුරස්ථ වැඩතල කාර්ය සාධනය

Disadvantages of High Latency
ඉහළ ගුප්තතාවයකදී ඇති අවාසි

- Delayed responses
  ප්‍රමාද වූ ප්‍රතිචාර
- Lag in online games
  පරිගණක ක්‍රීඩා වලදී ඇතිවන ප්‍රමාදයන්
- Delay during video calls
  වීඩියෝ ඇමතුම් අතරතුර සිදුවන ප්‍රමාදයන්
- Slow loading of websites
  වෙබ් අඩවි පූරණය වීම මන්දගාමී වීම
- Poor user experience
  දුර්වල පරිශීලක අත්දැකීම

Examples

High bandwidth + High latency
ඉහළ කලාප පළල + ඉහළ ගුප්තතාව

- Satellite Internet
  චන්ද්‍රිකා අන්තර්ජාලය

Can transmit a lot of data, but with noticeable delay.

විශාල දත්ත ප්‍රමාණයක් සම්ප්‍රේෂණය කළ හැකි වුවද, පැහැදිලි ප්‍රමාදයක් පවතී.

High bandwidth + Low latency
ඉහළ කලාප පළල + අඩු ගුප්තතාව

- Local fiber-optic network
  දේශීය ප්‍රකාශ තන්තු ජාල

Ideal for gaming, streaming, and large file transfers.

පරිගණක ක්‍රීඩා, වීඩියෝ ප්‍රවාහය සහ විශාල ගොනු හුවමාරු කිරීම් සඳහා වඩාත්ම සුදුසුයි.

Low bandwidth + Low latency
අඩු කලාප පළල + අඩු ගුප්තතාව

- Older Ethernet connections
  පැරණි ඊතර්නෙට් සබැඳි

Quick responses but limited data capacity.

වේගවත් ප්‍රතිචාර ලැබුනද, දත්ත ධාරිතාව සීමිතය.

Low bandwidth + High latency
අඩු කලාප පළල + ඉහළ ගුප්තතාව

- Congested mobile network
  තදබදය සහිත ජංගම දුරකථන ජාල

Slow transfers and delayed responses.

මන්දගාමී දත්ත හුවමාරුව සහ ප්‍රමාද වූ ප්‍රතිචාර දැකගත හැක.

Throughput

Throughput refers to the actual amount of data that is successfully transmitted over a network or communication channel in a given period of time.

Throughput එක යනු යම් කාල සීමාවක් තුළ ජාලයක් හෝ සන්නිවේදන නාලිකාවක් හරහා සාර්ථකව සම්ප්‍රේෂණය වන සත්‍ය දත්ත ප්‍රමාණයයි.

It is typically measured in bits per second (bps), megabits per second (Mbps), or gigabits per second (Gbps).

එය සාමාන්‍යයෙන් මනිනු ලබන්නේ තත්පරයකට බිටු (bps), තත්පරයට මෙගාබිටු (Mbps) හෝ තත්පරයට ගිගාබිටු (Gbps) වලින් ය.

While bandwidth is the maximum capacity of the channel (how much data it could theoretically handle), throughput is the realized data rate, the amount of data that is successfully transferred.

කලාප පළල යනු නාලිකාවේ උපරිම ධාරිතාව වන අතර (න්‍යායාත්මකව හැසිරවිය හැකි දත්ත ප්‍රමාණය), throughput එක යනු සාක්ෂාත් කර ගත් දත්ත අනුපාතයයි, එනම් සාර්ථකව හුවමාරු කරන දත්ත ප්‍රමාණයයි.

Throughput is lower than the bandwidth
Throughput එක කලාප පළලට වඩා අඩුය.

1. Because of the factors affecting Latency
   ගුප්තතාවයට බලපාන සාධක නිසා

2. When data packets are lost or need to be re-sent, this decreases the throughput.
   දත්ත පැකට් නැති වූ විට හෝ නැවත යැවීමට අවශ්‍ය වූ විට, එමගින් throughput එක අඩු කරයි.

Example

Imagine you have a network connection with a theoretical bandwidth of 100 Mbps. However, due to these reasons, the actual throughput may only be 70 Mbps.

ඔබට න්‍යායාත්මකව 100Mbps කලාප පළලක් සහිත ජාල සම්බන්ධතාවයක් ඇතැයි සිතන්න. කෙසේ වෙතත් මෙම හේතූන් නිසා සැබෑ throughput එක 70 Mbps පමණක් විය හැකිය.

This means that while the connection can potentially handle 100 million bits per second, in reality, only 70 million bits are successfully being transmitted every second.

මෙයින් අදහස් කරන්නේ සම්බන්ධතාවයට තත්පරයකට බිටු මිලියන 100 ක් හැසිරවිය හැකි නමුත්, සැබැවින්ම සෑම තත්පරයකදීම සාර්ථකව සම්ප්‍රේෂණය වන්නේ බිටු මිලියන 70 ක් පමණක් බවයි.

NOTE:

Throughput is not a static value and can fluctuate over time depending on the current conditions of the network.

Throughput එක ස්ථිතික අගයක් නොවන අතර ජාලයේ වත්මන් තත්ත්වයන් අනුව කාලයත් සමඟ උච්චාවචනය විය හැක.

Bandwidth vs. Throughput

Aspect	Bandwidth	Throughput
Definition	Capability	Reality
Measurement	Hz & bps	bps
Type	Theoretical	Actual
Fluctuations	Stable	Variable

Transmission Impairments
සම්ප්‍රේෂණ බාධා

Unwanted changes that occur in a signal as it travels through a transmission medium.
සංඥාවක් සම්ප්‍රේෂණ මාධ්‍යයක් හරහා ගමන් කිරීමේදී සිදුවන අනවශ්‍ය වෙනස්වීම් වේ.

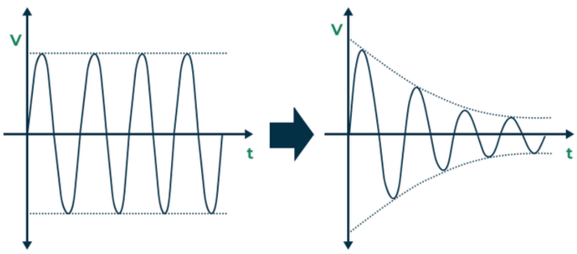
Impairments can reduce the quality of the transmitted signal and may cause errors during data communication.
මෙම දෝෂ හේතුවෙන් සම්ප්‍රේෂණය වන සංඥාවේ ගුණාත්මකභාවය අඩු විය හැකි අතර දත්ත සන්නිවේදනයේදී වැරදි ඇති විය හැක.

Mainly occur due to the physical properties of the transmission medium, electromagnetic interference, and environmental conditions.
ප්‍රධාන වශයෙන් සම්ප්‍රේෂණ මාධ්‍යයේ භෞතික ලක්ෂණ, විද්‍යුත් චුම්භක බාධා කිරීම් සහ පාරිසරික තත්ත්වයන් හේතුවෙන් මේවා සිදු වේ.

Attenuation
හායනය

The gradual reduction in the strength (amplitude) of a signal as it travels through a transmission medium.
සංඥාවක් සම්ප්‍රේෂණ මාධ්‍යයක් හරහා ගමන් කිරීමේදී එහි ප්‍රබලතාවය (විස්තාරය) ක්‍රමයෙන් අඩු වීම.

Attenuation is measured in decibels (dB).
හායනය ඩෙසිබෙල් (dB) මඟින් මනිනු ලබයි.



Causes of Attenuation / හායනයට හේතු

- Long transmission distance.
  දිගු සම්ප්‍රේෂණ දුර.
- Resistance of the transmission medium.
  සම්ප්‍රේෂණ මාධ්‍යයේ ප්‍රතිරෝධය.
- Signal absorption by the transmission medium.
  සම්ප්‍රේෂණ මාධ්‍යය මඟින් සංඥා අවශෝෂණය කරගැනීම.
- Signal scattering and leakage.
  සංඥා විසිරීම සහ කාන්දු වීම.

Effects of Attenuation
හායනය වීමේ බලපෑම්

- Weakens the received signal.
  ලැබෙන සංඥාව දුර්වල කරයි.
- Increases the probability of transmission errors.
  සම්ප්‍රේෂණ දෝෂ ඇතිවීමේ සම්භාවිතාව වැඩි කරයි.
- Reduces the maximum transmission distance.
  උපරිම සම්ප්‍රේෂණ දුර ප්‍රමාණය සීමා කරයි.

Methods to Reduce Attenuation
හායනය අවම කරගැනීමේ ක්‍රම

- Use repeaters or regenerators.
  රිපීටර් හෝ පුනර්ජනක භාවිත කිරීම.
- Use amplifiers (for analog signals).
  ඇම්ප්ලිෆයර් භාවිත කිරීම (ප්‍රතිසම සංඥා සඳහා).
- Use low-loss transmission media such as optical fiber.
  ඔප්ටිකල් ෆයිබර් වැනි අවම හානියක් සිදුවන සම්ප්‍රේෂණ මාධ්‍ය භාවිත කිරීම.

Examples / උදාහරණ:
- A Wi-Fi signal becomes weaker as the distance from the router increases.
  රවුටරයේ සිට ඇති දුර වැඩි වන විට Wi-Fi සංඥාව දුර්වල වීම.

Distortion
විකෘති වීම

The change in the shape or form of a signal as it travels through a transmission medium.
සංඥාවක් සම්ප්‍රේෂණ මාධ්‍යයක් හරහා ගමන් කිරීමේදී එහි හැඩය හෝ ස්වරූපය වෙනස් වීම.

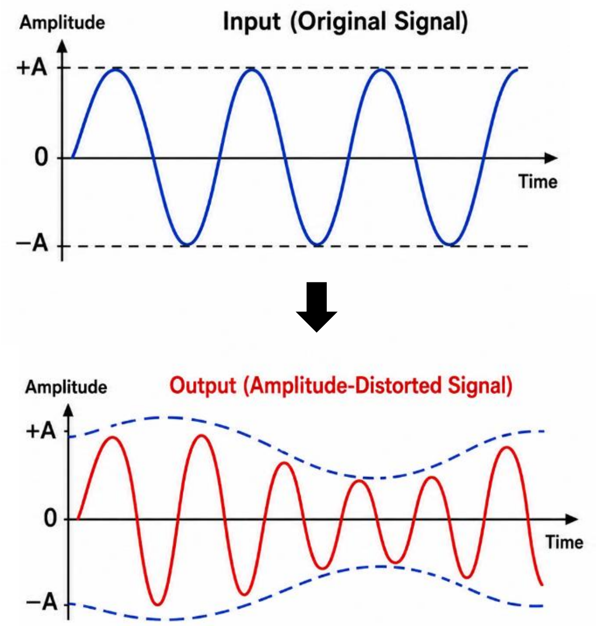
The standard types of distortion taught in data communication are:
දත්ත සන්නිවේදනයේදී උගන්වනු ලබන සම්මත විකෘති වීම් වර්ග වර්ගීකරණය පහත පරිදි වේ:

1. Frequency (Amplitude) Distortion
   සංඛ්‍යාත (විස්තාර) විකෘති වීම
2. Delay (Phase) Distortion
   ප්‍රමාද (කලා) විකෘති වීම
3. Harmonic (Non-linear) Distortion
   හාර්මොනික් (රේඛීය නොවන) විකෘති වීම

ictfromabc.com

1.Frequency (Amplitude) Distortion
සංඛ්‍යාත (විස්තාර) විකෘති වීම

Different frequency components of a signal are attenuated by different amounts.
සංඥාවක අඩංගු විවිධ සංඛ්‍යාත සංරචක, එකිනෙකට වෙනස් ප්‍රමාණ වලින් හායනය වීමකට ලක් වේ.



Causes / හේතු

- Limited bandwidth of the transmission medium.
  සම්ප්‍රේෂණ මාධ්‍යයේ පවතින සීමිත කලාප පළල.
- Frequency-dependent characteristics of communication devices.
  සන්නිවේදන උපාංගවල පවතින, සංඛ්‍යාතය මත පදනම් වන ලක්ෂණ.

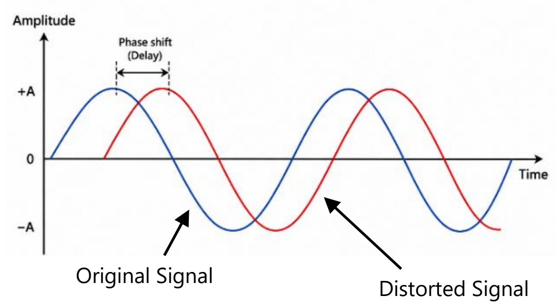
Effects / බලපෑම්

- Changes the signal amplitude.
  සංඥාවේ විස්තාරය වෙනස් කරයි.
- Alters the shape of the received signal.
  ලැබෙන සංඥාවේ හැඩය වෙනස් කරයි.
- Reduces signal quality.
  සංඥාවේ ගුණාත්මකභාවය අඩු කරයි.

Examples / උදාහරණ:
- Voice signals become distorted during transmission.
  සම්ප්‍රේෂණයේදී කටහඬ සංඥා විකෘති වීම.
- Audio systems produce uneven sound levels at different frequencies.
  ශ්‍රව්‍ය පද්ධති මඟින් විවිධ සංඛ්‍යාතයන්හිදී අසමාන ශබ්ද මට්ටම් නිපදවීම.

2.Delay (Phase) Distortion
ප්‍රමාද (කලා) විකෘති වීම

Different frequency components of a signal travel at different speeds and arrive at the receiver at different times.
සංඥාවක අඩංගු විවිධ සංඛ්‍යාත සංරචක එකිනෙකට වෙනස් වේගයන්ගෙන් ගමන් කිරීම නිසා, ඒවා ප්‍රතිග්‍රාහකයා වෙත එකිනෙකට වෙනස් කාලවලදී ළඟා වීමයි.



Causes / හේතු

- Non-uniform characteristics of the transmission medium.
  සම්ප්‍රේෂණ මාධ්‍යයේ පවතින ඒකාකාරී නොවන ලක්ෂණ.

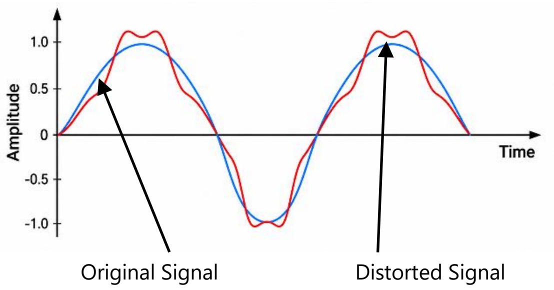
Effects / බලපෑම්

- Changes the signal shape.
  සංඥාවේ හැඩය වෙනස් කරයි.
- Causes overlapping of digital pulses.
  ඩිජිටල් ස්පන්ද එකිනෙක මත අතිච්ඡාදනය වීම (එක මත එක වැටීම) සිදු කරයි.
- Increases transmission errors.
  සම්ප්‍රේෂණ දෝෂ වැඩි කරයි.

Examples / උදාහරණ:
- Digital signals become deformed during long-distance transmission.
  දිගු දුර සම්ප්‍රේෂණයේදී අංකිත සංඥා විකෘති වීම හෝ හැඩය වෙනස් වීම.
- High-speed communication links experience pulse spreading.
  අධිවේගී සන්නිවේදන සබැඳි තුළ ස්පන්ද පැතිරීමේ තත්ත්වයන් ඇති වීම.

3.Harmonic (Non-linear) Distortion
හාර්මොනික් (රේඛීය නොවන) විකෘති වීම

Additional frequency components (harmonics) are generated due to the non-linear operation of communication devices.
සන්නිවේදන උපාංගවල පවතින රේඛීය නොවන ක්‍රියාකාරීත්වය හේතුවෙන්, මුල් සංඥාවට අමතරව තවත් නව සංඛ්‍යාත සංරචක ජනනය වීමයි.



Causes / හේතු

- Overloaded communication equipment.
  සන්නිවේදන උපකරණ අධිපූරණය වීම.
- Faulty electronic components.
  දෝෂ සහිත ඉලෙක්ට්‍රොනික සංරචක

Effects / බලපෑම්

- Introduces unwanted harmonic frequencies.
  අනවශ්‍ය හාර්මොනික් සංඛ්‍යාතයන් සංඥාවට ඇතුළත් කරයි.
- Alters the original signal.
  මුල් සංඥාව වෙනස් කරයි.
- Reduces communication quality.
  සන්නිවේදනයේ ගුණාත්මකභාවය අඩු කරයි.

Examples / උදාහරණ:

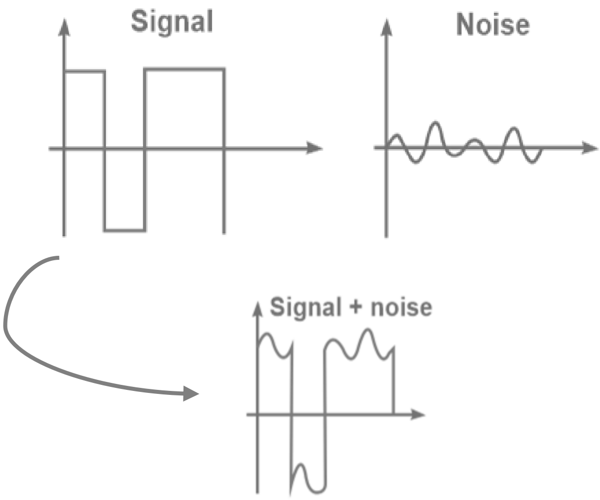
- Audio amplifiers producing distorted sound.
  ශ්‍රව්‍ය වර්ධක මඟින් විකෘති වූ ශබ්ද නිපදවීම.
- Communication equipment generating unwanted harmonic signals.
  සන්නිවේදන උපකරණ මඟින් අනවශ්‍ය හාර්මොනික් සංඥා ජනනය කිරීම.

Methods to Reduce Distortion
විකෘති වීම අවම කරගැනීමේ ක්‍රම

- Use transmission media with adequate bandwidth.
  ප්‍රමාණවත් කලාප පළලක් සහිත සම්ප්‍රේෂණ මාධ්‍ය භාවිත කිරීම.
- Use equalizers to compensate for signal distortion.
  සංඥා විකෘති වීම් මඟහරවා ගැනීමට equalizers භාවිත කිරීම.
- Use high-quality linear communication equipment.
  උසස් තත්ත්වයේ රේඛීය සන්නිවේදන උපකරණ භාවිත කිරීම.
- Keep communication devices properly calibrated.
  සන්නිවේදන උපාංග නිසි පරිදි ක්‍රමාංකනය කර තබා ගැනීම.
- Reduce excessive transmission distance where possible.
  හැකි සෑම විටම අධික සම්ප්‍රේෂණ දුර ප්‍රමාණයන් අවම කිරීම.
- Operate communication devices within their recommended limits.
  සන්නිවේදන උපාංග ඒවායේ නිර්දේශිත සීමාවන් තුළ ක්‍රියාත්මක කිරීම.

Noise
ඝෝෂාව

Any unwanted electrical or electromagnetic signal that is added to the original signal during transmission.
සම්ප්‍රේෂණයේදී මුල් සංඥාවට එකතු වන ඕනෑම ආකාරයක අනවශ්‍ය විද්‍යුත් හෝ විද්‍යුත් චුම්භක සංඥාවකි.



1.Thermal Noise / තාපජ ඝෝෂාව

Random electrical noise generated by the movement of electrons inside electronic components.
ඉලෙක්ට්‍රොනික සංරචක තුළ ඇති ඉලෙක්ට්‍රෝනවල චලිතය හේතුවෙන් අහඹු ලෙස ජනනය වන විද්‍යුත් ඝෝෂාවයි.

Causes / හේතු

- Thermal agitation of electrons.
  ඉලෙක්ට්‍රෝනවල තාපජ කැළඹීම

Effects / බලපෑම්

- Adds random noise to the signal.
  සංඥාවට අහඹු ඝෝෂාවක් එකතු කරයි.
- Reduces signal quality.
  සංඥාවේ ගුණාත්මකභාවය අඩු කරයි.

Examples / උදාහරණ

- Background noise in radio receivers.
  රේඩියෝ ප්‍රතිග්‍රාහකවල පසුබිමෙන් ඇසෙන සිහින් සලකුණු හඬ ("හිස්" හඬ).

2.Induced (Interference) Noise
ප්‍රේරිත ඝෝෂාව

Unwanted electrical noise caused by electromagnetic or radio frequency signals from external sources.
බාහිර ප්‍රභවයන්ගෙන් පැමිණෙන විද්‍යුත් චුම්භක හෝ රේඩියෝ සංඛ්‍යාත සංඥා හේතුවෙන් ඇතිවන අනවශ්‍ය විද්‍යුත් ඝෝෂාවයි.

The three common types are:
මෙහි පොදු වර්ග තුනකි:

a. Electromagnetic Interference (EMI)
   විද්‍යුත් චුම්භක බාධා කිරීම්
b. Radio Frequency Interference (RFI)
   රේඩියෝ සංඛ්‍යාත බාධා කිරීම්
c. Crosstalk / ක්‍රොස්ටෝක්

a) Electromagnetic Interference (EMI)
විද්‍යුත් චුම්භක බාධා කිරීම්

Electromagnetic noise caused by nearby electrical or electronic equipment.
අසල ඇති විද්‍යුත් හෝ ඉලෙක්ට්‍රොනික උපකරණ මඟින් ඇති කරන විද්‍යුත් චුම්භක ඝෝෂාවයි.

Causes / හේතු

- Electric motors. / විද්‍යුත් මෝටර්
- Power lines. / අධි බලැති විදුලි රැහැන්.
- Fluorescent lamps. / ප්‍රතිදීප්ත ලාම්පු.

Effects / බලපෑම්

- Introduces unwanted electromagnetic signals.
  අනවශ්‍ය විද්‍යුත් චුම්භක සංඥා ඇතුළත් කරයි.
- Reduces communication quality.
  සන්නිවේදනයේ ගුණාත්මකභාවය අඩු කරයි.

b) Radio Frequency Interference (RFI)
රේඩියෝ සංඛ්‍යාත බාධා කිරීම්

RFI is caused by radio frequency signals emitted by nearby wireless transmitters.
අසල ඇති රැහැන් රහිත සම්ප්‍රේෂක මඟින් නිකුත් කරන රේඩියෝ සංඛ්‍යාත සංඥා නිසා RFI ඇති වේ.

Causes / හේතු

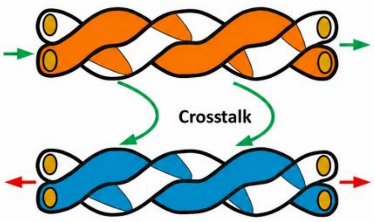
- Television transmitters.
  රූපවාහිනී සම්ප්‍රේෂක.
- Mobile phone base stations.
  ජංගම දුරකථන සන්නිවේදන කුළුණු

Effects / බලපෑම්

- Corrupts the transmitted signal.
  සම්ප්‍රේෂණය වන සංඥාව විකෘති/හානි කරයි.
- Increases transmission errors.
  සම්ප්‍රේෂණ දෝෂ වැඩි කරයි.

c) Crosstalk / ක්‍රොස්ටෝක්

Crosstalk occurs when a signal in one communication channel unintentionally interferes with another nearby channel.
එක් සන්නිවේදන නාලිකාවක ඇති සංඥාවක්, නොදැනුවත්වම අසල ඇති වෙනත් නාලිකාවකට බාධා කරන විට ක්‍රොස්ටෝක් ඇති වේ.



Causes / හේතු

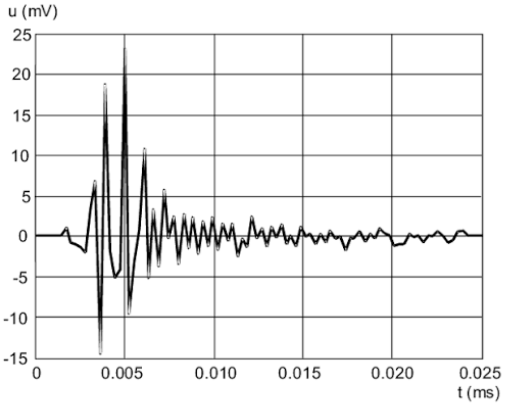
- Closely spaced communication cables.
  සන්නිවේදන කේබල් එකිනෙකට ඉතා සමීපව පිහිටීම.
- Poor cable shielding.
  කේබල්වල ආවරණය දුර්වල වීම.

Effects / බලපෑම්

- Reduces signal quality.
  සංඥාවේ ගුණාත්මකභාවය අඩු කරයි.

Impulse Noise

Impulse noise consists of sudden, high-amplitude spikes that occur for a very short duration.
ඉතා කෙටි කාලසීමාවක් තුළ ඇති වන, හදිසි සහ ඉහළ විස්තාරයකින් යුත් සංඥා කූරු හෝ උච්චාවචනයන් ය.



Causes / හේතු

- Lightning / අකුණු ගැසීම
- Switching of electrical equipment.
  විද්‍යුත් උපකරණ ක්‍රියාත්මක කිරීම සහ අක්‍රිය කිරීම.
- Power line disturbances.
  විදුලි රැහැන් පද්ධතිවල සිදුවන හදිසි බාධා කිරීම්.

Effects / බලපෑම්

- Corrupts transmitted data.
  සම්ප්‍රේෂණය වන දත්ත විකෘති/හානි කරයි.
- Causes burst errors.
  පිපිරුම් දෝෂ

Examples / උදාහරණ

- Noise caused by lightning strikes.
  අකුණු වැදීම් හේතුවෙන් සන්නිවේදන මාර්ගවල ඇති වන ඝෝෂාව.

Methods to Reduce Noise
ඝෝෂාව අවම කරගැනීමේ ක්‍රම

- Use shielded transmission media.
  ආවරණය කරන ලද සම්ප්‍රේෂණ මාධ්‍ය භාවිත කිරීම.
- Use twisted pair or optical fiber cables.
  ඇඹරුණු යුගල කේබල් හෝ ඔප්ටිකල් ෆයිබර් කේබල් භාවිත කිරීම.
- Keep communication cables away from power cables.
  සන්නිවේදන කේබල් , විදුලි රැහැන් වලින් ඈත් කර තැබීම.
- Use proper grounding.
  නිසි පරිදි භූගත කිරීම් සිදු කිරීම.
- Use filters to reduce unwanted signals.
  අනවශ්‍ය සංඥා ඉවත් කිරීම සඳහා පෙරහන් භාවිත කිරීම

SNR (Signal-to-Noise Ratio)

Engineers measure signal quality using SNR (Signal-to-Noise Ratio). It compares the strength of the "Good Data" to the "Bad Noise"
ඉංජිනේරුවන් සංඥා ගුණාත්මකභාවය මැනීම සඳහා (SNR) සංඥාව සහ ඝෝෂාව අතර අනුපාතය භාවිතා කරයි. එය “හොඳ දත්ත“ සහ
“නරක ඝෝෂාව“ අතර ශක්තිය සංසන්දනය කරයි.

$$\text{SNR} = \frac{\text{Signal Power}}{\text{Noise Power}}$$

SNR is commonly expressed in decibels (dB).
SNR සාමාන්‍යයෙන් ඩෙසිබෙල් (dB) ඒකකයෙන් ප්‍රකාශ කරනු ලබයි.

A higher SNR indicates better signal quality and less noise.
ඉහළ SNR අගයකින් පෙන්නුම් කරන්නේ වඩා හොඳ සංඥා ගුණාත්මකභාවයක් සහ අඩු ඝෝෂාකාරීත්වයක් පවතින බවයි.

A lower SNR indicates poorer signal quality and more noise.
පහළ SNR අගයකින් පෙන්නුම් කරන්නේ බාල හෝ දුර්වල සංඥා ගුණාත්මකභාවයක් සහ වැඩි ඝෝෂාකාරීත්වයක් පවතින බවයි.

Signal Encoding Schemes
සංඥා කේතන යෝජනා ක්‍රම

Signal encoding schemes are techniques used to represent digital information as electrical signals that can be transmitted over communication channels.
සංඥා කේතන ක්‍රමවේද යනු සන්නිවේදන නාලිකා ඔස්සේ සම්ප්‍රේෂණය කළ හැකි විද්‍යුත් සංඥා ලෙස ඩිජිටල් තොරතුරු නිරූපණය කිරීමට භාවිතා කරන ශිල්පීය ක්‍රම වේ.

These schemes are essential for converting digital data into a physical signal form for transmission and for helping the receiver recover the original data correctly.
මෙම ක්‍රමවේදයන්, ඩිජිටල් දත්ත සම්ප්‍රේෂණය සඳහා භෞතික සංඥා ස්වරූපයකට පරිවර්තනය කිරීමට සහ ලබන්නා විසින් මුල් දත්ත නිවැරදිව නැවත ලබා ගැනීමට උපකාරී වීම සඳහා අත්‍යවශ්‍ය වේ.

The need for signal coding systems
සංඥා කේතන පද්ධතිවල අවශ්‍යතාවය

Data Representation
දත්ත නිරූපණය

Converts data into a format suitable for transmission over a communication medium. Ensures that data can be accurately represented and transmitted as electrical, optical, or radio signals.
සන්නිවේදන මාධ්‍යයක් හරහා සම්ප්‍රේෂණය කිරීමට සුදුසු ආකෘතියකට දත්ත පරිවර්තනය කරයි. විද්‍යුත්, ප්‍රකාශ හෝ ගුවන්විදුලි සංඥා ලෙස දත්ත නිවැරදිව නිරූපණය කර සම්ප්‍රේෂණය කළ හැකි බව සහතික කරයි.

Error Detection and Correction
දෝෂ හඳුනාගැනීම සහ නිවැරදි කිරීම

Adds redundancy or uses algorithms to detect and correct errors during transmission. Improves reliability by ensuring data integrity despite noise or interference.
සම්ප්‍රේෂණය අතරතුර දෝෂ හඳුනා ගැනීමට සහ නිවැරදි කිරීමට අතිරික්ත එකතු කරයි හෝ ඇල්ගොරිතම භාවිතා කරයි. ඝෝෂාව හෝ බාධා කිරීම් නොතකා දත්ත අඛණ්ඩතාව සහතික කිරීම මගින් විශ්වසනීයත්වය වැඩි දියුණු කරයි.

Synchronization
සමමුහුර්තකරණය

Helps maintain timing between the transmitter and receiver. Ensures that the receiver correctly interprets the timing of data bits, preventing errors.
ග්‍රාහකයා දත්ත බිටු වල කාලය නිවැරදිව අර්ථකථනය කරන බව සහතික කරයි, දෝෂ වළක්වයි. සම්ප්‍රේෂකය සහ ග්‍රාහකය අතර කාලය පවත්වා ගැනීමට උපකාරී වේ.

Bandwidth Efficiency
කලාප පළල කාර්යක්ෂමතාව

Optimizes the use of available bandwidth, maximizing the amount of data transmitted within a given frequency range, improving overall efficiency.
පවතින කලාප පළල භාවිතය ප්‍රශස්ත කරමින්
දී ඇති සංඛ්‍යාත පරාසයක් තුළ සම්ප්‍රේෂණය වන දත්ත ප්‍රමාණය උපරිම කරයි, සමස්ත කාර්යක්ෂමතාවය වැඩි දියුණු කරයි.

Signal Quality
සංඥා ගුණාත්මකභාවය

Reduces distortion and noise in the signal, enhancing the clarity and quality of the transmitted signal, leading to better reception and fewer errors.
සංඥාවෙහි විකෘති කිරීම් සහ ඝෝෂාව අඩු කරමින් සම්ප්‍රේෂණය කරන ලද සංඥාවේ පැහැදිලි බව සහ ගුණාත්මකභාවය වැඩි දියුණු කරයි, වඩා හොඳ ග්‍රහණය කිරීමක් සහ අඩු දෝෂ ඇති කරයි.

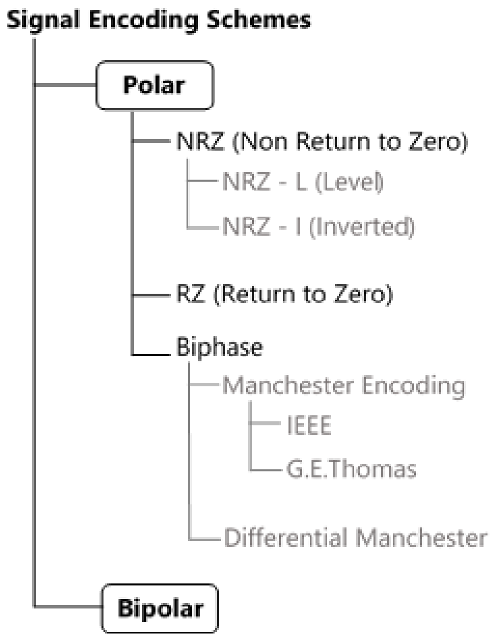
Compatibility
අනුකූලතාව

Ensures that data can be transmitted and understood by different systems and devices facilitating interoperability between various technologies and standards.
විවිධ පද්ධති සහ උපාංග මගින් දත්ත සම්ප්‍රේෂණය කර තේරුම් ගත හැකි බව සහතික කරමින්. විවිධ තාක්ෂණයන් සහ ප්‍රමිතීන් අතර අන්තර් ක්‍රියාකාරීත්වයට පහසුකම් සපයයි.

Reduction of Interference
බාධා කිරීම් අවම කිරීම

Proper coding methods help minimize the effect of external noise and interference on the transmitted signal. This improves the accuracy and stability of communication.
නිසි කේතන ක්‍රම මගින් බාහිර ශබ්දය සහ බාධා සංඥාවට ඇති කරන බලපෑම අවම කරයි. මෙය සන්නිවේදනයේ නිවැරදිතාවය සහ ස්ථායීතාවය වැඩි දියුණු කරයි.

Types of Signal encoding schemes
සංඥා කේතන යෝජනා ක්‍රම වර්ග



Fundamental knowledge

Voltage / Potential difference
වෝල්ටීයතාව / විභව අන්තරය

Voltage is a measure of the electrical potential energy difference between two points in a circuit.
වෝල්ටීයතාව යනු පරිපථයක ලක්ෂ්‍ය දෙකක් අතර විද්‍යුත් විභව ශක්ති වෙනසෙහි මිනුමක් වේ.

A higher voltage means a greater difference in potential energy, which can drive a larger current.
වැඩි වෝල්ටීයතාවයක් යනු විභව ශක්තියේ විශාල වෙනසක් වන අතර එමඟින් විශාල ධාරාවක් ධාවනය කළ හැකිය.

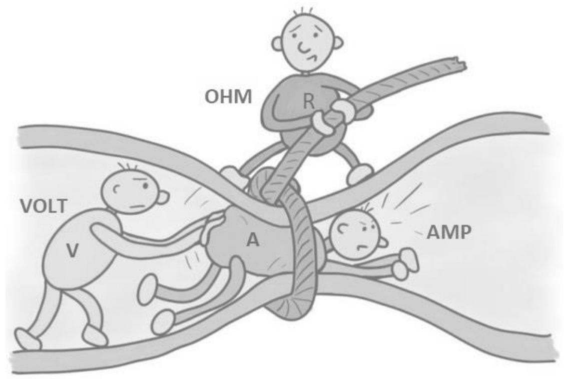
Current
ධාරාව

Current is a measure of the speed of flow of electric charge (electrons).
ධාරාව යනු විද්‍යුත් ආරෝපණ (ඉලෙක්ට්‍රෝන) ගලායාමේ සීඝ්‍රතාවයේ මිනුමක් වේ.

A higher current means more electric charge (electrons) is flowing per unit time.
වැඩි ධාරාවක් යනු ඒකක කාලයකදී වැඩි විද්‍යුත් ආරෝපණයක් (ඉලෙක්ට්‍රෝන) ගලා යන බවයි.

V = IR (Ohm's law)

V – Voltage (Volts/V)
I – Current (Ampere/A)
R – Resistance (Ohm/Ω)



How voltage and current work together in data transmission
දත්ත සම්ප්‍රේෂණයේදී වෝල්ටීයතාවය සහ ධාරාව එක්ව ක්‍රියා කරන ආකාරය

Binary 1
When transmitting a 1, the system applies a high voltage. In turn, this high voltage causes a higher current flow through the circuit.
1 සම්ප්‍රේෂණය කරන විටදී, පද්ධතිය ඉහළ වෝල්ටීයතාවයක් යොදයි. එම නිසා, මෙම ඉහළ වෝල්ටීයතාවය පරිපථය හරහා වැඩි ධාරා ප්‍රවාහයක් ඇති කරයි.

Binary 0
When transmitting a 0, the system applies a low voltage or no voltage. This results in a lower current flow through the circuit or no current at all.
0 සම්ප්‍රේෂණය කරන විටදී, පද්ධතිය අඩු වෝල්ටීයතාවයක් යොදයි හෝ කිසිම වෝල්ටීයතාවයක් නොයොදයි. මෙමගින් පරිපථය හරහා අඩු ධාරාවක් ගලා යාමක් හෝ කිසිම ධාරාවක් ගලා නොයෑමක් සිදු වේ.

The choice of voltage level affects signal transmission quality. Higher voltages are useful for long-distance transmission, while lower voltages are suitable for short distances and reducing power consumption.
වෝල්ටීයතා මට්ටම තෝරා ගැනීම, සංඥා සම්ප්‍රේෂණයේ ගුණාත්මකභාවයට බලපායි. දිගු දුර සම්ප්‍රේෂණය සඳහා ඉහළ වෝල්ටීයතාවන් ප්‍රයෝජනවත් වන අතර, කෙටි දුර ප්‍රමාණයන් සඳහා සහ බලශක්ති පරිභෝජනය අඩු කිරීම සඳහා අඩු වෝල්ටීයතාවන් සුදුසු වේ.

Non-Return to Zero
නැවත නොඑන ශුන්‍ය

This is a digital line coding technique that converts binary data, such as **0s and 1s**, into electrical signal patterns. In NRZ, the signal does not return to zero between bits; it stays at a selected voltage level for the full bit interval and changes only when required by
the data pattern.
Non-Return to Zero යනු 0 සහ 1 වැනි ද්විමය දත්ත විදුත් සංඥා රටාවන් බවට පරිවර්තනය කරන ඩිජිටල් රේඛා කේතන ක්‍රමයකි. NRZ හිදී, සංඥාව බිටු අතර ශූන්‍ය මට්ටමට නැවත නොඑන අතර, සම්පූර්ණ බිටු කාල පරතරය තුළ තෝරාගත් වෝල්ටීයතා මට්ටමක පවතින අතර දත්ත රටාවට අවශ්‍ය විට පමණක් වෙනස් වේ.

1. NRZ – L

(Non-Return to Zero – Level)

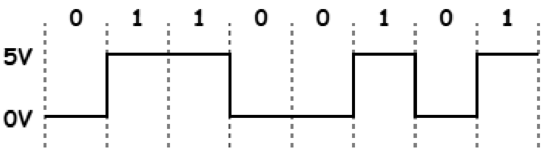
In NRZ – L, two different voltages for 0 and 1 bits are used to represent data and they remain constant during a bit interval.
NRZ – L හිදී, දත්ත නිරූපණය කිරීමට 0 සහ 1 බිටු සඳහා එකිනෙකට වෙනස් වෝල්ටීයතා දෙකක් භාවිතා කරන අතර ඒවා බිටු පරතරය තුළ නියතව පවතී.

There is no strict standard to decide which voltage level represents **1** or **0**. Therefore, the signal may start at either a high or low voltage level, depending on the first bit to be transmitted and the system design.
1 හෝ 0 නිරූපණය කරන්නේ කුමන වෝල්ටීයතා මට්ටමද යන්න තීරණය කරන දැඩි ප්‍රමිතියක් නොමැත. එබැවින්, සම්ප්‍රේෂණය කළ යුතු පළමු බිටුව සහ පද්ධති සැලසුම අනුව සංඥාව ඉහළ හෝ පහළ වෝල්ටීයතා මට්ටමකින් ආරම්භ විය හැකිය.

High Voltage for 1, Low Voltage for 0

The signal remains at a high voltage for the entire duration of the bit period when transmitting a 1.
1 සම්ප්‍රේෂණය කිරීමේදී සංඥාව බිටු කාල සීමාවේ මුළු කාලයම අධි වෝල්ටීයතාවයේ පවතී.

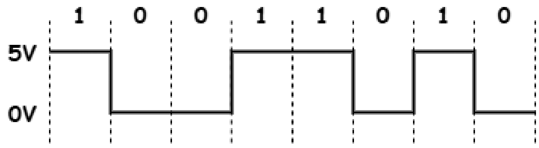
The signal remains at a low voltage for the entire duration of the bit period when transmitting a 0.
0 සම්ප්‍රේෂණය කරන විට බිටු කාල සීමාවේ සම්පූර්ණ කාලයම සංඥාව අඩු වෝල්ටීයතාවයකින් පවතී.



High Voltage for 0, Low Voltage for 1

The signal remains at a high voltage for the entire duration of the bit period when transmitting a 0.
0 සම්ප්‍රේෂණය කිරීමේදී සංඥාව බිටු කාල සීමාවේ සම්පූර්ණ කාලයම ඉහළ වෝල්ටීයතාවයකින් පවතී.

The signal remains at a low voltage for the entire duration of the bit period when transmitting a 1.
1 සම්ප්‍රේෂණය කිරීමේදී සංඥාව බිටු කාල සීමාවේ සම්පූර්ණ කාලයම අඩු වෝල්ටීයතාවයකින් පවතී.

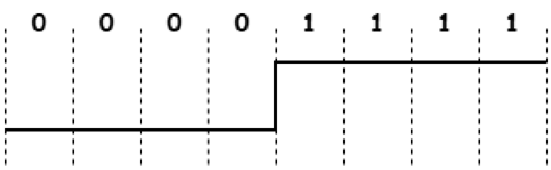


Problem with Long Sequences in NRZ-L
NRZ-L හි දිගු අනුපිළිවෙල සමඟ ඇති ගැටළුව

When there is a long sequence of 0s or 1s, the voltage level remains constant because no transitions occur.
0 හෝ 1 හි දිගු අනුපිළිවෙලක් ඇති විට, සංක්‍රාන්ති සිදු නොවන නිසා වෝල්ටීයතා මට්ටම නියතව පවතී.

This constant level leads to synchronization issues because the receiver has no transitions to track and loses its ability to distinguish where one bit ends and the next begins.
මෙම නියත මට්ටම සමමුහුර්ත කිරීමේ ගැටළු වලට තුඩු දෙයි, මන්ද ග්‍රාහකයාට හඹා යාමට සංක්‍රාන්ති නොමැති නිසා එක් බිටුවක් අවසන් වන තැන සහ ඊළඟ එක ආරම්භ වන ස්ථානය වෙන්කර හඳුනා ගැනීමේ හැකියාව නැති වේ.

Without transitions, the clock between sender and receiver can drift out of sync, causing decoding errors.
සංක්‍රාන්ති නොමැතිව, යවන්නා සහ ග්‍රාහකයා අතර විකේතන දෝෂ ඇති කරමින් ඝටිකාව සමමුහුර්තකරණයෙන් ඉවතට ප්ලාවනය විය හැක.



2. NRZ – I

(Non-Return to Zero – Inverted)

In this encoding scheme, a 1 is represented by a transition of the physical level, while a 0 has no transition.
මෙම කේතන ක්‍රමයේදී, 1, භෞතික මට්ටමේ සංක්‍රාන්තියක් මගින් නිරූපණය වන අතර 0 ට සංක්‍රාන්තියක් නොමැත.

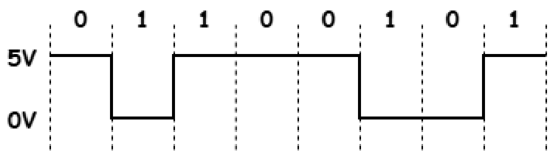
Each time a 1 is encountered in the data stream, the signal inverts (changes from high to low or low to high).
දත්ත ප්‍රවාහයේ 1ක් හමු වන සෑම අවස්ථාවකම, සංඥාව ප්‍රතිලෝම වේ (ඉහළ සිට පහළට හෝ පහළ සිට ඉහළට වෙනස් වේ).

When a 0 is encountered, the signal remains at the same level as the previous bit.
0 හමු වූ විට, සංඥාව පෙර බිටු මට්ටමේම පවතී.

The system can start the signal at either a high or low voltage level.
පද්ධතියට සංඥාව ඉහළ හෝ පහළ වෝල්ටීයතා මට්ටමකින් ආරම්භ කළ හැක.

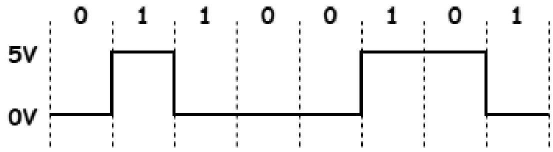
If the initial voltage is high
ආරම්භක වෝල්ටීයතාවය ඉහළ නම්

Binary **1** changes the signal from **high to low**, while a binary **0** keeps the signal at the **high**
ද්විමය 1 බිටුව සංඥාව **ඉහළ සිට පහළට** වෙනස් කරයි. ද්විමය 0 බිටුව සංඥාව **ඉහළ** මට්ටමේම පවත්වා ගනී.



If the initial voltage is low
ආරම්භක වෝල්ටීයතාවය පහළ නම්

Binary **1** changes the signal from **low to high**, while a binary **0** keeps the signal at the **low** level.
ද්විමය 1 බිටුව සංඥාව **පහළ සිට ඉහළට** වෙනස් කරයි. ද්විමය 0 බිටුව සංඥාව පහළ මට්ටමේම පවත්වා ගනී.

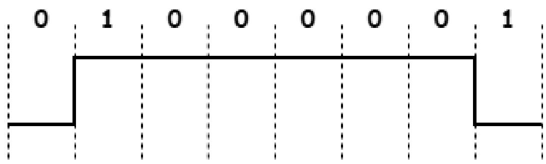


Problem with Long Sequences in NRZ-I
NRZ-I හි දිගු අනුපිළිවෙල සමඟ ඇති ගැටළුව

Although 1s provide transitions, long runs of 0s still create synchronization challenges.
1හීදී සංක්‍රාන්ති සපයන නමුත්, 0 හි දිගු අනුපිළිවෙලවල් තවමත් සමමුහුර්ත කිරීමේ ගැටලු නිර්මාණය කරයි.

When there is a long sequence of 0s, the signal stays at the same voltage level with no transitions.
0 හි දිගු අනුපිළිවෙලක් ඇති විට, සංඥාව සංක්‍රාන්ති නොමැතිව එකම වෝල්ටීයතා මට්ටමේ පවතී.

As in NRZ-L, this lack of transitions causes synchronization problems.
NRZ-L හි මෙන්, මෙම සංක්‍රාන්ති නොමැතිකම සමමුහුර්ත කිරීමේ ගැටළු ඇති කරයි.



ictfromabc.com

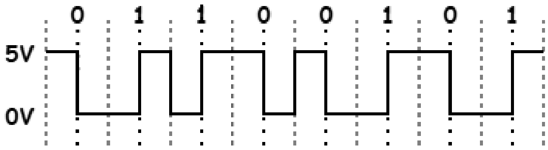
Manchester Encoding

In Manchester Encoding, each bit of data is represented by a transition in the signal rather than by a specific voltage level.
Manchester කේතනයේදී, එක් එක් දත්ත බිටු නිශ්චිත වෝල්ටීයතා මට්ටමකින් නොව සංඥාවේ සංක්‍රමණයකින් නිරූපණය කෙරේ.

Every bit period is divided into two equal halves, and there is always a transition in the middle of the bit period.
සෑම බිට් කාල සීමාවක්ම සමාන කොටස් දෙකකට බෙදා ඇති අතර, බිට් කාල සීමාව මධ්‍යයේදී සැමවිටම සංඥාවේ සංක්‍රාන්තියක් සිදු වේ.

Manchester Encoding (IEEE)

- Binary 1: The signal transitions from low to high in the middle of the bit period.
  බිටු කාල සීමාව මැදදී සංඥාව පහළ සිට ඉහළට සංක්‍රමණය වේ.
- Binary 0: The signal transitions from high to low in the middle of the bit period.
  බිටු කාල සීමාව මැදදී සංඥාව සිට ඉහළ සිට පහළට සංක්‍රමණය වේ.



Advantages

Synchronization
The frequent transitions make it easy to synchronize the receiver with the transmitter.
නිරන්තරව සිදුවන සංක්‍රාන්ති සම්ප්‍රේෂකය සමඟ ග්‍රාහකය සමමුහුර්ත කිරීම පහසු කරයි.

Error Detection
The regular changes in the signal help detect errors, as missing or extra transitions would indicate a problem.
නැතිවීම් හෝ අමතර සංක්‍රාන්ති මගින් ගැටලුවක් පෙන්නුම් කරන බැවින්, සංඥාවේ නිරන්තර වෙනස්වීම් දෝෂ හඳුනා ගැනීමට උපකාරී වේ.

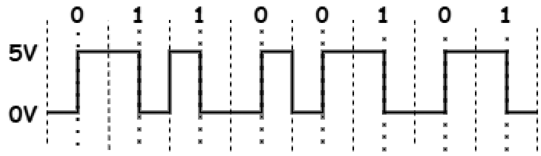
Disadvantages

Higher Bandwidth
Since Manchester encoding uses two voltage transitions per bit, it requires more bandwidth compared to other encoding schemes like NRZ.
Manchester කේතනය බිටු එකකට වෝල්ටීයතා සංක්‍රාන්ති දෙකක් භාවිතා කරන බැවින්, NRZ වැනි අනෙකුත් කේතීකරණ ක්‍රමවලට සාපේක්ෂව එයට වැඩි කලාප පළලක් අවශ්‍ය වේ.

Manchester Encoding (G.E Thomas)

The transition is reversed when compared with the IEEE Manchester standard.
IEEE Manchester ප්‍රමිතිය සමඟ සංසන්දනය කිරීමේදී මෙහි අර්ථය ප්‍රතිවිරුද්ධ වේ.

- Binary 1: The signal transitions from high to low in the middle of the bit period.
  බිටු කාල සීමාව මධ්‍යයේදී සංඥාව ඉහළ මට්ටමේ සිට පහළ මට්ටම දක්වා වෙනස් වේ.
- Binary 0: The signal transitions from low to high in the middle of the bit period.
  බිටු කාල සීමාව මධ්‍යයේදී මධ්‍යයේදී සංඥාව පහළ මට්ටමේ සිට ඉහළ මට්ටම දක්වා වෙනස් වේ.



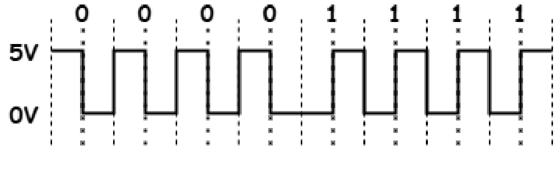
Manchester encoding is often regarded as a superior encoding scheme due to its inherent ability to provide reliable synchronization and robust error detection.
මැන්චෙස්ටර් කේතනය බොහෝ විට උසස් කේතීකරණ ක්‍රමයක් ලෙස සැලකෙන්නේ එහි විශ්වාසනීය සමමුහුර්තකරණය සහ ශක්තිමත් දෝෂ හඳුනාගැනීමේ හැකියාව නිසාය

How Manchester Encoding Solves the Problem
Manchester කේතනය මෙම ගැටළුව විසඳන ආකාරය

In Manchester encoding, each bit (whether 0 or 1) has a guaranteed transition in the middle of the bit period.
මැන්චෙස්ටර් කේතණයේදී, සෑම බිටුවකටම (0 හෝ 1) බිටු කාල සීමාවේ මැදදී සහතික කළ සංක්‍රාන්තියක් ඇත.

Because there is always a transition, even with long sequences of identical bits, the receiver can continuously synchronize with the sender.
සෑම විටම සංක්‍රාන්තියක් පවතින බැවින්, සමාන බිටු වල දිගු අනුපිළිවෙලක් සමඟ වුවද, ග්‍රාහකයාට යවන්නා සමඟ අඛණ්ඩව සමමුහුර්ත කළ හැක.

This **constant stream of transitions** prevents the clock from drifting out of sync, ensuring that the receiver can accurately interpret the data without losing track of the bit boundaries.
මෙම නිරන්තර සංක්‍රාන්ති ප්‍රවාහය ඝටිකාව සමමුහුර්තකරණයෙන් ඉවතට ගලා යාම වළක්වයි, ග්‍රාහකයාට බිටු මායිම් අහිමි නොවී දත්ත නිවැරදිව අර්ථ දැක්විය හැකි බව සහතික කරයි.



Bit rate of Manchester Encoding

In Manchester encoding, each bit is represented by two signal changes.
මැන්චෙස්ටර් ආකේතනයේදී, සෑම බිටුවක්ම සංඥා වෙනස්වීම් දෙකකින් නිරූපණය කෙරේ.

Since there are two signal changes (baud) for each bit, the bit rate is half the baud rate.
සෑම බිටුවක් සඳහාම සංඥා වෙනස්වීම් දෙකක් ඇති බැවින්, බිට් අනුපාතය අනුපාතයෙන් අඩකි.

The baud rate refers to the number of signal changes transmitted per second in a communication system.
Baud අනුපාතය යනු සන්නිවේදන පද්ධතියක තත්පරයකට සම්ප්‍රේෂණය වන සංඥා වෙනස්වීම් ගණනයි.

This means that Manchester encoding requires twice the bandwidth compared to simpler encoding schemes like NRZ, for the same bit rate.
මෙයින් අදහස් කරන්නේ NRZ වැනි සරල කේතීකරණ ක්‍රමවලට සාපේක්ෂව මැන්චෙස්ටර් කේතනය සඳහා කලාප පළල දෙගුණයක් අවශ්‍ය වන බවයි.

Error control in data transmission
දත්ත සම්ප්‍රේෂණයේදී දෝෂ පාලනය

When data is transmitted over a communication channel, it can be affected by various disturbances like noise, interference, or signal loss.
සන්නිවේදන නාලිකාවක් හරහා දත්ත සම්ප්‍රේෂණය කරන විට, එය ඝෝෂාව, බාධා කිරීම් හෝ සංඥා නැතිවීම වැනි විවිධ බාධා වීම් වලට ලක්විය හැකිය.

These disturbances may cause errors, where bits are altered during transmission.
මෙම බාධා කිරීම් සම්ප්‍රේෂණය අතරතුර බිටු වෙනස් කරමින් දෝෂ ඇති කළ හැක.

Error control mechanisms are used to detect and correct these errors to ensure the data received is accurate.
ලැබුණු දත්ත නිවැරදි බව සහතික කිරීම සඳහා මෙම දෝෂ හඳුනා ගැනීමට සහ නිවැරදි කිරීමට දෝෂ පාලන යාන්ත්‍රණ භාවිතා කරයි.

Error Detection
දෝෂ හඳුනාගැනීම

Error detection is the process of identifying whether the data bit has been altered during transmission.
දෝෂ හඳුනාගැනීම යනු සම්ප්‍රේෂණය අතරතුර දත්ත බිටු වෙනස් වී ඇත්ද යන්න හඳුනා ගැනීමේ ක්‍රියාවලියයි.

Error detection only tells us that an error has occurred.
දෝෂ හඳුනාගැනීම මගින් පවසන්නේ දෝෂයක් සිදුවී ඇති බව පමණි.

It doesn’t provide the ability to fix the error.
එය දෝෂය නිවැරදි කිරීමට හැකියාව ලබා නොදේ.

Error Correction
දෝෂ නිවැරදි කිරීම

Error correction is the process of identifying and correcting the altered data.
දෝෂ නිවැරදි කිරීම යනු වෙනස් වී ඇති දත්ත හඳුනාගෙන නිවැරදි කිරීමේ ක්‍රියාවලියයි.

This is achieved by using special encoding techniques that allow the receiver to figure out where the error occurred and how to fix it.
මෙය සාක්ෂාත් කරගනු ලබන්නේ විශේෂ කේතීකරණ ශිල්පීය ක්‍රම භාවිතා කිරීමෙන් ග්‍රාහකයාට දෝෂය සිදුවූයේ කොතැනද සහ එය නිවැරදි කරන්නේ කෙසේද යන්න සොයා ගැනීමට ඉඩ සලසමින්ය.

Error Recovery
දෝෂ ප්‍රතිසාධනය

Once an error is detected, error recovery mechanisms ensure that the actual (correct) data is delivered to the receiver.
දෝෂයක් අනාවරණය වූ පසු, දෝෂ ප්‍රතිසාධන යාන්ත්‍රණය මඟින් සත්‍ය (නිවැරදි) දත්ත ග්‍රාහකයා වෙත ලබා දෙන බව සහතික කරයි.

This involves using either error correction codes (to fix the error on the spot) or requesting the sender to retransmit the data.
මෙයට දෝෂ නිවැරදි කිරීමේ කේත භාවිතා කිරීම (එම ස්ථානයේදීම දෝෂය නිවැරදි කිරීමට) හෝ දත්ත නැවත සම්ප්‍රේෂණය කිරීමට යවන්නාගෙන් ඉල්ලීම ඇතුළත් වේ.

Error Detection mechanisms
දෝෂ හඳුනාගැනීමේ යාන්ත්‍රණ

Parity check
සමතාව පරීක්ෂාව

Party check is one simple error detection mechanism where an extra bit is added and sent along with the original data bits to make the number of 1s in the data as either even in the case of even parity, or odd in the case of odd parity.
සමතාව පරීක්ෂාව යනු එක් සරල දෝෂ හඳුනාගැනීමේ යාන්ත්‍රණයක් වන අතර එහිදී අමතර බිටුවක් මුල් දත්ත බිටු සමඟ එකතු කර දත්තවල 1හි බිටු ගණන ඉරට්ටේ සමතාවේදී ඉරට්ටේ ලෙස හෝ ඔත්තේ සමතාවේදී ඔත්තේ ලෙස සකසා යවනු ලැබේ.

The parity bit may be added either at the beginning or at the end of the data, depending on the communication protocol. However, in many systems, it is commonly added at the end of the data.
භාවිතා කරන සන්නිවේදන නියමාවලිය අනුව parity bit එක දත්තයේ ආරම්භයට හෝ අවසානයට එකතු කළ හැකිය. නමුත් බොහෝ පද්ධතිවලදී, එය සාමාන්‍යයෙන් දත්තයේ අවසානයට එකතු කරයි.

Let’s transmit A and C using ASCII. Each ASCII character has 7 bits.
ASCII භාවිතයෙන් A සහ C සම්ප්‍රේෂණය කරමු. සෑම ASCII අක්ෂරයකටම බිටු 7 බැගින් ඇත.

A – 65 – 1000001
C – 67 – 1000011

With parity bit set, there are 8 bits for each letter.
Parity bit එක ඇතුළත් කළ පසු, එක් එක් අකුර සඳහා බිටු 8 බැගින් ඇත.

1. Even Parity

In even parity, the parity bit is set so that the total number of 1s in the data including the parity bit is even.
ඉරට්ටේ සමතාවේ දී, දත්තවල ඇති මුළු 1 බිටු ගණන සමතා බිටුවද ඇතුළුව ඉරට්ටේ වන පරිදි සමතා බිටුව සකසා ඇත.

According to the above A and C scenario
ඉහත සඳහන් කළ A සහ C සිදුවීමට අනුව

A – 1000001 **0 ← Parity bit**
C – 1000011 **1 ← Parity bit**

2. Odd Parity

In odd parity, the parity bit is set so that the total number of 1s in the data (including the parity bit) is odd.
ඔත්තේ සමතාවේ දී, දත්තවල ඇති මුළු 1 බිටු ගණන (සමතා බිටුවද ඇතුළුව) ඔත්තේ වන පරිදි සමතා බිටුව සකසා ඇත.

According to the above A and C scenario
ඉහත සඳහන් කළ A සහ C සිදුවීමට අනුව

A – 1000001 **1 ← Parity bit**
C – 1000011 **0 ← Parity bit**

The receiver checks the parity of the received data.
ග්‍රාහකයා ලැබුණු දත්තවල සමතාව පරීක්ෂා කරයි.

If the number of 1s doesn’t match the expected parity (even or odd), it indicates that an error occurred during transmission.
1හි බිටු ගණන අපේක්ෂිත සමතාවට නොගැලපේ නම් (ඉරට්ටේ හෝ ඔත්තේ), එය සම්ප්‍රේෂණය අතරතුර දෝෂයක් සිදු වූ බව පෙන්නුම් කරයි.

Note
Parity bits can only detect single-bit errors. If two bits are flipped during transmission, the error might go undetected because the parity would still be correct.
සමතා බිටුවලට හඳුනාගත හැක්කේ තනි-බිටු දෝෂ පමණි. සම්ප්‍රේෂණය අතරතුර බිටු දෙකක් කනපිට පෙරලන්නේ නම්, සමතාව තවමත් නිවැරදි බැවින් දෝෂය අනාවරණය කරගත නොහැක.

Checksum

A checksum is an error detection method used in data transmission. It helps the receiver check whether the received data has been changed or damaged during transmission.
Checksum යනු දත්ත සම්ප්‍රේෂණයේදී දෝෂ හඳුනා ගැනීමට භාවිතා කරන ක්‍රමයකි. එය සම්ප්‍රේෂණය අතරතුර දත්ත වෙනස් වී තිබේද හෝ හානි වී තිබේද යන්න පරීක්ෂා කිරීමට ග්‍රාහකයාට උපකාරී වේ.

A checksum helps find multiple bit errors in received data.
Checksum මඟින්, ලැබුණු දත්තවල බහු බිට් කිහිපයක දෝෂ සොයා ගැනීමට උපකාරී වේ

How Checksum Works
Checksum ක්‍රියා කරන ආකාරය

Sender's Side
The data is divided into smaller fixed-size blocks (usually 8, 16, or 32 bits).
දත්ත කුඩා ස්ථාවර ප්‍රමාණයේ කොටස් වලට බෙදනු ලබයි (සාමාන්‍යයෙන් බිටු 8, 16, හෝ 32).

A mathematical operation (often addition) is performed on these blocks.
මෙම කොටස් මත ගණිතමය මෙහෙයුමක් (බොහෝ විට එකතු කිරීම) සිදු කරනු ලැබේ.

The result of the operation is called the checksum, which is then added to the end of the data before transmission.
මෙහෙයුමේ ප්‍රතිඵලය චෙක්සම් ලෙස හැඳින්වේ, පසුව සම්ප්‍රේෂණයට පෙර දත්ත අවසානයේ එය එකතු කරනු ලැබේ.

Receiver's Side
The receiver receives the data and the checksum.
ග්‍රාහකයා දත්ත සහ checksum ලබා ගනී.

The same mathematical operation is applied to the received data blocks.
ලැබුණු දත්ත කොටස් වලට සමාන ගණිතමය මෙහෙයුමක් යොදනු ලැබේ.

The receiver then compares its calculated checksum with the transmitted checksum.
If they match, the data is assumed to have been transmitted correctly; if they don't, an error is detected.
එවිට ග්‍රාහකය එහිදී ගණනය කළ චෙක්සම්, සම්ප්‍රේෂණය කළ චෙක්සම් සමඟ සංසන්දනය කරයි. ඒවා ගැලපෙන්නේ නම්, දත්ත නිවැරදිව සම්ප්‍රේෂණය වී ඇතැයි උපකල්පනය කෙරේ;එසේ නොවේ නම්, දෝෂයක් අනාවරණය වේ.

Example
Marks of 3 subjects are to be submitted.
ලැබුණු විෂයන් 3හි ලකුණු එකතු කරයි

Science – 75 → In binary 01001011
Maths – 80 → In binary 01010000
English – 95 → In binary 01011111

Sum – 250 → In binary 11111010

If this result is more than 8 bits, the checksum must be adjusted according to the checksum method used. For example, the system may use only the lower 8 bits or handle the extra carry bits according to its design.
මෙම ප්‍රතිඵලය 8-bit ට වඩා වැඩි නම්, භාවිතා කරන checksum ක්‍රමය අනුව checksum අගය සකස් කළ යුතුය. උදාහරණයක් ලෙස, පද්ධතිය පහළ 8-bit පමණක් භාවිතා කළ හැකි අතර, අමතර carry bits පද්ධති සැලසුම අනුව සැලකිය හැකිය

The final checksum is sent together with the data. The receiver repeats the same calculation and compares its result with the received checksum. If both values match, the data is considered valid; otherwise, an error is detected.
අවසාන checksum අගය දත්ත සමඟ යවනු ලබයි. ග්‍රාහකයා එම ගණනය කිරීම නැවත සිදු කර තම ප්‍රතිඵලය ලැබුණු checksum අගය සමඟ සසඳයි. අගයන් දෙක ගැළපේ නම්, දත්ත වලංගු ලෙස සලකයි; නොගැළපේ නම්, දෝෂයක් හඳුනා ගනී.

Transmitted 01001011 01010000 01011111
With checksum 11111010

In the other side, first 3 are added to check if the sum matches the checksum
එසේ එකතු කර ලබාගන්නා අගය, දත්ත සමඟ එවා ඇති Checksum අගය හා සමානදැයි පරීක්ෂා කරයි.

If yes – Possibly no errors
ඔව් නම්: බොහෝ දුරට දෝෂ නොමැත

If no – Possibly an error
නැත නම්: දෝෂයක් සිදුවී ඇත.

Cyclic Redundancy Check (CRC)

Cyclic Redundancy Check is a more advanced error detection technique used in digital communication systems to ensure data integrity.
Cyclic Redundancy Check යනු දත්ත අඛණ්ඩතාව සහතික කිරීම සඳහා ඩිජිටල් සන්නිවේදන පද්ධතිවල භාවිතා කරන වඩාත් දියුණු දෝෂ හඳුනාගැනීමේ තාක්ෂණයකි.

CRC works by treating the data as a large binary number and dividing it by a predefined polynomial.
CRC ක්‍රියා කරනුයේ දත්ත විශාල ද්විමය සංඛ්‍යාවක් ලෙස සැලකීමෙන් සහ එය පූර්ව නිර්වචනය කළ බහුපදයකින් බෙදීමෙනි.

The remainder from this division is called the CRC code or simply the CRC, which is appended to the data before transmission.
මෙම බෙදීමේ ඉතිරි කොටස CRC කේතය හෝ සරලව CRC ලෙස හැඳින්වේ, එය සම්ප්‍රේෂණය කිරීමට පෙර දත්ත වලට එකතු වේ.

When the receiver gets the data, it performs the same division and checks if the remainder (CRC) matches.
ග්‍රාහකයාට දත්ත ලැබුණු විට, එය විසින්ද එම බෙදීමම සිදු කර ඉතිරිය (CRC) ගැලපේදැයි පරීක්ෂා කරයි.

If the remainder is different, it indicates that an error occurred during transmission.
ඉතිරිය වෙනස් නම්, එය සම්ප්‍රේෂණය කිරීමේදී දෝෂයක් සිදු වූ බව පෙන්නුම් කරයි.

Hashing

Hashing is a method used to convert data of any size into a fixed-size value called a hash value, hash code, or message digest. This is done using a special mathematical function called a hash function.
Hashing යනු ඕනෑම ප්‍රමාණයක දත්ත, ස්ථිර ප්‍රමාණයක අගයක් වන hash value, hash code හෝ message digest බවට පරිවර්තනය කරන ක්‍රමයකි. මෙය hash function ලෙස හැඳින්වෙන විශේෂ ගණිතමය ක්‍රියාවලියක් භාවිතයෙන් සිදු කරයි.

How Hashing Works
Hashing ක්‍රියා කරන ආකාරය

First, the original data is given as input to a hash function. The input may be a message, password, file, or any other digital data.
පළමුව, මුල් දත්ත hash function එකකට ආදානයක් ලෙස ලබා දෙයි. මෙම ආදානය එක පණිවිඩයක්, මුරපදයක්, ගොනුවක් හෝ වෙනත් ඩිජිටල් දත්තයක් විය හැකිය.

The hash function processes the input data and produces a fixed-size hash value. For the same input, the same hash function always produces the same hash value.
Hash function එක ආදාන දත්ත සැකසීමෙන් ස්ථිර ප්‍රමාණයක hash value එකක් ලබා දෙයි. එකම ආදානයකටම, එකම hash function එක සෑම විටම එකම hash අගය එක ලබා දෙයි.

When the data is received or checked later, the same hash function is applied again. If the newly calculated hash value matches the original hash value, the data is considered unchanged. If the hash values are different, it means the data has been changed or corrupted.
පසුව දත්ත ලබාගත් විට හෝ පරීක්ෂා කරන විට, එම hash function එක නැවත භාවිතා කරයි. අලුතින් ගණනය කළ hash අගය එක මුල් hash අගය එකට ගැළපේ නම්, දත්ත වෙනස් නොවී ඇතැයි සලකයි. Hash අගය දෙක වෙනස් නම්, දත්ත වෙනස් වී හෝ හානි වී ඇති බව අදහස් වේ.

Synchronization
සමමුහුර්තකරණය

The process of matching the timing between the transmitter and the receiver during data communication.
දත්ත සන්නිවේදනයේදී සම්ප්‍රේෂකයා සහ ග්‍රාහකයා අතර කාල ගැලපීම සිදු කිරීමේ ක්‍රියාවලියයි.

Both transmitter and receiver must follow the same timing pattern. If their clocks are not synchronized, the receiver may read the signal at the wrong time.
සම්ප්‍රේෂකයා සහ ග්‍රාහකයා යන දෙකම එකම කාල රටාවකට අනුගත විය යුතුය. ඔවුන්ගේ ඔරලෝසු (clocks) සමකාලීන වී නොමැති නම්, ග්‍රාහකයා විසින් වැරදි වේලාවකදී සංඥාව කියවීමට ඉඩ ඇත.

If the receiver reads the signal too early or too late, the received data may be incorrect.
ග්‍රාහකයා විසින් සංඥාව නියමිත වේලාවට වඩා කලින් හෝ ප්‍රමාද වී කියවීම සිදු කළහොත්, ලැබෙන දත්ත වැරදි විය හැක.

When the end are not synchronized:
අග්‍ර සමමුහුර්ණය වී නොමැති විට:

- The receiver may read bits incorrectly.
  ග්‍රාහකයා විසින් බිටු වැරදි ලෙස කියවීමට ඉඩ ඇත.
- Some bits may be skipped.
  සමහර බිටු මඟ හැරී යාමට ඉඩ ඇත.
- Extra bits may be assumed.
  අතිරේක බිටු පවතින බවට උපකල්පනය කිරීමට ඉඩ ඇත.
- Bit boundaries may be lost.
  බිටු සීමාවන් අහිමි වී යා හැක.
- Data may become corrupted.
  දත්ත විකෘති වීමකට ලක් විය හැක.
- Error detection may be needed to identify wrong data. (Parity check)
  වැරදි දත්ත හඳුනා ගැනීම සඳහා දෝෂ හඳුනාගැනීමේ ක්‍රම අවශ්‍ය විය හැක. (සමතා පරීක්ෂාව)

Clocks

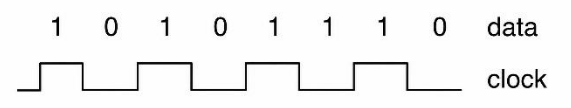
An Electronic circuit that generates a continuous sequence of equally spaced electrical pulses at a constant frequency.
නියත සංඛ්‍යාතයකින් යුත්, සමාන පරතර ඇති විද්‍යුත් ස්පන්ද අඛණ්ඩ අනුක්‍රමයක් ජනනය කරනු ලබන විද්‍යුත් පරිපථයකි.

Each network device has an internal clock.
සෑම ජාල උපාංගයකටම අභ්‍යන්තර ඔරලෝසුවක් (internal clock) පවතී.

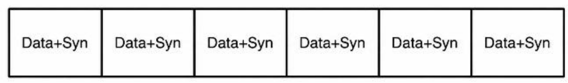
The transmitter uses its clock to decide when to send each bit or signal element.
සම්ප්‍රේෂකයා විසින් සෑම බිටුවක් හෝ සංඥා අංගයක්ම යැවිය යුත්තේ කිනම් වේලාවකදැයි තීරණය කිරීමට තමාගේ ඔරලෝසුව භාවිත කරයි.

The receiver uses its clock to decide when to read each bit or signal element.
ග්‍රාහකයා විසින් සෑම බිටුවක් හෝ සංඥා අංගයක්ම කියවිය යුත්තේ කිනම් වේලාවකදැයි තීරණය කිරීමට තමාගේ ඔරලෝසුව භාවිත කරයි.

Usually, a clock signal is transmitted together with the data stream to maintain proper signal timing and synchronization.
නිවැරදි සංඥා කාලකරණය සහ සමමුහුර්තකරනය පවත්වා ගැනීම සඳහා, සාමාන්‍යයෙන් ඔරලෝසු සංඥාවක්, දත්ත ප්‍රවාහය සමඟ එකට සම්ප්‍රේෂණය කරනු ලබයි.



In some line coding techniques, such as Manchester encoding, the clock information is embedded within the data signal.
මැන්චෙස්ටර් කේතනය වැනි සමහර රේඛීය කේතන ශිල්ප ක්‍රමවලදී , ඔරලෝසු තොරතුරු දත්ත සංඥාව තුළම තැන්පත් කර ඇත.



Why is a Clock Needed?

The clock controls when a device should:
උපාංගයක් විසින් පහත ක්‍රියාවන් සිදු කළ යුත්තේ කුමන වෙලාවේ ද යන්න ඔරලෝසුව මඟින් පාලනය කරයි:

- Execute an instruction.
  උපදෙසක් ක්‍රියාත්මක කිරීම.
- Send data. / දත්ත යැවීම.
- Receive data. / දත්ත ලබා ගැනීම.
- Read from or write to memory.
- මතකයෙන් කියවීම හෝ මතකයට ලිවීම.
- Change its signal state.
  එහි සංඥා තත්ත්වය වෙනස් කිරීම.

Without a clock, different parts of the system would operate at different times.
ඔරලෝසුවක් නොමැති නම්, පද්ධතියේ විවිධ කොටස් එකිනෙකට වෙනස් කාලවලදී ක්‍රියාත්මක වනු ඇත.

ictfromabc.com

Clock Frequency / ඔරලෝසු සංඛ්‍යාතය

The number of clock ticks (pulses) generated by a clock in one second.
තත්පරයකදී ඔරලෝසුවක් මගින් ජනනය කරනු ලබන (clock ticks) හෝ ස්පන්ද ගණනයි.

It is measured in Hertz (Hz).
එය හර්ට්ස් (Hz) මගින් මනිනු ලබයි.

1 Hz = 1 pulse per second
1 kHz = 1,000 pulses per second
1 MHz = 1,000,000 pulses per second
1 GHz = 1,000,000,000 pulses per second

Clock Tick (Clock Pulse)

Single pulse generated by a clock at regular time intervals.
නියමිත කාල පරාසයන් තුළ ඔරලෝසුවක් මගින් ජනනය කරනු ලබන තනි ස්පන්දයකි.

Each clock tick acts as a timing signal that synchronizes electronic operations.
සෑම ඔරලෝසු ටික් එකක්ම (clock tick), විද්‍යුත් ක්‍රියාවලි එකිනෙක සමමුහුර්ත කරන කාල සංඥාවක් ලෙස ක්‍රියා කරයි.

Clock Difference / ඔරලෝසු වෙනස

Clock difference means the transmitter clock and receiver clock do not run at exactly the same speed.
ඔරලෝසු වෙනස යනු සම්ප්‍රේශකයේ ඔරලෝසුව සහ ග්‍රාහකයේ ඔරලෝසුව හරියටම එකම වේගයකින් ධාවනය නොවේ.

Examples / උදාහරණ:

- The transmitter sends one bit every 1 millisecond.
  සම්ප්‍රේශකයා විසින් සෑම මිලිතත්පර 1කටම වරක් බිටු එක බැගින් යවයි.
- The receiver expects one bit every 1.1 milliseconds.
  ග්‍රාහකයා විසින් සෑම මිලිතත්පර 1.1කටම වරක් බිටු එක බැගින් බලාපොරොත්තු වෙයි.

Clock Drift / ඔරලෝසු ප්ලාවිතය

Clock drift means two device clocks slowly move away from each other over time.
ඔරලෝසු ප්ලාවිතය යන්නෙන් අදහස් කරන්නේ කාලයත් සමඟ උපාංග දෙකක clocks සෙමින් එකිනෙකින් බැහැරට ගමන් කිරීමයි.

No two hardware clocks are perfectly equal. Because of this, even a small clock difference can create errors during long data transmission.
දෘඩාංග ඔරලෝසු දෙකක් කිසිසේත්ම පරිපූර්ණ ලෙස සමාන නොවේ. මේ හේතුව නිසා, කුඩා ඔරලෝසු වෙනසක් වුවද දිගු දත්ත සම්ප්‍රේෂණයකදී දෝෂ ඇති කිරීමට හේතු විය හැක.

Timing / කාලකරණය

The exact instant at which an event occurs with respect to a clock signal.
ඔරලෝසු සංඥාවකට සාපේක්ෂව, කිසියම් සිදුවීමක් සිදුවන නිශ්චිත මොහොතයි.

A clock signal generates regular clock ticks, and timing determines when each operation should occur at those clock ticks.
ඔරලෝසු සංඥාවක් මගින් නිතිපතා ඔරලෝසු ටික්ස් ජනනය කරනු ලබන අතර, කාලකරණය මගින් එම ඔරලෝසු ටික්ස්වලදී එක් එක් ක්‍රියාවලිය සිදුවිය යුත්තේ කවදාදැයි තීරණය කරයි.

Examples / උදාහරණ:

- Transmit a bit. / බිටුවක් ප්‍රේෂණය කිරීම.
- Receive a bit. / බිටුවක් ප්‍රතිග්‍රහණය කිරීම.
- Change the signal level. / සංඥා මට්ටම වෙනස් කිරීම.

NOTE:
Errors caused by synchronization problems can be detected using parity check, which will be discussed later.
සමමුහුර්තකරණ ගැටලු නිසා ඇතිවන දෝෂ, සමතා පරීක්ශාව භාවිතයෙන් හඳුනාගත හැකි අතර, ඒ පිළිබඳව පසුව සාකච්ඡා කරනු ලැබේ.

Why We Need Modulation?
මුහුර්ජණය අවශ්‍ය වන්නේ ඇයි?

Encoding schemes represent bits as voltage levels. This works only when there is a wire to carry that voltage.
කේතකරණ ක්‍රම මඟින් බිට් (bits) වෝල්ටීයතා මට්ටම් ලෙස නිරූපණය කරයි. මෙය ක්‍රියාත්මක වන්නේ එම වෝල්ටීයතාව ගෙනයාමට වයරයක් ඇති විට පමණි.

Problems arise when there is no wire, wireless transmission, optical fiber, or long-distance links.
වයරයක් නොමැති විට, රැහැන් රහිත සම්ප්‍රේෂණයේදී, ප්‍රකාශ තන්තු හෝ දිගු දුර සබැඳිවලදී ගැටලු මතු වේ.

No wire means no voltage to send
වයරයක් නැති විට වෝල්ටීයතාවක් යැවීමට නොහැක.
Voltage signals need a closed circuit. Air and light have no such path.
වෝල්ටීයතා සංඥා සඳහා සංවෘත පරිපථයක් අවශ්‍ය වේ. වාතය සහ ආලෝකය සතුව එවැනි මාර්ගයක් නොමැත.

Signals weaken over distance
දුරත් සමඟ සංඥා දුර්වල වේ
Voltage-based signals lose strength and pick up noise over long distances, even on wire.
වෝල්ටීයතාවය මත පදනම් වූ සංඥා දිගු දුරක් යන විට ශක්තිය නැති වී යන අතර වයර් මත වුවද ඝෝෂාවන් (noise) එකතු වේ.

Multiple signals can't share a medium
බහුවිධ සංඥාවලට එකම මාධ්‍යයක ගමන් කල නොහැක
Many devices may need to transmit through the same channel (e.g., air) at once. Raw voltage signals provide no way to separate or distinguish them.
බොහෝ උපාංගවලට එකම නාලිකාවක් (උදා: වාතය) හරහා එකවර සම්ප්‍රේෂණය කිරීමට අවශ්‍ය විය හැක. සරල වෝල්ටීයතා සංඥා මඟින් ඒවා වෙන් කිරීමට හෝ හඳුනා ගැනීමට ක්‍රමයක් නොසපයයි.

Solution / විසඳුම

Instead of sending bits as direct voltage levels, use a high-frequency wave called a carrier, and vary one of its properties according to the bit pattern. The three properties that can be varied are,
බිට් සෘජු වෝල්ටීයතා මට්ටම් ලෙස යවනවා වෙනුවට, වාහක තරංගයක් (carrier wave) ලෙස හැඳින්වෙන අධි-සංඛ්‍යාත තරංගයක් භාවිතා කර, බිට් රටාව අනුව එහි එක් ගුණාංගයක් වෙනස් කරන්න. වෙනස් කළ හැකි ගුණාංග තුන වන්නේ,

Amplitude - Amplitude Shift Keying (ASK)
Frequency - Frequency Shift Keying (FSK)
Phase - Phase Shift Keying (PSK)

This process of representing data by varying a carrier wave's property is called **Modulation.**
වාහක තරංගයක ගුණාංගයක් වෙනස් කිරීම මඟින් දත්ත නිරූපණය කිරීමේ මෙම ක්‍රියාවලිය **මුහුර්ජණය** (Modulation) ලෙස හැඳින්වේ.

Why modulation solves the problems above
එය ඉහත ගැටලුවලට විසඳුමක් වන්නේ ඇයි

The carrier frequency can be chosen high enough to radiate efficiently and pass through the medium.
වාහක සංඛ්‍යාතය කාර්යක්ෂමව විකිරණය වීමට සහ මාධ්‍යය හරහා ගමන් කිරීමට තරම් ඉහළ අගයකින් තෝරා ගත හැක.

Different devices can be assigned different carrier frequencies, allowing them to share the same medium without interference.
විවිධ උපාංග සඳහා විවිධ වාහක සංඛ්‍යාත වෙන් කළ හැකි අතර, එමඟින් මැදිහත්වීම් නොමැතිව එකම මාධ්‍යය බෙදා ගැනීමට ඒවාට ඉඩ සලසයි.

A carrier-based signal can travel farther and is easier to recover at a distance than a raw baseband voltage signal.
වාහකයක් මත පදනම් වූ සංඥාවකට වඩා දුරක් ගමන් කළ හැකි අතර සරල බේස්බෑන්ඩ් (baseband) වෝල්ටීයතා සංඥාවකට වඩා දුරින්දී නැවත ලබා ගැනීම පහසුය.

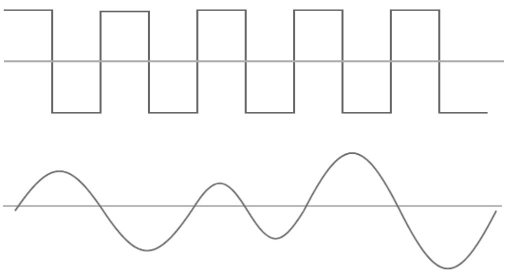
Modulation
මුහුර්ජණය

Modulation is the process of varying one or more properties (such as its amplitude, frequency, or phase) of periodic waveform called the carrier signal to encode information for transmission over a communication channel.
මුහුර්ජණය යනු සන්නිවේදන නාලිකාවක් හරහා සම්ප්‍රේෂණය සඳහා තොරතුරු කේතනය කිරීමට වාහක සංඥාව ලෙසින් හැඳින්වෙන ආවර්තික තරංග ආකෘතියක ගුණාංග එකක් හෝ කිහිපයක් (එහි විස්තාරය, සංඛ්‍යාතය හෝ කලාව වැනි) වෙනස් කිරීමේ ක්‍රියාවලියයි.

Parts of the modulation process
මුහුර්ජන ක්‍රියාවලියේ කොටස්

1. Information Signal (Baseband Signal)
තොරතුරු සංඥාව

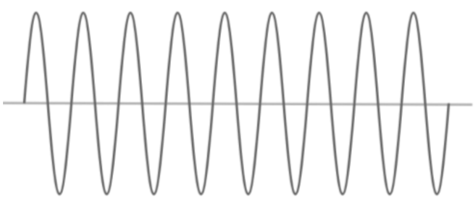
This is the original signal that contains the information you want to transmit.
ඔබට සම්ප්‍රේෂණය කිරීමට අවශ්‍ය තොරතුරු අඩංගු මුල් සංඥාව මෙයයි.



It can be anything from audio, video, or digital data. It’s the signal that you want to communicate to the receiver.
එය ශ්‍රව්‍ය, දෘශ්‍ය හෝ ඩිජිටල් දත්ත වලින් ඕනෑම දෙයක් විය හැක. ඔබට ග්‍රාහකයාට සන්නිවේදනය කිරීමට අවශ්‍ය සංඥාව එයයි.

2. The Carrier wave
වාහක තරංගය

A carrier signal is a high-frequency wave used to transport an information signal over a communication channel.
වාහක සංඥාවක් යනු සන්නිවේදන නාලිකාවක් හරහා තොරතුරු සංඥාවක් ප්‍රවාහනය කිරීමට භාවිතා කරන අධි-සංඛ්‍යාත තරංගයකි.



It acts as a "carrier" for the information, allowing it to be transmitted over long distances.
එය තොරතුරු සඳහා “වාහකයක්“ ලෙස ක්‍රියා කරයි, එමගින් සංඥාව දිගු දුරක් සම්ප්රේෂණය කිරීමට ඉඩ සලසයි.

Characteristics of a carrier signal
වාහක සංඥාවක ලක්ෂණ

High Frequency
ඉහළ සංඛ්‍යාත සහිතයි
Has a much higher frequency than the information signal, enabling efficient long-distance transmission.
තොරතුරු සංඥාවට වඩා බොහෝ ඉහළ සංඛ්‍යාතයක් ඇති අතර, කාර්යක්ෂම දිගු දුර සම්ප්‍රේෂණය සක්‍රීය කරයි.

Continuous Wave
සන්තතික තරංගයකි
Transmitted continuously without interruptions.
බාධාවකින් තොරව අඛණ්ඩව සම්ප්‍රේෂණය වේ.

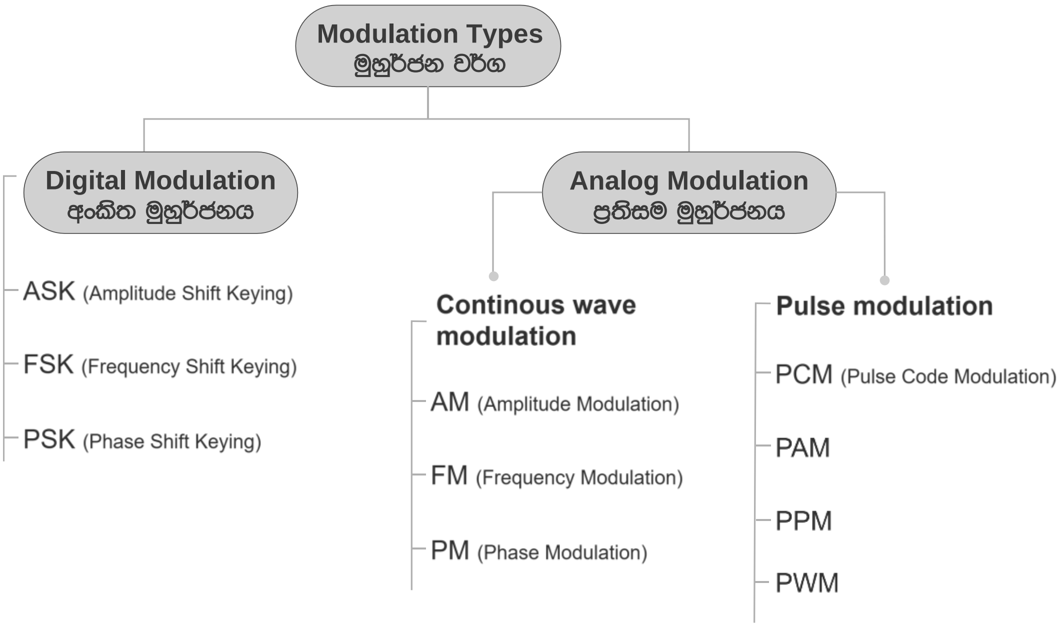
Sinusoidal Shape
Sin ආකාර වේ
Usually has a sine-wave form.
බොහෝ විට ශබ්ද තරංගයකට සමාන සයිනාකාර හැඩයක් ගනී.

3. Modulated Signal
මුහුර්ජනය කල සංඥාව

This is the result of the modulation process, where the carrier signal’s properties (amplitude, frequency, or phase) are varied according to the information signal.
මෙය මුහුර්ජන ක්‍රියාවලියේ ප්‍රතිඵලයයි, එහිදී වාහක සංඥාවේ ගුණාංග (විස්තාරය, සංඛ්‍යාතය හෝ කලාව) තොරතුරු සංඥාව අනුව වෙනස් වේ.

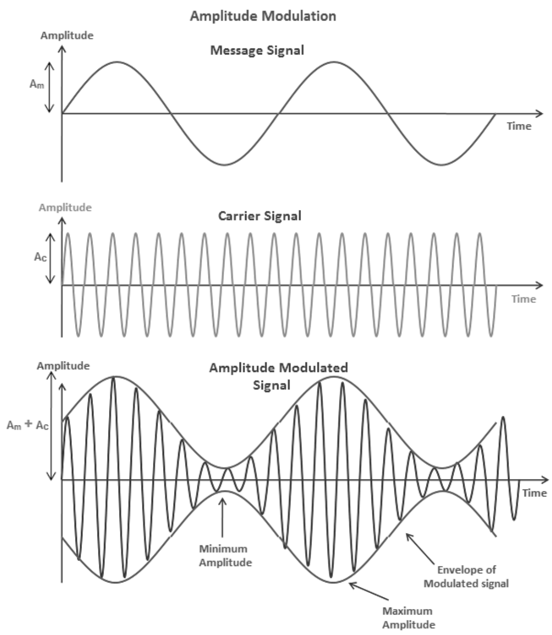
The modulated signal combines the carrier and information signals so that the information can be transmitted effectively.
මුහුර්ජිත සංඥාව මගින් වාහකය සහ තොරතුරු සංඥා ඒකාබද්ධ කරන අතර එමඟින් තොරතුරු ඵලදායී ලෙස සම්ප්රේෂණය කළ හැකිය.

Types of modulations
මුහුර්ජන වර්ග



Analog modulation
ප්‍රතිසම මුහුර්ජනය

1. Amplitude Modulation (AM)
විස්තාර මූර්ජනය



In amplitude modulation, the amplitude of the carrier signal is varied in proportion to the amplitude of the information (baseband) signal, while the frequency and phase of the carrier remain constant.
විස්තාරය මුහුර්ජනයේදී, වාහක සංඥාවේ විස්තාරය තොරතුරු සංඥාවේ විස්තාරයට සමානුපාතිකව වෙනස් කරන අතර, වාහකයේ සංඛ්‍යාතය සහ කලාව නියතව පවතී.

A low-amplitude message signal is represented by a low carrier amplitude, while a high-amplitude message signal is represented by a high carrier amplitude
වාහක තරංගයේ අඩු විස්තාරයකින්, අඩු විස්තාරයක් සහිත පණිවිඩ සංඥාවක් ද, වාහක තරංගයේ ඉහළ විස්තාරයකින්, ඉහළ විස්තාරයක් සහිත පණිවිඩ සංඥාවක් ද නිරූපණය කෙරේ.

Advantages
වාසි

Simple and inexpensive because it only varies the amplitude of the carrier wave while keeping its frequency constant.
වාහක තරංගයේ සංඛ්‍යාතය නියතව තබා ගනිමින් එහි විස්තාරය පමණක් වෙනස් කරන බැවින් මෙය සරල මෙන්ම වියදම් අඩු ක්‍රමයකි.

Easy to modulate and demodulate because simple electronic circuits can detect changes in the signal's amplitude.
සංඥාවේ විස්තාරයේ සිදුවන වෙනස්වීම් සරල ඉලෙක්ට්‍රොනික පරිපථ මඟින් හඳුනාගත හැකි බැවින් මූර්ජනය සහ විමූර්ජනය කිරීම පහසුය.

Requires less bandwidth because only two sidebands are transmitted around the carrier frequency.
වාහක සංඛ්‍යාතය දෙපසින් Sidebands දෙකක් පමණක් සම්ප්‍රේෂණය වන බැවින් අඩු කලාප පළලක් ප්‍රමාණවත් වේ.

Disadvantages
අවාසි

Easily affected by noise because noise mainly changes the amplitude of the signal, which carries the information.
තොරතුරු රැගෙන යනු ලබන සංඥාවේ විස්තාරයට බාහිර ඝෝෂාවන්ගෙන් පහසුවෙන් බලපෑම් එල්ල විය හැක.

Less power-efficient because most of the transmitted power is used by the carrier, which does not contain useful information.
සම්ප්‍රේෂණය වන බලයෙන් වැඩි ප්‍රමාණයක් වැය වන්නේ ප්‍රයෝජනවත් තොරතුරක් අඩංගු නොවන වාහක තරංගය සඳහා බැවින් මෙහි බල කාර්යක්ෂමතාව අඩුය.

Has poor sound quality because it is more susceptible to noise and has a limited audio frequency range.
ඝෝෂාවන්ට ගොදුරු වීමේ ප්‍රවණතාව වැඩි වීම සහ සීමිත ශ්‍රව්‍ය සංඛ්‍යාත පරාසයක් තිබීම නිසා මෙහි ශබ්දයේ ගුණාත්මකභාවය බාල මට්ටමක පවතියි.

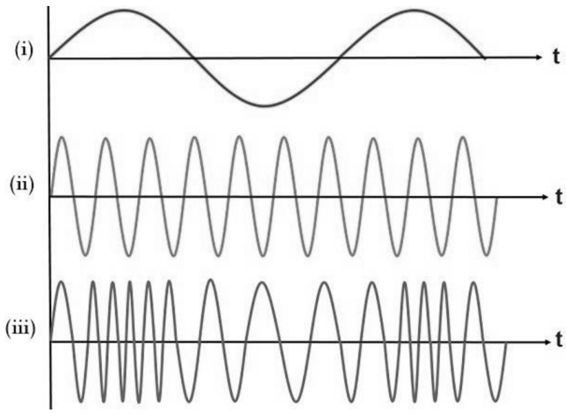
Applications of AM
AM හි යෙදුම්

- Radio broadcasting
  ගුවන්විදුලි විකාශනය
- Amateur radio
  ආධුනික ගුවන්විදුලි ක්‍රියාකරුවන්
- Early telephone systems
  මුල් කාලයේ දුරකථන පද්ධතිවල

2. Frequency modulation (FM)
සංඛ්‍යාත මූර්ජනය

In frequency modulation, the frequency of the carrier signal is varied in proportion to the amplitude of the information (baseband) signal, while the amplitude and phase of the carrier remain constant.
සංඛ්‍යාත මුහුර්ජනයේදී, වාහක සංඥාවේ සංඛ්‍යාතය තොරතුරු සංඥාවේ විස්තාරයට සමානුපාතිකව වෙනස් කරන අතර, වාහකයේ විස්තාරය සහ කලාව නියතව පවතී.

A high-frequency message signal is represented by carrier waves that are closer together, while a low-frequency message signal is represented by carrier waves that are farther apart.
ඉහළ සංඛ්‍යාත පණිවිඩ සංඥාවක් එකිනෙකට සමීප වාහක තරංග මඟින්ද, අඩු සංඛ්‍යාත පණිවිඩ සංඥාවක් එකිනෙකට ඈතින් පිහිටි වාහක තරංග මඟින්ද නිරූපණය කෙරේ.



i. Modulating signal
මුහුර්ජන සංඥාව
ii. Carrier waveform
වාහක තරංග ආකාරය
iii. Frequency modulated signal
සංඛ්‍යාත මුහුර්ජන කළ සංඥාව

Applications of FM
FM හි යෙදුම්

- Radio broadcasting
  ගුවන්විදුලි විකාශනය
- Television broadcasting
  රූපවාහිනී විකාශනය
- Wireless microphones
  රැහැන් රහිත මයික්‍රෆෝන

ictfromabc.com

Advantages
වාසි

More resistant to noise because information is carried by changes in frequency rather than amplitude.
තොරතුරු රැගෙන යන්නේ විස්තාරයේ වෙනස්වීම් මඟින් නොව සංඛ්‍යාතයේ වෙනස්වීම් මඟින් බැවින් බාහිර ඝෝෂාවන්ට වඩා හොඳින් ඔරොත්තු දේ.

Provides better sound quality because it is less affected by noise and interference.
ඝෝෂා සහ බාධා කිරීම්වලින් අවම බලපෑමක් ඇති වන බැවින් ගුණාත්මකභාවයෙන් ඉහළ ශබ්දයක් ලබා දෙයි.

Has higher fidelity because it reproduces the original audio signal more accurately over a wider range of frequencies.
පුළුල් සංඛ්‍යාත පරාසයක් ඔස්සේ මුල් ශ්‍රව්‍ය සංඥාව වඩාත් නිවැරදිව ප්‍රතිනිර්මාණය කරන බැවින් මෙහි නිවැරදිතාවය ඉහළය.

Disadvantages
අවාසි

Requires a larger bandwidth because the carrier frequency varies over a wider range to transmit the information.
තොරතුරු සම්ප්‍රේෂණය සඳහා වාහක සංඛ්‍යාතය පුළුල් පරාසයක වෙනස් වන බැවින් විශාල කලාප පළලක් අවශ්‍ය වේ.

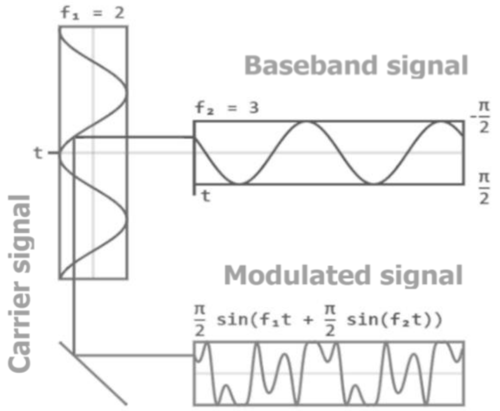
Requires more complex circuits because generating and detecting frequency variations is more complicated than amplitude variations.
සංඛ්‍යාත වෙනස්වීම් ඇති කිරීම සහ ඒවා හඳුනා ගැනීම විස්තාර වෙනස්වීම්වලට වඩා සංකීර්ණ වන බැවින් මේ සඳහා වඩාත් සංකීර්ණ පරිපථ අවශ්‍ය වේ.

---

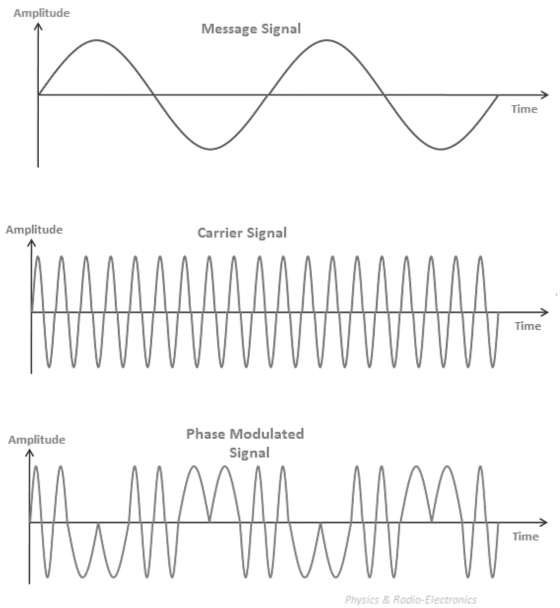
3. Phase modulation (PM)
කලා මූර්ජනය

In phase modulation, the phase of the carrier signal is varied in proportion to the amplitude of the information (baseband) signal, while the carrier's amplitude and frequency remain constant.
කලා මූර්ජනයේදී, වාහක සංඥාවේ කලාව තොරතුරු සංඥාවේ විස්තාරයට සමානුපාතිකව වෙනස් කරන අතර, වාහකයේ විස්තාරය සහ සංඛ්‍යාතය නියතව පවතියි.

Example / උදාහරණ 1



Example / උදාහරණ 2



Applications of PM
PM හි යෙදුම්

- In microwave links and satellite communications.
  ක්ෂුද්‍ර තරංග සම්බන්ධතා සහ චන්ද්‍රිකා සන්නිවේදන වල.
- In some RFID systems
  සමහර RFID පද්ධතිවල

Advantages
වාසි

More resistant to noise than AM because information is carried by changes in the phase of the carrier wave rather than its amplitude.
තොරතුරු රැගෙන යන්නේ වාහක තරංගයේ කලාවේ සිදුවන වෙනස්වීම් මඟින් බැවින් AM වලට වඩා ඝෝෂාවන්ට ඔරොත්තු දීමේ හැකියාව ඇත.

Forms the basis of many digital communication systems because digital data can be efficiently represented by changes in the carrier wave's phase.
වාහක තරංගයේ කලාවේ වෙනස්වීම් මඟින් ඩිජිටල් දත්ත කාර්යක්ෂමව නිරූපණය කළ හැකි බැවින් මෙය බොහෝ ඩිජිටල් සන්නිවේදන පද්ධතිවල පදනම වේ.

Disadvantages
අවාසි

More complex because it requires precise control and detection of phase changes in the carrier signal.
වාහක සංඥාවේ කලා වෙනස්වීම් ඉතා නිවැරදිව පාලනය කිරීම සහ හඳුනා ගැනීම අවශ්‍ය වන බැවින් මෙය වඩාත් සංකීර්ණ වේ.

More difficult to visualize and understand because changes in phase are less intuitive and harder to observe than changes in amplitude or frequency.
විස්තාරයේ හෝ සංඛ්‍යාතයේ වෙනස්වීම්වලට සාපේක්ෂව කලාවේ වෙනස්වීම් සහජයෙන්ම වටහා ගැනීමට සහ නිරීක්ෂණය කිරීමට අපහසුය.

Digital Modulation
අංකිත මූර්ජනය

1. Amplitude Shift Keying (ASK)
විස්තාර සීරු මාරුව

The amplitude of the carrier signal is varied to represent different data bits.
විවිධ දත්ත බිටු නියෝජනය කිරීම සඳහා වාහක සංඥාවේ විස්තාරය වෙනස් කෙරේ.

In other words, the height of the carrier wave is changed to encode the information.
වෙනත් වචන වලින් කිවහොත්, තොරතුරු කේතනය කිරීම සඳහා වාහක තරංගයේ විස්තාරය වෙනස් කෙරේ.

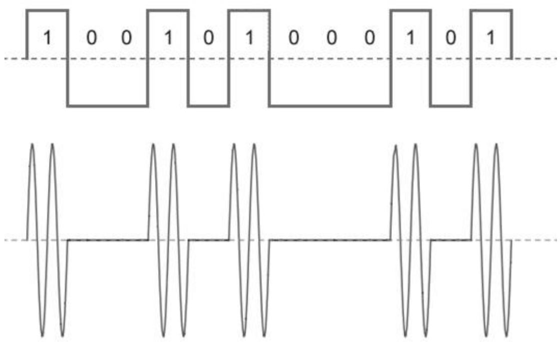
Only the amplitude of the carrier wave changes, while its frequency and phase remain constant.
වාහක තරංගයේ විස්තාරය පමණක් වෙනස් වන අතර, එහි සංඛ්‍යාතය සහ කලාව නියතව පවතියි.

Applications of ASK
ASK හි යෙදුම්

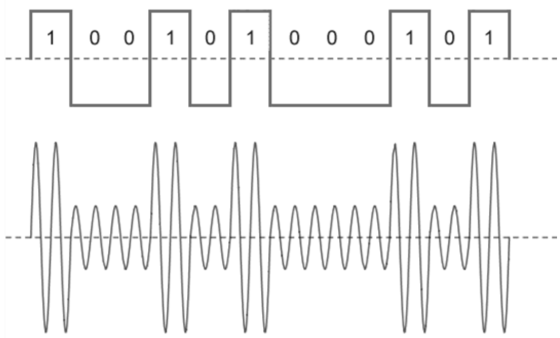
- RFID systems for data transmission between tags and readers.
  ටැග් සහ රීඩර් අතර දත්ත සම්ප්‍රේෂණය සඳහා RFID පද්ධතිවල ASK බහුලව භාවිතා වේ.
- Remote control systems.
  දුරස්ථ පාලන පද්ධතිවල.
- Other data transmission
  අනෙකුත් දත්ත සම්ප්‍රේෂණ

Types of ASK
ASK වර්ග

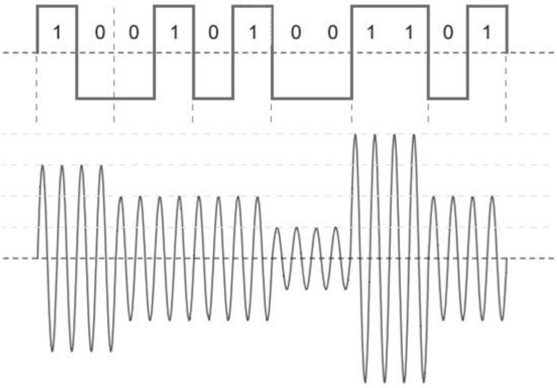
On-off keying (OOK)
The carrier signal is either present (on) or absent (off) to represent the data bits.
දත්ත බිටු නියෝජනය කිරීම සඳහා වාහක සංඥාව සක්‍රිය හෝ අක්‍රිය ලෙස භාවිතා වේ.



Two-level ASK (Binary ASK)
The carrier signal can have two amplitude levels, representing the data bits 0 and 1.
දත්ත බිටු 0 සහ 1 නියෝජනය කරමින් වාහක සංඥාවට විස්තාර මට්ටම් දෙකක් තිබිය හැක.



Multi-level ASK
The carrier signal can have multiple amplitude levels, representing more than two data bits.
දත්ත බිටු දෙකකට වඩා නියෝජනය කරමින් වාහක සංඥාවට බහු විස්තාර මට්ටම් තිබිය හැක.



Advantages
වාසි

Simple to implement because only the amplitude of the carrier wave is changed to represent digital data.
ඩිජිටල් දත්ත නිරූපණය කිරීම සඳහා වාහක තරංගයේ විස්තාරය පමණක් වෙනස් කරන බැවින් ක්‍රියාත්මක කිරීමට ඉතා සරල ය.

Uses inexpensive hardware because it requires simple transmitter and receiver circuits.
සරල සම්ප්‍රේෂක සහ ග්‍රාහක පරිපථ පමණක් අවශ්‍ය වන බැවින් වියදම් අඩු දෘඩාංග භාවිතා කළ හැක.

Easy to modulate and demodulate because the receiver only needs to detect changes in the carrier amplitude.
ග්‍රාහකයාට අවශ්‍ය වන්නේ වාහක විස්තාරයේ වෙනස්වීම් හඳුනා ගැනීම පමණක් බැවින් මූර්ඡන ක්‍රියාවලිය ඉතා පහසුය.

Disadvantages
අවාසි

Highly affected by noise because noise mainly alters the amplitude of the signal, which carries the information.
තොරතුරු අඩංගු විස්තාරයට බාහිර ඝෝෂාවන්ගෙන් දැඩි ලෙස බලපෑම් එල්ල විය හැක.

Has low reliability because noise and interference can easily cause errors in detecting the transmitted data.
ඝෝෂා සහ බාධා කිරීම් නිසා සම්ප්‍රේෂණය වන දත්ත හඳුනා ගැනීමේදී දෝෂ ඇති වීමේ ඉඩකඩ වැඩි බැවින් විශ්වසනීයත්වය අඩුය.

Has low power efficiency because a significant portion of the transmitted power is carried by the carrier signal rather than the information.
සම්ප්‍රේෂණය වන බලයෙන් සැලකිය යුතු කොටසක් තොරතුරු වෙනුවට වාහක සංඥාව විසින්ම රැගෙන යන බැවින් බල කාර්යක්ෂමතාව අඩුය.

---

2. Frequency shift keying (FSK)
සංඛ්‍යාත සීරු මාරුව

The frequency of a carrier signal is changed according to the digital data signal.
අංකිත දත්ත සංඥාව අනුව වාහක සංඥාවක සංඛ්‍යාතය වෙනස් කෙරේ.

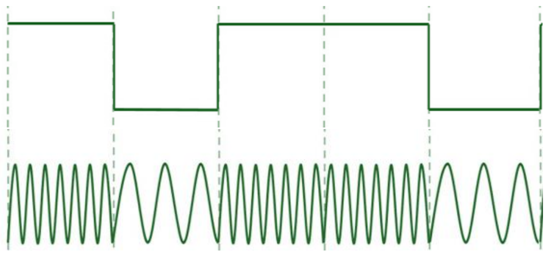
Only the frequency of the carrier wave changes, while its amplitude and phase remain constant.
වාහක තරංගයේ සංඛ්‍යාතය පමණක් වෙනස් වන අතර, එහි විස්තාරය සහ කලාව නියතව පවතියි.

Applications of FSK
FSK හි යෙදුම්

- Radio frequency identification (RFID)
  ගුවන්විදුලි සංඛ්‍යාත හඳුනාගැනීම (RFID)
- Remote control / දුරස්ථ පාලකය
- Data transmission / දත්ත සම්ප්‍රේෂණය

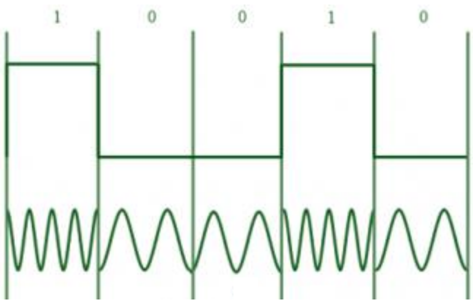
Types of FSK
FSK වර්ග

Continuous phase FSK (CPFSK)
The phase of the carrier signal is continuous between frequency shifts, which can improve the spectral efficiency of FSK.
FSK හි සංඛ්‍යාත වර්ණාවලි කාර්යක්ෂමතාව වැඩිදියුණු කළ හැකි සංඛ්‍යාත මාරුවීම් අතර වාහක සංඥාවේ කලාව අඛණ්ඩව පවතී.



Minimum shift keying (MSK)

A special case of CPFSK where the frequency shift is exactly half the bit rate, which provides good spectral efficiency and noise immunity.
වඩා හොඳ සංඛ්‍යාත වර්ණාවලි කාර්යක්ෂමතාවයක් සහ ඝෝෂා ප්‍රතිශක්තියක් සපයන සංඛ්‍යාත මාරුව හරියටම බිටු අනුපාතයෙන් අඩක් වන CPFSK හි විශේෂ අවස්ථාවකි.



Advantages
වාසි

More resistant to noise than ASK because information is carried by changes in frequency rather than amplitude.
තොරතුරු රැගෙන යන්නේ සංඛ්‍යාතයේ වෙනස්වීම් මගින් බැවින් ASK වලට වඩා හොඳින් ඝෝෂාවන්ට ඔරොත්තු දේ.

More reliable because frequency changes are less likely to be affected by noise and interference.
සංඛ්‍යාත වෙනස්වීම්වලට බාහිර ඝෝෂා සහ බාධා කිරීම්වලින් බලපෑම් ඇති වීමට ඇති ඉඩකඩ අඩු බැවින් විශ්වසනීයත්වය වැඩිය.

The carrier wave's amplitude remains constant, which allows for efficient amplification and less distortion.
වාහක තරංගයේ විස්තාරය නියතව පවතින බැවින්, සංඥාව විකෘති වීමකින් තොරව කාර්යක්ෂමව වර්ධනය කළ හැක.

Disadvantages
අවාසි

Requires a larger bandwidth because different frequencies are used to represent binary data.
ද්වීමය දත්ත නිරූපණය කිරීම සඳහා විවිධ සංඛ්‍යාතයන් භාවිතා කරන බැවින් විශාල කලාප පළලක් අවශ්‍ය වේ.

More complex than ASK because it requires circuits that can accurately generate and detect multiple frequencies.
විවිධ සංඛ්‍යාතයන් නිවැරදිව නිපදවිය හැකි සහ හඳුනාගත හැකි පරිපථ අවශ්‍ය වන බැවින් මෙය ASK වලට වඩා සංකීර්ණ වේ.

3. Phase shift keying (PSK)
කලා සීරු මාරුව

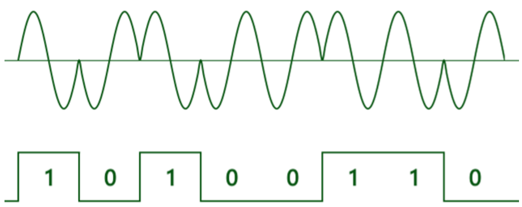
The phase of the carrier signal is changed in response to the digital data signal.
අංකිත දත්ත සංඥාවට ප්‍රතිචාර වශයෙන් වාහක සංඥාවේ කලාව වෙනස් කෙරේ.

In other words, the starting point of the carrier wave is changed to encode the information.
වෙනත් වචන වලින් කිවහොත්, තොරතුරු කේතනය කිරීමට වාහක තරංගයේ ආරම්භක ලක්ෂ්‍යය වෙනස් කෙරේ.

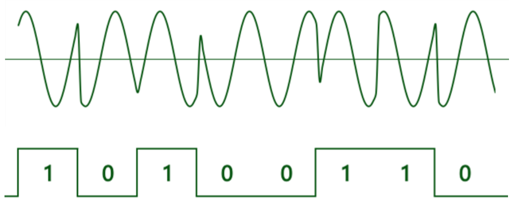
Only the phase of the carrier wave changes, while its amplitude and frequency remain constant.
වාහක තරංගයේ කලාව පමණක් වෙනස් වන අතර, එහි විස්තාරය සහ සංඛ්‍යාතය නියතව පවතියි.

Types of PSK

Binary phase shift keying (BPSK)
The carrier signal is shifted by either 0 or 180 degrees to represent the data bits 0 and 1.
0 සහ 1 දත්ත බිටු නියෝජනය කිරීම සඳහා වාහක සංඥාව අංශක 0 හෝ 180 කින් මාරු කරනු ලැබේ.



Quadrature phase shift keying (QPSK)
The carrier signal is shifted by one of four possible phases (0, 90, 180, or 270 degrees) to represent two bits of data.
දත්ත බිටු දෙකක් නියෝජනය කිරීම සඳහා පැවතිය හැකි කලා හතරකින් එකකින් (අංශක 0, 90, 180, හෝ 270) වාහක සංඥාව මාරු කරනු ලැබේ.



Applications of PSK / PSK හි යෙදුම්

- Wireless communication systems.
  රැහැන් රහිත සන්නිවේදන පද්ධතිවල.
- PSK is used for data transmission between satellites and ground stations.
  චන්ද්‍රිකා සහ භූමි ස්ථාන අතර දත්ත සම්ප්‍රේෂණය සඳහා PSK භාවිතා වේ.
- PSK can be used for digital audio and video transmission.
  PSK අංකිත ශ්‍රව්‍ය සහ දෘශ්‍ය සම්ප්‍රේෂණය සඳහා භාවිතා කළ හැකිය.

ictfromabc.com

Advantages
වාසි

Has excellent noise immunity because information is carried by changes in the carrier wave's phase, which is less affected by noise.
තොරතුරු රැගෙන යන්නේ ඝෝෂාවන්ගෙන් අවම බලපෑමක් ඇති වන කලාවේ වෙනස්වීම් මඟින් බැවින් මෙයට විශිෂ්ට ඝෝෂා ප්‍රතිරෝධයක් ඇත.

Has high bandwidth efficiency because multiple bits can be transmitted per symbol using different phase states.
විවිධ කලා තත්ත්වයන් භාවිතා කරමින් එක් සංකේතයක් හරහා බිටු කිහිපයක් සම්ප්‍රේෂණය කළ හැකි බැවින් කලාප පළල ඉතා කාර්යක්ෂමව භාවිතා වේ.

Disadvantages
අවාසි

More complex to implement because it requires accurate generation and detection of phase changes.
කලා වෙනස්වීම් නිවැරදිව නිපදවීම සහ හඳුනා ගැනීම අවශ්‍ය වන බැවින් මෙය ප්‍රායෝගිකව ක්‍රියාත්මක කිරීම සංකීර්ණ වේ.

Requires precise synchronization because the receiver must accurately detect the carrier wave's phase to recover the transmitted data.
සම්ප්‍රේෂණය කළ දත්ත නැවත ලබා ගැනීමට නම් ග්‍රාහකයා විසින් වාහක තරංගයේ කලාව ඉතා නිවැරදිව හඳුනාගත යුතු බැවින් නිශ්චිත සමමුහුර්තකරණයක් අත්‍යවශ්‍ය වේ.

Pulse Code Modulation (PCM)
ස්පන්දන කේත මූර්ජනය

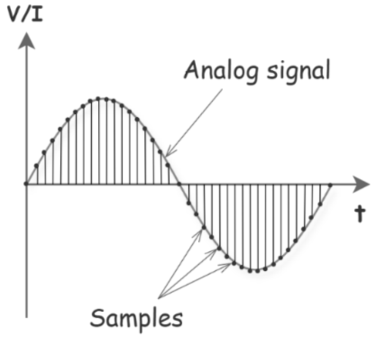
Pulse Code Modulation encoding is a technique used to convert analog signals into digital signals.
ස්පන්දන කේත මූර්ජනය යනු ප්‍රතිසම සංඥා අංකිත සංඥා බවට පරිවර්තනය කිරීම සඳහා භාවිතා කරන තාක්ෂණයකි.

It involves three main steps.
එයට ප්‍රධාන පියවර තුනක් ඇතුළත් වේ.

- Sampling
- Quantizing
- Encoding

Sampling
Sampling is the process of measuring the amplitude (or strength) of an analog signal at regular intervals.
Sampling යනු ප්‍රතිසම සංඥාවක විස්තාරය (හෝ ශක්තිය) නිත්‍ය කාල පරාසයන් තුළ මැනීමේ ක්‍රියාවලියයි.

These measurements capture **snapshots** of the continuous analog signal.
මෙම මිනුම් සන්තතික ප්‍රතිසම සංඥාවේ **snapshots** ලබා ගනී.



Nyquist Theorem
Nyquist ගේ න්‍යාය
According to the Nyquist theorem, the sampling rate (number of samples taken per second) must be at least twice the highest frequency of the analog signal to accurately represent it without losing any information.
Nyquist ගේ න්‍යායට අනුව, කිසිදු තොරතුරක් අහිමි නොවී සංඥාව නිවැරදිව නිරූපණය කිරීම සඳහා නියැදි ලබා ගැනීමේ අනුපාතය (තත්පරයට ගන්නා ලද සාම්පල ගණන) අවම වශයෙන් ප්‍රතිසම සංඥාවේ ඉහළම සංඛ්‍යාතය මෙන් දෙගුණයක් විය යුතුය.

This minimum sampling rate is called the **Nyquist rate**.
මෙම අවම නියැදි අනුපාතය **Nyquist අනුපාතය** ලෙස හැඳින්වේ.
If the sampling rate is too low, it causes aliasing, where higher-frequency components of the signal are misinterpreted as lower frequencies.
නියැදි අනුපාතය ඉතා අඩු නම්, එය අන්වර්ථකරණයට හේතු වේ, එහිදී සංඥාවේ ඉහළ සංඛ්‍යාත සංරචක අඩු සංඛ්‍යාත ලෙස වැරදි ලෙස අර්ථකථනය කෙරේ.

If the sampling rate is sufficiently high, the analog signal can be accurately represented in digital form without distortion.
නියැදි අනුපාතය ප්‍රමාණවත් තරම් ඉහළ නම්, ප්‍රතිසම සංඥාව විකෘති වීමකින් තොරව අංකිත ආකාරයෙන් නිවැරදිව නිරූපණය කළ හැකිය.

Example
In audio recording, standard digital audio is sampled at 44.1 kHz, meaning 44,100 samples are taken every second, which is more than twice the highest frequency humans can hear (about 20 kHz).
ශ්‍රව්‍ය පටිගත කිරීමේදී, සම්මත සංඛ්‍යාංක ශ්‍රව්‍ය 44.1 kHz හීදී නියැදි කෙරේ, එනම් සෑම තත්පරයකටම සාම්පල 44,100ක් ගනු ලැබේ, එය මිනිසුන්ට ඇසෙන ඉහළම සංඛ්‍යාතය (20 kHz පමණ) මෙන් දෙගුණයකටත් වඩා වැඩිය.

ictfromabc.com

Quantizing

Quantizing is the process of converting the sampled analog values into a finite set of levels.

Quantizing යනු නියැදි ලබාගත් ප්‍රතිසම අගයන් සීමිත මට්ටම් කට්ටලයක් බවට පරිවර්තනය කිරීමේ ක්‍රියාවලියයි.

This step maps the infinite range of amplitudes of the analog signal to a limited number of **discrete values**.

මෙම පියවර මගින් ප්‍රතිසම සංඥාවේ අසීමිත පරාසය සීමිත විවික්ත අගයන් ගණනකට සිතියම්ගත කරයි.

The more levels available, the more accurately the signal can be represented.

පවතින මට්ටම් වැඩි වන තරමට සංඥාව වඩාත් නිවැරදිව නිරූපණය කළ හැකිය.

Example

If we have 8 bits for each sample, we can have 2^8 = 256 possible levels to represent the amplitude.

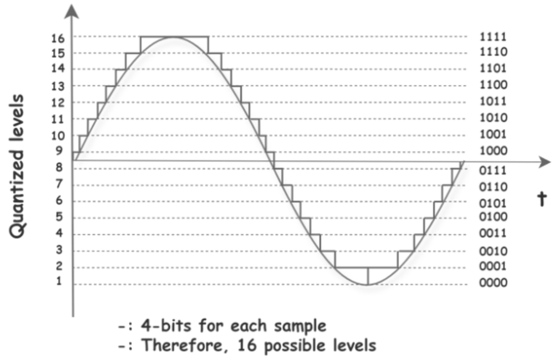
අපට එක් එක් නියැදිය සඳහා බිටු 8ක් තිබේ නම්, විස්තාරය නිරූපණය කිරීමට හැකි මට්ටම් 2^8 = 256ක් තිබිය හැක.

With 16 bits, we have 2^{16} = 65,536 levels, which leads to a more accurate representation of the signal.

බිටු 16 කින්, අපට 2^{16} = 65,536 මට්ටම් ඇත, එය සංඥාව වඩාත් නිවැරදිව නිරූපණය කිරීමට මග පාදයි.

Since quantization involves rounding the continuous analog values to the nearest available level, some information is lost, introducing a small error called quantization error.

Quantization වලට අඛණ්ඩ ප්‍රතිසම අගයන් ළඟම ඇති මට්ටමට වැටයීම ඇතුළත් වන බැවින්, සමහර තොරතුරු නැති වී යන අතර, quantization error නම් කුඩා දෝෂයක් හඳුන්වා දෙයි.



Encoding

Encoding is the process of converting each quantized sample into a binary number.

Encoding යනු එක් එක් ප්‍රමාණාත්මක සාම්පල ද්විමය සංඛ්‍යාවක් බවට පරිවර්තනය කිරීමේ ක්‍රියාවලියයි.

Each level from the quantization process is represented by a binary code, which is then transmitted or stored.

Quantization ක්‍රියාවලියේ සෑම මට්ටමක්ම ද්විමය කේතයකින් නිරූපණය වන අතර එය සම්ප්‍රේෂණය හෝ ගබඩා කරනු ලැබේ.

Example

After quantizing an audio signal, if the value is 160 (out of 256 possible levels), its binary representation in an 8-bit system would be 10100000. This binary value is then transmitted as part of the digital signal.

ශ්‍රව්‍ය සංඥාවක් quantize කිරීමෙන් පසු, අගය 160 (මට්ටම් 256න්) නම්, බිටු 8හි පද්ධතියක එහි ද්විමය නිරූපණය 10100000 වේ. මෙම ද්විමය අගය ඩිජිටල් සංඥාවේ කොටසක් ලෙස සම්ප්‍රේෂණය වේ.

AM vs. FM vs. PM

Property	**AM**	**FM**	**PM**
Modulated Aspect මූර්ජනය වන අංගය	Amplitude විස්තාරය	Frequency සංඛ්‍යාතය	Phase කලාව
Bandwidth කලාප පළල	Narrow පටු	Wide පුළුල්	Medium මධ්‍යස්ථ
Noise Resistance ඝෝෂා ප්‍රතිරෝධය	Low අඩු	High ඉහළ	High ඉහළ
Signal Quality සංඥාවේ ගුණාත්මකභාවය	Affected බලපෑමට ලක්වේ	Stable ස්ථාවර	Stable ස්ථාවර
Applications භාවිතයන්	AM Radio, TV AM රේඩියෝ, රූපවාහිනී	FM Radio, TV FM රේඩියෝ, රූපවාහිනී	Satellite, Radio චන්ද්‍රිකා, රේඩියෝ
Efficiency කාර්යක්ෂමතාව	Low අඩු	Medium මධ්‍යස්ථ	Medium මධ්‍යස්ථ
Complexity සංකීර්ණත්වය	Low අඩු	Medium මධ්‍යස්ථ	Medium මධ්‍යස්ථ

ASK vs. FSK vs. PSK

Property	**ASK**	**FSK**	**PSK**
Modulated Aspect මූර්ජනය වන අංගය	Amplitude විස්තාරය	Frequency සංඛ්‍යාතය	Phase කලාව
Bandwidth කලාප පළල	Narrow පටු	Wide පුළුල්	Medium මධ්‍යස්ථ
Noise Resistance ඝෝෂා ප්‍රතිරෝධය	Low අඩු	High ඉහළ	Moderate මධ්‍යස්ථ
Signal Stability සංඥා ස්ථායීතාව	Less Stable ස්ථායීතාව අඩුයි	More Stable වඩා ස්ථායීයි	More Stable වඩා ස්ථායීයි
Applications භාවිතයන්	IR, Remote Controls අධෝරක්ත කිරණ, දුරස්ථ පාලක	Modems, Radio මොඩම්, ගුවන්විදුලිය	Satellite, Wi-Fi චන්ද්‍රිකා තාක්ෂණය, Wi-Fi
Efficiency කාර්යක්ෂමතාව	Low අඩු	Medium මධ්‍යස්ථ	High ඉහළ
Complexity සංකීර්ණත්වය	Low අඩු	Medium මධ්‍යස්ථ	Medium මධ්‍යස්ථ

The importance of modulation
මූර්ජණයෙහි වැදගත්කම

1. Multiplexing
බහුපතකරණය

Allows multiple signals to be transmitted simultaneously by assigning different frequency bands to each signal, making efficient use of the available spectrum.
එක් එක් සංඥාව සඳහා විවිධ සංඛ්‍යාත පරාසයන් වෙන් කරදීම මඟින් සංඥා කිහිපයක් එකවර සම්ප්‍රේෂණය කිරීමට ඉඩ සලසයි. එමඟින් පවතින සංඛ්‍යාත අවකාශය කාර්යක්ෂමව භාවිතා කළ හැක.

2. Efficient Signal Transmission
කාර්යක්ෂම සංඥා සම්ප්‍රේෂණය

Enables low-frequency signals to be transmitted over long distances by converting them into high-frequency carrier signals.
අඩු සංඛ්‍යාත සංඥා, ඉහළ සංඛ්‍යාත වාහක සංඥා බවට පරිවර්තනය කිරීම මඟින් ඒවා දුර බැහැර ස්ථාන වෙත කාර්යක්ෂමව සම්ප්‍රේෂණය කිරීමට මඟ පාදයි.

3. Maximizing Bandwidth Usage
කලාප පළල උපරිමව භාවිත කිරීම

Improves bandwidth utilization by allowing multiple communication channels to share the same transmission medium using techniques such as Frequency Division Multiplexing (FDM).
සංඛ්‍යාත විභාජන බහුපතකරණය වැනි තාක්ෂණයන් හරහා එකම සන්නිවේදන මාධ්‍යය බෙදා ගැනීමට සන්නිවේදන නාලිකා කිහිපයකට ඉඩ සලසමින් කලාප පළල උපරිමව ප්‍රයෝජනයට ගනියි.

4. Reducing Interference and Noise
බාධා කිරීම් සහ ඝෝෂාවන් අවම කිරීම

Shifts signals to frequency ranges that are less affected by interference and electrical noise, improving transmission reliability.
බාහිර බාධා කිරීම් සහ විද්‍යුත් ඝෝෂාවන්ගෙන් අඩු බලපෑමක් ඇති සංඛ්‍යාත පරාසයන් වෙත සංඥාවන් විස්ථාපනය කිරීම මඟින් සම්ප්‍රේෂණයේ විශ්වසනීයත්වය ඉහළ නංවයි.

5. Improved Signal Quality
වැඩිදියුණු කළ සංඥා ගුණාත්මකභාවය

Improves signal quality by matching the signal to the transmission medium, with techniques like FM providing better noise resistance than AM.
සන්නිවේදන මාධ්‍යයට ගැළපෙන පරිදි සංඥාව සකස් කිරීම මඟින් සංඥා ගුණාත්මකභාවය ඉහළ නංවයි. උදාහරණයක් ලෙස, FM තාක්ෂණය මඟින් AM වලට වඩා හොඳ ඝෝෂා ප්‍රතිරෝධයක් ලබා දෙයි.

Routing methods in networking
ජාලකරණයේ ඇති මාර්ගගත කිරීමේ ක්‍රම

1. Circuit Switching

Circuit switching is a communication method where a dedicated communication path or circuit is established between two devices before data transmission begins.
Circuit switching යනු දත්ත සම්ප්‍රේෂණය ආරම්භ වීමට පෙර උපාංග දෙකක් අතර ඒවාටම වෙන්වූ සන්නිවේදන මාර්ගයක් හෝ පරිපථයක් ස්ථාපිත කරන සන්නිවේදන ක්‍රමයකි.

This path remains reserved for the entire duration of the communication session.
මෙම මාර්ගය සන්නිවේදන සැසියේ මුළු කාලය සඳහාම වෙන් කර ඇත.

There's no need to reassemble the data since the dedicated circuit maintains the sequence.
වෙන්වූ පරිපථය දත්ත අනුපිළිවෙල පවත්වා ගෙන යන බැවින් නැවත එකලස් කිරීමේ අවශ්‍යතාවයක් නොමැත.

After the communication is complete, this dedicated path is released.
සන්නිවේදනය අවසන් වූ පසු, මෙම වෙන් කරගත් මාර්ගය මුදා හරිනු ලැබේ.

Advantages

Since the path is dedicated, there's no delay caused by routing or congestion.
මාර්ගය වෙන්වී ඇති බැවින්, මාර්ගගත කිරීම හෝ තදබදය හේතුවෙන් ප්‍රමාදයක් නොමැත.

Guaranteed bandwidth ensures constant performance throughout the communication.
සහතික කළ කලාප පළල සන්නිවේදනය පුරා නියත කාර්ය සාධනය සහතික කරයි.

Disadvantages

The dedicated path is reserved even if no data is being transmitted, leading to wasted resources.
දත්ත සම්ප්‍රේෂණය නොකෙරෙන අවසථාවාලදී පවා මාර්ගය වෙන් කර ඇති බැවින් සම්පත් අපතේ යයි.

Maintaining dedicated circuits can be expensive, especially for large networks.
විශේෂයෙන් විශාල ජාල සඳහා වෙන්වූ පරිපථ නඩත්තු කිරීම මිල අධික විය හැක.

Public Switched Telephone Networks (PSTN)

A worldwide public telephone network (also called the traditional/landline telephone network) that enables voice communication over long distances.
දිගු දුරක් පුරා හඬ සන්නිවේදනය සක්‍රීය කරනු ලබන, ලොව පුරා විහිදුණු පොදු දුරකථන ජාලයකි (මෙය සාම්ප්‍රදායික/ස්ථාවර දුරකථන ජාලය ලෙසද හැඳින්වේ).

How It Works / එය ක්‍රියා කරන ආකාරය

1. Caller dials a number
   ඇමතුම්කරු අංකයක් ආදානය කරයි
2. Exchange identifies destination
   මධ්‍යස්ථානය මඟින් ගමනාන්තය හඳුනා ගනී
3. Connection established
   සම්බන්ධතාවය ගොඩනඟයි
4. Users communicate
   පරිශීලකයින් සන්නිවේදනය කරයි
5. Connection terminated after the call.
   ඇමතුම අවසන් වූ පසු සම්බන්ධතාවය විසන්ධි වේ

Analog Voice Transmission
PSTN was originally designed to carry analog voice signals. When you speak into a phone, your voice creates analog sound waves, which are converted into electrical signals and transmitted over telephone lines.
PSTN මුලින් නිර්මාණය කර ඇත්තේ ප්‍රතිසම හඬ සංඥා රැගෙන යාමටය. ඔබ දුරකථනයකට කතා කරන විට, ඔබේ හඬ ප්‍රතිසම ශබ්ද තරංග නිර්මාණය කරයි, ඒවා විදුලි සංඥා බවට පරිවර්තනය කර දුරකථන මාර්ග හරහා සම්ප්‍රේෂණය වේ.

Circuit Switching
PSTN uses circuit switching technology. When you make a call, a dedicated communication path (or circuit) is established between the caller and the receiver for the duration of the call.
PSTN circuit switching තාක්ෂණය භාවිතා කරයි. ඔබ ඇමතුමක් ගන්නා විට, ඇමතුමේ කාලසීමාව පුරා අමතන්නා සහ ග්‍රාහකයා අතර වෙන්වූ සන්නිවේදන මාර්ගයක් (හෝ පරිපථයක්) පිහිටුවා ඇත.

Modems for Digital Data
When computers use the PSTN to connect to the internet (Ex. Dial-Up / ISDN), a modem is required. Modems are used for modulation and demodulation.
අන්තර්ජාලයට සම්බන්ධ වීමට පරිගණක PSTN භාවිතා කරන විට (උදා. Dial-Up / ISDN), මොඩමයක් අවශ්‍ය වේ. ප්‍රමිතකරණය සහ ප්‍රතිප්‍රමිතකරණය සඳහා මොඩම් භාවිතා කරනු ලැබේ.

Main Components of PSTN
PSTN හි ප්‍රධාන සංරචක

- Telephone (sends/receives voice)
  දුරකථනය (හඬ සංඥා යැවීම සහ ලබා ගැනීම සිදු කරයි)
- Communication Channel (twisted pair, cables, wireless links)
  සන්නිවේදන නාලිකාව (ඇඹරුණු කම්බි යුගල, කේබල් හෝ රැහැන් රහිත සබැඳි මඟින් සමන්විත වේ.)
- Telephone Exchange (switching center).
  දුරකථන මධ්‍යස්ථානය (ඇමතුම් නිවැරදි දිශාවට යොමු කරන මාරු කිරීමේ මධ්‍යස්ථානයයි)

Services Provided by PSTN
PSTN මඟින් සපයනු ලබන සේවාවන්

Voice calls ඇමතුම්	Call forwarding ඇමතුම් ඉදිරියට යැවීම
Caller ID අමතන්නා හඳුනාගැනීම	Conference calling සම්මන්ත්‍රණ ඇමතුම්

Advantages and disadvantages of PSTN
PSTN හි වාසි සහ අවාසි

Advantages වාසි	**Disadvantages අවාසි**
Wide coverage පුළුල් ආවරණයක් පැවතීම	Slower than modern systems නවීන පද්ධතිවලට වඩා වේගයෙන් අඩු වීම
Reliable විශ්වාසවන්තභාවය	Higher Costs වැඩි පිරිවැයක් වැය වීම
Easy to use භාවිතය පහසු වීම	Limited multimedia support සීමිත බහුමාධ්‍ය සහාය
Well-established infrastructure හොඳින් ස්ථාපිත වූ යටිතල පහසුකම්	Being gradually replaced ක්‍රමයෙන් භාවිතයෙන් ඉවත් වෙමින් පැවතීම

PSTN vs. VoIP

Feature	**PSTN**	**VoIP**
Switching	Circuit	Packet
Network	Telephone	IP
Bandwidth	Dedicated	Shared
Cost	Higher	Lower
Voice Quality	Consistent	Depends on network
Scalability	Lower	Higher

Technologies that use PSTN
PSTN භාවිතා කරන තාක්ෂණයන්

Internet access technologies using PSTN
PSTN භාවිතා කරන අන්තර්ජාල ප්‍රවේශ තාක්ෂණයන්

- Dial-up Internet
- DSL (ADSL, VDSL, SDSL, etc.)
- ISDN (Integrated Services Digital Network)

Telephone services using PSTN
PSTN භාවිතා කරන දුරකථන සේවාවන්

- Traditional landline telephone service
  සාම්ප්‍රදායික ස්ථාවර දුරකථන සේවාව
- Emergency telephone services
  හදිසි දුරකථන සේවාවන්

Other PSTN-based communication technologies / PSTN මත පදනම් වූ වෙනත් සන්නිවේදන තාක්ෂණයන්

- Fax (Group 3 Fax)
- Old POS terminals
  පැරණි POS පර්යන්ත
- Elevator emergency phones
  විදුලි සෝපාන හදිසි දුරකථන

Technologies that do NOT use PSTN
PSTN භාවිතා නොකරන තාක්ෂණයන්

- Cable Internet using coaxial cable
- Fiber Internet, such as FTTH/FTTP
- Fixed wireless Internet
- Mobile Internet, such as 3G, 4G, and 5G
- Satellite Internet (Starlink)
- Wi-Fi

Time Division Multiplexing (TDM)
කාල විභජන බහුපථකරණය

PSTN carries multiple calls over the same line simultaneously by dividing bandwidth into time slots
PSTN මඟින් කලාප පළල කාල කොටස් වලට බෙදීම මඟින් එකම මාර්ගය ඔස්සේ එකවර ඇමතුම් කිහිපයක් රැගෙන යයි.

Note:
Many countries (UK, USA, Japan, etc.) are actively decommissioning PSTN and migrating entirely to IP-based networks.
බොහෝ රටවල් (එක්සත් රාජධානිය, ඇමරිකා එක්සත් ජනපදය, ජපානය, ආදිය) සක්‍රීයව PSTN භාවිතයෙන් ඉවත් කරමින් සම්පූර්ණයෙන්ම IP මත පදනම් වූ ජාල (IP-based networks) වෙත සංක්‍රමණය වෙමින් පවතී.

2. Packet Switching

Packet switching is a communication method where data is broken down into smaller chunks called packets, and each packet is sent independently over the network.
Packet switching යනු දත්ත පැකට්ටු ලෙස හැඳින්වෙන කුඩා කොටස් වලට බෙදා ඇති සන්නිවේදන ක්‍රමයකි, එහිදී සෑම පැකට්ටුවක්ම ජාලය හරහා ස්වාධීනව යවනු ලැබේ.

Unlike circuit switching, this has no dedicated path; each packet can take a different route to reach the destination.
Circuit switching, මෙන් නොව, මෙයට වෙන්වූ මාර්ගයක් නොමැත; එක් එක් පැකට්ටුව ගමනාන්තයට ළඟා වීමට වෙනස් මාර්ගයක් ගත හැකිය.

Packets
Data is broken into small packets, and each packet has the sender's and receiver's address as well as sequencing information.
දත්ත කුඩා පැකට් වලට කැඩී ඇති අතර, සෑම පැකට්ටුවකම යවන්නාගේ සහ ලබන්නාගේ ලිපිනය මෙන්ම අනුක්‍රමික තොරතුරුද ඇත.

Dynamic Routing
Each packet can take different routes to reach the destination, based on network conditions, congestion, and availability.
ජාල තත්වය, තදබදය සහ පවතින බව මත පදනම්ව එක් එක් පැකට්ටුවකට ගමනාන්තයට ළඟා වීමට විවිධ මාර්ග ගත හැක.

Reassembly
At the receiver's end, packets are reassembled in the correct order using sequencing information.
ග්‍රාහක අන්තයේදී, අනුක්‍රමික තොරතුරු භාවිතයෙන් පැකට් නිවැරදි අනුපිළිවෙලින් නැවත සකස් කරනු ලබයි.

Protocols
Packet switching relies on communication protocols such as IP (Internet Protocol) for addressing and routing packets, TCP for reliable delivery, and UDP for faster, real-time transmission.
පැකට් සඳහා ලිපින ලබාදීමට සහ ඒවා නිවැරදි මාර්ග ඔස්සේ යැවීමට IP වැනි සන්නිවේදන ප්‍රොටෝකෝල මතද, විශ්වාසදායක ලෙස දත්ත බෙදා හැරීම සඳහා TCP මතද, සහ වඩාත් වේගවත්, තථ්‍ය කාලීන සම්ප්‍රේෂණය සඳහා UDP මතද පදනම් වේ.

Note:
How the Internet Uses Packet Switching
අන්තර්ජාලය Packet Switching භාවිතා කරන ආකාරය

When you load a webpage or send a message, your data is broken into small chunks called packets. Each packet contains
ඔබ වෙබ් පිටුවක් load කරන විට හෝ පණිවිඩයක් යවන විට, ඔබගේ දත්ත පැකට් ලෙස හැඳින්වෙන කුඩා කොටස් වලට කඩනු ලැබේ. සෑම පැකට්ටුවකම අඩංගු වන්නේ

- A piece of the data / දත්තවලින් කොටසක්
- The sender's IP address
  යවන්නාගේ IP ලිපිනය
- The destination IP address
  ලබන්නාගේ IP ලිපිනය
- A sequence numbers / අනුක්‍රමික අංකයක්

Packets travel independently across the internet different packets from the same file may take entirely different routes through different routers, depending on congestion and availability.
පැකට් අන්තර්ජාලය හරහා ස්වාධීනව ගමන් කරයි. තදබදය සහ පවතින හැකියාව මත පදනම්ව, එකම ගොනුවක විවිධ පැකට්, විවිධ රවුටර (routers) හරහා සම්පූර්ණයෙන්ම වෙනස් මාර්ග ඔස්සේ ගමන් කළ හැකිය.

At the destination, the protocol (usually TCP) uses the sequence numbers to reassemble the packets in the correct order, requesting retransmission of any that were lost.
ලබන ස්ථානයේදී, ප්‍රොටෝකෝලය (සාමාන්‍යයෙන් TCP) මඟින් පැකට් නිවැරදි අනුපිළිවෙලට නැවත එකලස් කිරීම සඳහා අනුක්‍රමික අංක භාවිතා කරන අතර, අතරමඟදී අහිමි වූ ඕනෑම පැකට්ටුවක් නැවත එවන ලෙස ඉල්ලා සිටියි.

This design makes the internet highly resilient if one router or link fails, packets simply find another path. It also allows the internet to serve millions of users simultaneously without dedicating a fixed circuit to each one.
මෙම සැලසුම අන්තර්ජාලය ඉහළ ප්‍රත්‍යස්ථතාවයකින් (resilient) යුක්ත කරයි. එනම් එක් රවුටරයක් හෝ සබැඳියක් බිඳ වැටුනහොත්, පැකට් වෙනත් මාර්ගයක් සොයා ගනී. එමෙන්ම එක් එක් පරිශීලකයා සඳහා ස්ථාවර පරිපථයක් (fixed circuit) වෙන් කිරීමකින් තොරව මිලියන සංඛ්‍යාත පරිශීලකයින්ට එකවර සේවා සැපයීමට ද මෙය අන්තර්ජාලයට ඉඩ සලසයි.

Advantages of Packet Switching
Packet Switching හි වාසි

1. Efficient use of bandwidth
   කලාප පළල කාර්යක්ෂමව භාවිත කිරීම
2. Multiple users can share the same network
   පරිශීලකයන් කිහිපදෙනෙකුට එකම ජාලය බෙදාහදා ගත හැකි වීම
3. No dedicated connection required
   වෙන් කරන ලද සම්බන්ධතාවක් අවශ්‍ය නොවීම
4. Supports data, voice, video, and multimedia
   දත්ත, හඬ, වීඩියෝ සහ බහුමාධ්‍ය සඳහා සහය දැක්වීම
5. Can reroute packets if a path fails
   ගමන් මාර්ගයක් අවහිර වුවහොත් පැකට් වෙනත් මාර්ගයකින් යැවිය හැකි වීම
6. Cost-effective for large networks
   විශාල ජාල සඳහා පිරිවැය අවම වීම
7. Scalable and easy to expand
   පහසුවෙන් පුළුල් කළ හැකි වීම

Disadvantages of Packet Switching
Packet Switching හි අවාසි

1. Variable delay (latency)
   වෙනස් වන ප්‍රමාද කාලය
2. Packets may arrive out of order
   පැකට් පිළිවෙළකින් තොරව ළඟා විය හැකි වීම
3. Packet loss can occur during congestion
   ජාලය තුළ තදබදයක් පවතින විට පැකට් නැති වී යා හැකි වීම
4. Jitter can affect real-time applications
   ජිටර් තත්ත්වයන් නිසා සජීවී යෙදුම්වලට බාධා ඇති විය හැකි වීම
5. Requires packet reassembly at the destination
   ගමනාන්තයේදී පැකට් නැවත මුල සිට පිළිවෙළකට සැකසීමට සිදු වීම
6. More complex than circuit switching
   සර්කිට් ස්විචින් වලට වඩා සංකීර්ණ වීම
7. Quality of service is not always guaranteed
   සේවාවේ ගුණාත්මකභාවය සැමවිටම සහතික කළ නොහැකි වීම

Packet Switching vs Circuit Switching

Feature / ලක්ෂණය	**Packet Switching**	**Circuit Switching**
Bandwidth **කලාප පළල**	Shared among users dynamically පරිශීලකයන් අතර ගතිකව හවුලේ පරිහරණය වේ	Dedicated per connection එක් සම්බන්ධතාවයකට වෙන් කර ඇත
Efficiency **කාර්යක්ෂමතාව**	High (idle bandwidth is reused) ඉහළයි (පවතින කලාප පළල නැවත භාවිත කෙරේ)	Lower (bandwidth reserved even when idle) අඩුයි (භාවිතයේ නොමැති විට පවා කලාප පළල වෙන් කර තබා ගනී)
Delay (latency) **ප්‍රමාදය**	Variable (packets may queue at routers) විචල්‍ය වේ (පැකට් රවුටර වල පෝලිම් ගැසිය හැක)	Predictable and consistent පුරෝකථනය කළ හැකි සහ ස්ථාවර වේ
Connection setup **සම්බන්ධතාවය පිහිටුවීම**	None (data is sent immediately) අවශ්‍ය නොවේ (දත්ත වහාම යවනු ලැබේ)	Required before any data can flow ඕනෑම දත්තයක් ගලා යාමට පෙර අවශ්‍ය වේ
Data delivery **දත්ත බෙදා හැරීම**	Packets may arrive out of order; reassembled at destination පැකට් අනුපිළිවෙලින් තොරව පැමිණිය හැක; ලබන ස්ථානයේදී නැවත එකලස් කෙරේ	Arrives in-order over a fixed path ස්ථාවර මාර්ගයක් ඔස්සේ නිවැරදි අනුපිළිවෙලට පැමිණේ
Fault tolerance **දෝෂ දරා ගැනීමේ හැකියාව**	High (packets re-route around failures) ඉහළයි (දෝෂ මඟහරිමින් පැකට් වෙනත් මාර්ග ඔස්සේ ගමන් කරයි)	Low (circuit breaks if the path fails) අඩුයි (මාර්ගය බිඳ වැටුනහොත් පරිපථය ඇනහිටී)
Used by / භාවිතය	The Internet (TCP/IP) අන්තර්ජාලය	PSTN

Data transmission modes
දත්ත සම්ප්රේෂණ විධි
Data transmission modes refer to the ways in which data is transmitted between two devices in a communication system.
දත්ත සම්ප්‍රේෂණ විධි යනු සන්නිවේදන පද්ධතියක උපාංග දෙකක් අතර දත්ත සම්ප්‍රේෂණය වන ආකාරයයි.

There are three data transmission modes.
මූලික දත්ත සම්ප්‍රේෂණ ක්‍රම තුනක් ඇත.

1. Simplex / ඒක පථ
2. Half-Duplex / අර්ධ ද්වීපථ
3. Full-Duplex / පූර්ණ ද්වීපථ

1. Simplex transmission
ඒක පථ සම්ප්‍රෙෂණය

In simplex mode, data transmission occurs in only one direction.
ඒක පථ සම්ප්‍රේෂණයේදී, දත්ත සම්ප්‍රේෂණය සිදු වන්නේ එක් දිශාවකට පමණි.

One device sends the data, and the other receives it.
එක් උපාංගයක් දත්ත යවන අතර අනෙක එය ලබා ගනී.

Examples:
උදාහරණ:

- Radio Broadcasting
  ගුවන්විදුලි සම්ප්‍රේෂණය
- Television Broadcasting
  රූපවාහිනී සම්ප්‍රේෂණය
- Keyboard to Computer
  යතුරුපුවරුවේ සිට පරිගණකය දක්වා

2. Half-duplex transmission
අර්ධ ද්වි පථ සම්ප්‍රෙෂණය

In half-duplex mode, data transmission can happen in both directions, but not at the same time.
අර්ධ ද්වි පථ සම්ප්‍රේෂණයේදී, දත්ත සම්ප්‍රේෂණය දෙපසටම සිදු විය හැකිය. නමුත් එකම අවස්ථාවේදී නොවේ.

Examples:
උදාහරණ:

- Walkie-Talkies
- Internet Browsing (Dial-up connections)

Hubs
Hubs function in half-duplex mode. This means that data can only travel in one direction at a time across the network
උදාහරණයක් ලෙස, හබ් එකකට සම්බන්ධ එක් උපාංගයක් දත්ත යවන්නේ නම්, අනෙක් සියලුම උපාංග තමන්ගේ දත්ත යැවීමට පෙර සම්ප්‍රේෂණය සම්පූර්ණ වන තෙක් රැඳී සිටිය යුතුය.

If one device connected to a hub is sending data, all other devices must wait until the transmission is complete before they can send their own data.
නාබි අර්ධ ද්වීපථ ක්‍රමයෙන් ක්‍රියා කරයි. මෙයින් අදහස් කරන්නේ දත්ත ජාලය හරහා ගමන් කළ හැක්කේ එක් දිශාවකට පමණක් බවයි.

Fax machines
When two fax machines communicate, one machine sends data (the scanned document) while the other receives it.
ෆැක්ස් යන්ත්‍ර දෙකක් සන්නිවේදනය කරන විට, එක් යන්ත්‍රයක් දත්ත (ස්කෑන් කරන ලද ලේඛනය) යවන අතර අනෙක එය ලබා ගනී.

After the sender has transmitted the document, the receiving fax machine might send back a confirmation signal (like a receipt acknowledgment).
යවන්නා ලේඛනය සම්ප්‍රේෂණය කළ පසු, ග්‍රාහක ෆැක්ස් යන්ත්‍රය තහවුරු කිරීමේ සංඥාවක් ආපසු එවිය හැකිය (රිසිට්පත් පිළිගැනීමක් වැනි).

Both fax machines don't transmit data at the same time.
ෆැක්ස් යන්ත්‍ර දෙකම එකම අවස්ථාවේදී දත්ත සම්ප්‍රේෂණය කරන්නේ නැත.

3. Full-Duplex transmission
පූර්ණ ද්වීපථ සම්ප්‍රේෂණය

Full-duplex mode allows data to be transmitted in both directions simultaneously.
පූර්ණ ද්වීපථ සම්ප්‍රේෂණය මගින් දත්ත දෙපැත්තටම එකවර සම්ප්‍රේෂණය කිරීමට ඉඩ සලසයි.

Examples:
උදාහරණ:

- Telephone Calls
- Internet Browsing (ADSL connections)
- Network Switches

ictfromabc.com

Casting methods

1. Unicasting

Unicasting is a one-to-one communication method where data is sent from a single source to a single destination in the network.
Unicasting යනු ජාලය තුළ එක් මූලාශ්‍රයකින් එක් ගමනාන්තයකට දත්ත යවන one-to-one සන්නිවේදන ක්‍රමයකි.

Examples

- Phone calls
  දුරකථන ඇමතුම්
- Text messages
  කෙටි පණිවිඩ
- Whatsapp personal messages
  Whatsapp පුද්ගලික පණිවිඩ

2. Multicasting

In multicasting, data is sent to a specific group of recipients within the network.
Multicasting වලදී, ජාලය තුළ දත්ත, තෝරාගත් ලබන්නන් කණ්ඩායමකට යවනු ලැබේ.

Only the devices that are part of this multicast group will receive the data.
මෙම multicasting සමූහයේ කොටසක් වන උපාංග වලට පමණක් දත්ත ලැබෙනු ඇත.

Examples:
උදාහරණ:

- Groups calls
  කණ්ඩායම් ඇමතුම්
- Group chats
  කණ්ඩායම් කතාබස්

3. Broadcasting

In broadcasting, data is sent from a single source to all devices on the network.
Broadcasting හිදී, දත්ත එක් මූලාශ්‍රයක සිට ජාලයේ සියලුම උපාංග වෙත යවනු ලැබේ.

Every device on the network receives the data, regardless of whether they need it or not.
ජාලයේ සෑම උපාංගයකටම අවශ්‍යද නැද්ද යන්න නොසලකා දත්ත ලැබේ.

Examples:
උදාහරණ:

- **ARP Requests**
  In a local area network (LAN), when a device wants to know the MAC address associated with an IP address, it sends an ARP (Address Resolution Protocol) request.
  ස්ථානීය ජාලයක (LAN), උපාංගයකට IP ලිපිනයක් හා සම්බන්ධ MAC ලිපිනය දැන ගැනීමට අවශ්‍ය වූ විට, එය (ARP ලිපින විභේදන නියමාවලිය) ඉල්ලීමක් යවයි.

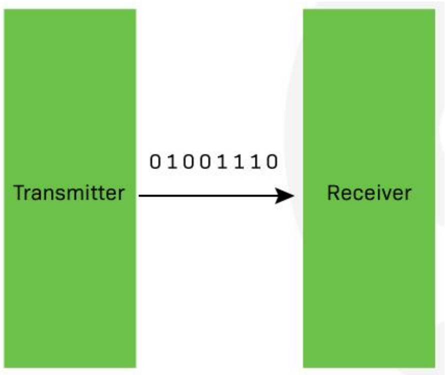
  This request is broadcasted to all devices on the network, and only the device with the matching IP address responds.
  මෙම ඉල්ලීම ජාලයේ සියලුම උපාංග වෙත විකාශනය වන අතර, ගැලපෙන IP ලිපිනය සහිත උපාංගය පමණක් ප්‍රතිචාර දක්වයි.

- **TV or Radio Broadcasts**

modems
Summary

Transmission Mode	**Examples**
Unicasting	Web Browsing, File Transfer (FTP), Video Calls, Direct Messaging වෙබ් බ්‍රවුස් කිරීම, ගොනු හුවමාරුව (FTP), වීඩියෝ ඇමතුම්, සෘජු පණිවිඩ යැවීම
Multicasting	Online Multiplayer Gaming මාර්ගගත බහු ක්‍රීඩක ක්‍රීඩා
Broadcasting	DHCP protocol DHCP නියමාවලිය

Serial Transmission / අනුක්‍රමික සම්ප්‍රේෂණය



Data is transmitted one bit at a time through a single communication line.
තනි සන්නිවේදන මාර්ගයක් හරහා වරකට බිට් එක බැගින් දත්ත සම්ප්‍රේෂණය වේ.

Requires fewer wires and simpler hardware connections.
අඩු වයර් සහ සරල දෘඩාංග සම්බන්ධතා අවශ්‍ය වේ.

Suitable for long-distance communication.
දිගු දුර සන්නිවේදනය සඳහා සුදුසු වේ.

Less signal interference and timing issues compared to parallel transmission.
සමාන්තර සම්ප්‍රේෂණයට සාපේක්ෂව අඩු සංඥා බාධා කිරීම් සහ කාල ගැටළු.

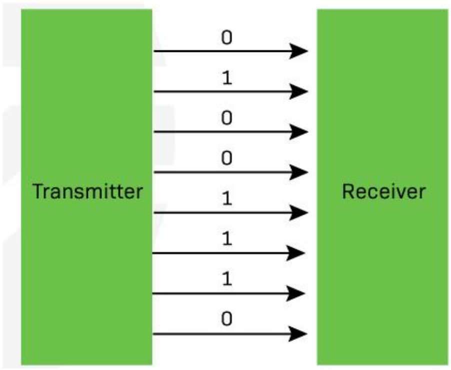
Usually slower than parallel transmission for short distances.
කෙටි දුර සඳහා සාමාන්‍යයෙන් සමාන්තර සම්ප්‍රේෂණයට වඩා මන්දගාමී වේ.

Used to transmit large data sets.
විශාල දත්ත කට්ටල සම්ප්‍රේෂණය කිරීම සඳහා භාවිතා කරයි.

Examples:
උදාහරණ:

Networking
USB — Universal Serial Bus (විශ්ව ශ්‍රේණිගත බස්)
SATA—Serial Advanced Technology Attachment

Parallel Transmission / සමාන්තර සම්ප්‍රේෂණය



Data is transmitted multiple bits simultaneously through multiple lines.
දත්ත බහු රේඛා හරහා එකවර බිට් කිහිපයක් සම්ප්‍රේෂණය වේ.

Each bit of a byte is sent through a separate wire at the same time.
බයිට් එකක සෑම බිට් එකක්ම එකවර වෙනම වයරයක් හරහා යවනු ලැබේ.

Provides faster data transfer over short distances.
කෙටි දුර හරහා වේගවත් දත්ත හුවමාරුවක් සපයයි.

Requires more wires and more complex hardware.
වැඩි වයර් සහ වඩාත් සංකීර්ණ දෘඩාංග අවශ්‍ය වේ.

Can suffer from signal interference and synchronization problems (skew) over long distances.
දිගු දුර හරහා සංඥා බාධා කිරීම් සහ සමමුහුර්ත කිරීමේ ගැටළු ඇති විය හැක.

Used in internal computer communication such as memory buses and old printer ports.
මතක බස් සහ පැරණි මුද්‍රණ යන්ත්‍ර වරායන් වැනි අභ්‍යන්තර පරිගණක සන්නිවේදනයේ භාවිතා වේ.

Used to transmit small sets of data.
කුඩා දත්ත කට්ටල සම්ප්‍රේෂණය කිරීමට භාවිතා කරයි.

Examples:
උදාහරණ:

Pararell port (සමාන්තරගත කෙවෙනිය)
IDE — Integrated Drive Electronics
System Bus*

Network Models
ජාල ආකෘති

1. Client-Server Model
සේවාලාභී-සේවාදායක ආකෘතිය

A network architecture in which clients request services or resources, and servers provide those services or resources over a network.
ජාලයක් හරහා සේවාලාභීන් විසින් සේවාවන් හෝ සම්පත් ඉල්ලා සිටින අතර, සේවාදායකයන් විසින් එම සේවාවන් හෝ සම්පත් සපයනු ලබන ජාල ගෘහ නිර්මාණ ශිල්පයකි.

Server
සේවාදායකය

The server is a powerful computer or a central device that provides services, resources, or data to the clients.
සේවාදායකය යනු සේවාලාභීන්ට සේවා, සම්පත් හෝ දත්ත සපයන බලවත් පරිගණකයක් හෝ මධ්‍යම කේන්ද්‍රස්ථානයකි.

Client
සේවාලාභියා

The clients are usually individual computers or devices that request these resources.
සේවාලාභීන් යනු සාමාන්‍යයෙන් මෙම සම්පත් ඉල්ලා සිටින තනි පරිගණක හෝ උපාංග වේ.

How the Client–Server Model Works
සේවාලාභී-සේවාදායක ආකෘතිය ක්‍රියාත්මක වන ආකාරය

The user opens a website or requests a file, and the client sends a request to the server.
පරිශීලකයා වෙබ් අඩවියක් විවෘත කරන විට හෝ ගොනුවක් ඉල්ලා සිටින විට, සේවාලාභියා විසින් සේවාදායකය වෙත ඉල්ලීමක් යවනු ලබයි.

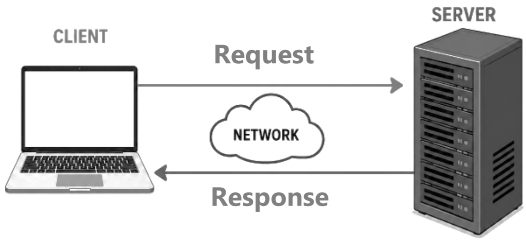
The request travels through switches and routers to the destination server.
මෙම ඉල්ලීම ස්විච සහ රවුටර හරහා ගමන් කර අදාළ සේවාදායකයා වෙත ලඟා වේ.

The server receives and identifies the client's request.
සේවාදායකය විසින් සේවාලාභියාගේ ඉල්ලීම ලබාගෙන එය හඳුනා ගනී.

The server processes the request by retrieving data, running an application, or performing the required task.
සේවාදායකය දත්ත ලබා ගැනීම, යෙදුමක් ක්‍රියාත්මක කිරීම හෝ වෙනත් අවශ්‍ය කාර්යයක් සිදු කිරීම මඟින් එම ඉල්ලීම සකසනු ලබයි.

The server sends the requested data or results back to the client.
සේවාදායකය විසින් ඉල්ලා සිටි දත්ත හෝ ප්‍රතිඵල නැවත සේවාලාභියා වෙත යවනු ලබයි.

The client receives the response and displays the webpage, file, image, or other requested content.
සේවාලාභියාට එම ප්‍රතිචාරය ලැබෙන අතර, එය මඟින් වෙබ් පිටුව, ගොනුව, පින්තූරය හෝ වෙනත් ඉල්ලා සිටි අන්තර්ගතය දර්ශනය කරනු ලබයි.



Charactristics
ලක්ෂණ

Centralized resource management
මධ්‍යගත සම්පත් කළමනාකරණය

Clients request services; servers provide services
සේවාලාභීන් සේවාවන් ඉල්ලා සිටින අතර, සේවාදායකයන් එම සේවාවන් සපයයි

Supports multiple clients simultaneously
එකවර සේවාලාභීන් රැසකට සහය දක්වයි

Scalable by upgrading or adding servers
සේවාදායකයන් උත්ශ්‍රේණි කිරීම (upgrade) හෝ අලුතින් එකතු කිරීම මඟින් ධාරිතාව පුළුල් කළ හැක

Provides centralized security and administration
මධ්‍යගත ආරක්ෂාවක් සහ පරිපාලනයක් සපයයි

Data is stored on the server
දත්ත ගබඩා කරනු ලබන්නේ සේවාදායකය තුළයි

Easy to maintain and update
නඩත්තු කිරීම සහ යාවත්කාලීන කිරීම පහසුය

Reliable and efficient for large networks
විශාල ජාල සඳහා විශ්වාසදායක සහ කාර්යක්ෂම වේ

Examples
Websites, email services, and file-sharing systems like Google Drive, Banks
වෙබ් අඩවි, ඊමේල් සේවා, සහ Google Drive වැනි ගොනු හුවමාරු පද්ධති, බැංකු.

2. Peer-to-Peer (P2P) Model
සම-සම ආකෘතිය

The Peer-to-Peer (P2P) Model is a network architecture in which all computers (peers) have equal status and can both request and provide resources directly to each other without relying on a central server.
සම-සම ආකෘතිය යනු මධ්‍යගත සේවාදායකයක් මත රඳා නොපවතිමින්, ජාලයේ ඇති සියලුම පරිගණක සමාන තත්ත්වයක් දරන සහ සෘජුවම එකිනෙකාගෙන් සම්පත් ඉල්ලා සිටීමට මෙන්ම සැපයීමටද හැකි ජාල ගෘහ නිර්මාණ ශිල්පයකි.

In a P2P network, every computer can act as both a client and a server.
P2P ජාලයක් තුළ, සෑම පරිගණකයකටම සේවාලාභියෙකු සහ සේවාදායකයෙකු යන දෙයාකාරයෙන්ම ක්‍රියා කළ හැක.

A peer is a computer or device connected to the network that can both request and share resources with other peers.
Peer යනු ජාලයට සම්බන්ධ කර ඇති, අනෙකුත් උපාංග සමඟ සම්පත් හුවමාරු කර ගැනීමට සහ ඒවා ඉල්ලා සිටීමට හැකි පරිගණකයක් හෝ උපාංගයකි.

How the Peer-to-Peer Model Works
සම-සම ආකෘතිය ක්‍රියාත්මක වන ආකාරය

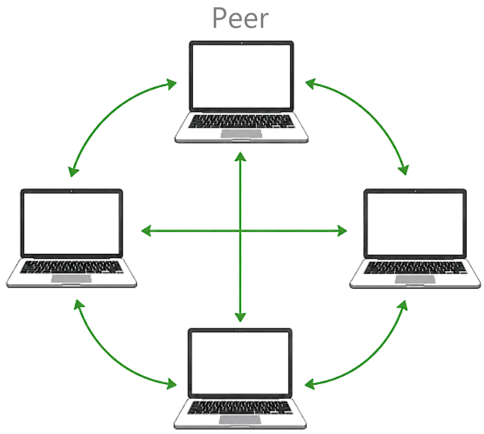
A peer requests a file, data, or service from another peer on the network.
එක් උපාංගයක් විසින් ජාලයේ ඇති වෙනත් උපාංගයකින් ගොනුවක්, දත්ත හෝ සේවාවක් ඉල්ලා සිටියි.

The request is sent directly to the peer that has the requested resource.
මෙම ඉල්ලීම අදාළ සම්පත සතු උපාංගය වෙත සෘජුවම යවනු ලබයි.

The requested peer checks whether it has the requested file or service.
ඉල්ලීම ලැබුණු උපාංගය විසින් තමා සතුව එම ගොනුව හෝ සේවාව තිබේදැයි පරීක්ෂා කරයි.

If the resource is available, the peer sends it directly to the requesting peer.
එම සම්පත තිබේ නම්, එය ඉල්ලීම සිදු කළ උපාංගය වෙත සෘජුවම යවනු ලබයි.

The requesting peer receives the data and can also share it with other peers if required.
ඉල්ලීම සිදු කළ උපාංගයට එම දත්ත ලැබෙන අතර, අවශ්‍ය නම් එය අනෙකුත් උපාංග සමඟද බෙදා ගැනීමට හැකියාව පවතී.



Characteristics
ලක්ෂණ

Acts as both a client and a server.
සේවාලාභියෙකු මෙන්ම සේවාදායකයෙකු ලෙසද ක්‍රියා කරයි.

Shares its own files, storage, or processing power.
තමා සතු ගොනු, ගබඩා ධාරිතාව හෝ සැකසුම් බලය බෙදා හදා ගනී.

Communicates directly with other peers.
අනෙකුත් peers සමඟ සෘජුවම සන්නිවේදනය කරයි.

Has equal authority with other peers.
අනෙකුත් peers හා සමාන බලතල/අධිකාරියක් පවතී.

Can join or leave the network at any time.
ඕනෑම අවස්ථාවක ජාලයට සම්බන්ධ වීමට හෝ ජාලයෙන් ඉවත් වීමට හැකියාව ඇත.

Examples
File-sharing systems like BitTorrent, blockchain networks, and some messaging apps.
BitTorrent, blockchain ජාල, සහ සමහර පණිවිඩ යෙදුම් වැනි ගොනු හුවමාරු පද්ධති.

ictfromabc.com

Advantages and disadvantages
වාසි හා අවාසි

Client-Server Model	Peer-to-Peer (P2P) Model
Advantages	
Centralized management of resources and security. සම්පත් සහ ආරක්ෂාව පිළිබඳ මධ්‍යගත කළමනාකරණය.	Decentralized, no central authority needed. විමධ්‍යගතය, මධ්‍යම අධිකාරියක් අවශ්‍ය නැත.
Handles large requests with proper infrastructure. නිසි යටිතල පහසුකම් සහිත විශාල ඉල්ලීම් හසුරුවයි.	Effective for small networks. කුඩා ජාල සඳහා ඵලදායී වේ.
Easier to enforce security policies. ආරක්ෂක ප්‍රතිපත්ති ක්‍රියාත්මක කිරීම පහසුය.	No server failure risk. සේවාදායකය අසමත් වීමේ අවදානමක් නොමැත.
Scales well with powerful servers. බලවත් සේවාදායකයන් සමඟ හොඳින් පරිමාණය වෙයි.	Easily scalable with new peers. නව සමඟ පහසුවෙන් පරිමාණය කළ හැකිය
Centralized backup and recovery. මධ්‍යගත උපස්ථ සහ ප්‍රතිසාධනය.	Data distributed across peers. Peers අතර දත්ත බෙදා හැර ඇත.
Disadvantages	
Server failure affects the whole network. සේවාදායකයේ අසාර්ථකත්වය මුළු ජාලයටම බලපායි.	Network performance degrades if many peers fail. Peers කිහිපයක් අසමත් වුවහොත් ජාල කාර්ය සාධනය පිරිහී යයි.
Expensive to set up and maintain. සැකසීමට සහ නඩත්තු කිරීමට මිල අධිකය.	Lower cost, no server required. අඩු පිරිවැය, සේවාදායකයක් අවශ්‍ය නොවේ.
Server bottlenecks if overloaded. අධික ලෙස ඉල්ලීම් ඇත්නම් සේවාදායක අවහිර විය හැක.	Varies based on peer resources. සම සම්පත් මත පදනම්ව වෙනස් වේ.
Requires skilled management. මනා කළමනාකරණයක් අවශ්‍යය.	Hard to manage security across peers. Peers අතර ආරක්ෂාව කළමනාකරණය කිරීමට අපහසුය.
Servers are high-value attack targets. සේවාදායකයන් ඉහළ වටිනාකමකින් යුත් ප්‍රහාර ඉලක්ක වේ.	Harder to secure a decentralized network. විමධ්‍යගත ජාලයක් සුරක්ෂිත කිරීම අපහසුය ය.
Centralized storage, susceptible to data loss. මධ්‍යගත ආචයනය, දත්ත නැතිවීමට ඉඩ ඇත.	Inconsistent data copies across peers. Peers අතර නොගැලපෙන දත්ත පිටපත් පැවතිය හැක.

ictfromabc.com

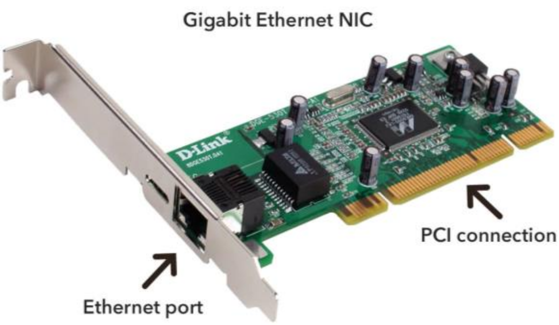
Networking devices
ජාල උපාංග

Network devices are hardware components that facilitate the operation and connectivity of computer networks.
ජාල උපාංග යනු පරිගණක ජාල වල ක්‍රියාකාරීත්වය සහ සම්බන්ධතාවය පහසු කරන දෘඩාංග සංරචක වේ.

They enable devices to communicate, share resources, and access information across various network types
විවිධ ජාල වර්ග හරහා සන්නිවේදනය කිරීමට, සම්පත් බෙදා ගැනීමට සහ තොරතුරු වෙත ප්‍රවේශ වීමට ඒවා උපාංග සක්‍රීය කරයි.

They form the backbone of modern network infrastructure, supporting both wired and wireless connectivity, and are essential for establishing and maintaining effective network communication and performance.
ඒවා නවීන ජාල යටිතල ව්‍යුහයේ කොඳු නාරටිය වන අතර, රැහැන්ගත සහ රැහැන් රහිත සම්බන්ධතා දෙකටම සහාය වන අතර, ඵලදායී ජාල සන්නිවේදනය සහ කාර්ය සාධනය ස්ථාපිත කිරීම සහ පවත්වාගෙන යාම සඳහා අත්‍යවශ්‍ය වේ.

Network Interface Card (NIC)
ජාලකරණ අතුරුමුහුණත් කාඩ්පත (NIC)



Also, known as a network adapter or network interface controller, critical hardware component that enables computers to connect to a network.
ජාල ඇඩැප්ටරය හෝ ජාල අතුරුමුහුණත් පාලකයක් ලෙසද හැඳින්වේ, පරිගණකවලට ජාලයකට සම්බන්ධ වීමට හැකි තීරණාත්මක දෘඩාංග සංරචකයකි.

Works at OSI Layers 1 and 2, transmitting and receiving signals on the physical medium while also using MAC addresses to send and receive Ethernet frames.
භෞතික මාධ්‍යය ඔස්සේ සංඥා සම්ප්‍රේෂණය කිරීම සහ ලබා ගැනීම සිදු කරන අතරම, ඊතර්නෙට් රාමු යැවීම සහ ලබා ගැනීම සඳහා MAC ලිපිනද භාවිතා කරමින්,OSI මාදිලියේ 1 සහ 2 ස්තරයන්හි ක්‍රියාත්මක වේ

The NIC serves as the interface between the computer and the physical network medium, whether that be through wired connections like Ethernet or wireless connections like Wi-Fi.
NIC පරිගණකය සහ භෞතික ජාල මාධ්‍යය අතර අතුරු මුහුණත ලෙස ක්‍රියා කරයි, එය Ethernet වැනි රැහැන්ගත සම්බන්ධතා හරහා හෝ Wi-Fi වැනි රැහැන් රහිත සම්බන්ධතා හරහා ක්‍රියාත්මක වේ.

Primary functions
මූලික කාර්යයන්

Data Conversion
දත්ත පරිවර්තනය
The NIC converts digital data from the computer into signals suitable for transmission over the network medium. It also translates incoming signals back into digital data that the computer can process.
ජාලකරණ අතුරුමුහුණත පරිගණකයේ ඇති ඩිජිටල් දත්ත ජාල මාධ්‍ය හරහා සම්ප්‍රේෂණය කිරීමට සුදුසු සංඥා බවට පරිවර්තනය කරයි. එය පැමිණෙන සංඥා පරිගණකයට සැකසිය හැකි ඩිජිටල් දත්ත බවට පරිවර්තනය කරයි

Data Transfer
දත්ත හුවමාරුව
It handles the actual sending and receiving of data packets.
එය දත්ත පැකට් සැබෑ යැවීම සහ ලැබීම හසුරුවයි. NIC ජාල සන්නිවේදනය සඳහා සුදුසු රාමු ව්‍යුහය තුළ දත්ත ගොනු කරයි

Addressing
ලිපිනකරණය
Each NIC has a unique MAC address, which is essential for identifying the device on the network and ensuring accurate packet delivery.
සෑම ජාල අතුරුමුහුනත් කාඩ්පතකටම අනන්‍ය MAC ලිපිනයක් ඇත, එය ජාලයේ උපාංගය හඳුනා ගැනීමට සහ නිවැරදි පැකට් බෙදා හැරීම සහතික කිරීමට අත්‍යවශ්‍ය වේ.

Traffic Control
තදබදය පාලනය
The NIC manages data flow to prevent collisions and reduce network congestion, employing various algorithms and protocols.
NIC විවිධ ඇල්ගොරිතම සහ ප්‍රොටෝකෝල භාවිතා කරමින් ගැටුම් වැළැක්වීමට සහ ජාල තදබදය අඩු කිරීමට දත්ත ප්‍රවාහය කළමනාකරණය කරයි.

Error Detection and Correction
දෝෂ හඳුනා ගැනීම සහ නිවැරදි කිරීම
It checks data packets for errors and can request retransmission or attempt to correct errors based on the protocols in use.
එය දෝෂ සඳහා දත්ත පැකට් පරීක්ෂා කරන අතර නැවත සම්ප්‍රේෂණය ඉල්ලීමට හෝ භාවිතයේ ඇති ප්‍රොටෝකෝල මත පදනම්ව දෝෂ නිවැරදි කිරීමට උත්සාහ කළ හැකිය.

Buffering
අන්තරාස්‍රිතකරණය
To accommodate differences in data transfer rates and processing speeds, the NIC temporarily stores incoming or outgoing packets in a buffer, enhancing transmission efficiency.
දත්ත හුවමාරු අනුපාතවල සහ සැකසුම් වේගයේ වෙනස්කම්වලට අනුගත වීම සඳහා, සම්ප්‍රේෂණ කාර්යක්ෂමතාව ඉහළ නංවමින්, පැමිණෙන හෝ පිටතට යන පැකට් තාවකාලිකව NIC ගබඩා කරයි.

How an NIC works
NIC එකක ක්‍රියාකාරිත්වය

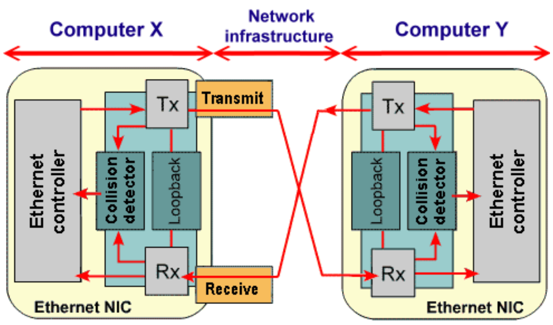
1. When a device is turned on, the NIC initializes and configures itself to communicate with the network. This includes setting up the MAC address and possibly requesting an IP address from a DHCP server.
උපාංගයක් සක්‍රිය කර ඇති විට, NIC ජාලය සමඟ සන්නිවේදනය කිරීමට ආරම්භ කර වින්‍යාස කරයි. MAC ලිපිනය පිහිටුවීම සහ DHCP සේවාදායකයකින් IP ලිපිනයක් ඉල්ලා සිටීම මෙයට ඇතුළත් වේ.

2. Data from the computer is encapsulated into frames by the NIC. Each frame includes the data payload, source and destination MAC addresses, and error-checking information.
පරිගණකයේ දත්ත ජාල අතුරුමුහුනත් කාඩ්පත් මගින් රාමු වලට කොටු කර ඇත. සෑම රාමුවකටම දත්ත ගෙවීම, මූලාශ්‍රය සහ ගමනාන්ත MAC ලිපින සහ දෝෂ පරීක්ෂා කිරීමේ තොරතුරු
ඇතුළත් වේ.

3. The NIC transmits these frames onto the network medium, which could be a wired connection (e.g., Ethernet) or a wireless connection (e.g., Wi-Fi).
NIC මෙම රාමු ජාල මාධ්‍ය වෙත සම්ප්‍රේෂණය කරයි, එය රැහැන්ගත සම්බන්ධතාවයක් (උදා: ඊතර්නෙට්) හෝ රැහැන් රහිත සම්බන්ධතාවයක් (උදා:Wi-Fi) විය හැකිය.

4. The NIC listens for incoming frames. When a frame addressed to its MAC address is detected, the NIC captures the frame, checks for errors, and if it's error-free, passes the data to the computer's operating system.
එන රාමු සඳහා NIC සවන් දෙයි. එහි MAC ලිපිනයට ආමන්ත්‍රණය කරන ලද රාමුවක් අනාවරණය වූ විට, NIC විසින් රාමුව ග්‍රහණය කර, දෝෂ සඳහා පරීක්ෂා කර, එය දෝෂ රහිත නම්, දත්ත පරිගණකයේ මෙහෙයුම් පද්ධතියට යවයි.

5. The operating system processes the data received and passes it to the appropriate application, allowing for network communication like browsing the internet, sending emails, or streaming media
මෙහෙයුම් පද්ධතිය ලැබුණු දත්ත සකසන අතර එය සුදුසු යෙදුමට යවයි, අන්තර්ජාලයේ සැරිසැරීම, ඊමේල් යැවීම හෝ මාධ්‍ය ප්‍රවාහය වැනි ජාල සන්නිවේදනයට ඉඩ සලසයි.



Types of NICs by Connection Medium
සම්බන්ධක මාධ්‍යය අනුව NIC වර්ග

1. **Wired NICs**
   රැහැන්ගත NIC

Use physical cables to transmit data between devices and the network.
උපාංග සහ ජාලය අතර දත්ත සම්ප්‍රේෂණය කිරීම සඳහා භෞතික රැහැන් භාවිතා කරයි.

- Twisted Pair Ethernet NIC (RJ-45) – Uses standard Ethernet cables (Cat5e, Cat6, etc.).
  ඇඹරි යුගල රැහැන් NIC (RJ-45) – සම්මත ඊතර්නෙට් කේබල් (Cat5e, Cat6 ආදිය) භාවිතා කරයි.
- Fiber Optic NIC – Uses for high-speed, long-distance communication.
  ප්‍රකාශ තන්තු NIC – අධිවේගී සහ දුරස්ථ සන්නිවේදනය සඳහා භාවිතා කරයි.
- Coaxial NIC (Legacy) – Mostly found in older networks.
  සමාක්ෂ NIC (පැරණි) – මේවා බහුලව දක්නට ලැබෙන්නේ පැරණි ජාල වලය.

2. **Wireless NICs**
   රැහැන් රහිත NIC

Use radio waves instead of cables to connect devices to a network.
ජාලයකට උපාංග සම්බන්ධ කිරීම සඳහා කේබල් වෙනුවට ගුවන් විදුලි තරංග භාවිතා කරයි.

- Wi-Fi NIC – Connects devices to wireless local area networks (WLANs).
  Wi-Fi NIC – රැහැන් රහිත ස්ථානීය ජාල වෙත උපාංග සම්බන්ධ කරයි.
- Bluetooth NIC – Commonly used for short-range communication in IoT and personal devices.
  Bluetooth NIC – සාමාන්‍යයෙන් IoT (Internet& of Things) සහ පුද්ගලික උපාංගවල කෙටි දුර සන්නිවේදනය සඳහා භාවිතා කරයි.
- Cellular NIC (4G/5G) – Connects devices through mobile network providers.
  Cellular NIC (4G/5G) – ජංගම දුරකථන ජාල සේවා සපයන්නන් හරහා උපාංග සම්බන්ධ කරයි.

Types of NICs by Installation
ස්ථාපනය කිරීම අනුව NIC වර්ග

1.Internal NIC
- Installed inside the computer through PCI or PCIe slots.
  PCI හෝ PCIe ස්ලොට් හරහා පරිගණකය තුළ ස්ථාපනය කරනු ලබයි.
- Commonly used in desktop computers and servers.
  සාමාන්‍යයෙන් මේස පරිගණක සහ සේවාදායකවල බහුලව භාවිතා වේ.

2. **External NIC**

- Connected externally through a USB port.
  USB අග්‍රයක් හරහා බාහිරව සම්බන්ධ කරනු ලබයි.
- Commonly used when a built-in NIC is unavailable or damaged.
  සාමාන්‍යයෙන් පරිගණකය තුළ ඇති NIC එකක් නොමැති විට හෝ එයට හානි වී ඇති විට බහුලව භාවිතා වේ.

3. **Integrated NIC**
- Built directly into the motherboard.
  මවුපුවරුව මතම සෘජුවම නිපදවා ඇත.
- Network connectivity is provided without additional hardware.
  අමතර දෘඩාංග නොමැතිව ජාල සන්නිවේදනය සපයයි.
- Commonly found in modern desktops and laptops.
  සාමාන්‍යයෙන් නවීන ඩෙස්ක්ටොප් සහ ලැප්ටොප් පරිගණකවල දක්නට ලැබේ.

Repeater
වර්ධකය

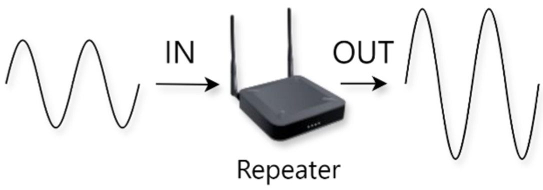
A repeater is a network device used to extend the range of a network by amplifying and retransmitting signals.
වර්ධකයක් යනු සංඥා විස්තාරණය කිරීම සහ නැවත සම්ප්‍රේෂණය කිරීම මගින් ජාලයක පරාසය පුළුල් කිරීමට භාවිතා කරන ජාල උපාංගයකි.

It operates at the Physical Layer (Layer 1) of the OSI model.
එය OSI ආකෘතියේ භෞතික ස්ථරයේ (1 වන ස්ථරයේ) ක්‍රියාත්මක වේ.

Signal Amplification
සංඥා විස්තාරණය

Analog Repeaters
ප්‍රතිසම වර්ධක

Used to receive a weak or degraded analog signal, amplify it, and retransmit it with greater strength.
දුර්වල වූ හෝ විකෘති වූ අංකිත සංඥාවක් ලබා ගැනීමට, එය වර්ධනය කිරීමට (බලගැන්වීමට) සහ වඩා වැඩි ප්‍රබලතාවයකින් යුතුව නැවත විකාශනය කිරීමට භාවිතා කරයි.



The received signal is amplified before being forwarded to the next section of the network.
ලැබුණු සංඥාව ජාලයේ ඊළඟ කොටස වෙත යොමු කිරීමට පෙර වර්ධනය කරනු (බලගන්වනු) ලබයි.

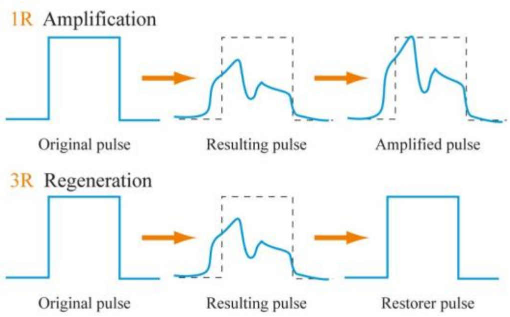
Example:
උදාහරණයක් ලෙස:
In long-distance telephone networks, analog repeaters are placed at intervals to amplify weakened voice signals and extend communication distance.
දිගු දුර දුරකථන ජාලවලදී, දුර්වල වූ හඬ සංඥා වර්ධනය කර සන්නිවේදන දුර ප්‍රමාණය වැඩි කිරීම සඳහා නිශ්චිත පරතරයන් ඇතුව අංකිත වර්ධක ස්ථාපනය කර ඇත.

Advantages
වාසි

- Transmission distance is extended.
  සම්ප්‍රේෂණ දුර ප්‍රමාණය වැඩි වේ.
- Signal strength is restored.
  සංඥා ප්‍රබලතාවය නැවත යථා තත්ත්වයට පත් කෙරේ.

Limitation
සීමාවන්

- Both the signal and noise are amplified.
  සංඥාව සහ ඝෝෂාව යන දෙකම වර්ධනය වේ.
- Signal quality may be degraded after repeated amplification
  නැවත නැවතත් වර්ධනය කිරීමෙන් පසු සංඥාවේ ගුණාත්මකභාවය අඩු විය හැක.
- Original signal distortion is also amplified and forwarded, causing signal quality to deteriorate over long distances.
  මුල් සංඥාවේ ඇති වූ විකෘතිතාවයන්ද වර්ධනය වී ඉදිරියට යවන බැවින්, දිගු දුරක් යෑමේදී සංඥාවේ ගුණාත්මකභාවය පිරිහීමට ලක්වේ.



Regeneration
පුනර්ජනනය

Digital Repeaters
සංඛ්‍යාංක වර්ධක

A digital repeater is used to receive a weakened digital signal, regenerate the original binary values (0s and 1s), and retransmit the regenerated signal.
සංඛ්‍යාංක වර්ධක භාවිතා කරනුයේ දුර්වල වූ ඩිජිටල් සංඥාවක් ලබාගෙන, එහි මුල් ද්විමය අගයන් 0 සහ 1 නැවත උත්පාදනය කර (ප්‍රතිනිර්මාණය කර), එම ප්‍රතිනිර්මාණය කරන ලද සංඥාව නැවත විකාශනය කිරීම සඳහාය.

Does not amplify noise
ඝෝෂාව වර්ධනය නොකරයි

Example:
උදාහරණයක් ලෙස:

Used in computer networks and fiber-optic communication systems to support long-distance data transmission.
දිගු දුර දත්ත සම්ප්‍රේෂණයට සහය වීම සඳහා පරිගණක ජාල සහ ප්‍රකාශ තන්තු සන්නිවේදන පද්ධතිවල භාවිතා කරනු ලැබේ.

Advantages
වාසි

- Signal strength is restored.
  සංඥා ශක්තිය නැවත යථා තත්ත්වයට පත් කෙරේ.
- Original digital data is regenerated.
  මුල් ඩිජිටල් දත්ත නැවත ජනනය කරනු ලැබේ.
- Noise and distortion effects are reduced.
  ඝෝෂාව සහ විකෘති වීම් මඟින් ඇති වන බලපෑම් අවම කෙරේ.

Limitation
සීමාවන්

- Can only be used with digital signals.
  ඩිජිටල් සංඥා සමඟ පමණක් භාවිතා කළ හැක.
- Higher cost and complexity are involved compared to analog repeaters.
  අංකිත වර්ධක සමඟ සසඳන විට ඉහළ පිරිවැයක් සහ සංකීර්ණත්වයක් අන්තර්ගත වේ.
- Additional processing is required for signal regeneration.
  සංඥා නැවත ජනනය කිරීම සඳහා අතිරේක සැකසුම් අවශ්‍ය වේ.

How a Repeater Works
වර්ධකයක ක්‍රියාකාරීත්වය

The repeater first receives the signal from the network.
වර්ධකය මුලින්ම ජාලයෙන් සංඥාව ලබා ගනී.

This could be an electrical signal in a wired network (like Ethernet) or a radio signal in a wireless network.
මෙය රැහැන්ගත ජාලයක (ඊතර්නෙට් වැනි) විදුලි සංඥාවක් හෝ රැහැන් රහිත ජාලයක රේඩියෝ සංඥාවක් විය හැකිය

1. Once the signal is received, the repeater amplifies it, boosting its power to counteract any loss that occurred as it traveled through the network medium.
සංඥාව ලැබුණු පසු, වර්ධකය එය විස්තාරණය කරයි, ජාල මාධ්‍යය හරහා ගමන් කරන විට සිදුවන ඕනෑම අලාභයක් වළක්වා ගැනීමට එහි බලය වැඩි කරයි.

2. The repeater then regenerates the signal. This involves re-shaping and re-timing the signal to remove any noise or distortion that might have been introduced during transmission.
එවිට වර්ධකය සංඥාව නැවත උත්පාදනය කරයි. සම්ප්‍රේෂණය අතරතුර හඳුන්වා දී ඇති ඕනෑම ශබ්දයක් හෝ විකෘතියක් ඉවත් කිරීම සඳහා සංඥාව නැවත හැඩ ගැන්වීම සහ නැවත වේලාව සැකසීම මෙයට ඇතුළත් වේ.

3. After amplification and regeneration, the repeater retransmits the signal onto the network.
විස්තාරණය සහ පුනර්ජනනය කිරීමෙන් පසුව, වර්ධකය ජාලය වෙත සංඥාව නැවත සම්ප්රේෂණය කරයි.

The retransmitted signal is nearly identical to the original signal sent by the source, ensuring clear and reliable communication over greater distances.
නැවත සම්ප්‍රේෂණය කරන ලද සංඥාව ප්‍රභවය විසින් යවන ලද මුල් සංඥාවට බොහෝ දුරට සමාන වන අතර, වැඩි දුරක් හරහා පැහැදිලි සහ විශ්වාසදායක සන්නිවේදනයක් සහතික කරයි.

Types of Repeaters
වර්ධක වර්ග

Wired Repeaters
රැහැන්ගත වර්ධක
These are used in wired networks (like Ethernet) to extend the reach of the network cabling. They can connect multiple segments of a network and help maintain signal strength.
මේවා රැහැන්ගත ජාල වල (ඊතර්නෙට් වැනි) ජාල කේබලයේ ප්‍රවේශය දිගු කිරීමට භාවිතා කරයි. ඔවුන්ට ජාලයක බහුවිධ කොටස් සම්බන්ධ කළ හැකි අතර සංඥා ශක්තිය පවත්වා ගැනීමට උපකාරී වේ.

Wireless Repeaters
රැහැන් රහිත වර්ධක
Also known as range extenders, these devices are used in wireless networks to amplify and retransmit Wi-Fi signals, helping to eliminate dead zones and improve coverage in larger spaces.
පරාස විස්තාරක ලෙසද හැඳින්වේ, මෙම උපාංග Wi-Fi සංඥා විස්තාරණය කිරීමට සහ නැවත සම්ප්‍රේෂණය කිරීමට රැහැන් රහිත ජාල වල භාවිතා කරයි, මිය ගිය කලාප ඉවත් කිරීමට සහ විශාල අවකාශයන්හි ආවරණය වැඩි දියුණු කිරීමට උපකාරී

Network Hub
ජාලකරණ නාබිය

A legacy networking device.
පැරණි ජාලකරණ උපාංගයකි.

Hubs operate in half-duplex mode
Hubs අර්ධ ද්විපථ ආකාරයෙන් ක්‍රියාත්මක වේ

A network hub is a basic networking device used to connect multiple computers or network devices in a Local Area Network (LAN).
නාබියක් යනු ස්ථානීය ප්‍රදේශ ජාලයක LAN බහු පරිගණක හෝ ජාල උපාංග සම්බන්ධ කිරීමට භාවිතා කරන මූලික ජාලකරණ උපාංගයකි.

It operates at the Physical Layer (Layer 1) of the OSI model and is considered a simple, unmanaged device.
එය OSI ආකෘතියේ භෞතික ස්ථරයේ (1 වන ස්ථරයේ) ක්‍රියාත්මක වන අතර එය සරල, කළමනාකරණය නොකළ උපාංගයක් ලෙස සැලකේ.

Acts as a multi-port repeater
බහු-අග්‍ර පුනරාවර්තකයක් ලෙස ක්‍රියා කරයි

Primary functions
මූලික කාර්යයන්

Data Transmission
දත්ත සම්ප්‍රේෂණය

A hub receives data from one device on the network and transmits it to all other connected devices, regardless of the intended recipient.
නාබියක් ජාලයේ එක් උපාංගයකින් දත්ත ලබා ගන්නා අතර අපේක්ෂිත ලබන්නා කුමක් වුවත් එය අනෙකුත් සියලුම සම්බන්ධිත උපාංග වෙත සම්ප්‍රේෂණය කරයි.

This broadcasting method is called a **flood**, where all devices on the network receive the data, but only the intended recipient processes it.
මෙම විකාශන ක්‍රමය flood ලෙස හැඳින්වේ, එහිදී ජාලයේ සියලුම උපාංග දත්ත ලබා ගනී, නමුත් අපේක්ෂිත ලබන්නා පමණක් එය සකසයි.

Extension of Network Ports
ජාල අග්‍ර දිගු කිරීම

Hubs provide multiple network ports, allowing several devices to be connected to the same network segment.
නාබියක්, බහු ජාල අග්‍ර සපයන අතර, එමඟින් උපාංග කිහිපයකට එකම ජාල කොටසකට සම්බන්ධ වීමට ඉඩ ලබා දේ.

This increases the number of devices that can communicate through a single network connection point.
මෙය තනි ජාල සම්බන්ධතා ලක්ෂ්‍යයක් හරහා සන්නිවේදනය කළ හැකි උපාංග සංඛ්‍යාව වැඩි කරයි.

Example:
උදාහරණයක් ලෙස:
A Cisco 8-port hub can be used to connect eight computers or other network devices in a small office or laboratory.
කුඩා කාර්යාලයක හෝ රසායනාගාරයක පරිගණක අටක් හෝ වෙනත් ජාල උපාංග සම්බන්ධ කිරීම සඳහා සිස්කෝ අග්‍ර 8ක නාබියක් භාවිතා කළ හැක.

Examples of Hubs By Number of Ports
අග්‍ර සංඛ්‍යාව අනුව නාබි සඳහා උදාහරණ

- 4-Port Hub
- 8-Port Hub
- 12-Port Hub
- 24-Port Hub

Features / ලක්ෂණ

Collision Domain
Collision වසම

All devices connected to a hub share the same collision domain, meaning that if two devices try to send data simultaneously, a collision occurs, and the data must be resent.
නාබියකට සම්බන්ධ සියලුම උපාංග එකම ඝට්ටන වසම බෙදා ගනී, එනම් උපාංග දෙකක් එකවර දත්ත යැවීමට උත්සාහ කළහොත් ගැටුමක් ඇති වන අතර දත්ත නැවත යැවිය යුතුය.

To manage this situation, networks use Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
මෙම තත්ත්වය කළමනාකරණය කිරීම සඳහා, ජාල මඟින් Carrier Sense Multiple Access with Collision Detection (CSMA/CD) යාන්ත්‍රණය භාවිත කරනු ලබයි.

No Intelligence
බුද්ධියක් නැත

Hubs do not have the capability to differentiate between different devices or manage traffic.
විවිධ උපාංග අතර වෙනස හඳුනා ගැනීමට හෝ ගමනාගමනය කළමනාකරණය කිරීමට හබ්වලට හැකියාවක් නැත.

They do not store MAC addresses or make any forwarding decisions based on address information.
ඒවා MAC ලිපින ගබඩා නොකරයි හෝ ලිපින තොරතුරු මත පදනම්ව ඉදිරියට යැවීමේ තීරණ නොගනී.

How a Network Hub Works
නාබියක ක්‍රියාකාරීත්වය

When a device on the network, such as a computer, sends data to another device, it transmits this data as electrical signals through the network cable connected to the hub.
පරිගණකයක් වැනි ජාලයේ ඇති උපාංගයක් වෙනත් උපාංගයකට දත්ත යවන විට, මෙම දත්ත නාබියට සම්බන්ධ ජාල කේබලය හරහා විදුලි සංඥා ලෙස සම්ප්‍රේෂණය කරයි.

The hub receives the data signals at one of its ports and immediately repeats the signal out to all other ports on the hub. This process is known as broadcasting.
නාබිය එහි එක් Port එකකින් දත්ත සංඥා ලබා ගන්නා අතර වහාම නාබිය මත ඇති අනෙකුත් සියලුම Ports වෙත සංඥාව යොමු කරයි. මෙම ක්‍රියාවලිය broadcasting ලෙස හැඳින්වේ.

Each device connected to the hub receives the broadcasted data and checks whether the data is intended for it by examining the destination MAC address in the data frame.
නාබියට සම්බන්ධ සෑම උපාංගයක්ම විකාශනය කළ දත්ත ලබා ගන්නා අතර දත්ත රාමුව තුළ ගමනාන්ත MAC ලිපිනය පරීක්ෂා කිරීමෙන් දත්ත ඒ සඳහා යොමු වන්නේ දැයි පරීක්ෂා කරයි.

Only the device with the matching MAC address processes the data, all other devices discard it.
ගැලපෙන MAC ලිපිනය සහිත උපාංගය පමණක් දත්ත ලබාගනී. අනෙකුත් සියලුම උපාංග එය ඉවතලයි.

Types of Hubs
නාබියක වර්ග

Active Hubs
These hubs have built-in electronics that regenerate and amplify incoming signals, allowing for longer distances between devices. They require a power source to function.
මෙම නාබියේ ඇති ඉලෙක්ට්‍රොනික උපකරණ ප්‍රතිනිර්මාණය කරන සහ එන සංඥා විස්තාරණය කරන අතර එමඟින් උපාංග අතර වැඩි දුරක් යාමට ඉඩ සලසයි. ඒවා ක්‍රියාත්මක වීමට බල ප්‍රභවයක් අවශ්‍ය වේ.

Passive Hubs
These simply connect devices without any signal processing. They do not amplify or regenerate signals and are typically used in smaller setups.
මේවා කිසිදු සංඥා සැකසීමකින් තොරව උපාංග සම්බන්ධ කරයි. ඒවා සංඥා වර්ධක හෝ ප්‍රතිජනනය නොකරන අතර සාමාන්‍යයෙන් කුඩා සැකසුම් වල භාවිතා වේ.

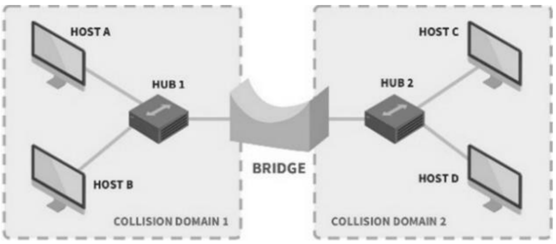
NOTE:

Intelligent Hubs
These hubs include management features that allow for monitoring and troubleshooting network issues, functioning similarly to switches but with some additional capabilities.
මෙම නාබියේ ජාල ගැටළු නිරීක්ෂණය කිරීමට සහ දෝශ නිරාකරණය කිරීමට ඉඩ සලසන කළමනාකරණ විශේෂාංග ඇතුළත් වේ, ස්විචවලට සමානව ක්‍රියා කරන නමුත් සමහර අමතර හැකියාවන් ඇත.

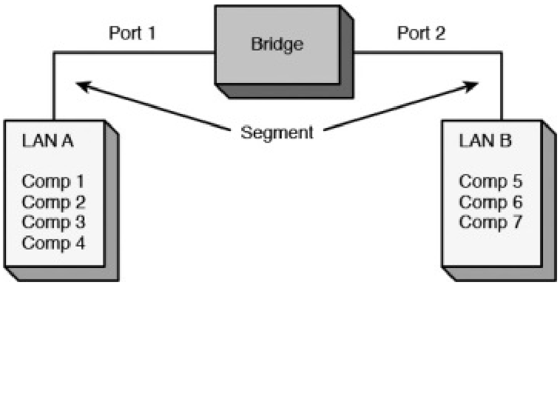
Bridge
සේතුව

A bridge in computer networking is a device that connects two local area networks (LANs) or network segments, enabling them to communicate with each other.
පරිගණක ජාලකරණයේ සේතුවක් මගින් ප්‍රාදේශීය ජාල (LANs) දෙකක් සම්බන්ධ කරන උපකරණයක් වන අතර, ඒවා එකිනෙකා සමඟ සන්නිවේදනය කිරීමට හැකියාව ලැබේ.

It operates at the data link layer (Layer 2) of the OSI model and reads the source MAC address of incoming data packets, forwarding them only to their target destination instead of broadcasting them to all connected segments.
එය OSI ආකෘතියේ දත්ත සම්බන්ධක ස්ථරයේ (Layer 2) ක්‍රියාත්මක වන අතර පැමිණෙන දත්ත පැකට් වල මූලාශ්‍ර MAC ලිපිනය කියවයි, ඒවා සම්බන්ධිත සියලුම කොටස් වෙත විකාශනය කිරීම වෙනුවට ඔවුන්ගේ ඉලක්ක ගමනාන්තයට පමණක් ඒවා යොමු කරයි.



Filtering and forwarding data packets based on their destination MAC address to reduce network congestion and improve performance is done by this
ජාල තදබදය අවම කිරීම සහ කාර්ය සාධනය වැඩි දියුණු කිරීම සඳහා ඔවුන්ගේ ගමනාන්ත MAC ලිපිනය මත පදනම්ව දත්ත පැකට් පෙරීම සහ යොමු කිරීම මෙමගින් සිදු කරයි



How bridges Works
සේතුවක ක්‍රියාකාරීත්වය

Receives data packets from both connected network segments
සම්බන්ධිත ජාල කොටස් දෙකෙන්ම දත්ත පැකට් ලබා ගනී

Builds an internal table of MAC addresses to track which devices are on which segment
කුමන අංශයේ කුමන උපාංග තිබේද යන්න නිරීක්ෂණය කිරීමට MAC ලිපිනවල අභ්‍යන්තර වගුවක් ගොඩනගයි

Filtering data
දත්ත පෙරීම

If a packet from segment A is meant for a device on the same segment, the bridge stops it from going further
A කොටසේ පැකට්ටුවක් එකම කොටසේ උපාංගයක් සඳහා අදහස් කරන්නේ නම්, සේතුව එය ඉදිරියට යාම නතර කරයි.

Forwarding data
දත්ත යොමු කිරීම

If a packet from segment A is meant for a device on segment B, the bridge sends it to the correct place on segment B.
A කොටසේ පැකට්ටුවක් B කොටසේ උපාංගයක් සඳහා අදහස් කරන්නේ නම්, පාලම එය B කොටසේ නිවැරදි ස්ථානයට යවයි

NOTE:
Bridges are used to improve network performance, enhance security by breaking up large LANs into smaller ones, and ensure reliability by establishing backup paths across the network.
ජාල ක්‍රියාකාරීත්වය වැඩි දියුණු කිරීමට, විශාල LANs කුඩා ඒවාට කැඩීමෙන් ආරක්ෂාව වැඩි කිරීමට සහ ජාලය හරහා උපස්ථ මාර්ග පිහිටුවීමෙන් විශ්වසනීයත්වය සහතික කිරීමට සේතු භාවිතා වේ

Network Switch
ජාල ස්විචය

A Network switch is a networking device that connects multiple devices within a Local Area Network (LAN) and intelligently forwards data to the specific device that needs it.
ජාල ස්විචයක් යනු Local Area Network (LAN) තුළ බහුවිධ උපාංග සම්බන්ධ කරන ජාලකරණ උපාංගයක් වන අතර එය අවශ්‍ය නිශ්චිත උපාංගයට බුද්ධිමත්ව දත්ත යොමු කරයි.

A switch acts as a multiport bridge because it performs the same function as a bridge but has many ports.
ස්විචයක් multi-port සේතුවක් ලෙස ක්‍රියා කරයි, මන්ද එය සේතුවක් හා සමාන කාර්යයක් ඉටු කරන නමුත් එහි Ports රාශියක් පවතින බැවිනි.

Switches can have several ports counts
ස්විච් වල විවිධ ports සංඛ්‍යාවන් තිබිය හැක

- 4-port switch
- 8-port switch
- 16-port switch
- 24-port switch
- 48-port switch

Each switch port is a separate collision domain, so devices connected to different ports do not interfere with each other.
සෑම ස්විච් පෝට් එකක්ම වෙනම ගැටුම් වසමකි එබැවින් විවිධ පෝට් වලට සම්බන්ධ කර ඇති උපාංග එකිනෙකට බාධා පමුණුවන්නේ නැත.

Because collision domains are separated, collisions do not occur between different ports, improving network efficiency.
මෙම ගැටුම් වසම් එකිනෙකින් වෙන් වී පවතින බැවින්, විවිධ පෝට් අතර දත්ත ගැටීම් සිදු නොවේ. මෙය ජාලයේ කාර්යක්ෂමතාව වැඩි දියුණු කරයි.

What if switch ports are not enough?
ස්විචයක ඇති Ports ප්‍රමාණය මදි වුවහොත් කුමක් සිදුවේද?

Replace the small switch with a higher-port switch (e.g., 8-port → 24-port).
කුඩා ස්විචය වෙනුවට වැඩි ports ප්‍රමාණයක් ඇති ස්විචයක් ආදේශ කිරීම (උදාහරණයක් :ports 8 ස්විචයක් වෙනුවට ports 24 ස්විචයක්).

An additional switch can be connected to increase the number of available ports.
මුළු ports ගණන වැඩි කර ගැනීමට තවත් ස්විචයක් සම්බන්ධ කළ හැකිය

Large networks use multiple switches in layers (core → distribution → access) to handle many devices efficiently.
විශාල ජාලයන්, උපාංග විශාල ප්‍රමාණයක් කාර්යක්ෂමව හැසිරවීම සඳහා ස්විච කිහිපයක් ස්ථර වශයෙන් භාවිතා කරයි (core → distribution → access).

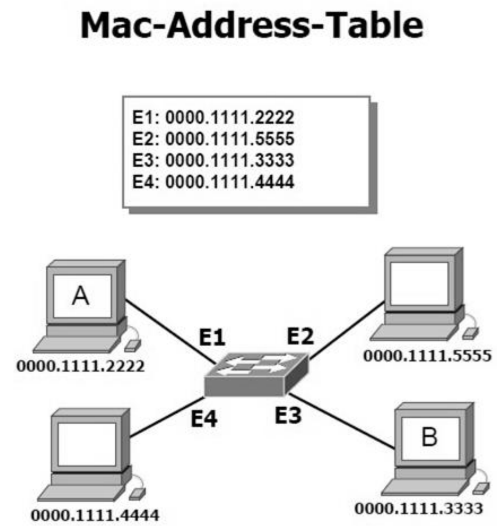
Many switches have special uplink ports to connect multiple switches with high speed.
බොහෝ ස්විචයන් සතුව ස්විච කිහිපයක් අධික වේගයකින් එකිනෙකට සම්බන්ධ කිරීම සඳහා විශේෂිත uplink ports පවතියි.

Features
ලක්ෂණ

MAC Address Learning
MAC ලිපින ඉගෙනීම

The switch learns and stores the MAC addresses of devices connected to its ports in a MAC address table.
ස්විචය එහි ports සම්බන්ධ උපාංගවල MAC ලිපින MAC ලිපින වගුවක ඉගෙන ගෙන ගබඩා කරයි.

This allows the switch to efficiently route packets to the correct destination without broadcasting to all ports.
සියලුම් Ports වෙත විකාශනය නොකර නිවැරදි ගමනාන්තය වෙත පැකට් කාර්යක්ෂමව ගමන් කිරීමට මෙය ස්විචයට ඉඩ සලසයි.



Packet Forwarding
පැකට් ඉදිරියට යැවීම

The switch receives incoming data packets and forwards them to the appropriate destination port based on the MAC address. This targeted forwarding reduces unnecessary traffic on the network.
ස්විචයට ලැබෙන දත්ත පැකට් ලැබෙන අතර ඒවා MAC ලිපිනය මත පදනම්ව සුදුසු ගමනාන්ත port එක වෙත යොමු කරයි. මෙම ඉලක්කගත යොමු කිරීම ජාලයේ අනවශ්‍ය තදබදය අඩු කරයි

Full-Duplex Communication
පූර්ණ-ද්විත්ව සන්නිවේදනය

Switches support full-duplex communication, allowing simultaneous data transmission and reception on each port.
ස්විචයන් පූර්ණ-ද්විත්ව සන්නිවේදනය සඳහා සහය වන අතර, එක් එක් Port මත එකවර දත්ත සම්ප්‍රේෂණයට සහ පිළිගැනීමට ඉඩ සලසයි.

Broadcast, Multicast, Unicast Handling
විකාශනය බහු විකාශන සහ ඒක-විකාශන හැසිරවීම

A switch can handle unicast and multicast traffic, and it has always been capable of broadcasting. It forwards unicast frames to a specific destination device, multicast frames to a selected group of devices, and broadcast frames to all devices within the same VLAN or network segment.
ස්විචයකට unicast සහ multicast දත්ත ගමනාගමනයන් හැසිරවිය හැකි අතර, broadcast කිරීමේ හැකියාව එයට පෙර සිටම පවතී. එය unicast frames කිසියම් නිශ්චිත ගමනාන්ත උපාංගයක් වෙතද, multicast frames තෝරාගත් උපාංග සමූහයක් වෙතද, සහ broadcast frames එකම VLAN එකක් හෝ ජාල කොටසක් තුළ ඇති සියලුම උපාංග වෙතද යොමු කරයි.

Security Features
ආරක්ෂක විශේෂාංග
Switches can implement security measures such as port security, which restricts access to specific devices.
ස්විච් මඟින් නිශ්චිත උපාංග සඳහා පමණක් ප්‍රවේශය සීමා කරන port security වැනි ආරක්ෂණ පියවරයන් ක්‍රියාත්මක කළ හැක.

How Network Switch Works
ජාල ස්විචයක ක්‍රියාකාරීත්වය

1. When a switch is first connected to the network, it doesn't initially know which MAC addresses are associated with which ports.
ස්විචයක් මුලින්ම ජාලයට සම්බන්ධ වූ විට, කුමන MAC ලිපින කුමන Port එකත් සමඟ සම්බන්ධ වී ඇත්දැයි එය මුලින් නොදනී.

When a device sends data, the switch records the source MAC address and the port it came from in its MAC address table.
උපාංගයක් දත්ත යවන විට, ස්විචය එහි MAC ලිපින වගුවේ මූලාශ්‍ර MAC ලිපිනය සහ එය පැමිණි Port එක වාර්තා කරයි.

2. When the switch receives a data frame, it checks the destination MAC address. If the address is found in the MAC address table, the switch forwards the data to the corresponding port.
ස්විචයට දත්ත රාමුවක් ලැබුණු විට, එය ගමනාන්ත MAC ලිපිනය පරීක්ෂා කරයි. ලිපිනය MAC ලිපින වගුවේ තිබේ නම්, ස්විචය දත්ත අදාළ Port එක වෙත යොමු කරයි.

3. If the destination MAC address is not in the table, the switch will broadcast the frame to all ports (except the one it was received on), similar to how a hub operates.
ගමනාන්ත MAC ලිපිනය වගුවේ නොමැති නම්, ස්විචය හබ්යක් ක්‍රියා කරන ආකාරය හා සමානව (එය ලැබුණු එක හැර) සියලු Ports වෙත රාමුව විකාශනය කරයි.

Once the destination device responds, the switch updates its MAC address table with the new information.
ගමනාන්ත උපාංගය ප්‍රතිචාර දැක්වූ පසු, ස්විචය එහි MAC ලිපින වගුව නව තොරතුරු සමඟ යාවත්කාලීන කරයි.

4. If the switch receives a data frame intended for a device that is on the same port as the sender, it filters out the frame and does not forward it to other ports.
යවන්නා සිටින එකම Ports ඇති උපාංගයක් සඳහා අදහස් කරන ලද දත්ත රාමුවක් ස්විචය ලබා ගන්නේ නම්, එය රාමුව පෙරහන් කරන අතර එය වෙනත් Ports වෙත යොමු නොකරයි.

This reduces unnecessary network traffic.
මෙය අනවශ්‍ය ජාල තදබදය අඩු කරයි.

5. While unicast traffic is sent only to the specific destination, switches also handle broadcast and multicast traffic.
Unicast ගමනාගමනය නිශ්චිත ගමනාන්තයට පමණක් යවන අතර, ස්විචයන් Broadcast සහ Multi-Cast ගමනාගමනය ද හසුරුවයි.

6. Broadcast communication reaches every device in the network segment, whereas multicast communication reaches only selected devices.
Broadcast මඟින් දත්ත ජාලයේ ඇති සියලුම උපාංග වෙත යවන අතර, Multicast දත්ත ගමනාගමනයන් යවනු ලබන්නේ එම දත්ත ලබාගැනීමට උනන්දුවක් දක්වන උපාංග සමූහයක් වෙත පමණි.

Types of Network Switches
ජාල ස්විච වර්ග

Unmanaged Switch
කළමනාකරණය නොකළ ස්විචය
A simple plug-and-play device with no configuration options. It is used in small networks where traffic management and security are not major concerns.
වින්‍යාස විකල්ප නොමැති සරල plug-and-play උපාංගයකි. එය ජාල කළමනාකරණය සහ ආරක්ෂාව ප්‍රධාන ගැටළු නොවන කුඩා ජාල වල භාවිතා වේ.

Managed Switch
කළමනාකරණය කළ ස්විචය
A switch that allows for configuration and management, providing features like VLANs, Quality of Service (QoS), link aggregation, and network monitoring.
වින්‍යාස කිරීම සහ කළමනාකරණය සඳහා ඉඩ දෙන ස්විචයක්, VLAN සේවාවේ ගුණාත්මකභාවය QoS සබැඳි එකතු කිරීම සහ ජාල අධීක්ෂණය වැනි විශේෂාංග සපයයි.

NOTE:
Layer 3 Switch (Multilayer Switch)
ස්ථර 3 ස්විචය (බහු ස්ථර ස්විචය)

Combines the functions of a switch (Layer 2) and a router (Layer 3), enabling it to perform routing functions in addition to switching.
ස්විචයක (ලේයර් 2) සහ රවුටරයක (ලේයර් 3) ක්‍රියාකාරකම් ඒකාබද්ධ කරයි, එය මාරු කිරීමට අමතරව මාර්ගගත කිරීමේ කාර්යයන් සිදු කිරීමට හැකියාව ලබා දෙයි.

This allows for more efficient handling of traffic between different subnets.
විවිධ උපජාල අතර ගමනාගමනය වඩාත් කාර්යක්ෂමව හැසිරවීමට මෙය ඉඩ සලසයි.

Connects several networks together
ජාල කිහිපයක් එකිනෙකට සම්බන්ධ කරයි.
Router
මාර්ගකය

A router is a key network device that manages and directs traffic between networks.
රවුටරයක් ජාල අතර ගමනාගමනය කළමනාකරණය කරන සහ මෙහෙයවන ප්‍රධාන ජාල උපාංගයකි.

It forwards data packets between computer networks
එය පරිගණක ජාල අතර දත්ත පැකට් යොමු කරයි

How Routers Work
මාර්ගකයක ක්‍රියාකාරීත්වය

When a data packet arrives at a router, the router examines the packet's header to identify its destination IP address.
දත්ත පැකට්ටුවක් රවුටරයකට පැමිණි විට, රවුටරය එහි ගමනාන්ත IP ලිපිනය හඳුනා ගැනීමට පැකට්ටුවේ ශීර්ෂය පරීක්ෂා කරයි.

Using a routing table, which contains information about available paths, the router determines the best next hop for the packet.
පවතින මාර්ග පිළිබඳ තොරතුරු අඩංගු මාර්ගගත කිරීමේ වගුවක් භාවිතා කරමින්, රවුටරය පැකට්ටුව සඳහා හොඳම ඊළඟ හොප් එක තීරණය කරයි.

The router then forwards the packet to the next device or router along the path, continuing this process until the packet reaches its final destination.
රවුටරය පසුව පැකට්ටුව ඊළඟ උපාංගයට හෝ මාර්ගය ඔස්සේ රවුටරයට යොමු කරයි, පැකට්ටුව එහි අවසාන ගමනාන්තය කරා ළඟා වන තෙක් මෙම ක්‍රියාවලිය දිගටම කරගෙන යයි.

NOTE:
Home routers combine multiple functions such as default gateway, modem, switch, access point, firewall, and DHCP server in a single device.
නිවෙස් වල භාවිතා කරන රවුටර මඟින් Default gateway, Modem, Switch, Access point, Firewall, සහ DHCP server වැනි බහුවිධ කාර්යයන් රාශියක් එකම උපාංගයක් තුළට ඒකාබද්ධ කර ඇත.

However, in industrial or enterprise networks, these functions are implemented using separate dedicated devices for better performance, security, and scalability.
කෙසේ වෙතත්, කාර්මික හෝ විශාල ව්‍යාපාරික ජාලයන්හි වඩා හොඳ කාර්ය සාධනයක්, ආරක්ෂාවක් සහ පරිමාණය කිරීමේ හැකියාවක් ලබා ගැනීම සඳහා මෙම කාර්යයන් වෙන වෙනම වෙන් කරන ලද සුවිශේෂී උපාංග භාවිතයෙන් ක්‍රියාත්මක කරනු ලැබේ.

Routers are computers
Routers ද පරිගණක වේ.
Routers can be built from standard computer parts but are mostly specialized purpose-built computers. Early routers used software-based forwarding, running on a CPU.

රවුටර සාමාන්‍ය පරිගණක කොටස් වලින් සෑදිය හැකි නමුත් ඒවා බොහෝ විට විශේෂිත අරමුණක් ඇති පරිගණක වේ. මුල් රවුටර CPU මත ක්‍රියාත්මක වන මෘදුකාංග මත පදනම් වූ ඉදිරියට යැවීම භාවිතා කරන ලදී.

More sophisticated devices use application-specific integrated circuits (ASICs) to increase performance or add advanced filtering and firewall functionality.
කාර්ය සාධනය වැඩි කිරීමට හෝ උසස් පෙරහන සහ ෆයර්වෝල් ක්‍රියාකාරීත්වය එක් කිරීමට වඩාත් සංකීර්ණ උපාංග යෙදුම්-විශේෂිත ඒකාබද්ධ පරිපථ (ASICs) භාවිතා කරයි.

Features
ලක්ෂණ

Routers allow devices to connect and share data over the Internet or an intranet
රවුටර මඟින් උපාංගවලට අන්තර්ජාලය හෝ අන්තඃජාලය හරහා දත්ත සම්බන්ධ කිරීමට සහ බෙදා ගැනීමට ඉඩ ලබා දේ

They use the Internet Protocol (IP) to send IP packets containing data and IP addresses of sending and destination devices located on separate local area networks
ඒවා වෙනත් ස්ථානීය ප්‍රදේශ ජාල තුල පවතින උපාංග අතර යවන්නාගේ සහ ලබන්නාගේ IP ලිපින සහ දත්ත ඇතුලත් පැකට් හුවමාරු කිරීමට අන්තර්ජාල නියමාවලිය භාවිත කරයි

Routers maintain routing tables that list directions for forwarding data to particular network destinations
විශේෂිත ජාල ගමනාන්ත වෙත දත්ත යොමු කිරීම සඳහා මාර්ගෝපදේශ ලැයිස්තුගත කරන මාර්ගගත වගු රවුටර විසින් පවත්වාගෙන යයි

They can perform Network Address Translation (NAT) to shield private IP addresses and improve security
පුද්ගලික IP ලිපින ආරක්ෂා කිරීමට සහ ආරක්ෂාව වැඩි දියුණු කිරීමට ඔවුන්ට ජාල ලිපින පරිවර්තනය NAT සිදු කළ හැක

NOTE:
What is Intranet ?
අන්තඃජාලය යනු කුමක්ද ?
A private network used within an organization to share information, resources, and services securely among employees.
මෙය සේවකයින් අතර තොරතුරු, සම්පත් සහ සේවාවන් ආරක්ෂිතව බෙදා හැරීම සඳහා සංවිධානයක් හෝ ආයතනයක් තුළ පමණක් භාවිතා කරන පුද්ගලික ජාලයකි

It uses the same technologies as the internet (like web browsers and TCP/IP) but is accessible only to authorized users inside the organization.
මේ සඳහා අන්තර්ජාලයේ භාවිතා වන තාක්ෂණයන්ම (Web browsers සහ TCP/IP වැනි) භාවිතා කරන නමුත්, මෙයට ප්‍රවේශ විය හැක්කේ ආයතනය තුළ සිටින බලයලත් පරිශීලකයින්ට පමණි.

Types of Routers
මාර්ගක වර්ග

Core routers
Designed to operate in the Internet backbone, or core.
Internet backbone හී ක්‍රියාත්මක වීමට නිපැයුම් කර ඇත.

Distribution Router
Distribution routers control and manage traffic for area networks within some ISP networks.
සමහර අන්තර්ජාල සේවා සපයන්නන්ගේ ජාල තුළ පවතින කලාපීය ජාලයන්හි දත්ත ගමනාගමනය පාලනය කිරීම සහ කළමනාකරණය කිරීම Distribution routers මඟින් සිදු කරනු ලබයි.

Edge routers
Represent the border crossing between internal and external networks .
අභ්‍යන්තර සහ බාහිර ජාල අතර මායිම් හරස් කිරීම නියෝජනය කරයි.

Modem
මොඩමය

A modem (modulator-demodulator) is a device that enables communication between your home network and your Internet Service Provider (ISP).
මොඩමයක් (modulator-demodulator) යනු ඔබගේ නිවසේ ජාලය සහ ඔබගේ අන්තර්ජාල සේවා සපයන්නා ISP අතර සන්නිවේදනය සක්‍රීය කරන උපාංගයකි.

Without a modem, your devices wouldn't be able to connect to the internet.
මොඩමයක් නොමැතිව, ඔබගේ උපාංගවලට අන්තර්ජාලයට සම්බන්ධ වීමට නොහැකි වනු ඇත.

The modem acts as a translator between the digital signals used by your devices and the analog signals used by traditional communication lines.
මොඩමය ඔබගේ උපාංග භාවිතා කරන ඩිජිටල් සංඥා සහ සම්ප්‍රදායික සන්නිවේදන මාර්ග භාවිතා කරන ප්‍රතිසම සංඥා අතර පරිවර්තකයක් ලෙස ක්‍රියා කරයි.

Built-in Routers- Many modern modems come with integrated routers, allowing them to handle both the modem and routing functions in one device. බොහෝ නවීන මොඩමයන් ඒකාබද්ධ රවුටර සමඟ එන අතර, එක් උපාංගයක් තුළ මොඩම සහ රවුටින් යන කාර්යයන් දෙකම හැසිරවීමට ඉඩ සලසයි.

How modem Works
මොඩමයක ක්‍රියාකාරිත්වය

Signal Modulation (Outbound Data)

Digital to Analog

Your computer, smartphone, or other devices generate data in a digital format (0s and 1s).
ඔබේ පරිගණකය, ස්මාර්ට් ජංගම දුරකථනය හෝ වෙනත් උපාංග සංඛ්‍යාංක ආකෘතියකින් දත්ත ජනනය කරන්නේ 0 සහ 1 ලෙසයි.

When you send data, such as a request for a web page, the modem converts this digital data into an analog signal.
ඔබ වෙබ් පිටුවක් සඳහා ඉල්ලීමක් වැනි දත්ත යවන විට, මොඩමය මෙම ඩිජිටල් දත්ත ප්‍රතිසම සංඥාවක් බවට පරිවර්තනය කරයි.

This process is called modulation. The analog signal is suited for transmission over telephone lines, cable systems, or fiber optics.
මෙම ක්‍රියාවලිය (Modulation) ලෙස හැඳින්වේ. ඇනලොග් සංඥා දුරකථන මාර්ග, කේබල් පද්ධති හෝ ප්‍රකාශ තන්තු හරහා සම්ප්‍රේෂණය කිරීම සඳහා සුදුසු වේ.

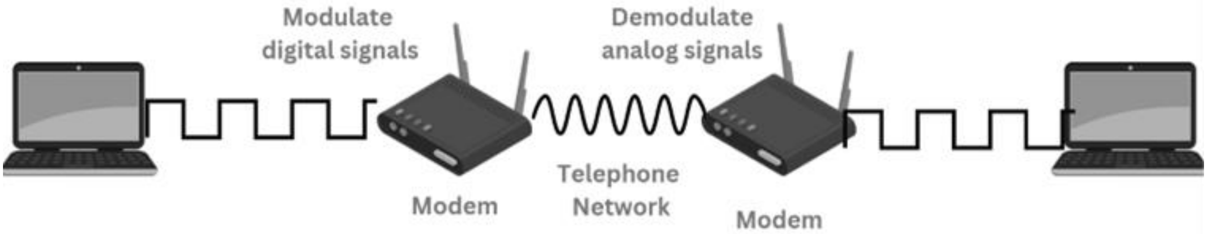
Transmission
The analog signal is transmitted through the communication line (telephone line, cable line, or fiber optic cable) to your ISP.
ප්‍රතිසම සංඥාව සන්නිවේදන මාර්ගය (දුරකථන මාර්ගය, කේබල් මාර්ගය හෝ ෆයිබර් ඔප්ටික් කේබලය) හරහා ඔබේ ISP වෙත සම්ප්‍රේෂණය වේ.

Signal Demodulation (Inbound Data)

Analog to Digital

When data reaches your ISP, it's converted back into a digital format.
දත්ත ඔබේ ISP වෙත ළඟා වූ විට, එය නැවත ඩිජිටල් ආකෘතියක් බවට පරිවර්තනය වේ.

This process is called demodulation. The ISP then routes this digital data through their network and to the specific online destination you requested.
මෙම ක්‍රියාවලිය demodulation ලෙස හැඳින්වේ. ISP පසුව මෙම ඩිජිටල් දත්ත ඔවුන්ගේ ජාලය හරහා සහ ඔබ ඉල්ලූ නිශ්චිත සබැඳි ගමනාන්තය වෙත යොමු කරයි.



Types of Modems
මොඩම් වර්ග

1. Based on Transmission Medium
සම්ප්‍රේෂණ මාධ්‍යය මත පදනම්ව

A. Wired Modems
Use physical cables for communication.
සන්නිවේදනය සඳහා භෞතික කේබල් භාවිතා කරයි.

Type / වර්ගය	Description / විස්තර ය
Dial-Up Modem	Uses telephone lines for internet access. අන්තර්ජාල ප්‍රවේශය සඳහා දුරකථන මාර්ග භාවිතා කරයි.
DSL Modem	Uses digital subscriber telephone lines. ඩිජිටල් ග්‍රාහක දුරකථන මාර්ග භාවිතා කරයි.
Cable Modem	Uses coaxial cable TV networks. සමාක්ෂ කේබල් රූපවාහිනී ජාල භාවිතා කරයි
Fiber Optic Modem (ONT/ONU)	Uses fiber-optic cables for very high-speed internet. අධිවේගී අන්තර්ජාලය සඳහා ප්‍රකාශ තන්තු කේබල් භාවිතා කරයි.

B. Wireless Modems

Type / වර්ගය	Description / විස්තරය
Cellular Modem	Connects to mobile networks for internet access. Often available as a USB modem (dongle/data card) that plugs directly into a computer's USB port. අන්තර්ජාල ප්‍රවේශය සඳහා ජංගම ජාල වෙත සම්බන්ධ වේ. බොහෝ විට පරිගණකයක USB කෙවෙනියට සෘජුවම සම්බන්ධ කරන USB මොඩමයක් (dongle/data card) ලෙස ලබා ගත හැකිය.
Satellite Modem	Uses satellites for internet connectivity. අන්තර්ජාල සම්බන්ධතාවය සඳහා චන්ද්‍රිකා භාවිතා කරයි.
WiMAX Modem	Uses WiMAX wireless broadband technology. WiMAX රැහැන් රහිත බ්‍රෝඩ්බෑන්ඩ් තාක්ෂණය භාවිතා කරයි.

2. Based on Installation Method
ස්ථාපන ක්‍රමය මත පදනම්ව

A. Internal Modem
- Installed inside the computer.
  පරිගණකය තුළ ස්ථාපනය කර ඇත.
- Connected directly to the motherboard.
  මවු පුවරුවට කෙලින්ම සම්බන්ධ කර ඇත.

B. External Modem
- Separate device connected via USB or Ethernet.
  USB හෝ Ethernet හරහා සම්බන්ධ කර ඇති වෙනම උපාංගයකි.
- Easy to install and troubleshoot.
  ස්ථාපනය කිරීමට සහ දෝශ නිරාකරණය කිරීමට පහසුය.
- Portable and flexible.
  අතේ ගෙන යා හැකි සහ නම්‍යශීලී වේ.

3. Based on Signal Type
සංඥා වර්ගය මත පදනම්ව

A. Analog Modem
- Converts digital data into analog signals and back. (ASK/FSK/PSK/QAM)
  අංකිත දත්ත ප්‍රතිසම සංඥා සහ ප්‍රතිසම දත්ත අංකිත සංඥා බවට පරිවර්තනය කරයි.
- Commonly used in dial-up connections.
  Dial-up සම්බන්ධතා වල බහුලව භාවිතා වේ.

B. Broadband Modem
- Use advanced modulation or optic signaling for digital communication.
  ඩිජිටල් සන්නිවේදනය සඳහා උසස් මූර්ජන ක්‍රමවේද හෝ දෘශ්‍ය සංඥාකරණය භාවිත කරයි.

  Ex: DSL, Cable, and Fiber modems.

4. Based on Network Technology
ජාල තාක්ෂණය මත පදනම්ව
- Dial-Up Modem
- ISDN Modem
- DSL Modem
- Cable Modem
- Fiber Optic Modem
- Cellular (3G/4G/5G) Modem
- Satellite Modem

Firewall
ගිනිපවුර

A firewall is a network security system designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules.
ගිනිපවුර යනු කලින් තීරණය කරන ලද ආරක්ෂක නීති මත පදනම්ව පැමිණෙන සහ පිටතට යන ජාල ගමනාගමනය නිරීක්ෂණය කිරීම, පෙරීම සහ පාලනය කිරීම සඳහා නිර්මාණය කර ඇති ජාල ආරක්ෂණ පද්ධතියකි.

Firewalls can be hardware-based, software-based, or a combination of both.
ගිනිපවුර දෘඩාංග මත පදනම් වූ, මෘදුකාංග පදනම් වූ හෝ දෙකේම එකතුවක් විය හැක.%

Their main purpose is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and threats.
ඔවුන්ගේ ප්‍රධාන අරමුණ වන්නේ අනවසර පිවිසීම් සහ තර්ජන වැළැක්වීම සඳහා විශ්වාසදායක අභ්‍යන්තර ජාලයක් සහ අන්තර්ජාලය වැනි විශ්වාස නොකළ බාහිර ජාල අතර බාධකයක් ඇති කිරීමයි.

A firewall inspects and filters traffic between private and public networks, allowing authorized communication from private to public networks and controlling or blocking unauthorized access from public to private networks to maintain security.
ගිනිපවුරක් මඟින් පුද්ගලික සහ පොදු ජාල අතර ගලායන දත්ත ගමනාගමනය පරීක්ෂා කිරීම සහ පෙරීම සිදු කරයි. එහිදී ආරක්ෂාව පවත්වාගෙන යාම සඳහා පුද්ගලික ජාලයේ සිට පොදු ජාලය වෙත බලයලත් සන්නිවේදනයට ඉඩ ලබා දෙන අතර, පොදු ජාලයේ සිට පුද්ගලික ජාලය වෙත සිදුවන අනවසර ප්‍රවේශයන් පාලනය කිරීම හෝ අවහිර කිරීම සිදු කරනු ලබයි.

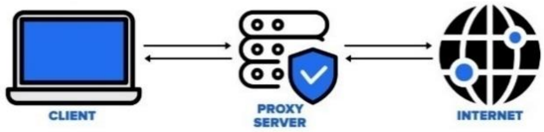
How Firewalls Work
ගිනිපවුරක ක්‍රියාකාරීත්වය

Packet Filtering
Firewalls inspect packets of data sent between devices on the network. Each packet is analyzed based on rules defined by the firewall.
ගිනිපවුර ජාලයේ උපාංග අතර යවන ලද දත්ත පැකට් පරීක්ෂා කරයි. සෑම පැකට්ටුවක්ම ගිනිපවුර විසින් නිර්වචනය කර ඇති නීති මත පදනම්ව විශ්ලේෂණය කෙරේ.

If a packet matches the criteria (e.g., allowed IP addresses, port numbers), it is allowed through; otherwise, it is blocked.
පැකට්ටුවක් නිර්ණායකයට ගැලපේ නම් (Ex. allowed IP addresses, port numbers), එය හරහා අවසර දෙනු ලැබේ එසේ නොමැති නම්, එය අවහිර කරනු ඇත.

Stateful Firewall
Monitors and tracks the state of active network connections connection wise .
සක්‍රීය ජාල සම්බන්ධතාවල වත්මන් තත්ත්වය සම්බන්ධතාවය සම්බන්ධයෙන් ගත් විට නිරන්තරයෙන් නිරීක්ෂණය කරන අතර ඒ පිළිබඳ වාර්තා තබා ගනියි.

Stateless Firewall
Examines each packet independently without maintaining information about previous packets or connection states.
පෙර හුවමාරු වූ දත්ත පැකට්ටු හෝ සම්බන්ධතාවල තත්ත්වයන් පිළිබඳ කිසිදු තොරතුරක් මතක තබා නොගෙන සෑම දත්ත පැකට්ටුවක්ම එකිනෙකින් ස්වාධීනව තනි තනිව පරීක්ෂා කර බලයි.

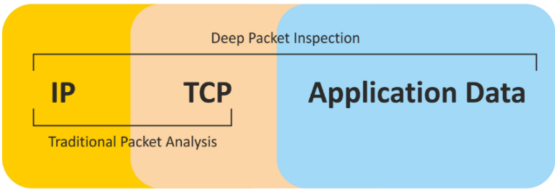
Proxy Services


Some firewalls can act as intermediaries between a user and the internet.
සමහර ගිනිපවුරු වලට පරිශීලකයෙකු සහ අන්තර්ජාලය අතර අතරමැදියන් ලෙස ක්‍රියා කළ හැක.

Requests are made through the firewall, which then requests the data from the internet on behalf of the user.
ගිනිපවුර හරහා ඉල්ලීම් සිදු කරනු ලබන අතර, පසුව පරිශීලකයා වෙනුවෙන් අන්තර්ජාලයෙන් දත්ත ඉල්ලා සිටී.

This helps to mask the user's IP address and can inspect and block malicious content.
මෙය පරිශීලකයාගේ IP ලිපිනය වසං කිරීමට උපකාරී වන අතර අනිෂ්ට අන්තර්ගතයන් පරීක්ෂා කර අවහිර කළ හැක.

Deep Packet Inspection (DPI)



DPI examines the data part (payload) of the packet in addition to the header.
DPI ශීර්ෂයට අමතරව පැකට්ටුවේ දත්ත කොටස (payload) පරීක්ෂා කරයි.

This allows for more thorough analysis, such as identifying and blocking malware or enforcing data privacy rules.
මෙය අනිෂ්ට මෘදුකාංග හඳුනා ගැනීම සහ අවහිර කිරීම හෝ දත්ත රහස්‍යතා නීති බලාත්මක කිරීම වැනි වඩාත් සවිස්තරාත්මක විශ්ලේෂණයකට ඉඩ සලසයි.

Purpose of Firewalls
ගිනි පවුරක අරමුණු

- Firewalls block unauthorized users or programs from accessing your network or system.
  ෆයර්වෝල් මඟින් අනවසර පරිශීලකයන් හෝ වැඩසටහන් ඔබේ ජාලයට හෝ පද්ධතියට ප්‍රවේශ වීම අවහිර කරයි.
- They help monitor traffic to and from a network and enforce policies about what is allowed or disallowed.
  ඔවුන් ජාලයකට සහ ඉන් පිටත ගමනාගමනය නිරීක්ෂණය කිරීමට සහ අවසර දී ඇති හෝ අනුමත නොකළ දේ පිළිබඳ ප්‍රතිපත්ති බලාත්මක කිරීමට උදවු කරයි.
- Firewalls can block known threats, such as viruses, worms, and other malware, from entering or spreading within a network.
  ෆයර්වෝල් වලට වෛරස්, worms සහ වෙනත් අනිෂ්ට මෘදුකාංග වැනි තර්ජන ජාලයකට ඇතුළු වීමෙන් හෝ පැතිරීමෙන් අවහිර කළ හැක.
- Organizations can restrict access to certain websites, applications or services.
  සංවිධානවලට ඇතැම් වෙබ් අඩවි, යෙදුම් හෝ සේවාවන් වෙත ප්‍රවේශ වීම සීමා කළ හැකිය.
- Records network connections and security events for auditing and troubleshooting.
  විගණනය සහ දෝෂ නිරාකරණය සඳහා ජාල සම්බන්ධතා සහ ආරක්ෂක සිදුවීම් වාර්තා කර තබා ගනියි.

Access Point (AP)

An Access Point (AP) is a networking device that allows wireless devices to connect to a wired network using Wi-Fi or other wireless standards.
ප්‍රවේශ ලක්ෂ්‍යයක් AP යනු රැහැන් රහිත උපාංග (Wi-Fi) හෝ වෙනත් රැහැන් රහිත ප්‍රමිතීන් භාවිතයෙන් රැහැන්ගත ජාලයකට සම්බන්ධ වීමට ඉඩ සලසන ජාලකරණ උපාංගයකි.

It enables them to communicate with each other and access network resources.
ඔවිට ඔවුන්ට එකිනෙකා සමඟ සන්නිවේදනය කිරීමට සහ ජාල සම්පත් වෙත ප්‍රවේශ වීමට හැකි වේ.

It is connected to the switch or also can be connected to the router. Most modern devices come integrated.
එය ස්විචයට හෝ රවුටරයට සම්බන්ධ කළ හැකිය. බොහෝ නවීන උපාංග මේවා ඒකාබද්ධ කර නිපදවා ඇත.

Key Features
ප්‍රධාන ලක්ෂණ

Wireless Connectivity
රැහැන් රහිත සම්බන්ධතාව

The primary function of an access point is to provide wireless connectivity to devices, such as smartphones, laptops, tablets, and IoT devices, enabling them to join the network without physical cables.
රැහැන් රහිත සම්බන්ධතාව : ප්‍රවේශ ලක්ෂ්‍යයක මූලික කාර්යය වන්නේ ස්මාට්ෆෝන්, ලැප්ටොප්, ටැබ්ලට්, සහ IoT උපාංග වැනි උපාංග වෙත රැහැන් රහිත සම්බන්ධතාවක් සැපයීම, භෞතික කේබල් නොමැතිව ජාලයට සම්බන්ධ වීමට ඔවුන්ට හැකියාව ලබා දීමයි.

Network Bridging
ජාල සේතුකරණය

An access point connects wireless devices to a wired network, often through an Ethernet cable. This allows wireless devices to access the broader network, including resources like servers, printers, and internet connections.
ප්‍රවේශ ලක්ෂ්‍යයක් මඟින් රැහැන් රහිත උපාංග, බොහෝ විට ඊතර්නෙට් කේබලයක් හරහා, රැහැන් සහිත ජාලයකට සම්බන්ධ කරනු ලබයි. මෙමඟින් සේවාදායක, මුද්‍රණ යන්ත්‍ර සහ අන්තර්ජාල සම්බන්ධතා වැනි සම්පත් ඇතුළුව පුළුල් ජාලයකට ප්‍රවේශ වීමට රැහැන් රහිත උපාංගවලට අවස්ථාව ලැබේ.

Signal Transmission and Reception
සංඥා සම්ප්රේෂණය සහ පිළිගැනීම

The access point transmits wireless signals (radio waves) that cover a specific area, known as a "coverage area" or "wireless cell." Devices within this area can connect to the network through the access point.
ප්‍රවේශ ලක්ෂ්‍යය "ආවරණ ප්‍රදේශය" හෝ "wireless cell" ලෙස හඳුන්වන විශේෂිත ප්‍රදේශයක් ආවරණය කරන රැහැන් රහිත සංඥා (රේඩියෝ තරංග) සම්ප්‍රේෂණය කරයි.

It also receives signals from connected wireless devices and forwards them to the wired network or other wireless devices.
මෙම ප්‍රදේශය තුළ ඇති උපාංග ප්‍රවේශ ස්ථානය හරහා ජාලයට සම්බන්ධ විය හැක.
එය සම්බන්ධිත රැහැන් රහිත උපාංගවලින් සංඥා ලබාගෙන ඒවා රැහැන්ගත ජාලයට හෝ වෙනත් රැහැන් රහිත උපාංග වෙත යොමු කරයි.

SSID Broadcasting
SSID විකාශනය

The access point broadcasts a Service Set Identifier (SSID), which is the name of the wireless network. Devices use this SSID to identify and connect to the network.
ප්‍රවේශ ස්ථානය රැහැන් රහිත ජාලයේ නම වන සේවා කට්ටල හඳුනාගැනීමක් SSID විකාශනය කරයි. උපාංග හඳුනා ගැනීමට සහ ජාලයට සම්බන්ධ වීමට මෙම SSID භාවිතා කරයි.

Security Management
ආරක්ෂක කළමනාකරණය

Access points often support various security protocols, such as WPA3 (Wi-Fi Protected Access 3) or WPA2, to encrypt data transmitted over the wireless network and prevent unauthorized access.
රැහැන් රහිත ජාලය හරහා සම්ප්‍රේෂණය වන දත්ත සංකේතනය කිරීමට සහ අනවසරයෙන් ප්‍රවේශ වීම වැළැක්වීමට ප්‍රවේශ ස්ථාන බොහෝ විට WPA3 (Wi-Fi ආරක්ෂක ප්‍රවේශ 3) හෝ WPA2 වැනි විවිධ ආරක්ෂක ප්‍රොටෝකෝල සඳහා සහය දක්වයි.

How Access Point Works
Access Point ක්‍රියාකාරීත්වය

1. The access point generates and transmits a wireless signal over a certain frequency (usually 2.4 GHz or 5 GHz bands). This signal covers a specific area, creating a wireless network within that range.
ප්‍රවේශ ලක්ෂ්‍යය යම් සංඛ්‍යාතයක් (සාමාන්‍යයෙන් (2.4 GHz හෝ 5 GHz කලාප) හරහා රැහැන් රහිත සංඥාවක් ජනනය කර සම්ප්‍රේෂණය කරයි. මෙම සංඥාව නිශ්චිත ප්‍රදේශයක් ආවරණය කරයි, එම පරාසය තුළ රැහැන් රහිත ජාලයක් නිර්මාණය කරයි.

2. Wireless devices scan for available networks by detecting SSIDs broadcasted by access points. When a device selects an SSID, it sends a connection request to the access point.
රැහැන් රහිත උපාංග ප්‍රවේශ ස්ථාන මගින් විකාශනය කරන ලද SSID හඳුනා ගැනීමෙන් පවතින ජාල සඳහා පරිලෝකනය කරයි. උපාංගයක් SSID එකක් තෝරාගත් විට, එය ප්‍රවේශ ස්ථානයට සම්බන්ධතා ඉල්ලීමක් යවයි.

3. The access point authenticates the device using security protocols like WPA3/WPA2, and once authenticated, it allows the device to join the network.
පිවිසුම් ස්ථානය (WPA3/WPA2) වැනි ආරක්ෂක ප්‍රොටෝකෝල භාවිතයෙන් උපාංගය සත්‍යාපනය කරයි, සහ සත්‍යාපනය කළ පසු, එය උපාංගයට ජාලයට සම්බන්ධ වීමට ඉඩ සලසයි.

4. When a connected device sends data (such as a web request), the access point receives the data wirelessly, converts it into a format suitable for the wired network, and forwards it through the Ethernet connection to the router or other network devices.
සම්බන්ධිත උපාංගයක් දත්ත යවන විට (වෙබ් ඉල්ලීමක් වැනි), ප්‍රවේශ ලක්ෂ්‍යය රැහැන් රහිතව දත්ත ලබා ගනී, එය රැහැන්ගත ජාලයට සුදුසු ආකෘතියක් බවට පරිවර්තනය කරයි, සහ ඊතර්නෙට් සම්බන්ධතාවය හරහා රවුටරයට හෝ වෙනත් ජාල උපාංග වෙත යොමු කරයි.

5.Conversely, when data is sent to the wireless device from the network, the access point receives the data via the wired connection, converts it into wireless signals, and transmits it to the appropriate device.
අනෙක් අතට, ජාලයෙන් රැහැන් රහිත උපාංගය වෙත දත්ත යවන විට, පිවිසුම් ස්ථානය රැහැන්ගත සම්බන්ධතාවය හරහා දත්ත ලබා ගනී, එය රැහැන් රහිත සංඥා බවට පරිවර්තනය කර සුදුසු උපාංගයට සම්පෙෂණය කරයි.

Types of Access Points
ප්‍රවේශ ස්ථාන වර්ග

1. By Integration
ඒකාබද්ධතාවය අනුව

- **Standalone (Independent) Access Point**
  ස්වාධීන ප්‍රවේශ ලක්ෂ්‍යය

A dedicated device that only provides Wi-Fi and connects to a router or switch using an Ethernet cable, commonly used in offices, schools, and campuses.
Wi-Fi පහසුකම පමණක් සපයන සහ ඊතර්නෙට් කේබලයක් භාවිතයෙන් රවුටරයකට හෝ ස්විචයකට සම්බන්ධ වන වෙනමම උපාංගයකි. මෙය සාමාන්‍යයෙන් කාර්යාල, පාසල් සහ විශ්වවිද්‍යාල පරිශ්‍රයන්හි භාවිත වේ.

- **Built-in (Integrated) Access Point**
  කාවැද්දූ ප්‍රවේශ ලක්ෂ්‍යය

An access point built into another device, usually a wireless router, commonly used in homes and small offices.
වෙනත් උපාංගයක් (සාමාන්‍යයෙන් රැහැන් රහිත රවුටරයක්) තුළම නිපදවා ඇති ප්‍රවේශ ලක්ෂ්‍යයකි. මෙය සාමාන්‍යයෙන් නිවාස සහ කුඩා කාර්යාලවල භාවිත වේ.

2. By Installation
ස්ථාපනය අනුව

- **Indoor Access Point**
  ගෘහස්ථ ප්‍රවේශ ලක්ෂ්‍යය

Designed for indoor environments such as homes, offices, and schools.
නිවාස, කාර්යාල සහ පාසල් වැනි ගෘහස්ථ පරිසරයන් සඳහා සැලසුම් කර ඇත.

- **Outdoor Access Point**
  බාහිර ප්‍රවේශ ලක්ෂ්‍යය

Weatherproof and designed for outdoor areas such as campuses, parks, and stadiums.
දේශගුණික විපර්යාසයන්ට ඔරොත්තු දෙන ලෙස, විශ්වවිද්‍යාල පරිශ්‍ර, උද්‍යාන සහ ක්‍රීඩාංගණ වැනි එළිමහන් ස්ථාන සඳහා සැලසුම් කර ඇත.

3. By Frequency Band
සංඛ්‍යාත කලාපය අනුව

- **Single-Band Access Point**
  තනි කලාප ප්‍රවේශ ලක්ෂ්‍යය

Supports only one frequency band, typically 2.4 GHz.
සාමාන්‍යයෙන් 2.4 GHz වන එක් සංඛ්‍යාත කලාපයකට පමණක් සහය දක්වයි.

- **Dual-Band Access Point**
  ද්විත්ව කලාප ප්‍රවේශ ලක්ෂ්‍යය

Supports both 2.4 GHz and 5 GHz frequency bands.
2.4 GHz සහ 5 GHz යන සංඛ්‍යාත කලාප දෙකටම සහය දක්වයි.

- **Tri-Band Access Point**
  ත්‍රිත්ව කලාප ප්‍රවේශ ලක්ෂ්‍යය

Supports three frequency bands, typically 2.4 GHz with two 5 GHz bands or 2.4 GHz, 5 GHz, and 6 GHz in newer models.
සංඛ්‍යාත කලාප තුනකට සහය දක්වයි. සාමාන්‍යයෙන් 2.4 GHz සමඟ 5 GHz කලාප දෙකක් හෝ, නවීන මාදිලිවල 2.4 GHz, 5 GHz, සහ 6 GHz කලාප මේ සඳහා ඇතුළත් වේ.

4. By Power Source
බලශක්ති ප්‍රභවය අනුව

- **Standard Access Point**
  සම්මත ප්‍රවේශ ලක්ෂ්‍යය

Powered using a separate power adapter.
වෙනම Power Adapter භාවිතයෙන් විදුලිය ලබා ගනී.

- **PoE (Power over Ethernet) Access Point**
  PoE (Power over Ethernet) ප්‍රවේශ ලක්ෂ්‍යය

Receives both power and data through a single Ethernet cable and is widely used in enterprise networks.
එක් ඊතර්නෙට් කේබලයක් හරහා විදුලිය සහ දත්ත යන දෙකම ලබා ගන්නා අතර මෙය ආයතනික ජාල තුළ බහුලව භාවිත වේ.

Gateway
දොරටු මඟ

A gateway is a software or networking device that connects networks, which allows devices on one network to communicate with devices on a different technology network.
දොරටු මඟක් යනු විවිධ තාක්ෂණික ජාලයන් එකිනෙකට සම්බන්ධ කරන සහ එක් ජාලයක ඇති උපාංගවලට අනෙක් ජාලයේ ඇති උපාංග සමඟ සන්නිවේදනය කිරීමට ඉඩ සලසන ජාලකරණ උපාංගයක් හෝ මෘදුකාංගයකි

Most gateways are hardware devices, while software gateways are rare.
බොහෝ දොරටු මං දෘඩාංග උපාංග වන අතර, සමහරක් මෘදුකාංග මත පදනම් වූ ඒවා වේ.

How a Gateway Works
දොරටු මඟක ක්‍රියාකාරීත්වය

1. A device needs to sends data to a destination outside its local network.
   උපාංගයකට එහි ස්ථානීය ජාලයෙන් පිටත පිහිටි ගමනාන්තයක් වෙත දත්ත යැවීමට අවශ්‍ය වේ
2. The device forwards the data to its default gateway.
   එම උපාංගය විසින් අදාළ දත්ත තමන්ගේ පෙරනිමි ද්වාරය වෙත යොමු කරයි.
3. The gateway examines the destination address.
   ද්වාරය මඟින් එම දත්ත ලැබිය යුතු ගමනාන්ත ලිපිනය පරීක්ෂා කරයි.
4. If necessary, it translates protocols or data formats.
   අවශ්‍යතාවය අනුව, එය ජාල නියමාවලි හෝ දත්ත ආකෘති එකිනෙකට පරිවර්තනය කරයි.
5. The gateway forwards the data to the appropriate external network.
   ඉන්පසු ද්වාරය මඟින් එම දත්ත අදාළ බාහිර ජාලය වෙත ඉදිරියට යොමු කරයි.
6. The destination network receives and processes the request.
   ගමනාන්ත ජාලය වෙත මෙම දත්ත ලැබෙන අතර එය අදාළ ඉල්ලීම ක්‍රියාවට නංවයි.
7. The response returns through the gateway to the original device.
   ලැබෙන ප්‍රතිචාරය නැවතත් ද්වාරය හරහා මුල් උපාංගය වෙතම ගලා එයි.

Default Gateway
පෙරනිමි දොරටු මඟ

A default gateway is the network device (usually a router or gateway) that forwards data from a local network (LAN) to other networks, such as the Internet, when the destination is outside the local network.
පෙරනිමි දොරටු මඟක් යනු දත්ත ලැබිය යුතු ගමනාන්තය, ස්ථානීය ජාලයෙන් පිටත පිහිටා ඇති විට, එම දත්ත ස්ථානීය ජාලයේ සිට අන්තර්ජාලය වැනි වෙනත් බාහිර ජාල වෙත ඉදිරියට යොමු කරන ජාලකරණ උපාංගයකි (සාමාන්‍යයෙන් රවුටරයක් හෝ ද්වාරයක්).

Characteristics of a Gateway
දොරටු මඟක ලක්ෂණ

Links networks that use different technologies, architectures, or protocols.
විවිධ තාක්ෂණයන්, ව්‍යුහයන් හෝ නියමාවලි භාවිතා කරන ජාලයන් එකිනෙකට සම්බන්ධ කරයි.

Can translate data between different communication protocols when required.
අවශ්‍ය අවස්ථාවලදී විවිධ සන්නිවේදන ප්‍රොටෝකෝල අතර දත්ත පරිවර්තනය කළ හැකිය.

May function at several OSI layers, including the Application Layer.
යෙදුම් ස්ථරය ඇතුළුව OSI ස්ථර කිහිපයකම ක්‍රියාත්මක විය හැකිය.

Serves as the point through which traffic enters or leaves a network.
ජාලයකට දත්ත ගමනාගමනය ඇතුළු වන හෝ ඉන් පිටවන ප්‍රධාන ස්ථානය ලෙස සේවය කරයි.

Can connect LANs, WANs, the Internet, and other types of networks.
LAN, WAN, අන්තර්ජාලය සහ වෙනත් ඕනෑම වර්ගයක ජාලයන් එකිනෙකට සම්බන්ධ කළ හැකිය.

Analyzes traffic and determines the appropriate way to forward or translate data.
දත්ත ගමනාගමනය විශ්ලේෂණය කර, දත්ත ඉදිරියට යොමු කිරීමට හෝ පරිවර්තනය කිරීමට සුදුසුම ක්‍රමය තීරණය කරයි.

ictfromabc.com

Types of Gateways
දොරටු මං වර්ග

Network Gateway
ජාල දොරටු මඟ
Connects different networks (most common).
විවිධ ජාලයන් එකිනෙකට සම්බන්ධ කරයි (වඩාත්ම පොදු වර්ගයයි). (IPv4 → IPv6)

Internet Gateway
අන්තර්ජාල දොරටු මඟ
Connects a LAN to the Internet.
ස්ථානීය ජාලයක් අන්තර්ජාලය සමඟ සම්බන්ධ කරයි. (ISP/ Wi-Fi Router)

VoIP Gateway
VoIP දොරටු මඟ
Converts voice calls between telephone and IP networks.
දුරකථන ජාල සහ IP ජාල අතර හඬ ඇමතුම් එකිනෙකට පරිවර්තනය කරයි

Cloud Gateway
වලාකුළු දොරටු මඟ
Connects on-premises systems with cloud services.
ආයතනය තුළ ඇති පද්ධති වලාකුළු සේවාවන් සමඟ සම්බන්ධ කරයි.

IoT Gateway
IoT දොරටු මඟ
Connects IoT devices to networks or cloud platforms.
IoT උපාංග, ජාලයන් හෝ cloud platforms සමඟ සම්බන්ධ කරයි. (Zig bee)

Email Gateway
විද්‍යුත් තැපැල් දොරටු මඟ
Filters and routes email traffic.
විද්‍යුත් තැපැල් ගමනාගමනය පෙරීම සහ ගමන් මග තීරණය කිරීම සිදු කරයි

Difference Between Gateway and Router
දොරටු මඟ සහ රවුටරය අතර වෙනස.

- Although a router and a gateway are different devices, a router often acts as a gateway in home and office networks.
  රවුටරයක් සහ දොරටු මඟක් යනු එකිනෙකට වෙනස් උපාංග දෙකක් වුවද, නිවාස සහ කාර්යාලීය ජාලයන්හි රවුටරයක් බොහෝ විට දොරටු මඟක් ලෙස ක්‍රියා කරයි.

- All routers are gateways, but they can also route between internal networks
  සියලුම රවුටර දොරටු මං වන නමුත්, ඒවාට අභ්‍යන්තර ජාල අතර දත්ත මාර්ගගත කිරීම ද සිදු කළ හැකිය.

- All gateways are not routers. It's a device or software that when protocol translation or format conversion is involved
  සියලුම දොරටු මං රවුටර නොවේ. එය ප්‍රොටෝකෝල පරිවර්තනය හෝ දත්ත ආකෘති පරිවර්තනය ඇතුළත් වන අවස්ථාවලදී භාවිත වන උපාංගයක් හෝ මෘදුකාංගයකි

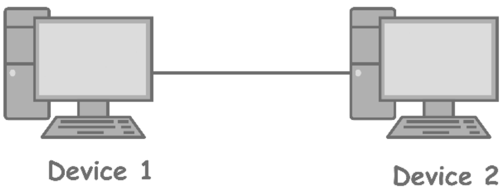
Gateway	Router
Connects different networks and may translate protocols. විවිධ ජාලයන් එකිනෙකට සම්බන්ධ කරන අතර නියමාවලි පරිවර්තනය කළ හැකිය.	Connects networks that usually use the same protocol (IP). එකම නියමාවලියක් භාවිතා කරන ජාලයන් එකිනෙකට සම්බන්ධ කරයි.
May include routing, NAT, firewall, VPN, and proxy functions. Routing, NAT, firewall, VPN සහ proxy කාර්යයන් ඇතුළත් විය හැකිය.	Primarily forwards packets between networks. මූලික වශයෙන් ජාලයන් අතර දත්ත පැකට්ටු ඉදිරියට යොමු කිරීම සිදු කරයි.
Can operate at multiple OSI layers. OSI ස්ථර කිහිපයකම ක්‍රියාත්මක විය හැකිය.	Primarily operates at the Network Layer (Layer 3). මූලික වශයෙන් ජාල ස්ථරයේ ක්‍රියාත්මක වේ.

Network Topologies
ජාල ස්ථල විද්‍යාව

Network topology refers to the arrangement of different elements like nodes, links, and devices in a computer network.
ජාල ස්ථල විද්‍යාව යනු පරිගණක ජාලයක ඇති nodes, links සහ උපාංග වැනි විවිධ මූලාංග සැකසීමයි.

It defines how these components are connected and interact with each other.
මෙම සංරචක එකිනෙක සම්බන්ධ වී අන්තර්ක්‍රියා කරන ආකාරය එයින් නිර්වචනය කරයි.

1.Point to Point Topology / සරල ස්ථලකය (Simple Topology)



The simplest type of network topology in which two devices are directly connected to each other through a dedicated communication link. Each device's network interface connects directly to the other device, with no intermediate networking devices.
උපාංග දෙකක්, සඳහා සන්නිවේදන සබැඳියක් හරහා එකිනෙකට සෘජුවම සම්බන්ධ වන සරලම ජාල ස්ථලක වර්ගය මෙයයි. මෙහිදී කිසිදු අතරමැදි ජාලකරණ උපාංගයකින් තොරව, එක් එක් උපාංගයේ ජාල අතුරුමුහුණත අනෙක් උපාංගය වෙත සෘජුවම සම්බන්ධ වේ.

The connection can be established using either wired media (such as Ethernet, fiber-optic, or serial cables) or wireless technologies (such as Bluetooth, Wi-Fi Direct, or microwave links).
මෙම සම්බන්ධතාවය රැහැන් සහිත මාධ්‍ය (Ethernet, ෆයිබර් ඔප්ටික් හෝ සීරියල් කේබල් වැනි) හෝ රැහැන් රහිත තාක්ෂණයන් (Bluetooth, Wi-Fi Direct) හෝ මයික්‍රෝවේව් සබැඳි වැනි) භාවිතයෙන් ස්ථාපනය කළ හැක.

To Establish a Simple Topology
සරල ස්ථලකයක් ස්ථාපනය කිරීමට

- 2 Devices / උපාංග 2ක්
- 2 NICs (one for each device) /ජාල අතුරුමුහුණත් කාඩ්පත් 2ක් (සෑම උපාංගයකටම එක බැගින්)
- 1 Dedicated Communication Link (wired or wireless)

  1 සන්නිවේදන සබැඳියක් (රැහැන් සහිත හෝ රැහැන් රහිත)

Examples / උදාහරණ:

- A computer directly connected to a network printer.

  ජාල මුද්‍රණ යන්ත්‍රයකට සෘජුවම සම්බන්ධ කර ඇති පරිගණකයක්.
- Two computers connected using an Ethernet cable.

  ඊතර්නෙට් කේබලයක් භාවිතයෙන් සම්බන්ධ කර ඇති පරිගණක දෙකක්.
- A Bluetooth connection between a laptop and a smartphone.

  ලැප්ටොප් පරිගණකයක් සහ ස්මාර්ට් ජංගම දුරකථනයක් අතර ඇති බ්ලූටූත් සම්බන්ධතාවයක්.

Advantages of Point-to-Point Topology
සරල ස්ථල විද්‍යාවෙහි වාසි

Has a simple structure because only two devices are connected.
මෙහි ඇත්තේ උපාංග දෙකක් පමණක් බැවින්, මෙහි සැලසුම තේරුම් ගැනීමට ඉතා පහසුය.

Requires only one direct communication link, making installation easy.
උපාංග දෙක අතර අවශ්‍ය වන්නේ එක් සෘජු සම්බන්ධතාවයක් පමණි.

Uses minimal hardware and cabling, resulting in a low setup cost.
අවම දෘඩාංග සහ කේබල් ප්‍රමාණයක් අවශ්‍ය වන බැවින් මෙය වියදම් අඩුය.

Provides fast communication since data travels directly between devices.
සබැඳිය තුළ උපාංග දෙකක් පමණක් ඇති බැවින් දත්ත හුවමාරුව වේගවත් වේ.

Offers better security because the dedicated link is not shared with other devices.
වෙනත් කිසිදු උපාංගයක් මෙම සබැඳිය හවුලේ භාවිත නොකරන බැවින්, දත්ත පිටතට නිරාවරණය වීමේ ඉඩකඩ අඩුය.

Eliminates data collisions as only two devices use the communication channel.
සන්නිවේදනය කරන්නේ උපාංග දෙකක් පමණක් බැවින්, දත්ත එකිනෙක ගැටීමේ අවස්ථාවක් නොමැත.

Makes fault detection easier due to the presence of a single communication path.
පවතින්නේ එක් සම්බන්ධතාවයක් පමණක් බැවින්, ගැටලු ඉතා ඉක්මනින් හඳුනාගත හැක.

Ensures reliable communication through a dedicated connection between devices.
තමාටම වෙන් වූ සබැඳියක් මඟින් ස්ථාවර සහ ඒකාකාරී සන්නිවේදනයක් සහතික කරයි.

Disadvantages of Point-to-Point Topology
සරල ස්ථල විද්‍යාවෙහි අවාසි

Supports communication between only two devices, limiting network size.
උපාංග දෙකක් අතර පමණක් සන්නිවේදනයට සහාය දක්වන බැවින් ජාලයේ ප්‍රමාණය සීමා වේ.

Cannot be scaled as additional devices require separate connections.
අතිරේක උපාංග සඳහා වෙනම සම්බන්ධතා අවශ්‍ය වන බැවින් පරිමාණය කල නොහැක

Is not suitable for large networks due to its limited connectivity.
පවතින සීමිත සම්බන්ධතාවය හේතුවෙන් විශාල ජාල සඳහා සුදුසු නොවේ.

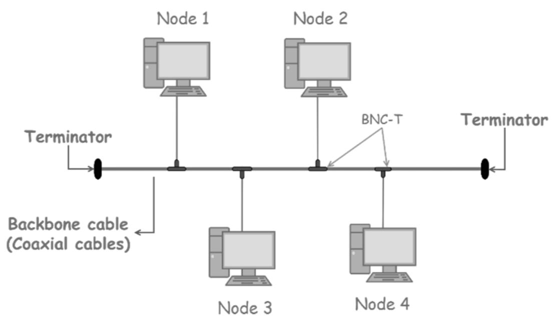
Restricts resource sharing to only the two connected devices.
සම්පත් බෙදාගැනීම සම්බන්ධිත උපාංග දෙකට පමණක් සීමා කරයි.

Stops communication completely if the communication link fails.
සන්නිවේදන සබැඳිය බිඳ වැටුණහොත් සන්නිවේදනය සම්පූර්ණයෙන්ම නතර වේ.

---

2. Bus Topology
බස් ස්ථලකය

Bus Topology is a network type in which every computer and network device is connected to a single cable.
බස් ස්ථල විද්‍යාව යනු සෑම පරිගණකයක්ම සහ ජාල උපාංගයක්ම තනි කේබලයකට සම්බන්ධ කර ඇති ජාල වර්ගයකි.



Bus topologies commonly use coaxial cables.
බස් ස්ථලකයක සාමාන්‍යයෙන් සමාංෂක රැහැන් භාවිතා කරයි.

Since all devices use the same communication channel, they belong to a single collision domain.
සියලුම උපාංග එකම සන්නිවේදන නාලිකාව භාවිත කරන බැවින්, ඒවා තනි ගැටුම් වසමකට අයත් වේ.

As a result, if two devices transmit data simultaneously, a collision may occur, affecting network performance.
එහි ප්‍රතිඵලයක් ලෙස, උපාංග දෙකක් එකවර දත්ත සම්ප්‍රේෂණය කළහොත්, දත්ත එකිනෙක ගැටීමක් සිදු විය හැකි අතර, එය ජාලයේ ක්‍රියාකාරීත්වයට බලපායි.

Terminators are installed at both ends of the backbone cable to absorb signals and prevent signal reflection, which could disrupt network communication.
ජාල සන්නිවේදනයට බාධා ඇති කළ හැකි සංඥා පරාවර්තනය වැළැක්වීම සහ සංඥා අවශෝෂණය කර ගැනීම සඳහා ප්‍රධාන කේබලයේ දෙකෙළවරටම අග්‍රස්ථ (terminators) සවි කර ඇත.

To Establish a Bus Topology
බස් ස්ථලකයක් ස්ථාපනය කිරීමට

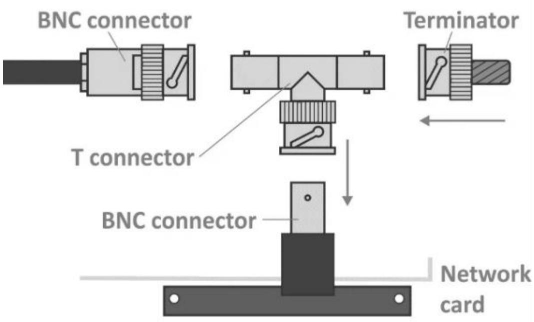
- n Devices / උපාංග n ප්‍රමාණයක්
- n NICs (one for each device) / ජාල අතුරුමුහුණත් පත් n ප්‍රමාණයක් (සෑම උපාංගයකටම එක බැගින්)
- 1 Backbone Cable / 1 ප්‍රධාන කේබලයක්
- n, T-Connectors (T-Junctions)
  T-සන්ධි n ප්‍රමාණයක්
- n Drop Lines / රැහැන් n ප්‍රමාණයක්
- 2 Terminators (one at each end of the backbone cable) / අග්‍රස්ථ 2ක් (ප්‍රධාන කේබලයේ දෙකෙළවරටම එක බැගින්)

Minimum Number of Computer/ අවම පරිගණක සංඛ්‍යාව: 3 or more / 3 හෝ වැඩිපුර
Maximum Number of Computers/ උපරිම පරිගණක සංඛ්‍යාව: Depends on the network standard and cable type. / ජාල ප්‍රමිතිය සහ කේබල් වර්ගය මත රඳා පවතී.

CSMA/CD
To reduce the impact of collisions, networks use Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
දත්ත ගැටීම්වල බලපෑම අවම කිරීම සඳහා, ජාල මඟින් Carrier Sense Multiple Access with Collision Detection (CSMA/CD) යාන්ත්‍රණය භාවිත කරනු ලබයි.

Examples උදාහරණ
- A small office network / කුඩා කාර්යාල ජාලයක්.

Connecting Devices Using a BNC T-Connector
BNC T-සම්බන්ධකයක් භාවිතයෙන් උපාංග සම්බන්ධ කිරීම



The main coaxial cable acts as the backbone and connects all devices in the network.
ප්‍රධාන සමාංශක කේබලය ප්‍රධාන ජාල රැහැන (backbone) ලෙස ක්‍රියා කරන අතර ජාලයේ ඇති සියලුම උපාංග එකිනෙකට සම්බන්ධ කරයි.

A BNC T-connector is inserted into the backbone cable at each device connection point.
සෑම උපාංග සම්බන්ධක ලක්ෂ්‍යයකදීම ප්‍රධාන කේබලයට BNC T-සම්බන්ධකයක් ඇතුළු කරනු ලැබේ.

The two horizontal ports of the T-connector connect to the backbone cable, allowing data to travel along the bus.
T-සම්බන්ධකයේ ඇති තිරස් කෙවෙනි දෙක ප්‍රධාන කේබලයට සම්බන්ධ වන අතර, එමඟින් දත්ත ජාලය දිගේ ගමන් කිරීමට ඉඩ සලසයි.

The vertical port connects to the device's Network Interface Card (NIC), enabling the device to send and receive data.
එහි සිරස් කෙවෙනි උපාංගයේ ජාල අතුරුමුහුණත් පතට සම්බන්ධ වන අතර, එමඟින් උපාංගයට දත්ත යැවීමට සහ ලබා ගැනීමට හැකියාව ලැබෙයි.

Advantages of Bus Topology
බස් ස්ථල විද්‍යාවෙහි වාසි

Has a low installation cost because it requires fewer networking components and less cabling.
අවම ජාලකරණ සංරචක සහ අඩු කේබල් ප්‍රමාණයක් අවශ්‍ය වන බැවින් ස්ථාපන පිරිවැය අඩුය.

Has a simple structure, making it easy to understand, install, and configure.
සරල ව්‍යුහයක් පවතින බැවින් තේරුම් ගැනීමට, ස්ථාපනය කිරීමට සහ වින්‍යාස කිරීමට පහසුය.

Does not require a central networking device such as a hub or switch for communication.
සන්නිවේදනය සඳහා හබ් හෝ ස්විච් වැනි මධ්‍යම ජාලකරණ උපාංගයක් අවශ්‍ය නොවේ.

Is suitable for temporary networks because it can be set up and removed quickly.
ඉතා ඉක්මනින් සැකසීමට සහ ඉවත් කිරීමට හැකි බැවින් තාවකාලික ජාල සඳහා සුදුසු වේ.

Allows new devices to be connected easily by attaching them directly to the backbone cable.
උපාංග සෘජුවම ප්‍රධාන කේබලයට සම්බන්ධ කිරීම මඟින් නව උපාංග පහසුවෙන් එක් කිරීමට ඉඩ සලසයි.

Other devices can continue communicating if one device fails.
එක් උපාංගයක් අක්‍රිය වුවද, අනෙක් උපාංගවලට දිගටම සන්නිවේදනය කළ හැක.

Disadvantages of Bus Topology
බස් ස්ථල විද්‍යාවෙහි අවාසි

If the main cable is damaged, communication stops for all devices.
ප්‍රධාන කේබලයට හානි වුවහොත්, සියලුම උපාංගවල සන්නිවේදනය නතර වේ

Experiences reduced performance as network traffic increases because all devices share the same communication channel.
සියලුම උපාංග එකම සන්නිවේදන නාලිකාව හවුලේ භාවිත කරන බැවින්, ජාල තදබදය වැඩි වන විට ක්‍රියාකාරිත්වය අඩු වේ.

Makes fault isolation difficult because identifying the source of a problem can be challenging.
ගැටලුවක් ඇති වූ මූලාශ්‍රය හඳුනාගැනීම අභියෝගාත්මක විය හැකි බැවින්, දෝෂ වෙන්කර හඳුනාගැනීම අපහසු කරයි.

Has a limited cable length, restricting the maximum distance over which devices can communicate.
සීමිත කේබල් දිගක් පවතින බැවින්, උපාංගවලට සන්නිවේදනය කළ හැකි උපරිම දුර සීමා වේ.

Supports only a limited number of devices before network performance begins to degrade.
ජාලයේ ක්‍රියාකාරිත්වය බිඳ වැටීමට පෙර සහාය දක්වනු ලබන්නේ සීමිත උපාංග සංඛ්‍යාවකට පමණි.

Provides lower security because data transmitted on the shared cable can potentially be accessed by other devices.
පොදු කේබලය හරහා සම්ප්‍රේෂණය වන දත්තවලට වෙනත් උපාංග මඟින් ප්‍රවේශ වීමේ හැකියාව පවතින බැවින් අඩු ආරක්ෂාවක් සපයයි.

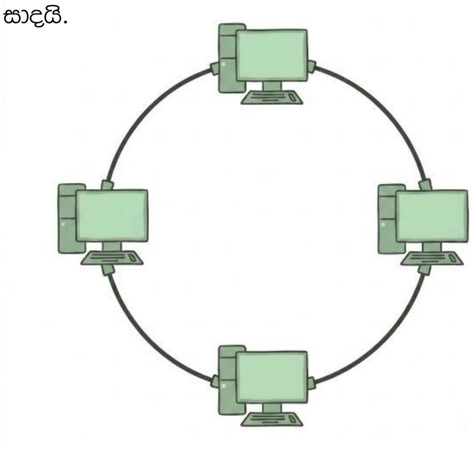
Makes troubleshooting more difficult as the network grows larger and more complex.
ජාලය විශාල සහ සංකීර්ණ වන විට දෝෂ නිරාකරණය වඩාත් අපහසු කරයි.

Is not suitable for large networks because performance and reliability decrease as the number of devices increases.
උපාංග සංඛ්‍යාව වැඩි වන විට ක්‍රියාකාරීත්වය සහ විශ්වසනීයත්වය අඩු වන බැවින් විශාල ජාල සඳහා සුදුසු නොවේ.

---

3. Ring Topology
වටමය ස්ථලකය

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices.
වටමය ස්ථල විද්‍යාව තුළ, එය හරියටම අසල්වැසි උපාංග දෙකක් සමඟ උපාංග සම්බන්ධක වළල්ලක් සාදයි.

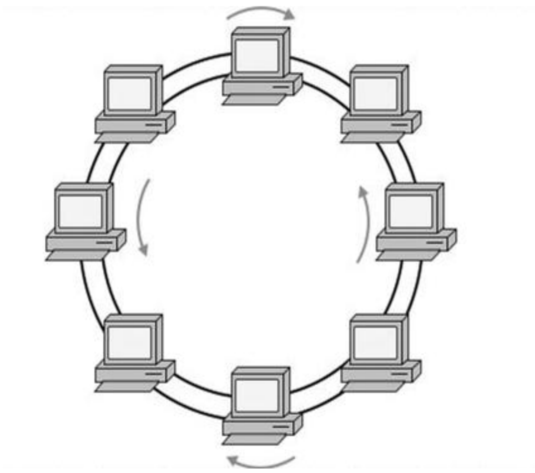


Each device acts as a repeater by receiving data from one device and forwarding it to the next device in the ring.
එක් උපාංගයකින් දත්ත ලබාගෙන එය වළල්ලේ ඇති ඊළඟ උපාංගය වෙත යොමු කිරීම මඟින් සෑම උපාංගයක්ම පුනරාවර්තකයක් (repeater) ලෙස ක්‍රියා කරයි.

All devices in the ring belong to a single collision domain.
වළල්ලේ ඇති සියලුම උපාංග තනි ගැටුම් වසමකට අයත් වේ.

The data flows in one direction, it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.
දත්ත එක් දිශාවකට ගලා යයි, එය ඒක දිශානුගත වේ, නමුත් එක් එක් ජාල Nodes අතර සම්බන්ධතා 2ක් තිබීමෙන් එය ද්විපාර්ශ්වික බවට පත් කළ හැකිය, එය ද්විමය වටමය ස්ථලක ලෙස හැඳින්වේ.

Double Ring Topology



To Establish a Ring Topology
වළලු ස්ථලකයක් ස්ථාපනය කිරීමට

- n Devices / උපාංග n ප්‍රමාණයක්
- n NICs (with each having two ports) / ජාල අතුරුමුහුණත් පත් n ප්‍රමාණයක් (සෑම උපාංගයකම කෙවෙනි දෙක බැගින් පවතින)
- n Communication Links connecting each device to its neighboring devices

එක් එක් උපාංගය එහි අසල ඇති උපාංග වෙත සම්බන්ධ කරන සන්නිවේදන සබැඳි n ප්‍රමාණයක්

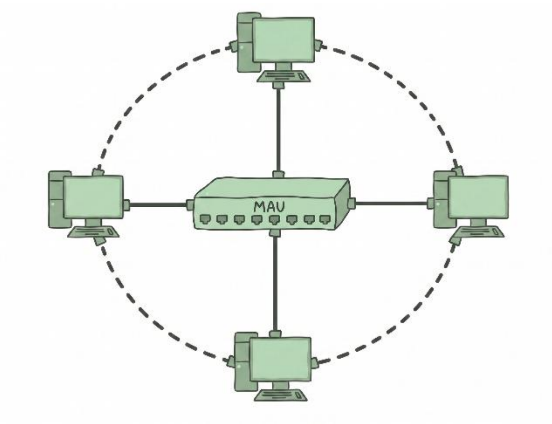
To Establish a Dual Ring Topology
ද්විත්ව වළලු ස්ථලකයක් ස්ථාපනය කිරීමට

A secondary ring is added alongside the primary ring, and each device is connected to two neighboring devices through both rings. The secondary ring provides an alternative communication path if the primary ring fails.
ප්‍රාථමික වළල්ලට අමතරව ද්විතීයික වළල්ලක් එක් කරනු ලබන අතර, සෑම උපාංගයක්ම වළලු දෙකම හරහා අසල ඇති උපාංග දෙකකට සම්බන්ධ වේ. ප්‍රාථමික වළල්ල බිඳ වැටුණහොත්, ද්විතීයික වළල්ල මඟින් විකල්ප සන්නිවේදන මාර්ගයක් සපයයි

ictfromabc.com

Legacy implementation of ring topology
වළලු ස්ථලකයේ පරණ ක්‍රියාත්මක කිරීම්

A Multistation Access Unit (MAU) with n ports is used to connect n devices through n cables. Although the devices are physically connected in a star topology, the MAU internally forms a logical ring and enables token passing communication between the devices.
කෙවෙනි n ප්‍රමාණයක් සහිත බහු-ප්‍රතිස්ථාපන ප්‍රවේශ ඒකකයක් , කේබල් n ප්‍රමාණයක් හරහා උපාංග n ප්‍රමාණයක් සම්බන්ධ කිරීමට භාවිත කරයි. මෙම උපාංග භෞතිකව තරු ස්ථලකයකට සම්බන්ධ වී තිබුණද, MAU උපාංගය අභ්‍යන්තරව තාර්කික වළල්ලක් සාදන අතර උපාංග අතර ටෝකන හුවමාරු සන්නිවේදනය සිදු කිරීමට ඉඩ සලසයි.



Examples / උදාහරණ
- IBM Token Ring networks
- Metropolitan Area Networks (MANs)
- Fiber Distributed Data Interface (FDDI) networks

Operations of Ring Topology
වටමය ස්ථලකයෙහි මෙහෙයුම්

A special packet called a token continuously circulates around the ring.
ටෝකනය (token) නමින් හැඳින්වෙන විශේෂ පැකට්ටුවක් වළල්ල වටා අඛණ්ඩව සංසරණය වේ.

A device must possess the token before it can transmit data.
උපාංගයකට දත්ත සම්ප්‍රේෂණය කිරීමට පෙර එම උපාංගය සතුව ටෝකනය තිබිය යුතුය.

Once the token is obtained, the device transmits its data to the intended destination.
ටෝකනය ලබා ගත් පසු, උපාංගය විසින් එහි දත්ත අදාළ ගමනාන්තය වෙත සම්ප්‍රේෂණය කරයි.

Only one device can hold the token at a time, preventing data collisions.
දත්ත එකිනෙක ගැටීම වැළැක්වීම සඳහා, එක් වරකට ටෝකනය රඳවා තබා ගත හැක්කේ එක් උපාංගයකට පමණි.

When no device has data to send, the token continues circulating around the ring.
කිසිදු උපාංගයකට යැවීමට දත්ත නොමැති විට, ටෝකනය දිගටම වළල්ල වටා සංසරණය වේ.

Token Release Techniques
ටෝකන මුදා හැරීමේ ශිල්පීය ක්‍රම

Early Token Release (ETR) – The token is released immediately after data transmission begins, improving network efficiency.
පූර්ව ටෝකන මුදා හැරීම – දත්ත සම්ප්‍රේෂණය ආරම්භ වූ වහාම ටෝකනය මුදා හරිනු ලබන අතර, එමඟින් ජාලයේ කාර්යක්ෂමතාවය වැඩි දියුණු වේ.

Delayed Token Release (DTR) – The token is released only after the transmitted data returns to the sender or acknowledgment is received.
ප්‍රමාදිත ටෝකන මුදා හැරීම – ටෝකනය මුදා හරිනු ලබන්නේ සම්ප්‍රේෂණය කරන ලද දත්ත නැවත එවන්නා වෙත පැමිණීමෙන් හෝ ලැබුණු බවට ස්ථිර කිරීමක් ලැබීමෙන් පසුව පමණි.

Advantages of Ring Topology
වටමය ස්ථලකයෙහි වාසි

Provides equal access to the network because every device receives the token in turn.
සෑම උපාංගයකටම අනුපිළිවෙලින් ටෝකනය ලැබෙන බැවින්, ජාලය වෙත සමාන ප්‍රවේශයක් ලබා දෙයි.

Delivers predictable network performance due to controlled data transmission.
පාලනය කරන ලද දත්ත සම්ප්‍රේෂණය හේතුවෙන්, කලින් පුරෝකථනය කළ හැකි ජාල ක්‍රියාකාරීත්වයක් ලබා දෙයි.

Maintains good performance even under heavy network traffic.
අධික ජාල තදබදයක් පවතින විට පවා හොඳ ක්‍රියාකාරීත්වයක් පවත්වා ගනී.

Does not require a central networking device for communication.
සන්නිවේදනය සඳහා මධ්‍යම ජාලකරණ උපාංගයක් අවශ්‍ය නොවේ.

Makes fault location easier than in a bus topology because data follows a defined path.
දත්ත නිශ්චිත මාර්ගයක් ඔස්සේ ගමන් කරන බැවින්, බස් ස්ථලකයකට වඩා පහසුවෙන් දෝෂ පවතින ස්ථාන හඳුනාගත හැක.

Utilizes network bandwidth efficiently by allowing only one device to transmit at a time.
එක් වරකට දත්ත සම්ප්‍රේෂණය කිරීමට ඉඩ ලබා දෙන්නේ එක් උපාංගයකට පමණක් බැවින්, ජාල කලාප පළල කාර්යක්ෂමව භාවිත කරයි.

Supports longer communication distances as each device regenerates and forwards signals.
සෑම උපාංගයක්ම සංඥා නැවත උත්පාදනය කර ඉදිරියට යොමු කරන බැවින්, දිගු සන්නිවේදන දුරක් සඳහා සහාය දක්වයි.

Disadvantages of Ring Topology
වටමය ස්ථලකයෙහි අවාසි

Can experience network disruption if a device fails or a communication link breaks.
තනි වළලු වින්‍යාසයකදී එක් උපාංගයක් අක්‍රිය වුවහොත් හෝ සන්නිවේදන සබැඳියක් බිඳ වැටුණහොත් ජාලයේ බිඳ වැටීමක් සිදු විය හැක.

May require temporary network interruption when adding or removing devices.
උපාංග එකතු කිරීමේදී හෝ ඉවත් කිරීමේදී තාවකාලිකව ජාලයේ ක්‍රියාකාරීත්වය නතර කිරීමට සිදු විය හැක.

Is more complex to install and configure than a bus topology.
බස් ස්ථලකයකට වඩා ස්ථාපනය සහ වින්‍යාස කිරීම සංකීර්ණ වේ.

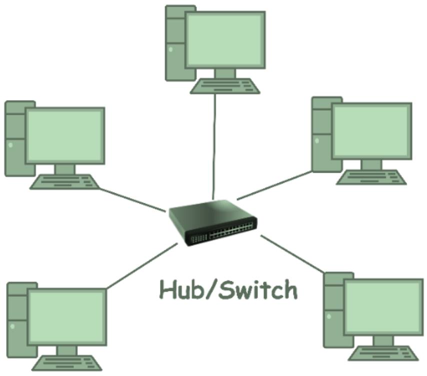
Can make troubleshooting difficult in large ring networks.
විශාල වළලු ජාලවල දෝෂ නිරාකරණය අපහසු විය හැක.

Involves higher installation costs than a bus topology.
බස් ස්ථලකයකට වඩා වැඩි ස්ථාපන පිරිවැයක් දැරීමට සිදු වේ.

May experience increased transmission delays as the number of devices grows.
උපාංග සංඛ්‍යාව වැඩි වන විට දත්ත සම්ප්‍රේෂණ ප්‍රමාදයන් වැඩි විය හැක.

4. Star Topology
තරු ස්ථලක

In Star Topology, all devices are connected to a central networking device such as a hub or switch.
තරු ස්ථල විද්‍යාවෙහි සියලුම උපාංග හබ් හෝ ස්විච් වැනි මධ්‍යම ජාලකරණ උපාංගයකට සම්බන්ධ කර ඇත.



Typically implemented using RJ-45 connectors and twisted-pair cables connected to a hub or switch.
සාමාන්‍යයෙන් මෙය ක්‍රියාත්මක කරනු ලබන්නේ හබ් හෝ ස්විච් එකකට සම්බන්ධ කරන ලද RJ-45 සම්බන්ධක සහ ඇඹරුණු යුගල කේබල් භාවිතයෙනි.

Although coaxial cables can be used, RJ-45 based Ethernet cabling is the most common implementation.
මේ සඳහා සමාක්ෂ කේබල් භාවිත කළ හැකි වුවද, වඩාත්ම පොදු ක්‍රියාත්මක කිරීම වන්නේ RJ-45 මත පදනම් වූ ඊතර්නෙට් කේබල් භාවිතයයි.

To Establish a Star Topology
තරු ස්ථලකයක් ස්ථාපනය කිරීමට

- n Devices / උපාංග n ප්‍රමාණයක්
- n NICs (one for each device) / ජාල අතුරුමුහුණත් පත් n ප්‍රමාණයක් (සෑම උපාංගයකටම එක බැගින්)
- 1 Hub or Switch with at least n Ports අවම වශයෙන් කෙවෙනි n ප්‍රමාණයක් සහිත 1 හබ් හෝ ස්විච් උපාංගයක්
- n Communication Cables

සන්නිවේදන කේබල් n ප්‍රමාණයක්

Examples / උදාහරණ
- Home networks connected through a Wi-Fi router./ Wi-Fi රවුටරයක් හරහා සම්බන්ධ කර ඇති නිවෙස්වල පවතින ජාල
- Office networks using Ethernet switches. ඊතර්නෙට් ස්විච් භාවිත කරන කාර්යාලීය ජාල

Advantages of Star Topology
තරු ස්ථල විද්‍යාවෙහි වාසි

Simplifies installation and network management through a central networking device.
මධ්‍යම ජාලකරණ උපාංගයක් භාවිත කිරීම නිසා ස්ථාපනය සහ ජාල කළමනාකරණය සරල කරයි.

Allows new devices to be added without affecting existing network connections.
පවතින ජාල සම්බන්ධතාවලට බාධා නොකර නව උපාංග එකතු කිරීමට ඉඩ සලසයි.

Makes fault detection and troubleshooting easier because each device has a dedicated connection.
සෑම උපාංගයකටම වෙන්වූ සම්බන්ධතාවයක් පවතින බැවින්, දෝෂ හඳුනාගැනීම සහ දෝෂ නිරාකරණය පහසු කරයි.

Prevents the failure of one device from affecting communication between other devices.
එක් උපාංගයක් අක්‍රිය වීමෙන් අනෙක් උපාංග අතර සිදුවන සන්නිවේදනයට බලපෑම් ඇතිවීම වළක්වයි.

Supports easy network expansion by connecting additional devices to the central device.
මධ්‍යම උපාංගයට අමතර උපාංග සම්බන්ධ කිරීම මඟින් පහසුවෙන් ජාලය ව්‍යාප්ත කිරීමට සහාය දක්වයි.

Supports a large number of devices when sufficient ports are available.
ප්‍රමාණවත් තරම් කෙවෙනි පවතින විට විශාල උපාංග සංඛ්‍යාවකට සහාය දක්වයි.

Disadvantages of Star Topology
තරු ස්ථල විද්‍යාවෙහි අවාසි

Requires a central networking device such as a hub or switch for operation.
ක්‍රියාකාරිත්වය සඳහා හබ් හෝ ස්විච් වැනි මධ්‍යම ජාලකරණ උපාංගයක් අවශ්‍ය වේ.

Causes the entire network to become unavailable if the central device fails.
මධ්‍යම උපාංගය අක්‍රිය වුවහොත් මුළු ජාලයම භාවිත කිරීමට නොහැකි තත්ත්වයට පත් වේ.

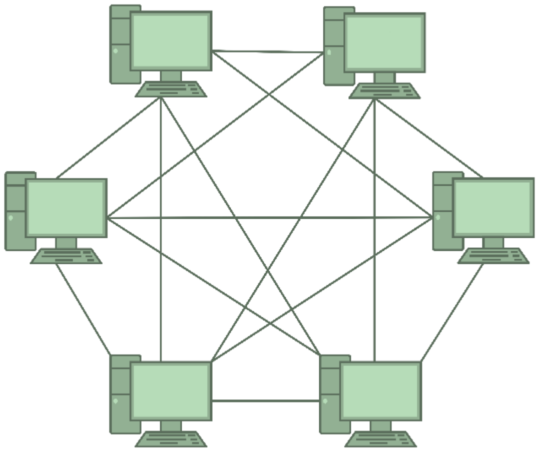
Results in higher installation costs than bus topology due to additional hardware and cabling.
අතිරේක දෘඩාංග සහ කේබල් භාවිතය නිසා බස් ස්ථලකයට වඩා වැඩි ස්ථාපන පිරිවැයක් ඇති වේ.

Depends heavily on the performance and reliability of the central device.
මධ්‍යම උපාංගයේ ක්‍රියාකාරිත්වය සහ විශ්වසනීයත්වය මත බෙහෙවින් රඳා පවතී.

Requires a continuous power supply for the central networking device.
මධ්‍යම ජාලකරණ උපාංගය සඳහා අඛණ්ඩ විදුලි සැපයුමක් අවශ්‍ය වේ

5. Mesh Topology
බැඳිමය/දැලිසමය ජාල ස්ථලකය

In a mesh topology, every device is connected to every other device via a particular channel.
දැලිසමය ජාල ස්ථලකය තුළ, සෑම උපාංගයක්ම විශේෂිත නාලිකාවක් හරහා අනෙකුත් සෑම උපාංගයකටම සම්බන්ධ වේ.



Fully connected Mesh

Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1.
උපක්‍රම N සංඛ්‍යාව දැලිසමය ජාල ස්ථලකය තුළ එකිනෙක සම්බන්ධ වී ඇතැයි සිතමු, එක් එක් උපාංගයට අවශ්‍ය වන මුළු කෙවෙනි ගණන N-1 වේ.

Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required (L) to connect them is,
උපක්‍රම N සංඛ්‍යාවක් දැලිසමය ජාල ස්ථලකය තුළ එකිනෙක සම්බන්ධ වී ඇතැයි සිතමු, එවිට ඒවා සම්බන්ධ කිරීමට අවශ්‍ය සබැඳි ගණන (L),

To Establish a Mesh Topology
දැලිසමය ස්ථලකයක් ස්ථාපනය කිරීමට

- n Devices / උපාංග n ප්‍රමාණයක්
- 1 NIC with (n − 1) Ports for each device
  සෑම උපාංගයක් සඳහාම කෙවෙනි n(n − 1) ප්‍රමාණයක් සහිත 1 ජාල අතුරුමුහුණත් පතක්
- n(n − 1)/2 Communication Links
  සන්නිවේදන සබැඳි n(n − 1)/2 ගණනක්

ictfromabc.com

Examples / උදාහරණ

- Internet / අන්තර්ජාලය
- Military communication networks / මිලිටරි/හමුදා සන්නිවේදන ජාල
- Data center networks / දත්ත මධ්‍යස්ථාන ජාල
- Wireless mesh networks / රැහැන් රහිත මෙෂ් ජාල

Advantages of Mesh Topology
දැලිසමය ජාල ස්ථලකයෙහි වාසි

Provides high reliability through multiple communication paths between devices.
උපාංග අතර බහුවිධ සන්නිවේදන මාර්ග පැවතීම හේතුවෙන් ඉහළ විශ්වසනීයත්වයක් ලබා දෙයි.

Maintains network operation even when one or more communication links fail.
සන්නිවේදන සබැඳි එකක් හෝ කිහිපයක් බිඳ වැටුණත් ජාලයේ ක්‍රියාකාරිත්වය අඛණ්ඩව පවත්වා ගනී.

Offers multiple paths for data transmission, improving communication flexibility.
දත්ත සම්ප්‍රේෂණය සඳහා මාර්ග කිහිපයක් ලබා දෙන බැවින්, සන්නිවේදන නම්‍යශීලීභාවය වැඩි දියුණු කරයි.

Eliminates single points of failure in a full mesh network.
පූර්ණ මෙෂ් ජාලයක තනි බිඳවැටීම් ලක්ෂ්‍ය සම්පූර්ණයෙන්ම නැති කර දමයි.

Provides high security because dedicated links are used between devices.
උපාංග අතර කැපවූ සබැඳි භාවිත වන බැවින් ඉහළ ආරක්ෂාවක් සපයයි.

Makes fault isolation easier due to direct device-to-device connections.
උපාංග අතර සෘජු සම්බන්ධතා පවතින බැවින්, දෝෂ වෙන්කර හඳුනාගැනීම පහසු කරයි.

Supports simultaneous data transmission across multiple links.
බහුවිධ සබැඳි හරහා එකවර දත්ත සම්ප්‍රේෂණය කිරීමට සහාය දක්වයි.

Is suitable for mission-critical applications that require continuous communication.
අඛණ්ඩ සන්නිවේදනයක් අවශ්‍ය වන ඉතා වැදගත් සහ තීරණාත්මක කාර්යයන් සඳහා සුදුසු වේ.

Disadvantages of Mesh Topology
දැලිසමය ජාල ස්ථලකයෙහි අවාසි

Involves high installation costs due to the large number of links required.
අවශ්‍ය වන සබැඳි විශාල සංඛ්‍යාව හේතුවෙන් ඉහළ ස්ථාපන පිරිවැයක් දැරීමට සිදු වේ.

Requires extensive cabling to establish direct connections between devices.
උපාංග අතර සෘජු සම්බන්ධතා ඇති කිරීම සඳහා පුළුල් ලෙස කේබල් එලීම (extensive cabling) අවශ්‍ය වේ.

Increases network management complexity as the number of devices grows.
උපාංග සංඛ්‍යාව වැඩි වන විට ජාල කළමනාකරණයේ සංකීර්ණත්වය වැඩි වේ.

Makes maintenance more difficult due to the large number of connections.
සම්බන්ධතා විශාල සංඛ්‍යාවක් පවතින බැවින් නඩත්තු කටයුතු වඩාත් අපහසු වේ.

Requires multiple network interfaces or ports on each device.
සෑම උපාංගයකම බහුවිධ ජාල අතුරුමුහුණත් හෝ කෙවෙනි තිබීම අවශ්‍ය වේ.

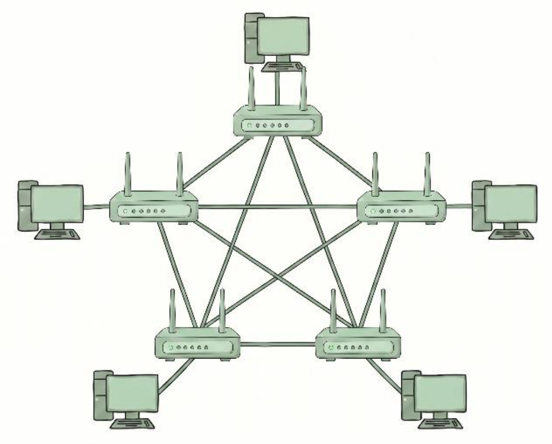
Requires more physical space for cabling and networking equipment.
කේබල් සහ ජාලකරණ උපකරණ සඳහා වැඩි භෞතික ඉඩක් අවශ්‍ය වේ.

Takes longer to deploy because every connection must be established and tested.
සෑම සම්බන්ධතාවයක්ම ස්ථාපනය කර පරීක්ෂා කළ යුතු බැවින්, ජාලය සක්‍රිය ලෙස යෙදවීමට වැඩි කාලයක් ගතවේ.

NOTE:
In a full mesh topology, every device is directly connected to every other device in the network.
පූර්ණ දැලිස ස්ථලකයක , ජාලයේ ඇති සෑම උපාංගයක්ම අනෙක් සියලුම උපාංග වෙත සෘජුවම සම්බන්ධ වී පවතී.

In a partial mesh topology, only selected devices have direct connections to multiple devices.
අර්ධ දැලිස ස්ථලකයක නම්, සෘජු සම්බන්ධතා පවතින්නේ තෝරාගත් උපාංග කිහිපයක් අතර පමණි.

Mesh Topology Using Routers
රවුටර භාවිතයෙන් දැලිසමය ස්ථලකය

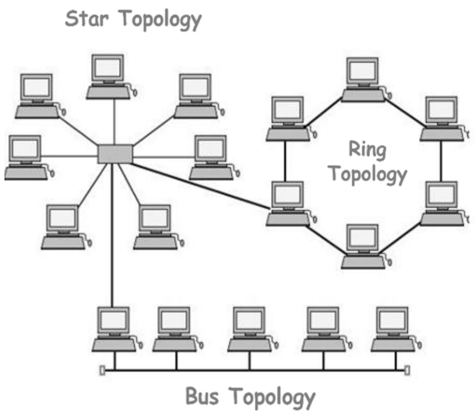


Each router is directly connected to one or more other routers through dedicated communication links.
සෑම රවුටරයක්ම වෙන්වූ සන්නිවේදන සබැඳි හරහා වෙනත් රවුටර එකක් හෝ කිහිපයක් වෙත සෘජුවම සම්බන්ධ වී පවතී.

Switches are generally not used in mesh topologies because they behave as a single interconnected network and cannot provide the path redundancy and automatic rerouting required in a mesh network.
ස්විච් මඟින් ක්‍රියා කරනු ලබන්නේ තනි අන්තර් සම්බන්ධිත ජාලයක් ලෙස බැවින් සහ දැලිසමය ජාලයකට අවශ්‍ය වන මාර්ග අතිරික්තතාවය මෙන්ම ස්වයංක්‍රීයව වෙනත් මාර්ග ඔස්සේ දත්ත යැවීමේ හැකියාව ලබා දීමට ඒවාට නොහැකි බැවින්, සාමාන්‍යයෙන් දැලිසමය ස්ථලක සඳහා ස්විච් භාවිත නොකෙරේ.

Routers can identify alternative paths and continue communication even when a link failure occurs.
රවුටර මඟින් විකල්ප මාර්ග හඳුනාගත හැකි බැවින්, සන්නිවේදන සබැඳියක් බිඳ වැටුණහොත් වුවද අඛණ්ඩව සන්නිවේදනය පවත්වා ගෙන යාමට ඒවාට හැකියාව පවතී.

6. Hybrid Topologies
දෙමුහුම් ස්ථලක



Hybrid Topology is a network topology that combines two or more different network topologies into a single network.
දෙමුහුන් ස්ථල විද්‍යාව යනු එකිනෙකට වෙනස් ජාල ස්ථල විද්‍යාවන් දෙකක් හෝ කිහිපයක් එකම ජාලයක් ලෙස ඒකාබද්ධ කරන ජාල ස්ථල විද්‍යාවකි.

It is designed to take advantage of the strengths of different topologies while reducing their limitations.
විවිධ ස්ථල විද්‍යාවන්හි ඇති සීමාවන්/අවාසි අවම කර ගනිමින්, ඒවායේ ඇති ශක්තීන් සහ වාසි ප්‍රයෝජනයට ගත හැකි වන පරිදි මෙය සැලසුම් කර ඇත.

Different sections of the network can use different topologies (such as Star, Bus, Ring, or Tree) based on their requirements.
ජාලයේ අවශ්‍යතා මත පදනම්ව එහි විවිධ කොටස් සඳහා විවිධ ස්ථල විද්‍යාවන් (තරු, බස්, රින්ග් හෝ වෘක්ෂ වැනි) භාවිත කළ හැකිය.

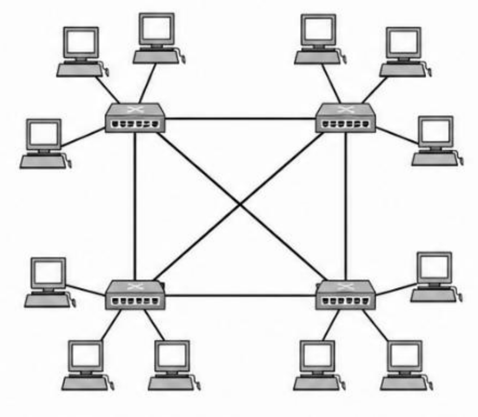
The connected topologies work together as one integrated network.
මෙලෙස සම්බන්ධ කරන ලද ස්ථල විද්‍යාවන් සියල්ල එකම ඒකාබද්ධ ජාලයක් ලෙස එකට එක්ව ක්‍රියා කරයි.

Hybrid topology provides high flexibility, scalability, and reliability, making it suitable for complex network environments.
දෙමුහුන් ස්ථල විද්‍යාව මඟින් ඉහළ නම්‍යශීලී බවක්, පද්ධතිය ප්‍රසාරණය කිරීමේ හැකියාවක් සහ විශ්වාසනීයත්වයක් ලබා දෙන බැවින්, එය සංකීර්ණ ජාල පරිසරයන් සඳහා බෙහෙවින් සුදුසු වේ.

It is commonly used in large organizations, universities, hospitals, data centers, and enterprise networks where different departments have different networking needs.
විවිධ දෙපාර්තමේන්තුවලට එකිනෙකට වෙනස් ජාලකරණ අවශ්‍යතා පවතින විශාල සංවිධාන, විශ්වවිද්‍යාල, රෝහල්, දත්ත මධ්‍යස්ථාන සහ ව්‍යවසාය ජාලයන්හි මෙය බහුලවම භාවිත වේ.

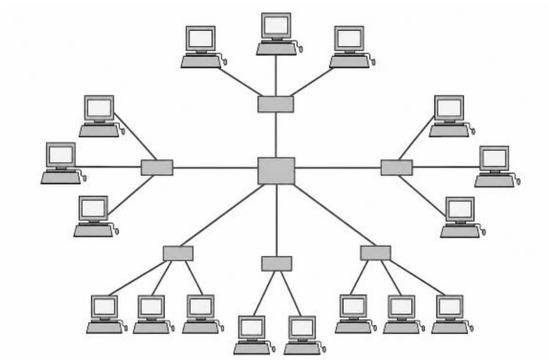
Types of Hybrid Topologies
දෙමුහුම් ස්ථල වර්ග

Star-Bus Topology
Multiple star networks connected through a common bus backbone.
පොදු බස් ප්‍රධාන සන්නිවේදන කේබලයක් හරහා එකිනෙකට සම්බන්ධ කරන ලද තරු ජාල කිහිපයක එකතුවකි.


Star-Mesh Topology

Star-Ring Topology
Several star networks connected in a ring for better reliability and management.
වඩා හොඳ විශ්වාසවන්තභාවයක් සහ කළමනාකරණයක් සඳහා වටමය ආකාරයට එකිනෙක සම්බන්ධ කරන ලද තරු ජාල කිහිපයකි.

Star-Mesh Topology
Star networks interconnected using mesh links to provide high redundancy and fault tolerance.
ඉහළ අතිරික්තතාවක් සහ දෝෂ ඉවසීමේ හැකියාවක් ලබා දීම සඳහා දැලිසමය සබැඳි භාවිතයෙන් එකිනෙකට සම්බන්ධ කරන ලද තරු ජාල වේ.


Snowflake Topology

Bus-Ring Topology
Combines a bus backbone with a ring structure to connect different network segments.
විවිධ ජාල කොටස් එකිනෙකට සම්බන්ධ කිරීම සඳහා බස් ප්‍රධාන කේබලයක් සහ වටමය ව්‍යුහයක් එකට එකතු කර නිර්මාණය කරන ලද්දකි.

Tree-Star Topology
Multiple star networks connected in a hierarchical tree structure using core and distribution switches.
ප්‍රධාන සහ බෙදාහැරීමේ ස්විචයන් භාවිතා කරමින්, ධුරාවලි වෘක්ෂ ව්‍යුහයකට එකිනෙකට සම්බන්ධ කරන ලද තරු ජාල කිහිපයකි.

Tree-Mesh Topology
A tree topology enhanced with mesh connections between key switches for redundancy.
අතිරික්තතාව සඳහා ප්‍රධාන ස්විචයන් අතර දැලිසමය සබැඳි එක් කරමින් තවදුරටත් දියුණු කරන ලද වෘක්ෂ ජාල ව්‍යුහයකි.

Snowflake Topology
An extended star (hierarchical) topology where secondary devices connect to additional devices, forming a snowflake-like structure.
ද්විතීයික උපාංග තවත් අතිරේක උපාංග සමඟ සම්බන්ධ වෙමින්, හිම පියල්ලක හැඩය ගන්නා පරිදි විහිදී යන, දියුණු කරන ලද තරු ජාල ව්‍යුහයකි.

Advantages of Hybrid Topology
දෙමුහුම් ස්ථල විද්‍යාවේ වාසි

Different topologies can be combined to meet specific network requirements.
නිශ්චිත ජාල අවශ්‍යතා සපුරාලීම සඳහා එකිනෙකට වෙනස් ස්ථල විද්‍යාවන් එකට ඒකාබද්ධ කළ හැකිය.

New devices or network segments can be added easily.
නව උපාංග හෝ ජාල කොටස් ඉතා පහසුවෙන් එකතු කළ හැකිය.

Different topologies can be optimized for different tasks.
විවිධ කාර්යයන් සඳහා විවිධ ස්ථල විද්‍යාවන් උපරිම ඵලදායීතාවක් ලැබෙන සේ සැකසිය හැකිය.

Disadvantages of Hybrid Topology
දෙමුහුම් ස්ථල විද්‍යාවේ අවාසි

Requires more networking devices and cabling.
මේ සඳහා වැඩිපුර ජාලකරණ උපාංග සහ කේබල් අවශ්‍ය වේ.

Planning and configuring the network is more difficult.
ජාලය සැලසුම් කිරීම සහ වින්‍යාසගත කිරීම වඩාත් අපහසු වේ.

Managing multiple topologies requires skilled administrators.
එකිනෙකට වෙනස් ස්ථල විද්‍යාවන් කිහිපයක් කළමනාකරණය කිරීම සඳහා දක්ෂ/පළපුරුදු ජාල පරිපාලකවරුන් අවශ්‍ය වේ.

Different topologies may need different networking equipment.
විවිධ ස්ථල විද්‍යාවන් සඳහා එකිනෙකට වෙනස් වූ ජාලකරණ උපකරණ අවශ්‍ය විය හැකිය.

Diagnosing issues across multiple topologies may take more time.
විවිධ ස්ථල විද්‍යාවන් කිහිපයක් ඔස්සේ පවතින ගැටලු නිවැරදිව හඳුනා ගැනීමට වැඩි කාලයක් ගත විය හැකිය.

Poor integration between topologies can reduce efficiency.
ස්ථල විද්‍යාවන් අතර පවතින දුර්වල ඒකාබද්ධතාව හේතුවෙන් ජාලයේ කාර්යක්ෂමතාව අඩු විය හැකිය.

7. Tree Topology
රුක් ආකාරයේ ජාල ස්ථලකය

Tree Topology is a network topology that combines the Star and Bus topologies.
වෘක්ෂ ස්වරූපී ස්ථල විද්‍යාව යනු තරු සහ බස් ස්ථල විද්‍යාවන් දෙකෙහි එකතුවක් වන ජාල ස්ථලකයකි.

Devices are organized into parent and child branches, similar to the branches of a tree.
ගසක අතු වැනි වූ, මව් සහ දරු ශාඛාවලට (parent and child branches) අනුව මෙහි උපාංග සංවිධානය කර ඇත.

Data travels through the hierarchy, moving from the root to branches or vice versa.
දත්ත ගමන් කරන්නේ මෙම ධුරාවලිය හරහා වන අතර, එහිදී දත්ත මුල සිට ශාඛා වෙත හෝ ශාඛාවල සිට නැවත මුල වෙත ගමන් කරයි.

It is commonly used in large organizations, campuses, schools, and enterprise networks where scalability and structured management are required.
පද්ධතිය විශාල කිරීමට ඇති හැකියාව සහ ව්‍යුහගත කළමනාකරණය අවශ්‍ය වන විශාල සංවිධාන, විශ්වවිද්‍යාල පරිශ්‍ර, පාසල් සහ ව්‍යවසාය ජාලයන්හි මෙය පොදුවේ භාවිත වේ.

Structure of tree topology
රුක් ආකාරයේ ජාල ස්ථලකයක ව්‍යුහය

A central root node (backbone or main hub) connects to secondary nodes.
මධ්‍යම මූල නෝඩයක් (කොඳුනාරටිය හෝ ප්‍රධාන Hub එක) ද්විතීයික නෝඩ වලට සම්බන්ධ වේ.

Each secondary node can further connect to additional child nodes, forming branches.
සෑම ද්විතීයික නෝඩයකටම අතිරේක ළමා නෝඩ වලට තවදුරටත් සම්බන්ධ වෙමින් ශාඛා නිර්මාණය කළ හැක.

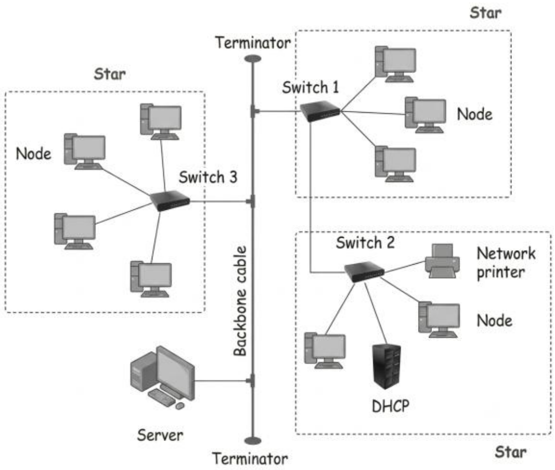
Data flows through defined hierarchical paths from root to leaf nodes.
දත්ත මූල නෝඩයේ සිට පත්‍ර නෝඩ දක්වා නිශ්චිත ධුරාවලි මාර්ග හරහා ගලා යයි.

There are two primary types of tree topology, distinguished by how the branches/segments are physically implemented.
ශාඛා/ඛණ්ඩ භෞතිකව ස්ථාපිත කර ඇති ආකාරය අනුව වෙන්කර හඳුනාගත හැකි ප්‍රධාන රුක් ආකාරයේ ජාල ස්ථලක වර්ග දෙකක් ඇත.

1. Bus-Based Tree Topology
බස් මත පදනම් වූ රුක් ආකාරයේ ජාල ස්ථලකය

2. Star-Based Tree Topology
තරු මත පදනම් වූ රුක් ආකාරයේ ජාල ස්ථලකය

Bus-Based Tree Topology / බස් ආකාරය මත පදනම් වූ රුක් ස්ථලකය
(Backbone Tree Topology)



A hierarchical network structure in which multiple star networks are connected to a single backbone cable (bus).
බහුවිධ තරු ජාල තනි ප්‍රධාන කේබලයකට (bus) සම්බන්ධ කර ඇති ධූරාවලි ජාල ව්‍යුහයකි

Each branch consists of a hub or switch with connected end devices, while all branches communicate through the shared backbone cable.
සෑම ශාඛාවක්ම සම්බන්ධිත අවසාන උපාංග සහිත හබ් එකකින් හෝ ස්විච් එකකින් සමන්විත වන අතර, සියලුම ශාඛා හවුල් ප්‍රධාන කේබලය හරහා සන්නිවේදනය කරයි.

Structure / ව්‍යුහය
A single backbone cable serves as the main communication path.
තනි ප්‍රධාන කේබලයක් ප්‍රධාන සන්නිවේදන මාර්ගය ලෙස ක්‍රියා කරයි.

Hubs or switches are connected to the backbone at different points.
හබ් හෝ ස්විච් විවිධ ස්ථානවලදී ප්‍රධාන කේබලයට සම්බන්ධ කර ඇත.

Each hub/switch forms a star topology with its connected end devices.
සෑම Hub එකක්/Switch එකක්ම තමන්ට සම්බන්ධ කර ඇති අවසාන උපාංග සමඟ තරුමය ස්ථලකයක් නිර්මාණය කරයි.

The backbone interconnects all branches, forming the tree.
ප්‍රධාන කේබලය මඟින් සියලුම ශාඛා එකිනෙකට සම්බන්ධ කරමින් රුක් ව්‍යුහය සාදයි.

How it works / ක්‍රියාකාරීත්වය
Each device sends data to its local hub or switch.
සෑම උපාංගයක්ම තමන්ගේ ප්‍රාදේශීය Hub එක වෙත හෝ Switch එක වෙත දත්ත යවයි.

The hub/switch forwards the data onto the backbone cable.
Hub /Switch මඟින් එම දත්ත ප්‍රධාන කේබලය වෙත යොමු කරයි.

The data travels along the backbone until it reaches the destination branch.
දත්ත ගමනාන්ත ශාඛාව වෙත ළඟා වන තෙක් ප්‍රධාන කේබලය දිගේ ගමන් කරයි.

The destination hub/switch then forwards the data to the intended device.
අනතුරුව ගමනාන්ත Hub/Switch එක මඟින් අදාළ උපාංගය වෙත දත්ත යොමු කරනු ලබයි.

Since all branches share the same backbone, communication between branches depends on the availability and performance of the backbone cable.
සියලුම ශාඛා එකම ප්‍රධාන කේබලය හවුලේ පරිහරණය කරන බැවින්, ශාඛා අතර සන්නිවේදනය ප්‍රධාන කේබලයේ පවතින උපදෙස්‍යතාවය (availability) සහ කාර්යසාධනය මත රඳා පවතී.

Characteristics / ලක්ෂණ

Cabling / කේබල් යෙදීම
Uses a single backbone cable (typically coaxial cable) with branch connections using hubs or switches. Requires less cabling than a star-based tree.
තනි ප්‍රධාන කේබලයක් (සාමාන්‍යයෙන් කෝඇක්සියල් කේබල්) භාවිතා කරන අතර ශාඛා සම්බන්ධතා සඳහා Hub හෝ Switch භාවිතා කරයි. තරු ආකාරය මත පදනම් වූ රුක් ස්ථලකයකට වඩා අඩු කේබල් ප්‍රමාණයක් අවශ්‍ය වේ.

Collision domain / ගැටුම් වසම
The backbone is a shared communication medium. If hubs are used, collisions can occur on the shared bus. Using switches reduces collisions within branches but the backbone remains a shared path.
ප්‍රධාන කේබලය යනු හවුලේ පරිහරණය වන සන්නිවේදන මාධ්‍යයකි. Hub භාවිතා කරන්නේ නම්, හවුල් බස් කේබලය මත දත්ත ගැටුම් (collisions) ඇති විය හැක. Switch භාවිතා කිරීමෙන් ශාඛා තුළ ගැටුම් අවම වන නමුත් ප්‍රධාන කේබලය හවුල් මාර්ගයක් ලෙසම පවතී.

Central device / මධ්‍යම උපාංගය

No single central switch for the entire network. Instead, multiple hubs or switches connect individual branches to the backbone.

මුළු ජාලය සඳහාම එකම මධ්‍යම Switch එකක් නොමැත. ඒ වෙනුවට, Hub හෝ Switch කිහිපයක් මඟින් එක් එක් ශාඛා ප්‍රධාන කේබලයට සම්බන්ධ කරයි.

Scalability / පරිමාණ්‍යතාව

Moderate. New branches can be added by connecting another hub or switch to the backbone, but excessive expansion can reduce network performance.

මධ්‍යස්ථය. ප්‍රධාන කේබලයට තවත් Hub එකක් හෝ Switch එකක් සම්බන්ධ කිරීමෙන් නව ශාඛා එකතු කළ හැකි නමුත්, අධික ලෙස ව්‍යාප්ත කිරීමෙන් ජාලයේ කාර්යසාධනය අඩු විය හැක.

Fault tolerance / දෝෂ ඉවසීමේ හැකියාව

Lower than a star-based tree. A failure of a branch hub affects only that branch, but damage to the backbone cable can disrupt communication for the entire network.

තරු ආකාරය මත පදනම් වූ රුක් ස්ථලකයකට වඩා අඩුය. ශාඛාවක Hub එකක් බිඳවැටීම බලපාන්නේ එම ශාඛාවට පමණක් වුවද, ප්‍රධාන කේබලයට සිදුවන හානියකින් මුළු ජාලයේම සන්නිවේදනය අඩාල විය හැක.

Advantages / වාසි

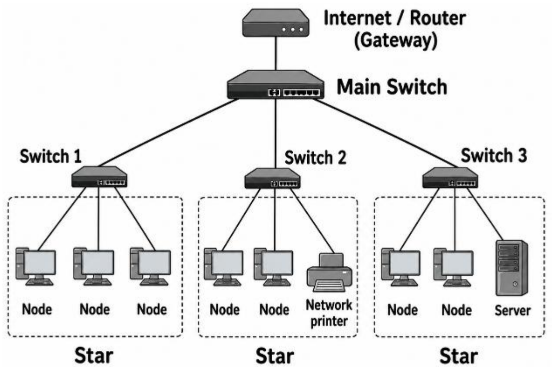
- Uses less cabling, reducing cost.
  අඩු කේබල් ප්‍රමාණයක් භාවිතා වන බැවින් පිරිවැය අඩු වේ.
- Easy to expand by adding new branches.
  නව ශාඛා එකතු කිරීමෙන් පහසුවෙන් ව්‍යාප්ත කළ හැක.
- Lower hardware cost.
  දෘඩාංග පිරිවැය අඩුය.
- Suitable for small to medium-sized networks.
  කුඩා හා මධ්‍යම ප්‍රමාණයේ ජාල සඳහා සුදුසු වේ.

Disadvantages / අවාසි

- Backbone failure can bring down the entire network.
  ප්‍රධාන කේබලය බිඳවැටීමකින් මුළු ජාලයම අක්‍රිය විය හැක.
- Performance decreases as more devices are added.
  උපාංග වැඩිපුර එකතු වන විට කාර්යසාධනය අඩු වේ.
- Harder to troubleshoot backbone faults.
  කොඳුනාරටියේ දෝෂ සෙවීම වඩාත් අපහසුය.

Star-Based Tree Topology

(Hierarchical Switched Tree)



A hierarchical structure where each branch operates as a star topology.

එක් එක් ශාඛාව තරුමය ස්ථලකයක් ලෙස ක්‍රියා කරන ධූරාවලි ව්‍යුහයකි.

Each node connects to a central switch/hub, and these hubs/switches are themselves connected hierarchically to form the tree.

සෑම නෝඩයක්ම මධ්‍යම Switch එකකට/ඝම්ඉ එකකට සම්බන්ධ වන අතර, මෙම Hub/Switch ද රුක් ව්‍යුහය සෑදීම සඳහා ධූරාවලිගතව එකිනෙකට සම්බන්ධ වී ඇත.

Structure / ව්‍යුහය

Root hub/switch connects to secondary hubs/switches.

මූල (Root) Hub/Switch එක ද්විතීයික Hub/Switch වෙත සම්බන්ධ වේ.

Each secondary hub/switch has its own set of connected end devices (star configuration).

සෑම ද්විතීයික Hub/Switch එකකටම තමන්ටම ආවේණික වූ අවසාන උපාංග සමූහයක් සම්බන්ධ කර ඇත (තරුමය වින්‍යාසය).

No shared bus cable; each device has a dedicated (point-to-point) connection to its hub.

හවුල් බස් කේබලයක් නොමැත; සෑම උපාංගයකටම තම Hub එක වෙත කැපවූ (point-to-point) සම්බන්ධතාවයක් ඇත.

How it works / ක්‍රියාකාරීත්වය

Each device connects independently to its local hub/switch via a dedicated link.

සෑම උපාංගයක්ම කැපවූ සබැඳියක් හරහා තම ප්‍රාදේශීය Hub /Switch එකට ස්වාධීනව සම්බන්ධ වේ.

Data from a device goes to its local hub, which forwards it up/down the hierarchy as needed based on the destination.

උපාංගයකින් එන දත්ත එහි ප්‍රාදේශීය Hub එක වෙත යන අතර, එය ගමනාන්තය මත පදනම්ව අවශ්‍ය පරිදි ධූරාවලිය ඔස්සේ ඉහළට හෝ පහළට යොමු කරයි.

Switches can filter and forward frames intelligently (if using switches rather than hubs), reducing unnecessary traffic.
Switch මඟින් දත්ත රාමු බුද්ධිමත් ලෙස පෙරීමට (filter) සහ යොමු කිරීමට හැකියාව ඇති බැවින් (Hub වෙනුවට Switch භාවිතා කරන්නේ නම්), අනවශ්‍ය දත්ත ගමනාගමනය (traffic) අඩු කරයි.

Characteristics / ලක්ෂණ

Cabling / කේබල් යෙදීම
Uses twisted pair (Ethernet) typically, more cable required
සාමාන්‍යයෙන් ඇඹරුණු යුගල කේබල් (twisted pair / Ethernet) භාවිතා කරයි, වැඩි කේබල් ප්‍රමාණයක් අවශ්‍ය වේ

Collision domain / ගැටුම් වසම
Each switch port creates a separate collision domain, so collisions are minimized or eliminated. This improves network performance.
සෑම Switch කෙවෙණියක්ම වෙනම ගැටුම් වසමක් සාදන බැවින් දත්ත ගැටුම් අවම කිරීම හෝ නැති කිරීම සිදු කරයි. මෙයින් ජාලයේ කාර්යසාධනය වැඩි දියුණු වේ.

Central device / මධ්‍යම උපාංගය
Every branch requires a hub or switch, with a root switch at the top of the hierarchy to connect all lower-level devices.
සෑම ශාඛාවකටම Hub එකක් හෝ Switch එකක් අවශ්‍ය වන අතර, පහළ මට්ටමේ සියලුම උපාංග සම්බන්ධ කිරීම සඳහා ධූරාවලියේ ඉහළින්ම මූල (root) Switch එකක් පවතී.

Scalability / පරිමාණ්‍යතාව
Highly scalable. New devices or entire branches can be added easily without affecting the existing network.
ඉහළ පරිමාණ්‍යතාවයකින් යුක්තය. පවතින ජාලයට බලපෑමක් නොකර අලුත් උපාංග හෝ සමස්ත ශාඛාම පහසුවෙන් එකතු කළ හැක.

Fault tolerance / දෝෂ ඉවසීමේ හැකියාව
A failure of a device or cable affects only that specific connection. However, if a hub or switch fails, all devices connected to it lose network access.
උපාංගයක හෝ කේබලයක සිදුවන බිඳවැටීමක් බලපාන්නේ එම නිශ්චිත සම්බන්ධතාවයට පමණි. කෙසේ වෙතත්, Hub එකක් හෝ Switch එකක් අක්‍රිය වුවහොත්, එයට සම්බන්ධ සියලුම උපාංගවලට ජාල ප්‍රවේශය අහිමි වේ.

Advantages / වාසි

- Easy to expand by adding new devices or branches.
  නව උපාංග හෝ ශාඛා එකතු කිරීමෙන් ව්‍යාප්ත කිරීම පහසුය.
- Good fault isolation.
  දෝෂ හුදකලා කිරීම හොඳ මට්ටමක පවතී.
- Easy to troubleshoot.
  දෝෂ සෙවීම පහසුය.
- High performance with switches.
  Switch භාවිතා කිරීමෙන් ඉහළ කාර්යසාධනයක් ලැබේ.

Disadvantages / අවාසි

- Requires more cabling.
  වැඩි කේබල් ප්‍රමාණයක් අවශ්‍ය වේ.
- Higher hardware cost.
  දෘඩාංග පිරිවැය ඉහළය.
- Failure of a hub/switch disconnects its entire branch.
  Hub/Switch එකක බිඳවැටීමකින් එහි සමස්ත ශාඛාවම ජාලයෙන් විසන්ධි වේ.

NOTE:
Bus-Based Tree Topology is no longer in use in modern networks.
නූතන ජාලකරණයේදී බස් ආකාරය මත පදනම් වූ රුක් ස්ථලකය තවදුරටත් භාවිත නොවේ.

Reasons / හේතු
Relied on coaxial cable, now replaced by twisted-pair and fiber-optic.
කෝඇක්සියල් කේබල් මත රඳා පැවති අතර, දැන් ඒවා වෙනුවට ඇඹරුණු යුගල සහ ප්‍රකාශ තන්තුකේබල් ආදේශ වී ඇත.

Shared bus segments caused collisions and bandwidth bottlenecks.
හවුලේ පරිහරණය වූ බස් ඛණ්ඩ හේතුවෙන් දත්ත ගැටුම් සහ කලාප පළල අවහිරතා ඇති විය.

Single backbone failure could disrupt the entire network.
තනි ප්‍රධාන කේබලයක බිඳවැටීමකින් මුළු ජාලයම අක්‍රිය වීමේ අවදානමක් පැවතුණි.

Internet Service Providers (ISP)
අන්තර්ජාල සේවා සපයන්නන්

Internet Service Providers (ISPs) are companies that provide individuals and organizations with access to the Internet.
අන්තර්ජාල සේවා සපයන්නන් (ISPs) යනු පුද්ගලයන්ට සහ සංවිධානවලට අන්තර්ජාලයට ප්‍රවේශය සපයන සමාගම් වේ.

They offer various types of internet connections, each with its own technologies and characteristics.
ඔවුන් විවිධ ආකාරයේ අන්තර්ජාල සම්බන්ධතා ලබා දෙයි, ඒ සෑම එකකටම ඒවාට වෙන්වූ තාක්ෂණයන් සහ ලක්ෂණ ඇත.

Types of ISPs
අන්තර්ජාල සේවා සපයන්නන් වර්ග

Dial-Up ISP
Transmission Type: Analog telephone line
සම්ප්‍රේෂණ වර්ගය: ඇනලොග් දුරකථන මාර්ග
Maximum Speed: 56 Kbps
උපරිම වේගය: 56 Kbps

ISDN (Integrated Services Digital Network)
Transmission Type: Digital telephone line
සම්ප්‍රේෂණ වර්ගය: ඩිජිටල් දුරකථන මාර්ග
Maximum Speed: 128 Kbps
උපරිම වේගය: 128 Kbps

DSL (Digital Subscriber Line)
Transmission Type: Copper telephone wires
සම්ප්‍රේෂණ වර්ගය: තඹ දුරකථන රැහැන්
Maximum Speed: 300 Mbps (VDSL2)
උපරිම වේගය: 300 Mbps (VDSL2)

Cable ISP
Transmission Type: Coaxial cable
සම්ප්‍රේෂණ වර්ගය: සමාක්ෂ කේබල්
Maximum Speed: 10 Gbps
උපරිම වේගය: 10 Gbps

Fiber Optic ISP (FTTH/ FTTP)
Transmission Type: Optical fiber cable
සම්ප්‍රේෂණ වර්ගය: ප්‍රකාශ තන්තු කේබල්
Maximum Speed: 100+ Gbps
උපරිම වේගය: 100+ Gbps

Satellite ISP
Transmission Type: Radio waves via satellites
සම්ප්‍රේෂණ වර්ගය: චන්ද්‍රිකා හරහා රේඩියෝ තරංග
Maximum Speed: 1 Gbps
උපරිම වේගය: 1 Gbps

Fixed Wireless ISP (WISP)
Transmission Type: Microwave/Radio signals
සම්ප්‍රේෂණ වර්ගය: ක්ෂුද්‍ර තරංග/රේඩියෝ සංඥා
Maximum Speed: 1–10 Gbps
උපරිම වේගය: 1-10 Gbps

Mobile Broadband ISP (3G/4G/5G)
Transmission Type: Cellular radio network
සම්ප්‍රේෂණ වර්ගය: සෙලියුලර් රේඩියෝ ජාලය
Maximum Speed: 20+ Gbps (5G theoretical)
උපරිම වේගය: 20+ Gbps (5G සෛද්ධාන්තික උපරිමය)

Connecting to ISP
ISP වෙත සම්බන්ධ වීම

1. Modems

A modem converts digital data from your computer into analog signals for transmission over phone lines, cable, or fiber optic cables, and vice versa.
මොඩමයක් මගින් ඔබගේ පරිගණකයෙන් ලැබෙන ඩිජිටල් දත්ත, දුරකථන මාර්ග, කේබල් හෝ ප්‍රකාශ තන්තු හරහා සම්ප්‍රේෂණය කළ හැකි පරිදි ඇනලොග් සංඥා බවට පරිවර්තනය කරන අතර, එහි ප්‍රතිලෝම ක්‍රියාවලිය ද (ඇනලොග් සංඥා නැවත ඩිජිටල් දත්ත බවට පරිවර්තනය කිරීම ද) සිදු කරයි.

For instance, in a cable internet setup, the cable modem translates the signal from the ISP's network into a format your computer or router can understand.
උදාහරණයක් ලෙස, කේබල් අන්තර්ජාල සැකසුමකදී කේබල් මොඩමය මගින් අන්තර්ජාල සේවා සපයන්නාගේ ජාලයෙන් එන සංඥා, ඔබගේ පරිගණකයට හෝ රවුටරයට තේරුම් ගත හැකි ආකෘතියකට පරිවර්තනය කරනු ලබයි.

2. Connection Type
සම්බන්ධතා වර්ගය

Option 1: Dial-Up Internet

Dial-up is a method of connecting to the Internet using a telephone line and a modem to communicate with an ISP
Dial-up යනු අන්තර්ජාල සේවා සපයන්නෙකු සමඟ සන්නිවේදනය කිරීම සඳහා දුරකථන රැහැනක් සහ මොඩමයක් භාවිතා කරමින් අන්තර්ජාලයට සම්බන්ධ වන ක්‍රමවේදයකි.

How Dial-Up Internet Works

The user starts the internet connection using a computer and a dial-up modem.
පරිශීලකයා පරිගණකයක් සහ ඩයල්-අප් මොඩමයක් භාවිතයෙන් අන්තර්ජාල සම්බන්ධතාවය ආරම්භ කරයි.

The modem dials the Internet Service Provider's (ISP) phone number through a telephone line.
මොඩමය මඟින් දුරකථන රැහැනක් ඔස්සේ අන්තර්ජාල සේවා සපයන්නාගේ දුරකථන අංකය අමතනු ලබයි.

The ISP's modem answers the call and establishes a connection with the user's modem.
ISP ආයතනයේ ඇති මොඩමය මඟින් එම ඇමතුමට ප්‍රතිචාර දක්වන අතර, පරිශීලකයාගේ මොඩමය සමඟ සම්බන්ධතාවයක් ගොඩනඟා ගනී.

The modem converts digital computer data into analog signals for transmission over the telephone network.
දුරකථන ජාලය ඔස්සේ සම්ප්‍රේෂණය කිරීම සඳහා, මොඩමය මඟින් පරිගණකයේ ඇති ඩිජිටල් දත්ත ඇනලොග් සංඥා බවට පරිවර්තනය කරයි.

The analog signals travel through the public telephone network to the ISP.
එම ඇනලොග් සංඥා පොදු දුරකථන ජාලය හරහා ISP වෙත ගමන් කරයි.

The ISP receives the data and forwards the request to the appropriate internet server.
ISP වෙත මෙම දත්ත ලැබෙන අතර, ඔවුන් එම ඉල්ලීම අදාළ අන්තර්ජාල සේවාදායකය වෙත යොමු කරයි.

The destination server processes the request and prepares the required response.
ගමනාන්ත සේවාදායකය මඟින් ඉල්ලීම සකසා අවශ්‍ය ප්‍රතිචාරය සූදානම් කරයි.

The server sends the response back through the ISP and telephone network.
සේවාදායකය විසින් අදාළ ප්‍රතිචාරය ISP සහ දුරකථන ජාලය හරහා නැවත එවනු ලබයි.

The modem converts the received analog signals back into digital data.
මොඩමය මඟින් තමන්ට ලැබුණු ඇනලොග් සංඥා නැවතත් පරිගණකයට තේරුම් ගත හැකි ඩිජිටල් දත්ත බවට පරිවර්තනය කරයි.

The computer receives the data and displays the requested webpage, email, or other online content.
පරිගණකයට එම දත්ත ලැබෙන අතර, පරිශීලකයා ඉල්ලා සිටි වෙබ් පිටුව, ඊමේල් පණිවිඩය හෝ වෙනත් සබැඳි අන්තර්ගතයක් තිරය මත දර්ශනය වේ.

Limitations of Dial-Up
Dial-Up තාක්ෂණයේ ඇති සීමාවන්

The telephone line remains occupied while connected.
අන්තර්ජාලයට සම්බන්ධ වී සිටින තාක් දුරකථන රැහැන වෙනත් කාර්යයකට යොදාගත නොහැකි ලෙස අවහිර වී පවතී.

You cannot normally use the phone and Internet simultaneously on the same line.
සාමාන්‍යයෙන් ඔබට එකම දුරකථන රැහැනක් ඔස්සේ එකම අවස්ථාවකදී දුරකථනය සහ අන්තර්ජාලය යන දෙකම භාවිතා කළ නොහැක.

Option 2: Mobile internet

Mobile internet is a wireless technology that allows users to access the internet using mobile devices such as smartphones and tablets.
Mobile internet යනු ස්මාර්ට්ෆෝන් සහ ටැබ්ලට් වැනි ජංගම උපාංග භාවිතයෙන් පරිශීලකයන්ට අන්තර්ජාලයට පිවිසීමට ඉඩ සලසන රැහැන් රහිත තාක්ෂණයකි

How Mobile Internet Works

The user opens a website, app, or online service on a mobile device.
පරිශීලකයා ජංගම උපාංගයක් මඟින් වෙබ් අඩවියක්, ඇප් එකක් හෝ සබැඳි සේවාවක් විවෘත කරයි.

The mobile device sends the request as radio signals through its antenna.
ජංගම උපාංගය එහි ඇන්ටනාව හරහා මෙම ඉල්ලීම රේඩියෝ සංඥා ලෙස පිටතට යොමු කරයි.

The nearest cell tower receives the signals from the mobile device.
ළඟම ඇති සන්නිවේදන සංඥා කුළුණ මඟින් ජංගම උපාංගයෙන් නිකුත් වූ සංඥා ග්‍රහණය කරගනු ලබයි.

The cell tower forwards the request to the mobile operator’s core network.
සංඥා කුළුණ මඟින් එම ඉල්ලීම ජංගම දුරකථන ක්‍රියාකරුගේ ප්‍රධාන මධ්‍යම ජාලය වෙත ඉදිරිපත් කරයි.

The network verifies the user's SIM/eSIM and data service permissions.
ජාලය මඟින් පරිශීලකයාගේ SIM/ eSIM පත සහ දත්ත සේවා භාවිත කිරීමේ අවසරය නිවැරදිදැයි පරීක්ෂා කර සහතික කරයි.

The mobile operator routes the request to the appropriate server on the internet.
ජංගම දුරකථන ක්‍රියාකරු විසින් මෙම ඉල්ලීම අන්තර්ජාලය ඔස්සේ අදාළ සර්වරය වෙත යොමු කරනු ලබයි.

The destination server processes the request and prepares the required data.
ගමනාන්ත සර්වරය මඟින් ඉල්ලීම සකසා අවශ්‍ය දත්ත සූදානම් කරයි.

The server sends the response back through the internet to the mobile operator.
සර්වරය විසින් අදාළ ප්‍රතිචාරය අන්තර්ජාලය හරහා නැවතත් ජංගම දුරකථන ක්‍රියාකරු වෙත එවනු ලබයි.

The mobile operator forwards the response to the serving cell tower, which transmits it to the mobile device.
ජංගම දුරකථන ක්‍රියාකරු විසින් එම ප්‍රතිචාරය අදාළ සේවා සපයන සංඥා කුළුණ වෙත යොමු කරන අතර, කුළුණ මඟින් එය නැවත ජංගම උපාංගය වෙත සම්ප්‍රේෂණය කරයි.

The mobile device receives the data and displays the requested content, such as a webpage, video, or message.
ජංගම උපාංගයට එම දත්ත ලැබෙන අතර, පරිශීලකයා ඉල්ලා සිටි වෙබ් පිටුව, වීඩියෝව හෝ පණිවිඩය තිරය මත දර්ශනය වේ.

Advantages of Mobile Internet

Mobile internet keeps you connected no matter where you are. As long as there's network coverage, information and communication are always within reach.
ඔබ කොතැනක සිටියත් ඔබව සම්බන්ධ කර තැබීමට මොබයිල් ඉන්ටර්නෙට් උපකාරී වේ. ජාල ආවරණය පවතින තාක් කල්, තොරතුරු සහ සන්නිවේදනය සැමවිටම ඔබට ළඟා විය හැකි මට්ටමක පවතී.

Mobile internet can be shared with other devices through a hotspot, turning your phone into a portable Wi-Fi router for instant connectivity anywhere.
ඔබගේ දුරකථනය ඕනෑම තැනක ක්ෂණික සම්බන්ධතාවයක් සඳහා අතේ ගෙන යා හැකි Wi-Fi රවුටරයක් බවට පත් කරමින්, හොට්ස්පොට් එකක් හරහා ජංගම අන්තර්ජාලය වෙනත් උපාංග සමඟ බෙදා ගත හැකිය.

Option 3: Fiber Optics internet

Fiber optic internet is a high-speed communication technology that uses light signals transmitted through optical fibers to provide fast, reliable, and efficient internet connectivity.
ෆයිබර් ඔප්ටික් අන්තර්ජාලය යනු වේගවත්, විශ්වාසදායී සහ කාර්යක්ෂම අන්තර්ජාල සබැඳියාවක් ලබා දීම සඳහා ප්‍රකාශ තන්තු හරහා සම්ප්‍රේෂණය වන ආලෝක සංඥා භාවිතා කරන අධිවේගී සන්නිවේදන තාක්ෂණයකි.

How Fiber Optic Internet Works

The user opens a website, app, or online service.
පරිශීලකයා වෙබ් අඩවියක්, ඇප් එකක් හෝ සබැඳි සේවාවක් විවෘත කරයි.

The request travels from the device through the router to the Optical Network Terminal
මෙම ඉල්ලීම උපාංගයේ සිට රවුටරය හරහා ඔප්ටිකල් නෙට්වර්ක් ටර්මිනලය වෙත ගමන් කරයි.

The ONT converts electrical signals into light signals.
ONT මඟින් විද්‍යුත් සංඥා ආලෝක සංඥා බවට පරිවර්තනය කරයි.

The light signals travel through fiber optic cables at high speed.
ආලෝක සංඥා ෆයිබර් ඔප්ටික් කේබල් හරහා ඉතා ඉහළ වේගයකින් ගමන් කරයි.

The ISP receives and routes the request to the destination server.
අන්තර්ජාල සේවා සපයන්නා වෙත මෙම ඉල්ලීම ලැබෙන අතර, ඔවුන් එය අදාළ ගමනාන්ත සර්වරය වෙත යොමු කරයි.

The server processes the request and prepares the required data.
සර්වරය මඟින් ඉල්ලීම සකසා අවශ්‍ය දත්ත සූදානම් කරයි.

The server sends the response back through the ISP's network.
සර්වරය විසින් අදාළ ප්‍රතිචාරය නැවතත් ISP ජාලය හරහා එවනු ලබයි.

The response travels as light signals through the fiber optic cables.
ප්‍රතිචාරය ආලෝක සංඥා ලෙස ෆයිබර් ඔප්ටික් කේබල් හරහා නැවත ගමන් කරයි.

The ONT converts the light signals back into electrical signals.
ONT මඟින් එම ආලෝක සංඥා නැවතත් විද්‍යුත් සංඥා බවට පරිවර්තනය කරයි.

The device receives the data and displays the requested content.
උපාංගයට එම දත්ත ලැබෙන අතර, පරිශීලකයා ඉල්ලා සිටි වෙබ් පිටුව හෝ අන්තර්ගතය තිරය මත දර්ශනය වේ.

Option 3: Satellite Internet

How Satellite Internet Works

The user opens a website, app, or online service.
පරිශීලකයා වෙබ් අඩවියක්, ඇප් එකක් හෝ සබැඳි සේවාවක් විවෘත කරයි.

The request travels from the device through the router to the satellite modem and dish.
මෙම ඉල්ලීම උපාංගයේ සිට රවුටරය සහ සැටලයිට් මොඩමය හරහා නිවසේ හෝ ගොඩනැඟිල්ලේ සවිකර ඇති සැටලයිට් ඇන්ටනාව වෙත ගමන් කරයි.

The satellite dish sends the request as radio signals to a satellite in orbit.
සැටලයිට් ඇන්ටනාව මඟින් එම ඉල්ලීම රේඩියෝ සංඥා ලෙස අභ්‍යවකාශයේ කක්ෂගත කර ඇති සැටලයිට් එක වෙත යොමු කරයි.

The satellite receives the signal and forwards it to a ground station (gateway).
සැටලයිට් එකට එම සංඥාව ලැබෙන අතර, එය පෘථිවියේ පිහිටි ප්‍රධාන භූගත මධ්‍යස්ථානයක් වෙත හරවා යවයි.

The ground station routes the request to the destination server on the internet.
භූගත මධ්‍යස්ථානය මඟින් එම ඉල්ලීම අන්තර්ජාලය ඔස්සේ අදාළ ගමනාන්ත සර්වරය වෙත යොමු කරනු ලබයි.

The server processes the request and prepares the required response.
සර්වරය මඟින් ඉල්ලීම සකසා අවශ්‍ය ප්‍රතිචාරය සූදානම් කරයි.

The server sends the response back to the ground station.
සර්වරය විසින් අදාළ ප්‍රතිචාරය නැවතත් භූගත මධ්‍යස්ථානය වෙත එවනු ලබයි.

The ground station transmits the response to the satellite.
භූගත මධ්‍යස්ථානය විසින් එම ප්‍රතිචාරය නැවතත් අභ්‍යවකාශයේ ඇති සැටලයිට් එක වෙත සම්ප්‍රේෂණය කරයි.

The satellite relays the response back to the user's satellite dish.
සැටලයිට් එක මඟින් එම ප්‍රතිචාර සංඥාව පරිශීලකයාගේ සැටලයිට් ඇන්ටනාව වෙත හරවා එවනු ලබයි.

The modem converts the signals into data, and the device displays the requested content.
මොඩමය මඟින් එම සංඥා නැවත දත්ත බවට පරිවර්තනය කරන අතර, උපාංගය මඟින් පරිශීලකයා ඉල්ලා සිටි අන්තර්ගතය තිරය මත දර්ශනය කරයි.

Advantages of Satellite Internet

Satellite internet reaches places where cables and cell towers cannot. Even in rural or isolated locations, users can stay connected without relying on ground-based infrastructure.
කේබල් සහ සෙලියුලර් කුළුණු ළඟා විය නොහැකි ස්ථාන කරා චන්ද්‍රිකා අන්තර්ජාලය ළඟා වේ. ග්‍රාමීය හෝ හුදකලා ප්‍රදේශවල පවා, භූමිය මත පදනම් වූ යටිතල පහසුකම් මත යැපීමකින් තොරව පරිශීලකයින්ට සම්බන්ධ වී සිටිය හැකිය.

Satellite internet is less affected by local disruptions like damaged cables or power outages. As long as the dish has a clear view of the sky, the connection remains stable.
හානි වූ කේබල් හෝ විදුලි බිඳවැටීම් වැනි දේශීය බාධාවන්ගෙන් චන්ද්‍රිකා අන්තර්ජාලයට එල්ල වන බලපෑම අවමය. චන්ද්‍රිකා තැටියට අහස පැහැදිලිව පෙනෙන තාක් කල්, සම්බන්ධතාවය ස්ථාවරව පවතී.

Since it operates from space, satellite internet is available across entire countries and continents. It is one of the few options that can provide truly global coverage.
එය අභ්‍යවකාශයේ සිට ක්‍රියාත්මක වන බැවින්, චන්ද්‍රිකා අන්තර්ජාලය මුළු රටවල් සහ මහාද්වීප පුරාම ලබා ගත හැකිය. සැබවින්ම ගෝලීය ආවරණයක් සැපයිය හැකි සීමිත විකල්පයන්ගෙන් එකක් වන්නේ මෙයයි.

Setting up satellite internet requires no digging or laying of cables. A dish and a receiver are all that's needed, making installation fast and straightforward.
චන්ද්‍රිකා අන්තර්ජාලය සැකසීම සඳහා පොළොව හැරීමක් හෝ කේබල් එලීමක් අවශ්‍ය නොවේ. මේ සඳහා අවශ්‍ය වන්නේ චන්ද්‍රිකා තැටියක් සහ ග්‍රාහකයක් පමණක් වන බැවින්, එය ස්ථාපනය කිරීම වේගවත් මෙන්ම සරල වේ.

ictfromabc.com

DSL (Digital Subscriber Line)

DSL uses frequency division multiplexing to separate voice and data signals.
හඬ සහ දත්ත සංඥා වෙන් කිරීම සඳහා DSL භාවිතා කරන්නේ සංඛ්‍යාත බෙදීමේ බහුපථකරණයයි.

This allows you to use the phone line for internet and voice calls simultaneously.
මෙමගින් ඔබට එකවර අන්තර්ජාල සහ හඬ ඇමතුම් සඳහා දුරකථන මාර්ගය භාවිතා කිරීමට ඉඩ සලසයි.

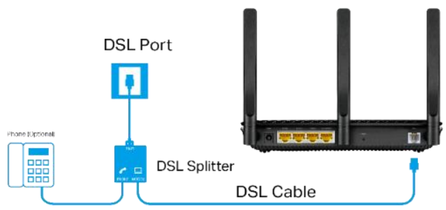
The performance of DSL is affected by the distance between your home and the ISP's central office.
DSL හි ක්‍රියාකාරිත්වයට ඔබගේ නිවස සහ ISP ගේ මධ්‍යම කාර්යාලය අතර ඇති දුර ප්‍රමාණය බලපායි.

DSL typically requires a DSL modem and may use filters (microfilters or splitters) to prevent interference between voice and data signals.
DSL තාක්ෂණය සඳහා සාමාන්‍යයෙන් DSL මොඩමයක් අවශ්‍ය වන අතර, හඬ සහ දත්ත සංඥා අතර බාධා ඇතිවීම වැළැක්වීම සඳහා පෙරහන් (Microfilters හෝ Splitters) භාවිතා කළ හැකිය.

The modem connects to the telephone line, and the filter is used to ensure clear voice communication while using the internet.
මෝඩමය දුරකථන මාර්ගයට සම්බන්ධ වන අතර, අන්තර්ජාලය භාවිතා කරන අතරතුර පැහැදිලි හඬ සන්නිවේදනය සහතික කිරීම සඳහා පෙරහන භාවිතා කරයි.

Without Phone Service

With Phone Service



Advantages of DSL

Independent Services
DSL allows you to maintain telephone service even if the internet connection has issues. Unlike cable services, problems with DSL do not typically affect your phone line.
අන්තර්ජාල සම්බන්ධතාවයේ ගැටළු ඇති වුවද දුරකථන සේවාව පවත්වා ගැනීමට DSL ඔබට ඉඩ සලසයි. කේබල් සේවා මෙන් නොව, DSL සමඟ ඇති ගැටළු සමාන්‍යයෙන් ඔබගේ දුරකථන මාර්ගයට බලපාන්නේ නැත.

Security
Each DSL connection is separate from others, providing better security. This isolation reduces vulnerability compared to cable modems, where multiple users share the same network and might be exposed to security risks.
සෑම DSL සම්බන්ධතාවක්ම අනෙක් ඒවාගෙන් වෙන්ව, වඩා හොඳ ආරක්ෂාවක් සපයයි. මෙම හුදකලා කිරීම කේබල් මොඩම් හා සසඳන විට අවදානම අඩු කරයි, එහිදී බහු පරිශීලකයින් එකම ජාලය බෙදා ගන්නා අතර ආරක්ෂක අවදානම් වලට නිරාවරණය විය හැකිය.

Integration
DSL easily integrates with various technologies like ATM (Asynchronous Transfer Mode), Nx64, and WAN (Wide Area Network), which can simplify network management and enhance telecommuting options.
DSL පහසුවෙන් ATM (Asynchronous Transfer Mode), Nx64 සහ WAN (Wide Area Network) වැනි විවිධ තාක්ෂණයන් සමඟ ඒකාබද්ධ වන අතර එමඟින් ජාල කළමනාකරණය සරල කිරීමට සහ විදුලි සංදේශ විකල්ප වැඩිදියුණු කළ හැක.

ADSL (Asymmetric DSL)

ADSL is asymmetric, meaning that it offers higher speeds for downloading (receiving data) and lower speeds for uploading (sending data).
ADSL අසමමිතික වේ, එනම් එය බාගත කිරීම (දත්ත ලබා ගැනීම) සඳහා වැඩි වේගයක් සහ උඩුගත කිරීම සඳහා (දත්ත යැවීම) අඩු වේගයක් ලබා දෙයි.

This suits typical internet usage where users often download more than they upload.
බොහෝ විට උඩුගත කරනවාට වඩා බාගත කරන සාමාන්‍ය අන්තර්ජාල භාවිතයට මෙය ගැලපේ.

ictfromabc.com

Advantages of ADSL

Cheaper Rates

ADSL often provides cost-effective internet service with high speeds and typically includes a static IP address. ISPs offer straightforward ADSL connections that are budget-friendly.

ADSL බොහෝ විට අධික වේගයකින් අඩු වියදම් සහිත අන්තර්ජාල සේවාවක් සපයන අතර සාමාන්‍යයෙන් ස්ථිතික IP ලිපිනයක් ඇතුළත් වේ. ISPs මගින් අයවැය-හිතකාමී සෘජු ADSL සම්බන්ධතා ලබා දෙයි.

Fully Configurable

WAN engineers can manage and adjust ADSL VPN tunnels flexibly, making it easier to address network issues or configuration changes as needed.

WAN ඉංජිනේරුවන්ට ADSL VPN මාර්ග නම්‍යශීලීව කළමනාකරණය කිරීමට සහ සැකසීමට හැකිය, එමඟින් ජාල ගැටළු විසඳීමට හෝ අවශ්‍ය පරිදි වින්‍යාස වෙනස් කිරීමට පහසු වේ.

High-Speed Access

ADSL offers significantly faster speeds for downloading and streaming compared to older narrowband technologies like ISDN and dial-up modems.

ISDN සහ ඩයල්-අප් මොඩමයන් වැනි පැරණි පටු බෑන්ඩ් තාක්ෂණයන්ට සාපේක්ෂව ADSL බාගත කිරීම සහ ප්‍රවාහය සඳහා සැලකිය යුතු වේගවත් වේගයක් ලබා දෙයි.

3. Creating a home LAN

නිවසේ LAN (ස්ථානීය ජාලයක්) නිර්මාණය කිරීම

A Network that connects devices within your home so they can communicate with each other and access the internet through the same router.

ඔබේ නිවස තුළ ඇති උපාංග එකිනෙකා සමඟ සන්නිවේදනය කිරීමට සහ එකම රවුටරයක් හරහා අන්තර්ජාලයට ප්‍රවේශ වීමට හැකි වන පරිදි ඒවා එකිනෙකට සම්බන්ධ කරන ජාලයකි.

Public IP Address

පොදු IP ලිපින

This is a globally unique IP address that can be accessed over the internet, much like a postal address. It identifies your home network to the outside world.

මෙය තැපැල් ලිපිනයක් මෙන් අන්තර්ජාලය හරහා ප්‍රවේශ විය හැකි ගෝලීය වශයෙන් අනන්‍ය IP ලිපිනයකි. එය ඔබගේ නිවසේ ජාලය බාහිර ලෝකයට හඳුනා දෙයි.

Private IP Address

පෞද්ගලික IP ලිපින

These are used within your home network to identify each device (computers, smartphones, tablets) connected to your router. These private addresses are not accessible from the internet.

ඔබේ රවුටරයට සම්බන්ධ එක් එක් උපාංගය (පරිගණක, ස්මාර්ට් ෆෝන්, ටැබ්ලට්) හඳුනා ගැනීමට නිවසේ ජාලය තුළ මේවා භාවිත කෙරේ. මෙම පුද්ගලික ලිපින වලට අන්තර්ජාලයෙන් ප්‍රවේශ විය නොහැක.

Your router is assigned a public IP address by your ISP, which allows it to communicate with the internet.

ඔබගේ ISP විසින් ඔබගේ රවුටරයට පොදු IP ලිපිනයක් ලබා දී ඇත, එය අන්තර්ජාලය සමඟ සන්නිවේදනය කිරීමට ඉඩ සලසයි.

The router then assigns private IP addresses to the devices within your home network using the DHCP.

එවිට රවුටරය DHCP භාවිතයෙන් ඔබගේ නිවසේ ජාලය තුළ ඇති උපාංග වෙත පුද්ගලික IP ලිපින පවරයි.

This setup helps isolate your devices from direct exposure to the internet, providing an added layer of security while enabling internal communication within the home.

මෙම සැකසුම ඔබගේ උපාංග අන්තර්ජාලයට සෘජුව නිරාවරණය වීමෙන් වැලැක්වීමට උපකාරී වන අතර, නිවස තුළ අභ්‍යන්තර සන්නිවේදනය සක්‍රීය කරන අතරම අමතර ආරක්ෂිත ස්තරයක්ද සපයයි.

4. Network Address Translation (NAT)

ජාල ලිපින පරිවර්තනය

NAT is a method used to translate private IP addresses used within a local network into a public IP address for communication over the internet.

NAT යනු ස්ථානීය ජාලයක් තුළ භාවිතා කරන පුද්ගලික IP ලිපින අන්තර්ජාලය හරහා සන්නිවේදනය සඳහා පොදු IP ලිපිනයක් බවට පරිවර්තනය කිරීමට භාවිතා කරන ක්‍රමයකි.

This allows multiple devices in a private network (such as a home or corporate LAN) to share a single public IP address provided by the ISP.

මෙය පුද්ගලික ජාලයක (නිවසක් හෝ ආයතනික LAN වැනි) බහුවිධ උපාංගවලට ISP විසින් සපයන ලද තනි පොදු IP ලිපිනයක් බෙදා ගැනීමට ඉඩ සලසයි.

How NAT Works
NAT ක්‍රියා කරන ආකාරය

Devices inside the LAN are assigned private IP addresses which are not accessible over the internet.
LAN තුළ ඇති උපාංගවලට අන්තර්ජාලයට ප්‍රවේශ විය නොහැකි පුද්ගලික IP ලිපින පවරනු ලැබේ.

A device in a private network (e.g. 10.0.0.1) sends a request to access the internet.
පුද්ගලික ජාලයක ඇති උපාංගයක් (උදාහරණයක් ලෙස - IP ලිපිනය: 10.0.0.1) අන්තර්ජාලයට පිවිසීමට ඉල්ලීමක් යවයි.

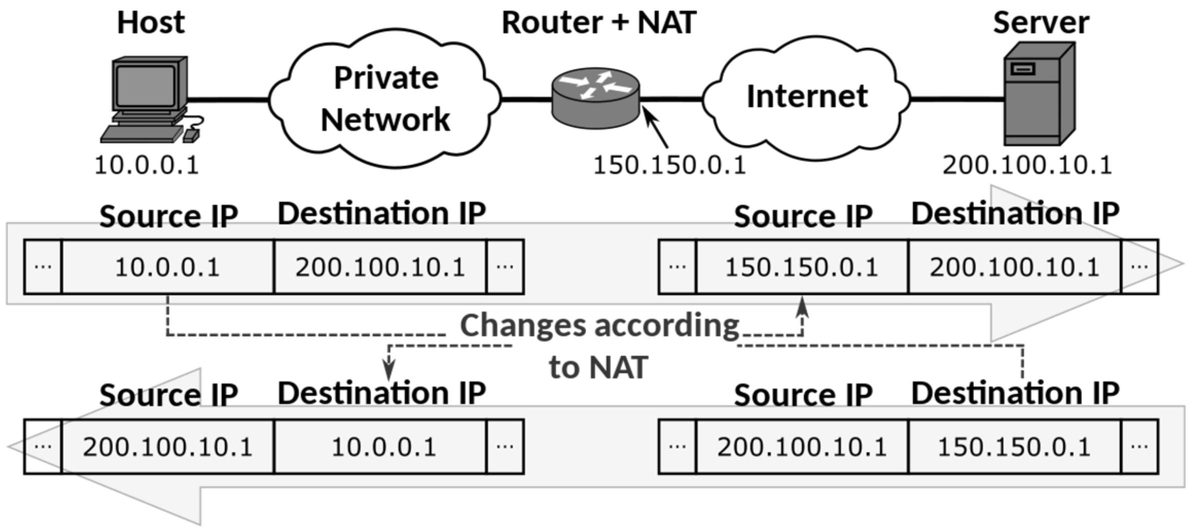
The router (with NAT enabled) replaces the private IP with its public IP address (e.g., 150.150.0.1).
NAT සක්‍රීය කර ඇති රවුටරය, එම උපාංගයේ පුද්ගලික IP ලිපිනය ඉවත් කර, ඒ වෙනුවට රවුටරයට අයත් පොදු IP ලිපිනය (උදා: 150.150.0.1) එයට ඇතුළත් කරයි.

The router keeps a NAT table to remember which internal device made the request.
අභ්‍යන්තරව සිටි කුමන උපාංගයද මෙම ඉල්ලීම සිදු කළේ යන්න මතක තබා ගැනීම සඳහා රවුටරය විසින් NAT වගුවක් පවත්වාගෙන යනු ලබයි.

Once the request reaches the destination server, the server sends a response back to the router's public IP.
ඉල්ලීම ගමනාන්ත සේවාදායකය වෙත ළඟා වූ පසු, සේවාදායකය රවුටරයේ පොදු IP වෙත ප්‍රතිචාරයක් යවයි.

When the response comes back from the internet (e.g. 200.100.10.1), the router checks the NAT table.
අන්තර්ජාලයෙන් අදාළ වෙබ් අඩවියේ දත්ත (උදාහරණයක් ලෙස - IP ලිපිනය: 200.100.10.1) රවුටරය වෙත ආපසු පැමිණි විට, රවුටරය සිය NAT වගුව පරීක්ෂා කර බලයි.

It then forwards the response to the correct private IP inside the network.
ඉන්පසු රවුටරය විසින් එම දත්ත ජාලය තුළ ඇති නිවැරදි පුද්ගලික IP ලිපිනය (ඉල්ලීම කල පරිගණකය) වෙතම යොමු කරනු ලබයි.



Advantages of NAT
NAT හි වාසි

IP Address Conservation
IP ලිපින පරිවර්තනය

NAT helps conserve public IP addresses, as one public IP can be used by many devices inside the private network.

NAT පොදු IP ලිපින සංරක්ෂණය කිරීමට උපකාර කරයි, මන්ද එක් පොදු IP ලිපිනයක් පුද්ගලික ජාලය තුළ බොහෝ උපාංග සඳහා භාවිතා කළ හැක.

Added Security
අතිරේක ආරක්ෂාව

By hiding the private IP addresses of internal devices, NAT prevents direct access from outside, adding a layer of protection against certain types of attacks.

අභ්‍යන්තර උපාංගවල පුද්ගලික IP ලිපින සඟවා තැබීමෙන්, NAT මගින් ඇතැම් ප්‍රහාරවලට එරෙහිව ආරක්ෂණ ස්ථරයක් එක් කරමින් බාහිරින් සිදු වන සෘජු ප්‍රවේශය වළක්වයි.

Reduces Cost
පිරිවැය අඩු කරයි

Organizations do not need a public IP address for every device.

සංවිධානවලට ඔවුන් සතු සෑම උපාංගයක් සඳහාම පොදු IP ලිපිනයක් තිබීම අවශ්‍ය නොවේ.

Supports Private Networks
පෞද්ගලික ජාල සඳහා සහය දක්වයි

Devices can use private IP addresses internally while still accessing the Internet.

උපාංගවලට අභ්‍යන්තරව පෞද්ගලික IP ලිපින භාවිතා කරමින් වුවද, බාහිරව අන්තර්ජාලයට පිවිසීමේ හැකියාව පවතී.

Simplifies Network Management
ජාල කළමනාකරණය සරල කරයි

Internal IP addressing can be changed without affecting external connectivity.

බාහිර සන්නිවේදනයට හෝ සබැඳියාවට කිසිදු බලපෑමක් නොකර, ජාලයේ අභ්‍යන්තර IP ලිපින වෙනස් කිරීමට හැකියාව ඇත.

Proxy Servers
නියෝජන සේවාදායක

A proxy server acts as an intermediary between client devices (such as computers, smartphones, or other network devices) and the internet.

නියෝජන සේවාදායකයක් සේවාලාභී උපාංග (පරිගණක, ස්මාර්ට් ෆෝන් හෝ වෙනත් ජාල උපාංග වැනි) සහ අන්තර්ජාලය අතර අතරමැදියෙකු ලෙස ක්‍රියා කරයි.

The main purpose of a proxy is to handle requests on behalf of the client and forward them to the appropriate destination on the internet.

නියෝජන සේවාදායකයක ප්‍රධාන අරමුණ වන්නේ සේවාලාභියා වෙනුවෙන් ඉල්ලීම් හසුරුවා ඒවා අන්තර්ජාලයේ සුදුසු ගමනාන්තයට යොමු කිරීමයි.

This can be situated inside & outside of a LAN

මෙය ස්ථානීය ප්‍රදේශ ජාලයක් ඇතුළත හෝ පිටත පිහිටුවිය හැක.

It acts as an application layer intermediary.

එය යෙදුම් ස්ථරයේ අතරමැදියෙකු ලෙස ක්‍රියා කරයි.

The proxy terminates the client connection, interprets the request, then opens a new connection to the destination on the client's behalf.

Proxy මඟින් සේවාලාභී සම්බන්ධතාවය අවසන් කර, ඉල්ලීම තේරුම් ගෙන, පසුව සේවාලාභියා වෙනුවෙන් ගමනාන්තය වෙත නව සම්බන්ධතාවයක් ආරම්භ කරයි.

Proxies can cache frequently requested content, reducing bandwidth usage and improving response times.

Proxies මඟින් නිතර ඉල්ලා සිටින අන්තර්ගතයන් කැෂ් කර තබා ගත හැකි අතර, එමඟින් කලාප පළල භාවිතය අඩු කර ප්‍රතිචාර දැක්වීමේ කාලය වැඩි දියුණු කරයි.

NAT vs. Proxy vs. VPN

Feature	NAT	Proxy	VPN
OSI Layer	L3	L7	L3/L2
Connection Termination	No	Yes	No
Protocol Awareness	None	Full	None
Encryption	No	Optional	Yes
Scope	All traffic	Per-application	All traffic
Primary Use	IP conservation	Filtering/caching	Privacy/remote access

Internal Proxy Server
අභ්‍යන්තර නියෝජන සේවාදායකය

An internal proxy server is a proxy located inside an organization's LAN that provides proxy services to internal users or internal applications.
අභ්‍යන්තර නියෝජන සේවාදායකයක් යනු සංවිධානයක LAN (දේශීය ජාලය) එකක් තුළ පිහිටා ඇති, එහි සිටින අභ්‍යන්තර පරිශීලකයින්ට හෝ අභ්‍යන්තර යෙදුම් සඳහා ප්‍රොක්සි සේවා සපයන සේවාදායකයකි.

Main functions / ප්‍රධාන කාර්යයන්

Controls users' access to Internet resources.
අන්තර්ජාල සම්පත් වෙත පරිශීලකයින්ට ඇති ප්‍රවේශය පාලනය කිරීම.

Authenticates users before allowing access.
ප්‍රවේශ වීමට ඉඩ දීමට පෙර පරිශීලකයින්ගේ අනන්‍යතාවය තහවුරු කිරීම.

Filters websites and content.
වෙබ් අඩවි සහ අන්තර්ගතයන් Filter කිරීම.

Monitors and logs user activity.
පරිශීලක ක්‍රියාකාරකම් නිරීක්ෂණය කිරීම සහ ඒවා සටහන් කර තබා ගැනීම.

Caches frequently accessed web pages to reduce bandwidth usage.
කළාප පළල භාවිතය අවම කිරීම සඳහා නිතර පිවිසෙන වෙබ් පිටු තාවකාලිකව ගබඩා කර (Cache කර) තබා ගැනීම.

Hides internal client IP addresses from external servers.
බාහිර සර්වර් වලින් අභ්‍යන්තර පරිශීලකයින්ගේ (IP) ලිපින සැඟවීම.

Examples: School, office, or university proxy server.

External Proxy Server
බාහිර නියෝජන සේවාදායකය

An external proxy server is a proxy server located outside an organization's LAN, usually on the Internet or operated by a third-party service provider.
බාහිර නියෝජන සේවාදායකයක් යනු සාමාන්‍යයෙන් අන්තර්ජාලයෙහි පිහිටි හෝ තෙවන පාර්ශවීය සේවා සපයන්නෙකු විසින් ක්‍රියාත්මක කරනු ලබන, සංවිධානයක LAN (දේශීය ජාලය) එකෙන් බාහිරව පිහිටා ඇති ප්‍රොක්සි සේවාදායකයකි.

Main functions / ප්‍රධාන කාර්යයන්

Hides the client's public IP address from external websites.
බාහිර වෙබ් අඩවි වලින් සේවාලාභියාගේ පොදු IP ලිපිනය සඟවයි.

Allows access to region-restricted or blocked online content (where permitted).
කලාපීයව සීමා කරන ලද හෝ අවහිර කරන ලද අන්තර්ජාල අන්තර්ගතයන් වෙත ප්‍රවේශ වීමට ඉඩ සලසයි (අවසර දී ඇති ස්ථානවලදී).

Routes internet traffic through servers in different geographic locations.
විවිධ භූගෝලීය පිහිටීම්වල ඇති සර්වර් හරහා අන්තර්ජාල ගමනාගමනය යොමු කරයි.

Distributes outgoing requests across multiple public IP addresses to reduce the chance of rate limiting.
වේග සීමා කිරීම් සිදුවීමේ සම්භාවිතාව අඩු කිරීම සඳහා, පිටතට යන ඉල්ලීම් පොදු IP ලිපින කිහිපයක් අතර බෙදා හරිනු ලබයි.

Examples: Cloud proxy services, public proxy servers, VPN provider proxy gateways.

Internal vs. External Proxy

Feature **ලක්ෂණය**	**Internal Proxy** **අභ්‍යන්තර නියෝජන සේවාදායකය**	**External Proxy** **බාහිර නියෝජන සේවාදායකය**
Location **ස්ථානය**	Inside the LAN LAN (දේශීය ජාලය) තුළ	Outside the LAN / cloud LAN එකෙන් පිටත (Cloud)
Primary Use **ප්‍රධාන භාවිතය**	Content filtering, caching, monitoring අන්තර්ගතය මතක තබා ගැනීම, නිරීක්ෂණය කිරීම	Anonymity, bypassing restrictions නිර්නාමිකභාවය, සීමාවන් මඟ හැරීම
Who Controls It **පාලනය**	Organization ආයතනය	Third-party provider තෙවන පාර්ශවීය සැපයුම්කරු
Typical Users **සාමාන්‍ය පරිශීලකයින්**	Employees within a network ජාලයක් තුළ සිටින සේවකයින්	Individual or remote users තනි පුද්ගල හෝ දුරස්ථ පරිශීලකයින්

How a Proxy Server Works
නියෝජන සේවාදායකයක් ක්‍රියා කරන ආකාරය

A client sends a request (such as a web page request) to the proxy server instead of directly to the internet.
සේවාලාභියෙකු සෘජුවම අන්තර්ජාලයට නොව නියෝජන සේවාදායකයට ඉල්ලීමක් (වෙබ් පිටු ඉල්ලීමක් වැනි) යවයි.

The proxy server processes the request, sends it to the destination server, and receives the response.
නියෝජන සේවාදායකය ඉල්ලීම ක්‍රියාවට නංවා එය ගමනාන්ත සේවාදායකයට යවා ප්‍රතිචාරය ලබා ගනී.

The response is then forwarded back to the client.
එවිට ප්‍රතිචාරය සේවාලාභියා වෙත ආපසු යවනු ලැබේ.

This indirect connection allows the proxy to handle various functions, including security, content filtering, logging, and caching.
මෙම වක්‍ර සම්බන්ධතාවය නියෝජනයට ආරක්ෂාව, අන්තර්ගත පෙරීම, ලොග් වීම සහ නිහිත කිරීම ඇතුළු විවිධ කාර්යයන් හැසිරවීමට ඉඩ සලසයි.

More functions of a Proxy Server
නියෝජන සේවාදායකයක කාර්යයන්

Helps multiple devices share internet access while managing IP addresses efficiently.
IP ලිපින කාර්යක්ෂමව කළමනාකරණය කරන අතරතුර, උපාංග කිහිපයකට එකම අන්තර්ජාල සබැඳියාව බෙදාහදා ගැනීමට (Share කර ගැනීමට) උපකාරී වේ.

Limits or prioritizes network traffic to improve performance.
ජාලයේ සමස්ත ක්‍රියාකාරීත්වය සහ වේගය වැඩි දියුණු කිරීම සඳහා, අන්තර්ජාල දත්ත ගමනාගමනය සීමා කිරීම හෝ ප්‍රමුඛතා ලබා දීම සිදු කරයි.

Distributes requests among multiple servers to prevent overload.
කිසියම් සර්වර් එකක් මත අධික තදබදයක් හෝ පීඩනයක් (Overload) ඇතිවීම වැළැක්වීම සඳහා, පරිශීලකයන්ගෙන් ලැබෙන ඉල්ලීම් සර්වර් කිහිපයක් අතර සමව බෙදා හරිනු ලබයි.

Compresses web content to reduce bandwidth usage.
අන්තර්ජාල දත්ත භාවිතය අවම කරගැනීම සඳහා, වෙබ් අඩවිවල ඇති දත්ත කුඩා කර පෙන්වයි.

Inspects traffic for malicious content before it reaches users.
අන්තර්ජාල දත්ත පරිශීලකයා වෙත ළඟා වීමට පෙර, ඒවායේ අහිතකර වෛරස් හෝ අනිෂ්ට මෘදුකාංග අඩංගු දැයි පරීක්ෂා කර බලයි.

Modern networking devices often combine multiple network functions, allowing routers and firewalls to perform proxy server operations in addition to their primary roles.
නූතන ජාලකරණ උපාංග බොහෝ විට ජාලකරණ කාර්යයන් කිහිපයක් එකට ඒකාබද්ධ කර ඇත. මේ නිසා routers සහ firewalls වලට ඒවායේ ප්‍රධාන කාර්යභාරයන්ට අමතරව ප්‍රොක්සි සර්වර් ක්‍රියාවලීන් ද සිදු කිරීමට හැකියාව ලැබී ඇත.

How Firewalls, Routers, and Proxies Differ

Firewalls inspect packets and filter or forward them based on predefined rules, controlling traffic flow and blocking unauthorized access.
Firewalls කල්තියා නිර්වචනය කරන ලද රීති මත පදනම්ව පැකට්ටු පරීක්ෂා කර ඒවා පෙරීම හෝ ඉදිරියට යැවීම සිදු කරයි, එමඟින් දත්ත ගමනාගමන ප්‍රවාහය පාලනය කර අනවසර ප්‍රවේශයන් අවහිර කරයි.

Routers are responsible for directing traffic between networks. Routers perform Network Address Translation (NAT) (mapping private IP addresses to public ones) rather than proxying.
රවුටර ජාල අතර දත්ත ගමනාගමනය මෙහෙයවීමට වගකිව යුතුය. රවුටර මඟින් ප්‍රොක්සි කිරීම වෙනුවට ජාල ලිපින පරිවර්තනය (NAT) (පුද්ගලික IP ලිපින පොදු ඒවා බවට පත් කිරීම) සිදු කරයි.

Proxies terminate the client connection, interpret the request, and open a new connection to the destination on the client's behalf, acting as an active intermediary rather than simply passing traffic through.
පරිශීලකයාගේ සම්බන්ධතාවය අවසන් කර, ඉල්ලීම විශ්ලේෂණය කර, පරිශීලකයා වෙනුවෙන් ගමනාන්තය වෙත නව සම්බන්ධතාවයක් ගොඩනඟයි. එමඟින් දත්ත ගමනාගමනය නිකම්ම ඉදිරියට යවනවා වෙනුවට සක්‍රීය අතරමැදියෙකු ලෙස ක්‍රියා කරයි.

ictfromabc.com

Types of Networks
ජාල වර්ග

Type	Coverage / ආවරණය
PAN	~10 m Around a single person එක් පුද්ගලයෙකු වටා (e.g. Bluetooth, USB)
LAN	~100 m A home, office, or single building නිවසක්, කාර්යාලයක් හෝ එක් ගොඩනැගිල්ලක්
CAN	~1 km A university or corporate campus විශ්වවිද්‍යාලයක් හෝ ආයතනික පරිශ්‍රයක්
MAN	~10–50 km A city or town / නගරයක්
WAN	Global Across countries (e.g. the Internet) රටවල් හරහා (උදා. අන්තර්ජාලය)

Personal Area Network (PAN)
පෞද්ගලික පෙදෙස් ජාල

A PAN is the smallest type of network, primarily used for connecting personal devices like smartphones, tablets, laptops, and wearable devices within a very short range.
PAN යනු කුඩාම ජාල වර්ගය වන අතර, මූලික වශයෙන් ස්මාර්ට් ෆෝන්, ටැබ්ලට්, ලැප්ටොප්, සහ පැළඳිය හැකි උපාංග වැනි පුද්ගලික උපාංග ඉතා කෙටි පරාසයක් තුළ සම්බන්ධ කිරීම සඳහා භාවිතා කරයි.

Owned by one person.
එක් පුද්ගලයෙකුට අයත් වේ.

Local Area Network (LAN)
ස්ථානීය පෙදෙස් ජාල

A LAN is used to connect devices in a small geographic area, like a home, office, or building.
නිවසක්, කාර්යාලයක් හෝ ගොඩනැගිල්ලක් වැනි කුඩා භූගෝලීය ප්‍රදේශයක උපාංග සම්බන්ධ කිරීමට LAN භාවිතා කරයි.

Owned by one person or one organization.
එක් පුද්ගලයෙකුට හෝ එක් සංවිධානයකට අයත් වේ.

Campus Area Network (CAN)
ආයතනික පෙදෙස් ජාල

A CAN is similar to a LAN but typically covers a larger area like a school, university campus, or a business campus. It connects multiple buildings and departments.
CAN එකක් LAN එකකට සමාන නමුත් සාමාන්‍යයෙන් පාසලක්, විශ්ව විද්‍යාල මණ්ඩපයක් හෝ ව්‍යාපාරික මණ්ඩපයක් වැනි විශාල ප්‍රදේශයක් ආවරණය කරයි. එය බහු ගොඩනැගිලි සහ දෙපාර්තමේන්තු සම්බන්ධ කරයි.

Owned by one organization.
එක් සංවිධානයකට අයත් වේ.

Metropolitan Area Network (MAN)
මහා නගර පෙදෙස් ජාල

A MAN covers a larger geographic area than a LAN but is smaller than a Wide Area Network (WAN).
MAN එකක් LAN එකකට වඩා විශාල භූගෝලීය ප්‍රදේශයක් ආවරණය කරන නමුත් පුළුල් පෙදෙස් ජාලයකට (WAN) වඩා කුඩා වේ.

It spans across a city and is typically used by government or large organizations to interconnect multiple LANs within a city.
එය නගරයක් හරහා විහිදෙන අතර සාමාන්‍යයෙන් රජය හෝ විශාල සංවිධාන විසින් නගරයක් තුළ LAN කිහිපයක් එකිනෙක සම්බන්ධ කිරීමට භාවිතා කරයි.

Many MANs involve a network service provider.
බොහෝ MAN ජාල සඳහා ජාල සේවා සපයන්නෙකු සම්බන්ධ වේ.

MANs may be owned by multiple organizations that are connected together.
ඒවා එකට සම්බන්ධ කර ඇති බහුවිධ සංවිධාන කිහිපයකට අයත් විය හැකිය.

Wide Area Network (WAN)
පුළුල් ප්‍රදේශ ජාලය

A WAN covers a broad geographic area, such as an entire country or even globally. It interconnects multiple LANs, MANs, and other smaller networks.
WAN මගින් මුළු රටක් හෝ ගෝලීය වශයෙන් පවා පුළුල් භූගෝලීය ප්‍රදේශයක් ආවරණය කරයි. එය බහු LANs, MANs, සහ අනෙකුත් කුඩා ජාල එකිනෙකට සම්බන්ධ කරයි.

The internet is the largest example of a WAN.
අන්තර්ජාලය WAN සඳහා විශාලතම උදාහරණයයි.

Can cover large geographic distances, from multiple cities to across countries and continents.
විවිධ නගරවල සිට රටවල් සහ මහාද්වීප දක්වා විශාල භූගෝලීය දුරක් ආවරණය කළ හැකිය.

Often involves several network service providers.
බොහෝ විට ජාල සේවා සපයන්නන් කිහිප දෙනෙකු සම්බන්ධ වේ.

Owned by multiple organizations.
බහුවිධ සංවිධාන කිහිපයකට අයත් වේ.

Wired & Wireless Implementation Across Network Types
ජාල වර්ග සඳහා රැහැන් සහිත සහ රැහැන් රහිත ක්‍රියාත්මක කිරීම්

Networks are not restricted to a single transmission medium, whether it is a LAN, MAN, or WAN, each can be implemented using wired, wireless, or a hybrid of both methods, depending on the needs of the environment.
ජාල, එක් සම්ප්‍රේෂණ මාධ්‍යයකට පමණක් සීමා නොවේ. එය LAN, MAN හෝ WAN වුවද, පරිසරයේ අවශ්‍යතා මත පදනම්ව රැහැන් සහිත, රැහැන් රහිත හෝ මෙම ක්‍රම දෙකෙහිම දෙමුහුන් එකතුවක් භාවිතයෙන් ක්‍රියාත්මක කළ හැකිය.

A PAN can be wired through a direct USB or lightning cable connection between personal devices, or wireless via Bluetooth, infrared, or Airdrop, commonly seen in connecting phones, laptops, smartwatches, and earbuds.
PAN එකක්, පුද්ගලික උපාංග අතර සෘජු USB හෝ lightning කේබල් සම්බන්ධතාවයක් හරහා රැහැන් සහිතව හෝ Bluetooth, infrared හෝ Airdrop හරහා රැහැන් රහිතව ක්‍රියාත්මක කළ හැකිය. මෙය සාමාන්‍යයෙන් දුරකථන, ලැප්ටොප්, ස්මාර්ට් ඔරලෝසු සහ earbuds සම්බන්ධ කිරීමේදී දැකිය හැකිය.

A LAN can run over Ethernet cables or operate entirely over Wi-Fi as a WLAN, with most modern setups combining both.
LAN එකක් ඊතර්නෙට් කේබල් හරහා ධාවනය විය හැකි අතර, නැතහොත් WLAN එකක් ලෙස සම්පූර්ණයෙන්ම Wi-Fi හරහා ක්‍රියාත්මක විය හැකිය. බොහෝ නවීන සැකසුම් තුළ මෙම ක්‍රම දෙකම ඒකාබද්ධව පවතී.

A MAN can be built using fiber optic cables connecting buildings across a city, or wirelessly using microwave links and WiMAX towers between locations.
MAN එකක්, නගරයක් පුරා ඇති ගොඩනැගිලි සම්බන්ධ කරන ෆයිබර් ඔප්ටික් කේබල් භාවිතයෙන් හෝ ස්ථාන අතර මයික්‍රෝවේව් සබැඳි සහ WiMAX කුළුණු භාවිතයෙන් රැහැන් රහිතව ගොඩනැගිය හැකිය.

A WAN can be established through physical infrastructure like undersea fiber optic cables and leased lines, or wirelessly via satellite links and cellular networks such as 4G/5G.
WAN එකක්, මුහුදු පතුල හරහා දිවෙන ෆයිබර් ඔප්ටික් කේබල් සහ බදු ගත් මාර්ග වැනි භෞතික යටිතල පහසුකම් හරහා හෝ චන්ද්‍රිකා සබැඳි සහ 4G/5G වැනි සෙලියුලර් ජාල හරහා රැහැන් රහිතව ස්ථාපිත කළ හැකිය.

In essence, the terms LAN, MAN, and WAN define the scope of a network, not its medium. The choice between wired and wireless is purely an implementation decision driven by factors like cost, mobility, reliability, and coverage.
මූලික වශයෙන් ගත් කල, LAN, MAN සහ WAN යන පද මගින් අර්ථ දැක්වෙන්නේ ජාලයක විෂය පථය මිස එහි මාධ්‍යය නොවේ. රැහැන් සහිත සහ රැහැන් රහිත ක්‍රම අතර තේරීම, පිරිවැය, සංචලතාව, විශ්වසනීයත්වය සහ ආවරණය වැනි සාධක මත පදනම් වූ තීරණයක් පමණි.

Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a technology that creates a secure and encrypted connection over a public or less secure network, such as the internet.
අතත්‍ය පුද්ගලික ජාල යනු අන්තර්ජාලය වැනි පොදු හෝ අඩු ආරක්ෂිත ජාලයක් හරහා ආරක්ෂිත සහ සංකේතාත්මක සම්බන්ධතාවයක් නිර්මාණය කරන තාක්ෂණයකි.

It allows users to send and receive data as if their devices were directly connected to a private network, ensuring data privacy and security.
එය පරිශීලකයින්ට ඔවුන්ගේ උපාංග පුද්ගලික ජාලයකට සෘජුවම සම්බන්ධ වී ඇති ආකාරයට දත්ත යැවීමට සහ ලබා ගැනීමට ඉඩ සලසයි, දත්ත පෞද්ගලිකත්වය සහ ආරක්ෂාව සහතික කරයි.

Components of a VPN
VPN සංරචක

VPN Client

The software or application on the user's device that connects to the VPN server. It encrypts data before sending it over the internet.

VPN) සේවාදායකයට සම්බන්ධ වන පරිශීලකයාගේ උපාංගයේ ඇති මෘදුකාංගය හෝ යෙදුම වේ. එය අන්තර්ජාලය හරහා දත්ත යැවීමට පෙර ඒවා කේතනය කරයි.

VPN Server

A remote server that receives the encrypted data from the client, decrypts it, and forwards it to the desired destination (Ex. a company's internal network or a website).

සේවාලාභියාගෙන් කේතනය කළ දත්ත ලබා ගන්නා දුරස්ථ සේවාදායකයකි, එමගින් එම දත්ත විකේතනය කර අපේක්ෂිත ගමනාන්තය වෙත යොමු කරයි (උදා. සමාගමක අභ්‍යන්තර ජාලයක් හෝ වෙබ් අඩවියක්).

Tunnel

The secure, encrypted pathway through which data travels between the client and server. This "tunneling" ensures privacy and security over public networks.

සේවාලාභියා සහ සේවාදායකයා අතර දත්ත ගමන් කරන ආරක්ෂිත, කේතිත මාර්ගයයි. මෙම මාර්ගය පොදු ජාල හරහා පුද්ගලිකත්වය සහ ආරක්ෂාව සහතික කරයි.

How VPN Works
VPN ක්‍රියා කරන ආකාරය

Initiating a VPN Connection

A user (client) starts a VPN connection through a VPN client, which could be an app or built-in software.

පරිශීලකයෙකු (සේවාලාභියෙකු) VPN සේවාලාභියෙක් හරහා VPN සම්බන්ධතාවයක් ආරම්භ කරයි, එය යෙදුමක් හෝ built-in මෘදුකාංගයක් විය හැකිය.

Encryption of Data

The VPN client encrypts the user's data before it leaves the device. This encrypted data is now unreadable to any unauthorized party.

VPN සේවාලාභියා විසින් පරිශීලකයාගේ දත්ත උපාංගයෙන් පිටවීමට පෙර කේතනය කරයි. මෙම කේතාත්මක දත්ත දැන් කිසිදු අනවසර පාර්ශවයකට කියවිය නොහැක.

Routing Through the VPN Server

The encrypted data is sent over the internet to the VPN server. This server acts as an intermediary, forwarding the user's requests to the intended destination (Ex. a website).

කේතනය කළ දත්ත අන්තර්ජාලය හරහා VPN සේවාදායකය වෙත යවනු ලැබේ. මෙම සේවාදායකය පරිශීලකයාගේ ඉල්ලීම් අපේක්ෂිත ගමනාන්තයට (උදා. වෙබ් අඩවියක්) යොමු කරමින් අතරමැදියෙකු ලෙස ක්‍රියා කරයි.

Data Forwarding

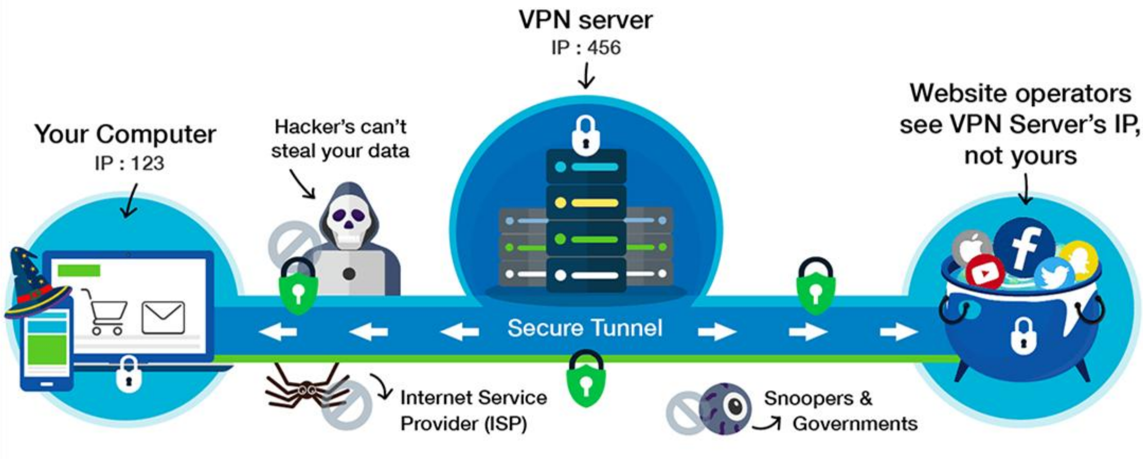
The VPN server decrypts the data and sends the request to the destination. When the destination responds, the VPN server encrypts the response and sends it back to the client.

VPN සේවාදායකය දත්ත විකේතනය කර ගමනාන්තයට ඉල්ලීම යවයි. ගමනාන්තය මගින් ප්‍රතිචාර දක්වන විට, VPN සේවාදායකය ප්‍රතිචාරය කේතනය කර සේවාලාභියා වෙත ආපසු යවයි.

Final Decryption at Client Side

The client receives the encrypted data from the VPN server, decrypts it, and presents it to the user as normal.

සේවාලාභියා විසින් VPN සේවාදායකයෙන් කේතාත්මක දත්ත ලබා ගනී, එය විකේතනය කර සාමාන්‍ය ආකාරයෙන් පරිශීලකයාට ඉදිරිපත් කරයි.



How VPNs hide our IP address
VPNs මගින් අපගේ IP ලිපිනය සඟවන ආකාරය

VPN server acts as a proxy to hide users IP address.
පරිශීලකයාගේ IP ලිපිනය සැඟවීම සඳහා VPN සේවාදායකය ප්‍රොක්සියක් (proxy) ලෙස ක්‍රියා කරයි.

For example, if you connect to a VPN server located in New York, your device will appear to have an IP address based in New York, even if you are physically located elsewhere.
උදාහරණයක් ලෙස, ඔබ නිව් යෝර්ක් හි පිහිටා ඇති VPN සේවාදායකයකට සම්බන්ධ වන්නේ නම්, ඔබ භෞතිකව වෙනත් ස්ථානයක සිටියත්, ඔබගේ උපාංගයට නිව් යෝර්ක් හි IP ලිපිනයක් ඇති බව පෙනේ.

Throughout this process, websites and online services only see the VPN server's IP address and location, not your actual IP address.
මෙම ක්‍රියාවලිය පුරාම, වෙබ් අඩවි සහ සබැඳි සේවා දකින්නේ VPN සේවාදායකයේ IP ලිපිනය සහ ස්ථානය මිස ඔබේ සැබෑ IP ලිපිනය නොවේ.

Example

Let's say you are in London, and you connect to a VPN server in New York.
ඔබ ලන්ඩන් හී සිටින බවත් නිව් යෝර්ක් හි VPN සේවාදායකයකට සම්බන්ධ වන බවත් සිතමු.

Your real IP address (in London) 82.45.123.67.

VPN server's IP address (in New York) 192.168.1.2.

Once connected to the VPN,

Before VPN
Websites see your real IP (82.45.123.67), and they know you are in London.
වෙබ් අඩවි මගින් ඔබේ සැබෑ IP ලිපිනය (82.45.123.67) දකින අතර, ඔබ ලන්ඩන් හී සිටින බව ඔවුන් දනී.

After VPN
Websites see the VPN server's IP (192.168.1.2), and they think you are in New York.
වෙබ් අඩවි VPN සේවාදායකයේ IP ලිපිනය (192.168.1.2) දකින අතර, ඔවුන් සිතන්නේ ඔබ නිව් යෝර්ක්හි සිටින බවයි.

Feature	**VPN**	**Proxy**
Operating Level **ක්‍රියාකාරී මට්ටම**	Entire device or selected applications. සමස්ත උපාංගයම හෝ තෝරාගත් යෙදුම්	Usually, specific applications or browsers. සාමාන්‍යයෙන් නිශ්චිත යෙදුම් හෝ බ්‍රවුසර
Encrypts Traffic **ගමනාගමනය සංකේතනය කිරීම**	Yes / ඔව්	Usually No සාමාන්‍යයෙන් නැත
Privacy **පුද්ගලිකත්වය**	High / ඉහළයි	Low to Moderate අඩු සිට මධ්‍යස්:
Hides IP Address **IP ලිපිනය සැඟවීම**	Yes / ඔව්	Yes / ඔව්
Protects on Public Wi-Fi **පොදු (උස-පස) ජාලවලදී ආරක්ෂා කිරීම**	Yes / ඔව්	No / නැත
Speed **වේගය**	Slightly slower. තරමක් මන්දගාමී වේ	Usually faster. සාමාන්‍යයෙන් වේගවත් වේ
Security **ආරක්ෂාව**	High / ඉහළයි	Low / අඩුයි
Setup **පිහිටුවීම**	Requires VPN software or built-in OS support. VPN මෘදුකාංග හෝ මෙහෙයුම් පද්ධතියේ ඇති සහය අවශ්‍ය වේ	Browser or application proxy settings. බ්‍රවුසරයේ හෝ යෙදුමේ ප්‍රොක්සි සැකසුම්
Cost **පිරිවැය**	Often paid (free options available). බොහෝ විට ගෙවීම් කළ යුතුය (නොමිලේ ලැබෙන සංස්කරණ ද ඇත)	Often free (paid options also available). බොහෝ විට නොමිලේ (ගෙවීම් කළ යුතු සංස්කරණ ද ඇත)

Networking Commands
ජාලකරණ විධාන

Networking commands are instructions used in a command-line interface to check, manage, and troubleshoot network connections.
ජාලකරණ විධාන යනු ජාල සම්බන්ධතා පරීක්ෂා කිරීම, කළමනාකරණය කිරීම සහ දෝෂ නිරාකරණය කිරීම සඳහා විධාන රේඛා අතුරුමුහුණතක භාවිතා කරන උපදෙස් වේ.

They help users find network details, test whether devices are connected, identify connection problems, and view information such as IP addresses, routes, and active connections.
ඒවා මඟින් පරිශීලකයින්ට ජාල විස්තර සෙවීමට, උපාංග සම්බන්ධ වී ඇත්දැයි පරීක්ෂා කිරීමට, සම්බන්ධතා ගැටලු හඳුනා ගැනීමට සහ IP ලිපින, මාර්ග (routes) සහ සක්‍රිය සම්බන්ධතා වැනි තොරතුරු බැලීමට උපකාරී වේ.

1) `ipconfig`

This command displays the IP address, subnet mask, and default gateway for all network adapters on your computer. Useful for troubleshooting network issues.
මෙම විධානය මඟින් ඔබේ පරිගණකයේ ඇති සියලුම ජාල ඇඩැප්ටර සඳහා IP ලිපිනය, උපජාල මාස්ක් සහ පෙරනිමි ද්වාරය පෙන්වයි. ජාල ගැටළු නිරාකරණය සඳහා ප්‍රයොජනවත් වේ.

Platforms

`ipconfig` - Windows
`ifconfig` - macOS, Linux (BSD systems)
`ip addr` - Linux (Modern)

Information it shows
එයින් දැනගත හැකි තොරතුරු

IPv4 Address
The unique address identifying this device on the local network
දේශීය ජාලය තුළ මෙම උපාංගය හඳුනා ගන්නා අනන්‍ය ලිපිනය

Subnet Mask
Defines which part of the IP address is the network vs the device
IP ලිපිනයේ කුමන කොටස ජාලයට ද සහ කුමන කොටස උපාංගයට ද යන්න නිර්වචනය කරයි

Default Gateway
The IP address of the router. (the doorway to the internet)
රවුටරයේ IP ලිපිනය. (අන්තර්ජාලයට පිවිසෙන දොරටුව)

Purpose / අරමුණ
It quickly confirms whether a computer is connected to a network and shows its currently assigned IP address.
එය පරිගණකයක් ජාලයකට සම්බන්ධ වී ඇත්දැයි ඉක්මනින් තහවුරු කරන අතර දැනට ඊට පවරා ඇති IP ලිපිනය පෙන්වයි.

Example (Windows)

```
> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
 Connection-specific DNS Suffix  . : localdomain
 IPv4 Address. . . . . . . . . . . : 192.168.1.105
 Subnet Mask . . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . . : 192.168.1.1
```

Useful Variations / ප්‍රයෝජනවත් ප්‍රභේදයන්

`ipconfig /release`
Drops the current IP address assigned by the router
රවුටරය මඟින් පවරා ඇති වත්මන් IP ලිපිනය ඉවත් කරයි

`ipconfig /renew`
Requests a new IP address from the router
රවුටරයෙන් නව IP ලිපිනයක් ඉල්ලා සිටියි

`ipconfig /flushdns`
Clears the saved list of website addresses (fixes some browsing issues)
සුරකින ලද වෙබ් අඩවි ලිපින ලැයිස්තුව මකා දමයි (සමහර බ්‍රවුස් කිරීමේ ගැටලු නිරාකරණය කරයි)

`ipconfig /all` (detailed `ipconfig`)

The extended/detailed version of ipconfig. It shows everything the basic command shows, plus much more about every network adapter on the device.
ipconfig හි දීර්ඝ/විස්තරාත්මක අනුවාදය. එය මූලික විධානය මඟින් පෙන්වන සියල්ල සහ උපාංගයේ ඇති සෑම ජාල අනුවර්තකයක් ගැනම තවත් බොහෝ තොරතුරු පෙන්වයි.

Additional information it shows
එය පෙන්වන අතිරේක තොරතුරු

Host Name
The name of this computer on the network
ජාලය තුළ මෙම පරිගණකයේ නම

Physical Address (MAC)
A unique hardware ID burned into the network adapter
ජාල අනුවර්තකය තුළට ස්ථිරවම ඇතුළත් කර ඇති අනන්‍ය දෘඩාංග හැඳුනුම්පතක්

DHCP Enabled
Yes = IP was assigned automatically
IP ලිපිනය ස්වයංක්‍රීයව පවරා ඇත;
No = IP was set manually
IP ලිපිනය හස්තීයව සකසා ඇත

DHCP Server
The device (usually the router) that assigned the IP ලිපිනය පවරා දුන් උපාංගය (සාමාන්‍යයෙන් රවුටරය)

IPDNS Servers
Servers that translate website names into IP addresses
වෙබ් අඩවි නාම IP ලිපින බවට පරිවර්තනය කරන සේවාදායකයන්

Lease Obtained
When the current IP address was assigned
වත්මන් IP ලිපිනය පවරා දුන් දිනය සහ වේලාව

Lease Expires
When the router will reassign a new IP address
රවුටරය විසින් නව IP ලිපිනයක් නැවත පවරනු ලබන දිනය සහ වේලාව

Example (Windows)

```
> ipconfig /all

Windows IP Configuration
   Host Name . . . . . . . . . : DESKTOP-AB12CD
   Primary Dns Suffix  . . . . :
   Node Type . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . : No
   WINS Proxy Enabled. . . . . : No
Wireless LAN adapter Wi-Fi:

   Description . . . . : Intel(R) Wi-Fi 6 AX201
   Physical Address. . : A4-C3-F0-85-2D-11
   DHCP Enabled. . . . : Yes
   IPv4 Address. . . . : 192.168.1.105(Preferred)
   Subnet Mask . . . . : 255.255.255.0
   Lease Obtained. . . : July 1, 2026 8:00:00 AM
   Lease Expires . . . : July 2, 2026 8:00:00 AM
   Default Gateway . . : 192.168.1.1
   DHCP Server . . . . : 192.168.1.1
   DNS Servers . . . . : 8.8.8.8
                         8.8.4.4
```

2) `ping` (All Platforms)

Ping is a command used to test whether a connection exists between your computer and another device, website, or server on a network or the internet.
Ping යනු ඔබේ පරිගණකය සහ ජාලයක හෝ අන්තර්ජාලයෙහි ඇති වෙනත් උපාංගයක්, වෙබ් අඩවියක් හෝ සේවාදායකයක් අතර සම්බන්ධතාවයක් පවතීදැයි පරීක්ෂා කිරීමට භාවිතා කරන විධානයකි.

Purpose / අරමුණ
Check basic connectivity to a destination
සේවාදායකයකට ඇති මූලික සම්බන්ධතාවය පරීක්ෂා කිරීම
Measure how long it takes for data to travel there and back
දත්ත එහි ගොස් නැවත පැමිණීමට කොපමණ කාලයක් ගතවේද යන්න මැන බැලීම
Identify if a connection problem is general (no internet at all) or specific (one site not responding)
සම්බන්ධතා ගැටලුවක් පොදු එකක්ද (අන්තර්ජාලය කිසිසේත්ම නැත) හෝ නිශ්චිත එකක්ද (එක් වෙබ් අඩවියක් පමණක් ප්‍රතිචාර නොදක්වයි) යන්න හඳුනා ගැනීම

How it works / ක්‍රියා කරන ආකාරය
Your computer sends 4 small test messages (called echo requests) to the destination. If the destination is reachable, it sends a reply back. Ping records whether each reply was received and how long it took.
ඔබේ පරිගණකය මඟින් ළඟාවිය යුතු ස්ථානය වෙත කුඩා පරීක්ෂණ පණිවිඩ 4ක් (echo requests ලෙස හැඳින්වේ) යවයි. එම ස්ථානයට ළඟා විය හැකි නම්, එය නැවත පිළිතුරක් එවයි. Ping මඟින් එක් එක් පිළිතුර ලැබුණේද යන්න සහ ඒ සඳහා කොපමණ කාලයක් ගත වූයේද යන්න වාර්තා කරයි.

Example (Successful ping)

```
> ping google.com

PING google.com (142.250.80.46): 56 data bytes
64 bytes from 142.250.80.46: icmp_seq=0 ttl=116
time=12.4 ms
64 bytes from 142.250.80.46: icmp_seq=1 ttl=116
time=11.9 ms
64 bytes from 142.250.80.46: icmp_seq=2 ttl=116
time=12.1 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss
round-trip min/avg/max = 11.9/12.1/12.4 ms
```

Example (Failed ping)

```
> ping google.com

Pinging google.com with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 142.250.185.46:
Packets: Sent = 4, Received = 0, Lost = 4
```

3) `tracert`

Traces the path packets take from your machine to a destination, showing each router (hop) along the way and the latency at each hop.
ඔබගේ යන්ත්‍රයේ සිට ගමනාන්තයක් දක්වා පැකට් ගමන් කරන මාර්ගය ලුහුබඳින අතර, අතරමඟ ඇති එක් එක් රවුටරය (hop) සහ එම එක් එක් ස්ථානයේදී සිදුවන ප්‍රලම්භනය (latency) පෙන්වයි.

Useful for diagnosing where a connection slows down or fails.
සබඳතාවක් මන්දගාමී වන්නේ හෝ බිඳවැටෙන්නේ කොතැනදැයි හඳුනා ගැනීමට ප්‍රයෝජනවත් වේ.

Platforms

tracert - Windows
traceroute - macOS, Linux

Purpose / අරමුණ

- See every point (called a "hop") that data passes through on its way to a destination
  දත්ත ලඟාවිය යුතු ස්ථානය කරා යන ගමනේදී පසුකර යන සෑම ලක්ෂ්‍යයක්ම (hop එකක් ලෙස හැඳින්වේ) දැකබලා ගැනීම
- Identify exactly where in that path a problem or delay is happening
  එම මාර්ගයේ ගැටලුවක් හෝ ප්‍රමාදයක් සිදුවන්නේ කුමන ස්ථානයකදැයි හරියටම හඳුනා ගැනීම

How it works / ක්‍රියා කරන ආකාරය

Data traveling across the internet passes through multiple intermediate routers before reaching its destination.
අන්තර්ජාලය හරහා ගමන් කරන දත්ත එහි ලඟාවිය යුතු ස්ථානයට පැමිණීමට පෙර අතරමැදි රවුටර කිහිපයක් පසුකර යයි.

tracert sends test messages with progressively increasing limits, causing each router along the path to respond one at a time. Each response is one "hop" in the list.
tracert මගින් අනුක්‍රමිකව වැඩි වන සීමාවන් සහිත පරීක්ෂණ පණිවිඩ යවන අතර, එමගින් මාර්ගය දිගේ ඇති එක් එක් රවුටරය එකින් එක ප්‍රතිචාර දක්වයි. එක් එක් ප්‍රතිචාරය ලැයිස්තුවේ ඇති එක් hop එකක් වේ.

Example (Windows)

```
> tracert google.com

Tracing route to google.com [142.250.80.46] over a
maximum of 30 hops:

  1     1 ms     1 ms     1 ms   192.168.1.1
  2    10 ms     9 ms    10 ms   10.0.0.1
  3     *        *        *      72.14.215.165
  4    12 ms    12 ms    13 ms   142.250.80.46

Trace complete.
```

A `* * *` in the output means a hop didn't respond, often due to firewalls, not necessarily a problem.
ප්‍රතිදානයේ `* * *` ලෙස දැක්වීමෙන් අදහස් වන්නේ අදාළ රවුටරය (hop) ප්‍රතිචාර නොදැක්වූ බවයි. මෙය බොහෝ විට firewalls හේතුවෙන් සිදුවන අතර, එය අනිවාර්යයෙන්ම ගැටලුවක් නොවේ.

Useful Variations / ප්‍රයෝජනවත් ප්‍රභේදයන්

`tracert -d google.com`
Skips converting IP addresses to names (runs faster)
IP ලිපින නාමයන් බවට පරිවර්තනය කිරීම මඟහරියි (වේගයෙන් ක්‍රියාත්මක වේ)

`tracert -h 15 google.com`
Limits trace to a maximum of 15 hops
පරීක්ෂණ මාර්ගය උපරිම hops 15 කට සීමා කරයි

When it is used / භාවිතා කරනු ලබන අවස්ථා

- When ping confirms a problem but doesn't show where it is
  ping මඟින් ගැටලුවක් ඇති බව තහවුරු කරන නමුත් එය කොතැනදැයි පෙන්වන්නේ නැති විට
- When a site loads slowly and you want to know which part of the route is causing the delay
  වෙබ් අඩවියක් සෙමින් ක්‍රියාත්මක වන විට සහ එම මාර්ගයේ ප්‍රමාදයට හේතුවන කොටස කුමක්දැයි ඔබට දැන ගැනීමට අවශ්‍ය වූ විට
- To determine whether a problem is on your end or your ISP's end
  ගැටලුව පවතින්නේ ඔබේ පාර්ශවයෙන්ද නැතහොත් ඔබේ අන්තර්ජාල සේවා සපයන්නාගේ (ISP) පාර්ශවයෙන්ද යන්න තීරණය කිරීමට

4) `nslookup`

Queries DNS servers to resolve domain names to IP addresses (and vice versa). Useful for diagnosing DNS issues.
වසම් නාම IP ලිපින බවට (සහ එහි අනෙක් පැත්තට) හැරවීම සඳහා DNS සේවාදායකයන්ගෙන් විමසීම් කරයි. DNS ගැටලු හඳුනා ගැනීමට ප්‍රයෝජනවත් වේ.

Platforms
`nslookup` - Windows, macOS, Linux
`dig` - macOS, Linux

`dig` provides more detailed output than `nslookup` in macOS and Linux.
macOS සහ Linux වලදී `dig` මඟින් `nslookup` වලට වඩා සවිස්තරාත්මක ප්‍රතිදානයක් ලබා දෙයි.

Example

```
$ nslookup github.com

Server:   8.8.8.8
Address:  8.8.8.8#53

Non-authoritative answer:
Name:   github.com
Address: 140.82.121.4
```

5) `netstat` (All Platforms)

Displays active network connections, listening ports, routing tables, and network interface statistics. Great for seeing what services are listening and what connections are currently open.
ක්‍රියාකාරී ජාල සම්බන්ධතා, ක්‍රියාකාරී වදරව්, රවුටින් වගු සහ ජාල අතුරුමුහුණත් සංඛ්‍යාලේඛන පෙන්වයි. කුමන සේවාවන් සක්‍රීයව පවතින්නේද සහ දැනට විවෘතව ඇති සම්බන්ධතා මොනවාදැයි බැලීමට ඉතා හොඳය.

Example

```
> netstat

Active Internet connections (servers and established)
Proto  Local Address         Foreign Address     State
tcp    0.0.0.0:22            0.0.0.0:*           LISTEN
tcp    192.168.1.105:52341   140.82.121.4:443    ESTABLISHED
tcp    192.168.1.105:52355   142.250.80.46:443   ESTABLISHED
udp    0.0.0.0:53            0.0.0.0:*
```

6) `arp` (All Platforms)

Useful for finding the MAC address of a device on your local network, or for troubleshooting IP conflicts.
දේශීය ජාලයේ ඇති උපාංගයක MAC ලිපිනය සෙවීමට හෝ IP ගැටුම් නිරාකරණය කිරීමට ප්‍රයෝජනවත් වේ.

Displays and modifies the ARP (Address Resolution Protocol) cache, which maps IP addresses to MAC addresses on the local network.
දේශීය ජාලය තුළ IP ලිපින MAC ලිපින සමඟ සිතියම්ගත කරන ARP (Address Resolution Protocol) කෑෂය (cache) පෙන්වන අතර එය වෙනස් කිරීමට ඉඩ සලසයි.

Example

```
> arp

Interface: 192.168.1.105
 Internet Address     Physical Address     Type
 192.168.1.1          d4-6e-0e-ab-12-34    dynamic
 192.168.1.110        a8-51-ab-cd-ef-00    dynamic
```

7) `curl` (All Platforms)

Transfers data from or to a server using various protocols (HTTP, HTTPS, FTP, etc.). Widely used to test APIs, download files, and inspect HTTP responses.
විවිධ ප්‍රොටෝකෝල (HTTP, HTTPS, FTP, ආදිය) භාවිතයෙන් සේවාදායකයක් (server) වෙත හෝ වෙතින් දත්ත හුවමාරු කරයි. API පරීක්ෂා කිරීමට, ගොනු බාගත කිරීමට සහ HTTP ප්‍රතිචාර පරීක්ෂා කිරීමට බහුලව භාවිත වේ.

Example

```
$ curl -I https://example.com

HTTP/2 200
content-type: text/html; charset=UTF-8
content-length: 1256
server: ECS (nyb/1D07)
last-modified: Thu, 17 Oct 2019 07:18:26 GMT
```

Networking Ports / ජාලකරණ කෙවෙණි

A port is a 16-bit logical number used by the transport layer (TCP or UDP) to identify the specific application or service that should send or receive network data on a device.
කෙවෙණියක් යනු උපාංගයක් මත ජාල දත්ත යැවිය යුතු හෝ ලැබිය යුතු නිශ්චිත යෙදුම හෝ සේවාව හඳුනා ගැනීම සඳහා ප්‍රවාහන ස්ථරය (TCP හෝ UDP) විසින් භාවිතා කරනු ලබන බිටු 16 ක තාර්කික අංකයකි.

Why are ports needed
කෙවෙණි අවශ්‍ය වන්නේ ඇයි

IP address / IP ලිපිනය
Identifies which device should receive data
දත්ත ලැබිය යුත්තේ කුමන උපාංගයටද යන්න හඳුනා ගනී

Port number / කෙවෙණි අංකය
Identifies which application on that device should handle the data
එම උපාංගයේ ඇති කුමන යෙදුම මඟින් දත්ත හැසිරවිය යුතුද යන්න හඳුනා ගනී

Without ports, the operating system would not know whether incoming data is meant for the web browser, email application, game, or another program.
Ports නොමැතිව, පැමිණෙන දත්ත පැමිනෙන්නේ වෙබ් බ්‍රවුසරය, විද්‍යුත් තැපැල් (email) යෙදුම, ක්‍රීඩාව හෝ වෙනත් වැඩසටහනක් සඳහාද යන්න මෙහෙයුම් පද්ධතියට දැන ගත නොහැක.

Simple analogy / සරල උදාහරණය

Think of a company building,
සමාගම් ගොඩනැගිල්ලක් ගැන සිතන්න,

IP address = the building's street address
IP ලිපිනය = ගොඩනැගිල්ලේ වීදි ලිපිනය

Port number = a specific office or room inside the building
කෙවෙණි අංකය = ගොඩනැගිල්ල ඇතුළත ඇති නිශ්චිත කාර්යාලයක් හෝ කාමරයක්

Application = the person working in that office
යෙදුම = එම කාර්යාලයේ වැඩ කරන පුද්ගලයා

The postal service delivers mail to the correct building (IP address), then routes it to the correct office (port), where the intended recipient (application) receives it.
තැපැල් සේවය විසින් ලිපි නිවැරදි ගොඩනැගිල්ලට (IP ලිපිනය) බෙදා හරින අතර, පසුව එය නිවැරදි කාර්යාලය (කෙවෙණිය) වෙත යොමු කරයි, එහිදී අදාළ ලබන්නා (යෙදුම) එය ලබා ගනී.

Port number ranges / කෙවෙණි අංක පරාසයන්

Ports are 16-bit numbers / කෙවෙණි බිටු 16ක අංක වේ
(2^{16} = 65,536 possible values, from 0 to 65535)
(2^{16} = 65,536 විය හැකි අගයන්, 0 සිට 65535 දක්වා)

0 – 1023 (Well-known ports)
Reserved for standard internet services (HTTP, FTP, SSH...)
සම්මත අන්තර්ජාල සේවාවන් සඳහා වෙන් කර ඇත (HTTP, FTP, SSH...)

1024 – 49151 (Registered ports)
Assigned to specific applications by IANA
IANA විසින් නිශ්චිත යෙදුම් වෙත පවරා ඇත
(e.g. MySQL: 3306)

49152 – 65535 (Dynamic / Ephemeral ports)
Temporary ports assigned by the OS to clients during a session
සමකාලනයක් අතරතුර මෙහෙයුම් පද්ධතිය විසින් සේවාලාභීන් වෙත පවරනු ලබන තාවකාලික කෙවෙණි

Common port numbers / පොදු කෙවෙණි අංක

Port	Service	Protocol	Purpose
20, 21	FTP	TCP	File transfer
22	SSH	TCP	Secure remote login
23	Telnet	TCP	Unsecured remote login
25	SMTP	TCP	Sending email
53	DNS	TCP/UDP	Domain name resolution
67, 68	DHCP	UDP	IP address assignment
80	HTTP	TCP	Web traffic
110	POP3	TCP	Download email (single device)
143	IMAP	TCP	Sync email across multiple devices
443	HTTPS	TCP	Web traffic
3306	MySQL	TCP	Database connections

How it works **(visiting a website)**
එය ක්‍රියා කරන ආකාරය (වෙබ් අඩවියකට පිවිසීම)

1. Your browser sends a request to the website's IP address
   ඔබගේ බ්‍රවුසරය වෙබ් අඩවියේ IP ලිපිනය වෙත ඉල්ලීමක් යවයි
2. The request is directed to port 443 (HTTPS)
   ඉල්ලීම 443 කෙවෙණිය (HTTPS) වෙත යොමු කෙරේ
3. The web server receives the request on port 443
   වෙබ් සේවාදායකය විසින් 443 කෙවෙණිය හරහා ඉල්ලීම ලබා ගනී
4. The server processes it and sends the response back to your browser
   සේවාදායකය එය සකසා ප්‍රතිචාරය නැවත ඔබගේ බ්‍රවුසරය වෙත යවයි

Physical vs Network ports
භෞතික සහ ජාල කෙවෙණි අතර වෙනස

A network port is not a physical connector like a USB port or Ethernet port.
Network port යනු USB හෝ ඊතර්නෙට් වැනි භෞතික සම්බන්ධකයක් නොවේ.

Physical port / භෞතික කෙවෙණි
A hardware socket where you plug in a cable (USB, Ethernet, HDMI)
ඔබ කේබලයක් සම්බන්ධ කරන දෘඩාංග සොකට් එකක් (USB, Ethernet, HDMI)

Network port / ජාල කෙවෙණි
A logical number used by TCP/UDP software to route data to the correct application, it has no physical form
දත්ත නිවැරදි යෙදුම වෙත යොමු කිරීම සඳහා TCP/UDP මෘදුකාංග විසින් භාවිතා කරනු ලබන තාර්කික අංකයක්, මෙයට භෞතික ස්වරූපයක් නොමැත

Port states / කෙවෙණි තත්ත්ව
A port on a device can be in one of three states
උපාංගයක් මත ඇති කෙවෙණියක් ප්‍රධාන තත්ත්ව තුනකින් එකක පැවතිය හැක

1. Open (actively listening)
2. Closed (reachable but no service)
3. Filtered (blocked by a firewall)

Port forwarding
Routers use this to forward traffic arriving on a specific port to a specific device on the local network.
රවුටර් විසින් දේශීය ජාලයේ ඇති නිශ්චිත උපාංගයක් වෙත, නිශ්චිත කෙවෙණියක් හරහා පැමිණෙන දත්ත ගමනාගමනය යොමු කිරීම සඳහා මෙය භාවිතා කරයි.

By forwarding ports 80 or 443 on your router to your local PC, you can host a website directly from your own computer, making it accessible to anyone on the internet.
ඔබගේ රවුටරයේ පෝට් 80 හෝ 443 ඔබගේ දේශීය පරිගණකයට forward කිරීම මඟින්, ඔබට සෘජුවම ඔබගේම පරිගණකයේ සිට වෙබ් අඩවියක් host කළ හැකි අතර, එමඟින් අන්තර්ජාලයේ සිටින ඕනෑම අයෙකුට එයට පිවිසිය හැකි වේ.

Socket **(IP address + port number)**

A socket is the combination of an IP address and a port number. It uniquely identifies a single connection endpoint. A full connection uses two sockets one at each end.
සොකට් එකක් යනු IP ලිපිනයක සහ කෙවෙණි අංකයක එකතුවකි. එය තනි සම්බන්ධතා අන්ත ලක්ෂ්‍යයක් අනන්‍ය ලෙස හඳුනා ගනී. සම්පූර්ණ සම්බන්ධතාවයක් සඳහා එක් එක් කෙළවරේ සොකට් එක බැගින් සොකට් දෙකක් භාවිතා කරයි.

When your computer connects to Google's web server over HTTPS, two sockets are created to form the connection.
ඔබගේ පරිගණකය HTTPS හරහා Google හි වෙබ් සේවාදායකය සමඟ සම්බන්ධ වන විට, සම්බන්ධතාවය ගොඩනැගීම සඳහා සොකට් දෙකක් නිර්මාණය වේ.

Google's side always uses port 443 (well-known HTTPS port).
Google හි පාර්ශවය සැමවිටම 443 කෙවෙණිය භාවිතා කරයි.

Your computer -> `192.168.1.1:51234`
Google's server -> `142.250.190.46:443`

The full connection is identified by the pair of sockets.
සම්පූර්ණ සම්බන්ධතාවය හඳුනා ගනු ලබන්නේ සොකට් යුගලය මඟිනි.

Port space per protocol
නියමාවලියකට ඇති කෙවෙණිය ඉඩ ප්‍රමාණය

Both TCP and UDP maintain their own independent port spaces.
TCP සහ UDP යන දෙකම තමන්ගේම ස්වාධීන කෙවෙණි ඉඩ ප්‍රමාණයන් පවත්වා ගනී.

TCP port 80 and UDP port 80 are separate endpoints.
TCP කෙවෙණි 80 සහ UDP කෙවෙණි 80 යනු වෙනස් අන්ත ලක්ෂ්‍යයන් දෙකකි.

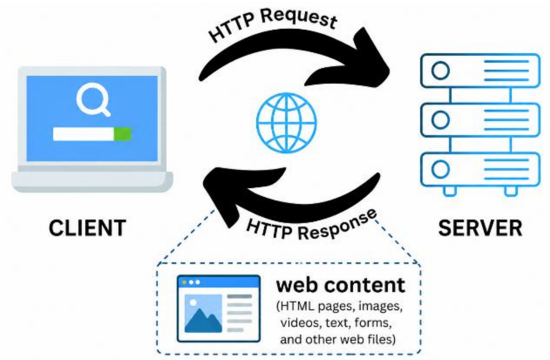
Protocols
නියමාවලි

A protocol is a set of rules and standards that define how data is transmitted, received, and interpreted between different devices in a network.
නියමාවලියක් යනු ජාලයක විවිධ උපාංග අතර දත්ත සම්ප්‍රේෂණය, ග්‍රහනය සහ අර්ථකථනය කරන ආකාරය නිර්වචනය කරන රීති සහ ප්‍රමිති සමූහයකි.

Ensures that communication between devices is reliable, secure, and efficient.
උපාංග අතර සන්නිවේදනය විශ්වසනීය, ආරක්ෂිත සහ කාර්යක්ෂම බව එමගින් සහතික කරයි.

Protocols determine the format, timing, sequencing, and error-checking methods used for data transmission.
නියමාවලි මගින් දත්ත සම්ප්‍රේෂණය සඳහා භාවිතා කරන ආකෘතිය, වේලාව, අනුක්‍රමණය සහ දෝෂ පරීක්ෂා කිරීමේ ක්‍රම තීරණය කරයි.

HTTP (Hypertext Transfer Protocol)



Used to transfer webpages on the internet.
අන්තර්ජාලයේ තුළ වෙබ් පිටු හුවමාරු කිරීමට භාවිතා කරයි.

Use port 80.
80 කෙවෙනිය භාවිත කරයි.

The foundation of data communication for the World Wide Web.
ලෝක විසිරි වියමන සඳහා දත්ත සන්නිවේදනයේ පදනමයි.

Operates in a client-server model.
සේවාලාභී-සේවාදායක ආකෘතියක් තුළ ක්‍රියා කරයි.

Works by sending requests from a client (usually a web browser) to a web server, which responds by sending the requested content
ක්‍රියා කරන්නේ සේවාලාභියෙකුගෙන් (සාමාන්‍යයෙන් වෙබ් බ්‍රවුසරයක්) වෙබ් සේවාදායකයකට ඉල්ලීම් යැවීමෙන් සහ එමගින් ඉල්ලන ලද අන්තර්ගතය යැවීමෙන් ප්‍රතිචාර දක්වමින්ය.

A stateless protocol, meaning each request is treated independently without remembering previous requests.
Stateless නියමාවලියකි, එනම්, පෙර සිදු කරන ලද ඉල්ලීම් පිළිබඳ මතකයක් තබා නොගනිමින්, සෑම ඉල්ලීමක් දෙසම ස්වාධීන වූ අලුත් ඉල්ලීමක් ලෙස බලනු ලබයි.

HTTP does not encrypt data, so transmitted information can be intercepted by attackers.
HTTP මඟින් දත්ත ගුප්තකේතනය නොකරන බැවින්, හුවමාරු වන තොරතුරු අතරමඟදී සයිබර් ප්‍රහාරකයින් අතට පත්වීමේ අවදානමක් පවතී.

Supports persistent connections (Keep-Alive), allowing multiple requests to use the same TCP connection and improving performance.
නිරන්තර සම්බන්ධතා සඳහා සහය දක්වයි: මේ නිසා එකම TCP සම්බන්ධතාවය හරහා ඉල්ලීම් කිහිපයක් සිදු කිරීමට ඉඩ සැලසෙන අතර, එමඟින් ජාලයේ සමස්ත ක්‍රියාකාරීත්වය වැඩිදියුණු වේ.

Follows a simple request-response model. A client makes a request, and the server returns a response.
සරල ඉල්ලීම්-ප්‍රතිචාර ආකෘතියක් අනුගමනය කරයි. සේවාලාභියෙක් ඉල්ලීමක් කරයි, සේවාදායකය ප්‍රතිචාරයක් ලබා දෙයි.

Common HTTP methods

GET	Requests data from the server. සේවාදායකයෙන් දත්ත ඉල්ලයි.
POST	Sends data to the server (Ex. form submission). සේවාදායකය වෙත දත්ත යවයි (උදා: ෆෝරම ඉදිරිපත් කිරීම).
PUT	Updates existing server data. සේවාදායකයේ දත්ත යාවත්කාලීන කරයි.
DELETE	Removes data from the server. සේවාදායකයෙන් දත්ත ඉවත් කරයි.

Requests and responses consist of two parts
ඉල්ලීම් සහ ප්‍රතිචාර කොටස් දෙකකින් සමන්විත වේ

1. Headers
Contain metadata, such as the type of request, encoding type, and information about the client.
ඉල්ලීම් වර්ගය, කේතීකරණ වර්ගය සහ සේවාලාභියා පිළිබඳ තොරතුරු වැනි පාර-දත්ත අඩංගු වේ.

2. Body
Contains the actual data being transmitted (like the webpage content).
සම්ප්‍රේෂණය වන සත්‍ය දත්ත අඩංගු වේ (වෙබ් පිටුවේ අන්තර්ගතය වැනි).

HTTP Status Codes

Servers respond to requests with status codes that indicate the outcome.
ප්‍රතිඵලය පෙන්නුම් කරන තත්ව කේත සමඟින් ඉල්ලීම්වලට සේවාදායකයන් ප්‍රතිචාර දක්වයි

200 OK	Request was successful. ඉල්ලීම සාර්ථක විය.
404 Not Found	Requested resource couldn't be found. ඉල්ලූ සම්පත සොයාගත නොහැකි විය.
500 Internal Server Error	A server-side issue occurred. සේවාදායක අන්තයේ ගැටලුවක් ඇති විය.

HTTPS (HTTP Secure)

An extension of the standard HTTP protocol that uses encryption
ගුප්තකේතනය භාවිතා කරන සාමාන්‍ය HTTP නියමාවලියේම දිගුවකි.

HTTPS operates on TCP port 443.
HTTPS ක්‍රියා කරන්නේ TCP 443 කෙවෙනිය හරහාය.

Uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt data during transmission.
දත්ත හුවමාරු වන විට ඒවා ගුප්තකේතනය කිරීම සඳහා SSL හෝ TLS තාක්ෂණය භාවිතා කරයි.

Provides confidentiality by preventing unauthorized access to transmitted data.
හුවමාරු වන දත්ත වෙත අනවසරයෙන් ප්‍රවේශ වීම වළක්වමින් රහස්‍යභාවය සපයයි.

Provides integrity by ensuring that data is not altered during transmission.
දත්ත හුවමාරු වන අතරතුර ඒවා වෙනස් නොවන බව සහතික කරමින් අඛණ්ඩතාව සපයයි.

Provides authentication by verifying the identity of websites through digital certificates.
අංකිත සහතික මඟින් වෙබ් අඩවිවල අනන්‍යතාවය තහවුරු කර සත්‍යාපනය සපයයි.

Widely used for secure login systems, online banking applications and e-commerce websites to protect financial transactions.
ආරක්ෂිත ලොගින් පද්ධති, මාර්ගගත බැංකු කටයුතු සහ මුදල් ගනුදෙනු ආරක්ෂා කිරීම සඳහා විද්‍යුත් වාණිජ වෙබ් අඩවි සඳහා බහුලව භාවිතා වේ.

Protects sensitive information such as usernames, passwords, and credit card details.
පරිශීලක නාම, මුරපද සහ ක්‍රෙඩිට් කාඩ් විස්තර වැනි සංවේදී තොරතුරු ආරක්ෂා කරයි.

FTP (File Transfer Protocol)

A standard network protocol used for transferring files between a client and a server.
සේවාලාභියෙකු සහ සේවාදායකයෙකු අතර ගොනු හුවමාරු කර ගැනීම සඳහා භාවිතා කරන සම්මත ජාල නියමාවලියකි.

Operates using the TCP protocol and uses TCP port 21 and 20.
TCP නියමාවලිය යටතේ ක්‍රියා කරන අතර TCP 21 සහ 20 කෙවෙනි භාවිතා කරයි.

Allow users to upload files to a remote server, manage files and directories and download files from a remote server.
දුරස්ථ සේවාදායකයකට ගොනු උඩුගත කිරීමට, ගොනු සහ ෆෝල්ඩර කළමනාකරණය කිරීමට සහ එතැනින් ගොනු බාගත කිරීමට පරිශීලකයින්ට ඉඩ සලසයි.

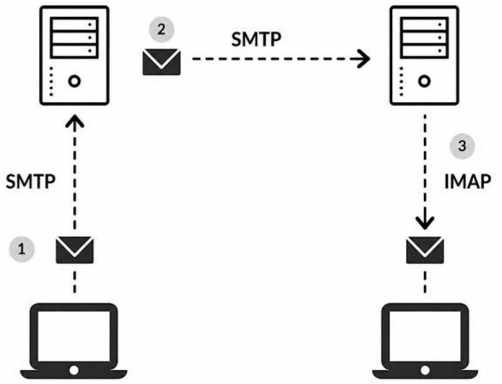
Uses a client-server architecture and supports both authenticated (username / password) and anonymous access.
Client-Server ව්‍යුහයක් භාවිතා කරන අතර, පරිශීලක නාම/මුරපද සහිතව හෝ රහිතව ප්‍රවේශ වීමට සහය දක්වයි.

FTP transfers data in plain text by default and does not provide built-in encryption.
FTP මඟින් දත්ත සාමාන්‍ය පෙළ/අකුරු ලෙස හුවමාරු කරන බැවින් එහි built-in ගුප්තකේතන පද්ධතියක් නැත.

Because of the lack of encryption, FTP is vulnerable to packet sniffing and unauthorized interception.
මේ නිසා, දත්ත සොරකම් කිරීම් සහ අනවසරයෙන් දත්ත අතරමඟදී ලබා ගැනීම්වලට ගොදුරු වීමේ අවදානමක් ඇත.

FTPS (using SSL/TLS) and SFTP (using SSH) are secure alternatives that provide encrypted communication and better security than FTP.
FTPS (SSL/TLS භාවිතා කරමින්) සහ SFTP (SSH භාවිතා කරමින්) යනු ගුප්තකේතනය කළ සන්නිවේදනයක් සහ FTP වලට වඩා හොඳ ආරක්ෂාවක් සපයන ආරක්ෂිත විකල්ප වේ.

SMTP (Simple Mail Transfer Protocol)



An application layer protocol used for sending emails between clients and mail servers as well as between mail servers.
සේවාලාභීන් සහ විද්‍යුත් තැපැල් සේවාදායකයන් අතර මෙන්ම, සේවාදායකයන් එකිනෙක අතරද විද්‍යුත් ලිපින යැවීම සඳහා භාවිතා කරන යෙදුම් ස්ථරයේ නියමාවලියකි.

Operates on TCP port 25, 587 or 465.
TCP 25, 587 හෝ 465 කෙවෙනි හරහා ක්‍රියා කරයි.

Responsible only for sending emails, while email retrieval is performed by IMAP or POP3.
විද්‍යුත් ලිපින යැවීම සඳහා වගකියනු ලබයි. විද්‍යුත් ලිපින ලබා ගැනීම IMAP හෝ POP3 මගින් සිදු කරයි.

Follows a push model in which emails are transferred from the sender's mail server to the recipient's mail server.
මෙය Push model අනුගමනය කරයි, එනම් යවන්නාගේ විද්‍යුත් ලිපින සේවාදායකයේ සිට ලබන්නාගේ විද්‍යුත් ලිපින සේවාදායකය වෙත ලිපින යවනු ලබයි.

Supports user authentication through SMTP AUTH and secure communication through SSL/TLS encryption.
SMTP AUTH හරහා පරිශීලක අනන්‍යතාවය තහවුරු කිරීමටත්, SSL/TLS ගුප්තකේතනය හරහා ආරක්ෂිත සන්නිවේදනයටත් සහය දක්වයි.

Widely used by email services such as Gmail, Outlook, and Yahoo Mail for outgoing email delivery.
Gmail, Outlook, සහ Yahoo Mail වැනි විද්‍යුත් ලිපින සේවාවන් මඟින් බාහිරට විද්‍යුත් ලිපින යැවීම සඳහා බහුලව භාවිතා වේ.

IMAP (Internet Message Access Protocol)

An application layer protocol used to access, manage, and synchronize emails stored on a mail server.
විද්‍යුත් තැපැල් සේවාදායකයක ගබඩා කර ඇති විද්‍යුත් ලිපින වෙත ප්‍රවේශ වීමට, කළමනාකරණය කිරීමට සහ සමමුහුර්ත කිරීමට භාවිතා කරන යෙදුම් ස්ථරයේ නියමාවලියකි.

Operates on TCP port 143 or port 993(Secure).
TCP 143 හෝ 993(ආරක්ෂිත) කෙවෙනි හරහා ක්‍රියා කරයි.

Stores emails on the mail server, allowing users to access the same mailbox from multiple devices.
විද්‍යුත් ලිපින පණිවිඩ, විද්‍යුත් ලිපින සේවාදායකයේම සුරැකිව තබා ගන්නා බැවින්, පරිශීලකයාට එකම විද්‍යුත් ලිපින ගිණුම උපාංග කිහිපයකින් පරිශීලනය කිරීමේ හැකියාව ලැබේ.

Synchronizes email status, folders, and messages across all connected devices in real time.
සියලුම සම්බන්ධිත උපාංග අතර විද්‍යුත් ලිපින වල තත්ත්වය, ෆෝල්ඩර සහ පණිවිඩ සජීවීව සමමුහුර්ත කරයි.

Supports server-side folder management, message flags, and partial email downloads, improving efficiency and mailbox organization.
සේවාදායකය පැත්තෙන් ෆෝල්ඩර කළමනාකරණය, පණිවිඩ සලකුණු කිරීම සහ විද්‍යුත් ලිපිනවල කොටස් වශයෙන් පමණක් බාගත කර බැලීමේ හැකියාව ලබා දෙන බැවින් මෙය ඉතා කාර්යක්ෂම වේ.

POP3 (Post Office Protocol) - **Legacy**

An application layer protocol used to retrieve emails from a mail server and download them to a local device.
විද්‍යුත් ලිපින සේවාදායකයෙන් විද්‍යුත් ලිපින ලබාගෙන ඒවා තමන්ගේ උපාංගයට බාගත කර ගැනීමට භාවිතා කරන නියමාවලියකි.

Operates on TCP port 110 or 995(Secure).
TCP 110 හෝ 995(ආරක්ෂිත) කෙවෙනි හරහා ක්‍රියා කරයි.

POP3 downloads emails from the mail server to the user's device and, by default, removes them from the server after retrieval.
POP3 මගින් විද්‍යුත් ලිපින පරිශීලකයාගේ උපාංගයට බාගත කරගත් පසු, සාමාන්‍යයෙන් ඒවා සේවාදායකයෙන් මකා දමනු ලබයි.

Does not synchronize email status, folders, or messages across multiple devices, making it more suitable for single-device access.
උපාංග කිහිපයක් අතර විද්‍යුත් ලිපින තත්ත්වයන් හෝ ෆෝල්ඩර සමමුහුර්ත නොකරන බැවින්, මෙය තනි උපාංගයකින් පමණක් විද්‍යුත් ලිපින පරිශීලනය කරන අයට වඩාත් සුදුසු වේ.

Requires less server storage space because emails are typically transferred from the server to the client device.
විද්‍යුත් ලිපින සියල්ල පරිශීලකයාගේ උපාංගයට මාරු වන බැවින්, සේවාදායකය තුළ විශාල ඉඩක් අවශ්‍ය නොවේ.

Provides faster email access on low-bandwidth networks since messages are downloaded and managed locally.
පණිවිඩ දේශීයව බාගත කර කළමනාකරණය කරන බැවින්, අන්තර්ජාල වේගය අඩු පරිසරයන්හිදී පවා විද්‍යුත් ලිපින වෙත වේගයෙන් ප්‍රවේශ වීමේ හැකියාව ලැබේ.

DNS (Domain Name System/Server)
වසම් නාම පද්ධතිය/සේවාදායකය

A hierarchical and decentralized naming system that translates human-readable domain names into IP addresses.
මිනිසුන්ට පහසුවෙන් මතක තබා ගත හැකි වසම් නාම පරිගණකවලට තේරුම් ගත හැකි IP ලිපිනයන්බවට පරිවර්තනය කරන, ධුරාවලිගත සහ විමධ්‍යගත නාමකරණ පද්ධතියකි.

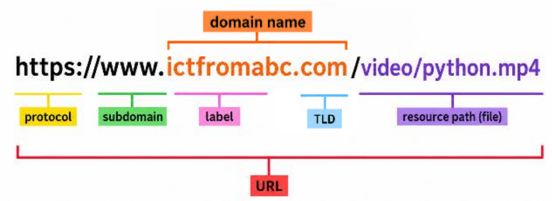
NOTE:
A domain name is a human-readable address used to identify a location on the internet.
වසම් නාමයක් යනු අන්තර්ජාලයේ ස්ථානයක් හඳුනා ගැනීමට භාවිතා කරන මිනිසුන්ට කියවිය හැකි ලිපිනයකි.

It corresponds to a specific IP address.
එය නිශ්චිත IP ලිපිනයකට අනුරූප වේ

Domain Names
වසම් නාම

A domain name is one part of a URL.
වසම් නාමයක් යනු URL එකක එක් කොටසක් වේ.

Parts of a URL
URL එකක කොටස්



What is a URL
A URL (Uniform Resource Locator) is the address used to locate a resource on the Internet.
URL එකක් යනු අන්තර්ජාලයෙහි පවතින සම්පතක් සොයා ගැනීම සඳහා භාවිත කරන ලිපිනයයි.

Top-Level Domain (TLD)
The rightmost part of a domain name, following the last dot, and it signifies the domain's type or geographical origin.
වසම් නාමයක අවසාන තිතට පසුව ඇති දකුණින්ම පිහිටි කොටස වන අතර, එමගින් වසමෙහි වර්ගය හෝ භූගෝලීය සම්භවය පෙන්නුම් කරයි.

Example / උදාහරණ
In example.com, .com is the Top-Level Domain (TLD).
example.com හි .com පළමු මට්ටමේ වසම වේ.
In example.org, .org is the Top-Level Domain (TLD).
example.org හි .org පළමු මට්ටමේ වසම වේ.

Second-Level Domain (SLD)
The part of the domain name directly to the left of the TLD.
වසම් නාමයේ TLDට සෘජුවම ඇති වම් කොටසයි.

It typically represents the specific name or brand of the organization or entity.
එය සාමාන්‍යයෙන් සංවිධානයේ හෝ ආයතනයේ නිශ්චිත නම හෝ වෙළඳ නාමය නියෝජනය කරයි.

Example / උදාහරණ
In example.com, example is the second-level domain.
example.com හි, example දෙවන මට්ටමේ වසම වේ.

Subdomains / උපවසම්

Any domain that exists below another domain, regardless of how many levels it contains. (not a numbered level)
වෙනත් වසමකට පහළින් පිහිටන ඕනෑම වසමක් උප-වසමක් ලෙස හැඳින්වේ.

So , an SLD is a subdomain of the TLD, and www is a subdomain of the SLD.
එබැවින්, SLD එකක් යනු TLD එකක උප-වසමක් වන අතර, 'www' යනු SLD එකෙහි උප-වසමකි.

Example / උදාහරණ
www.example.com , mail.example.com , cs.example.com , student.cs.example.com

All of these are subdomains of example.com, even though they are at different numbered levels.
මිය විවිධ අංකිත මට්ටම්වල පැවතුණද, මේ සියල්ල example.com හි උප-වසම් වේ."

Hostname
සත්කාරක නාමය
The part of the domain name that identifies a specific host or service within a domain.
වසමක් තුළ නිශ්චිත ධාරකයක් හෝ සේවාවක් හඳුනා ගන්නා වසම් නාමයේ කොටසයි.

It is often used interchangeably with subdomain.
එය බොහෝ විට උප වසම සමඟ හුවමාරු ලෙස භාවිතා වේ.

Example / උදාහරණ
mail.example.com – mail identifies the mail server within the example.com domain.
mail මගින් example.com වසම තුළ ඇති තැපැල් සේවාදායකය හඳුනා ගනී.

Domain Name Hierarchy
වසම් නාම ධුරාවලිය

The structure used by DNS to organize domain names. It is arranged in a tree-like hierarchy, with the most general level at the top and more specific levels below.
DNS මගින් වසම් නාම සංවිධානය කිරීම සඳහා භාවිතා කරන ව්‍යුහයයි. මෙය ගසක හැඩය ගත් ධුරාවලියක් ලෙස සකසා ඇති අතර, එහි වඩාත්ම පොදු මට්ටම ඉහළින්ම ද, වඩාත්ම නිශ්චිත මට්ටම් පහළින්ම ද පිහිටයි.

mail.cs.example.com

Level	**Name**
Root	.
Top-Level Domain (TLD)	com
Second-Level Domain (SLD)	Example
Third-Level Domain	cs
Fourth-Level Domain	mail

DNS Resolution Process
DNS විසඳුම් ක්‍රියාවලිය

When you enter a domain name into a web browser, the DNS (Domain Name System) resolution process begins.
ඔබ වෙබ් බ්‍රවුසරයකට වසම් නාමයක් ඇතුළත් කළ විට, DNS විසඳුම් ක්‍රියාවලිය ආරම්භ වේ.

Cache is an important part of the DNS resolution process. Before contacting DNS servers, the system first checks whether the required IP address has already been stored locally.
වාරක මතකය යනු DNS විසඳුම් ක්‍රියාවලියේ වැදගත් කොටසකි. DNS සේවාදායකයන් සම්බන්ධ කර ගැනීමට පෙර, පද්ධතිය මුලින්ම පරීක්ෂා කරනුයේ අවශ්‍ය IP ලිපිනය දැනටමත් ස්ථානීයව ගබඩා කර තිබේද යන්නයි.

The browser first checks its own DNS cache for the website's IP address.
බ්‍රවුසරය මුලින්ම වෙබ් අඩවියේ IP ලිපිනය සඳහා එහි ඇති බ්‍රවුසර් DNS වාරක මතකය පරීක්ෂා කරයි.

If the browser cache does not contain the IP address, the operating system (OS) checks its DNS cache, allowing other applications and browsers on the computer to use previously resolved addresses.
බ්‍රවුසර් වාරක මතකයෙහි අදාළ IP ලිපිනය නොමැති නම්, මෙහෙයුම් පද්ධතිය එහි DNS වාරක මතකය පරීක්ෂා කරයි. එමඟින් පරිගණකයේ ඇති අනෙකුත් යෙදුම් සහ බ්‍රවුසරවලට මීට පෙර විසඳන ලද ලිපින භාවිතා කිරීමට අවස්ථාව ලැබෙයි.

If the IP address is still not found, the query is sent to the local DNS resolver, which is usually provided by the Internet Service Provider (ISP).
IP ලිපිනය තවමත් සොයාගත නොහැකි නම්, එම විමසුම දේශීය DNS රිසෝල්වර් වෙත යවනු ලැබේ. මෙය සාමාන්‍යයෙන් සපයනු ලබන්නේ අන්තර්ජාල සේවා සපයන්නා විසිනි.

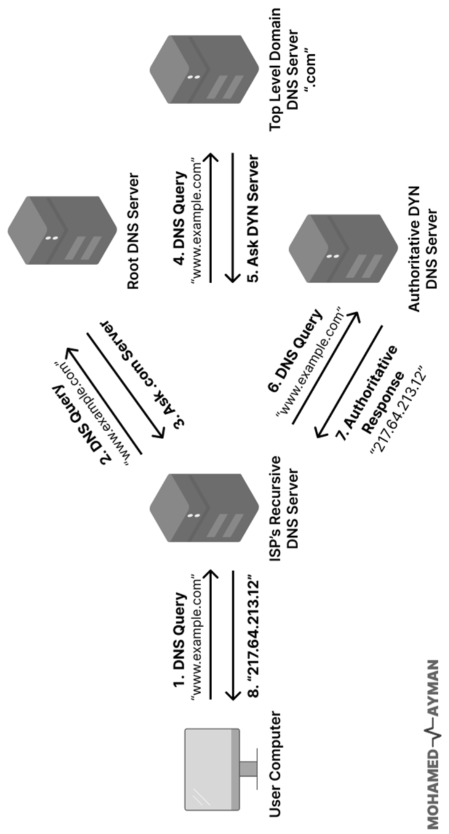
If the resolver has the IP address stored in its cache, it immediately returns the result to the computer.
රිසෝල්වර් එකෙහි වාරක මතකයේ එම IP ලිපිනය ගබඩා කර ඇත්නම්, එය වහාම එම ප්‍රතිඵලය පරිගණකය වෙත නැවත ලබා දෙයි.

If the resolver does not have the IP address, it queries other DNS servers (Root, TLD, and Authoritative DNS servers) until the correct IP address is located.
රිසෝල්වර් එක සතුව එම IP ලිපිනය නොමැති නම්, නිවැරදි IP ලිපිනය සොයා ගන්නා තෙක් එය අනෙකුත් ඍහි සේවාදායකයන්ගෙන් (Root, TLD, සහ Authoritative DNS servers) විමසීම් සිදු කරයි.

As the DNS response is returned, the DNS resolver caches the DNS record according to its Time to Live (TTL) value, allowing future requests for the same domain to be answered more quickly without repeating the entire lookup process.
(DNS ප්‍රතිචාරය නැවත ලැබෙන විට, DNS රිසෝල්වර් එක එහි ඇති “Time to Live” (TTL) අගයට අනුව එම DNS වාර්තාව වාරක මතකයේ තබා ගනී. එමඟින් එම වසම සඳහාම ඉදිරියේදී ලැබෙන ඉල්ලීම්වලට සම්පූර්ණ සෙවුම් ක්‍රියාවලිය නැවත සිදු නොකර වඩාත් ඉක්මනින් පිළිතුරු ලබා දීමට අවස්ථාව ලැබෙයි.

The resolved IP address is then returned to the computer, allowing the browser to connect to the requested website.
ඉන්පසු සොයාගත් IP ලිපිනය පරිගණකය වෙත ලබා දෙන අතර, එමඟින් ඉල්ලා සිටි වෙබ් අඩවිය සමඟ සම්බන්ධ වීමට බ්‍රවුසරයට හැකියාව ලැබෙයි.

Finally, the resolved IP address is cached by the browser and the operating system (according to its TTL), enabling faster access to the same website in future requests.
අවසානයේදී, සොයාගත් (විසඳන ලද) IP ලිපිනය බ්‍රවුසරය සහ මෙහෙයුම් පද්ධතිය මඟින් (එහි TTL අගයට අනුව) මතක තබා ගන්නා අතර, එමඟින් ඉදිරි ඉල්ලීම්වලදී එම වෙබ් අඩවියටම ඉතා වේගයෙන් පිවිසීමේ හැකියාව ලැබෙයි.



Distributed Structure of DNS servers
සේවාදායක වල බෙදා හරින ලද ව්‍යුහය

DNS is organized in levels
DNS මට්ටම් වලින් සංවිධානය වී ඇත

Root, Top-Level Domains (TLDs), Second-Level Domains, and Subdomains.

This hierarchy helps distribute the workload across different servers.
මෙම ධූරාවලිය විවිධ සේවාදායක හරහා වැඩ බර බෙදා හැරීමට උපකාරී වේ.

Root Servers
At the top of the DNS hierarchy are Root Servers. These servers store information about where to find the TLD servers (like .com, .org, .net).
DNS ධූරාවලියේ ඉහළින්ම ඇත්තේ Root Servers ය. මෙම සේවාදායකයන් TLD සේවාදායකයන් (.com, .org, .net වැනි) සොයා ගත යුතු ස්ථානය පිළිබඳ තොරතුරු ගබඩා කරයි.

There are 13 root server clusters around the world.
ලොව පුරා root සේවාදායක පොකුරු 13 ක් ඇත

TLD Servers

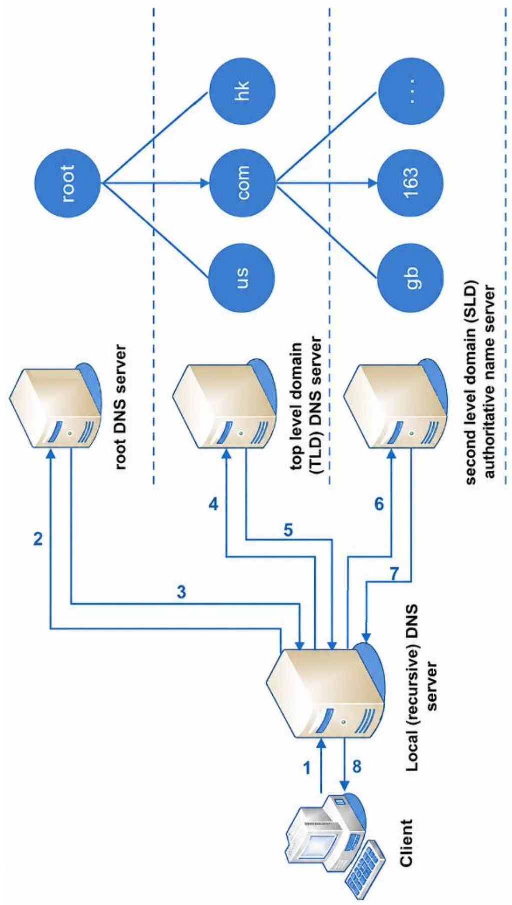
These servers hold information about specific top-level domains, such as .com, .org, or country codes like .uk.
මෙම සේවාදායකයන් .com, .org වැනි විශේෂිත ඉහළ මට්ටමේ වසම් හෝ .uk වැනි රට කේත පිළිබඳ තොරතුරු දරයි.

They direct queries to the appropriate second-level domain servers.
ඒවා සුදුසු දෙවන මට්ටමේ වසම් සේවාදායකයන් වෙත විමසුම් යොමු කරයි.

Authoritative Name Servers

Each domain (Ex. example.com) has authoritative name servers that hold the exact IP address of the website or service.
සෑම වසමකටම (Ex. example.com) වෙබ් අඩවියේ හෝ සේවාවේ නිශ්චිත IP ලිපිනය තබා ඇති බලයලත් නාම සේවාදායක ඇත.

These servers provide the final answer to a DNS query.
මෙම සේවාදායකයන් DNS විමසුමකට අවසාන පිළිතුර සපයයි.



ictfromabc.com

DHCP (Dynamic Host Configuration Protocol)
ගතික ධාරක වින්‍යාස නියමාවලිය

DHCP is a network protocol used to automatically assign IP addresses and other network configuration settings to devices on a network.
DHCP යනු ජාලයක උපාංග වෙත IP ලිපින සහ අනෙකුත් ජාල වින්‍යාස සැකසුම් ස්වයංක්‍රීයව පැවරීමට භාවිතා කරන ජාල නියමාවලියකි.

This eliminates the need for manual IP address configuration for each device.
මෙය එක් එක් උපාංගය සඳහා හස්තීය ලෙස IP ලිපින වින්‍යාස කිරීමේ අවශ්‍යතාවය ඉවත් කරයි.

When a device (like a computer or smartphone) connects to a network, it needs an IP address to communicate.
උපාංගයක් (පරිගණකයක් හෝ ස්මාර්ට් ජංගම දුරකතනයක් වැනි) ජාලයකට සම්බන්ධ වන විට, එයට සන්නිවේදනය කිරීමට IP ලිපිනයක් අවශ්‍ය වේ.

The device sends out a request called a DHCP Discover message to find DHCP servers on the network (Broadcast).
උපාංගය ජාලයේ DHCP සේවාදායකයන් සොයා ගැනීමට DHCP Discover message ලෙස ඉල්ලීමක් යවයි:(Broadcast).

DHCP servers respond with a DHCP Offer message, which includes an available IP address and configuration details (like subnet mask, gateway, and DNS servers).
DHCP සේවාදායකයන් DHCP Offer පණිවිඩයක් සමඟ ප්‍රතිචාර දක්වයි, එයට ලබා ගත හැකි IP ලිපිනයක් සහ වින්‍යාස කිරීමේ විස්තර (උපජාල ආවරණය, දොරටු සහ DNS සේවාදායක වැනි) ඇතුළත් වේ.

The device selects an offer and sends a DHCP Request message to the server, indicating that it wants to use the offered IP address.
පිරිනමන IP ලිපිනය භාවිතා කිරීමට අවශ්‍ය බව දක්වමින් උපාංගය එකක් තෝරා සේවාදායකයට DHCP ඉල්ලීම් පණිවිඩයක් යවයි.

Large organizations may have dedicated DHCP servers inside the local network.
විශාල සංවිධාන හෝ ආයතන සතු ස්ථානීය ජාලය තුළ, ඒ සඳහාම වෙන්වූ සුවිශේෂී DHCP සේවාදායකයන් තිබිය හැකිය.

Within a local network, the router acts as a DHCP server and assigns private IP addresses (LAN IP addresses) to connected devices.
දේශීය ජාලයක් තුළදී, මාර්ගගතය DHCP සේවාදායකයෙකු ලෙස ක්‍රියා කරමින් සම්බන්ධ වී ඇති උපාංග සඳහා පුද්ගලික IP ලිපින ලබා දෙයි.

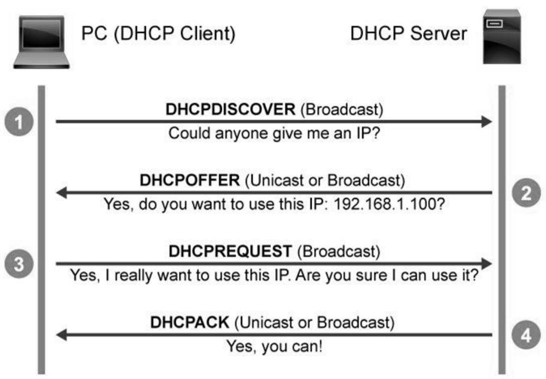
The Internet Service Provider (ISP) uses dedicated DHCP servers to efficiently assign public IP addresses (WAN IP addresses) to its customers.
අන්තර්ජාල සේවා සපයන්නා විසින් තම පාරිභෝගිකයන් වෙත පොදු IP ලිපින (WAN IP addresses) කාර්යක්ෂමව ලබා දීම සඳහා ඒ වෙනුවෙන්ම වෙන්වූ DHCP සේවාදායකයන් භාවිතා කරයි.

The DHCP server sends a DHCP Acknowledgment message to the device, confirming that the IP address and configuration settings are assigned.
IP ලිපිනය සහ වින්‍යාස සැකසුම් පවරා ඇති බව තහවුරු කරමින් DHCP සේවාදායකය විසින් උපාංගය වෙත DHCP පිළිගැනීමේ පණිවිඩයක් යවයි.

The device now uses the assigned IP address to communicate on the network.
උපාංගය දැන් ජාලයේ සන්නිවේදනය කිරීමට පවරා ඇති IP ලිපිනය භාවිතා කරයි.

The IP address is assigned for a specific period (lease time).
IP ලිපිනය නිශ්චිත කාල සීමාවක් සඳහා පවරා ඇත.

The device may need to renew the lease before it expires.
උපාංගය කල් ඉකුත් වීමට පෙර කල්බදු කාලය අලුත් කිරීමට අවශ්‍ය විය හැකිය.



Address Resolution Protocol (ARP)
ලිපින විභේදන නියමාවලිය

ARP is a network protocol used to map a device's IP address to its physical MAC (Media Access Control) address on a local network.
ARP යනු උපාංගයක IP ලිපිනය ස්ථානීය ජාලයක එහි භෞතික MAC (මාධ්‍ය ප්‍රවේශ පාලන) ලිපිනයට සිතියම්ගත කිරීමට භාවිතා කරන ජාල නියමාවලියකි.

How ARP Works
ARP ක්‍රියා කරන ආකාරය

First we should know the ip address of the destination.
පළමුවෙන්ම අප ගමනාන්තයේ (ඉෂ) ලිපිනය දැනගත යුතුය.

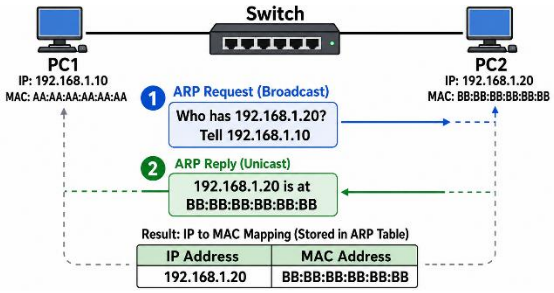
When a device wants to send data to another device on the same local network, it needs to know the recipient's MAC address, but it only knows the IP address.
උපාංගයකට එකම ස්ථානීය ජාලයේ වෙනත් උපාංගයකට දත්ත යැවීමට අවශ්‍ය වූ විට, එයට ග්‍රාහකයාගේ MAC ලිපිනය දැන ගැනීමට අවශ්‍ය වේ, නමුත් ග්‍රාහකයා දන්නේ IP ලිපිනය පමණි.

The device sends out an ARP Request message to all devices on the local network. This message includes the IP address for which the MAC address is being sought.
උපාංගය ස්ථානිය ජාලයේ සියලුම උපාංග වෙත ARP ඉල්ලීම් පණිවිඩයක් යවයි. මෙම පණිවිඩයේ MAC ලිපිනය සොයන උපාංගයට අදාල IP ලිපිනය ඇතුළත් වේ.

The device with the matching IP address replies with an ARP Reply message, providing its MAC address.
ගැළපෙන IP ලිපිනය සහිත උපාංගය එහි MAC ලිපිනය ලබා දෙමින් ARP පිළිතුරු පණිවිඩයක් සමඟ පිළිතුරු දෙයි.

The requesting device receives the ARP Reply and updates its ARP cache (a table storing IP-to-MAC address mappings) with this new information.
ඉල්ලා සිටින උපාංගයට ARP පිළිතුර ලැබෙන අතර මෙම නව තොරතුරු සමඟ එහි ARP නිහිතය IP-to-MAC ලිපින සිතියම්ගත කිරීම් ගබඩා කරන වගුවක්) යාවත්කාලීන කරයි.

With the MAC address now known, the device can send data packets to the recipient device using the MAC address.
දැන් දන්නා MAC ලිපිනය සමඟ, උපාංගයට MAC ලිපිනය භාවිතයෙන් දත්ත රාමු ග්‍රාහකයාගේ උපාංගයට යැවිය හැක.



ARP is only for local communication. A computer never tries to learn MAC address of a device on another network because MAC has local significance only.
ARP පවතින්නේ ස්ථානීය සන්නිවේදනය සඳහා පමණි. පරිගණකයක් කිසිවිටෙකත් වෙනත් ජාලයක ඇති උපාංගයක MAC ලිපිනය සෙවීමට උත්සාහ නොකරයි, මන්ද MAC ලිපිනයක් වැදගත් වන්නේ එම දේශීය ජාලය තුළ පමණක් බැවිනි.

Random Access Protocols
අහඹු ප්‍රවේශ නියමාවලි

1. ALOHA protocol

The ALOHA protocol was developed in the early 1970s by Norman Abramson and his team at the University of Hawaii.
ALOHA නියමාවලිය 1970 කාලයේ මුල් භාගයේදී හවායි විශ්ව විද්‍යාලයේ නෝමන් ඇබ්‍රම්සන් සහ ඔහුගේ කණ්ඩායම විසින් සංවර්ධනය කරන ලදී.

It was originally designed as a simple way to allow computers spread across the Hawaiian Islands to communicate with each other using radio waves (Wireless communication).
එය මුලින් නිර්මාණය කර ඇත්තේ හවායි දූපත් පුරා පැතිරී ඇති පරිගණකවලට රේඩියෝ තරංග භාවිතයෙන් එකිනෙකා සමඟ සන්නිවේදනය කිරීමට ඉඩ සලසන සරල ක්‍රමයක් ලෙස ය (රැහැන් රහිත සන්නිවේදනය).

So, ALOHA is a simple communication protocol used in network systems to manage access to a shared communication channel, ensuring that multiple devices can send data without causing constant collisions.
එබැවින්, ALOHA යනු හුවමාරු කරගත් සන්නිවේදන නාලිකාවකට ප්‍රවේශය කළමනාකරණය කිරීම සඳහා ජාල පද්ධතිවල භාවිතා කරන සරල සන්නිවේදන නියමාලියකි, එමගින් නිරන්තර ගැටුම් ඇති නොවී විවිධ උපාංගවලට දත්ත යැවිය හැකි බව සහතික කරයි.

How ALOHA Works
ක්‍රියා කරන ආකාරය

In ALOHA, devices do not check if the communication channel is clear before transmitting.
ALOHA හි, උපාංග මගින් සම්ප්‍රේෂණය කිරීමට පෙර සන්නිවේදන නාලිකාව පැහැදිලිදැයි පරීක්ෂා නොකරයි.

Uncoordinated Access

In ALOHA, devices can send data whenever they have information to transmit. There's no centralized control to manage when each device should send data.
ALOHA හි, සම්ප්‍රේෂණය කිරීමට උපාංගවලට තොරතුරු ඇති ඕනෑම අවස්ථාවක දත්ත යැවිය හැක. එක් එක් උපාංගය දත්ත යැවිය යුතු විට කළමනාකරණය කිරීමට මධ්‍යගත පාලනයක් නොමැත.

Collisions
Because devices send data without coordination, two or more devices might send data simultaneously, causing a collision. When this happens, the data gets garbled and needs to be resent.
උපාංග සම්බන්ධීකරණයකින් තොරව දත්ත යවන නිසා, උපාංග දෙකක් හෝ වැඩි ගණනක් එකවර දත්ත යැවිය හැකි අතර, එමගින් ගැටුමක් ඇති කරයි. මෙය සිදු වූ විට, දත්ත වෙනස් වන අතර නැවත යැවීමට සිදු වේ.

Acknowledgment
The sender waits for an acknowledgment from the receiver that the data was received successfully. If no acknowledgment is received, it assumes a collision occurred and resends the data after a random waiting time.
යවන්නා දත්ත සාර්ථකව ලැබුණු බවට ලබන්නාගෙන් පිළිගැනීමක් බලාපොරොත්තුවෙන් සිටී. පිළිගැනීමක් නොලැබුණේ නම්, එය ගැටුමක් සිදු වූ බව උපකල්පනය කරන අතර අහඹු රැඳී සිටීමේ කාලයකින් පසුව දත්ත නැවත යවයි.

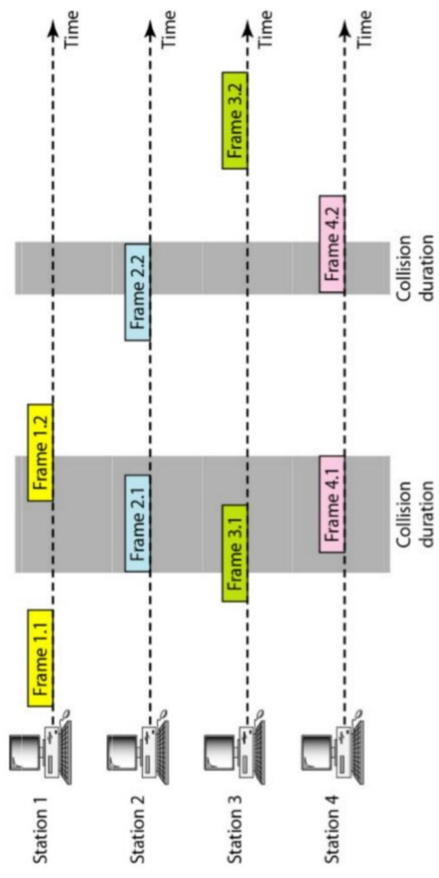
Randomized Retransmission
After a collision, devices wait for a random time before retransmitting. This reduces the chance of repeated collisions.
ගැටුමකින් පසු, උපාංග නැවත සම්ප්‍රේෂණය කිරීමට පෙර අහඹු වේලාවක් බලා සිටියි. මෙය නැවත නැවත ගැටීමේ සම්භාවිතාව අඩු කරයි.

In Pure ALOHA

Data can be transmitted to any device at any time.
ඕනෑම උපාංගයකට ඕනෑම අවස්ථාවකදී දත්ත සම්ප්‍රේෂණය කල හැක.

Since devices send data at random times, there is a high possibility that two or more devices may transmit at the same time, leading to collisions.
උපාංග අහඹු වේලාවන්හිදී දත්ත යවන බැවින්, එකවර උපාංග දෙකක් හෝ වැඩි ගණනක් සම්ප්‍රේෂණය කිරීමේ ඉහළ සම්භාවිතාවක් පවතින අතර එය ගැටුම් වලට තුඩු දෙයි.

This random wait time helps reduce the likelihood of repeated collisions.
මෙම අහඹු රැඳී සිටීමේ කාලය නැවත නැවත ගැටීමේ සම්භාවිතාව අඩු කිරීමට උපකාරී වේ.



Pure ALOHA has a relatively low efficiency because of frequent collisions.
නිතර ගැටෙන නිසා Pure ALOHA ට සාපේක්ෂව අඩු කාර්යක්ෂමතාවයක් ඇත.

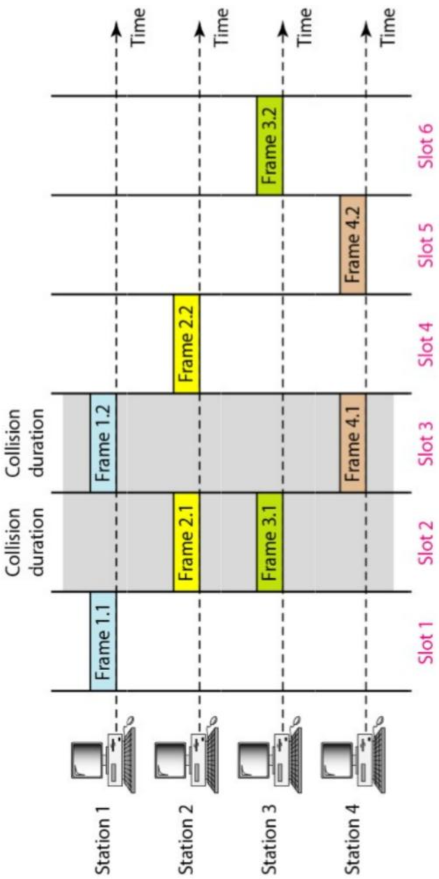
Slotted ALOHA

Slotted ALOHA improves efficiency by dividing time into discrete slots.
Slotted ALOHA මගින් කාලය විවික්ත slots වලට බෙදීමෙන් කාර්යක්ෂමතාව වැඩි දියුණු කරයි.

Devices can only send data at the beginning of a time slot.
උපාංගවලට දත්ත යැවිය හැක්කේ කාල පරාසයක ආරම්භයේදී පමණි.

Since devices can only send data at the start of a time slot, collisions are reduced compared to Pure ALOHA, where devices can transmit data at any time.
උපාංගවලට දත්ත යැවිය හැක්කේ කාල පරාසයක ආරම්භයේදී පමණක් බැවින්, උපාංගවලට ඕනෑම වේලාවක දත්ත සම්ප්‍රේෂණය කළ හැකි Pure ALOHA හා සසඳන විට මෙහි ගැටුම් අඩු වේ.

If a device misses out the allowed time, it must wait for the next time slot.
උපාංගයකට අවසර දී ඇති කාලය මග හැරී ගියහොත්, එය ඊළඟ time slot එක සඳහා රැඳී සිටිය යුතුය.



Applications
භාවිතයන්

Pure ALOHA is suitable for simple, unsynchronized communication systems, whereas Slotted ALOHA is suitable for systems that support synchronized transmission.
Pure ALOHA සරල, සමකාලීනකරණය නොකළ සන්නිවේදන පද්ධති සඳහා සුදුසු වන අතර, Slotted ALOHA සමකාලීන සම්ප්‍රේෂණයන් සඳහා සහය දක්වන පද්ධති සඳහා සුදුසු වේ.

Success Rate in ALOHA Protocols

The success rate in ALOHA protocols depends on the offered load (G), which represents the average number of transmission attempts during a frame time.
ALOHA නියමාවලිවල සාර්ථකත්ව අනුපාතය රඳා පවතින්නේ Offered Load (G) මතය. මෙමඟින් නිරූපණය වන්නේ එක් කුඩා කාලයක් තුළ දත්ත සම්ප්‍රේෂණය කිරීමට සිදුවන සාමාන්‍ය උත්සාහයන් ගණනයි.

As the number of transmitting devices increases, the offered load (G) increases, and the probability of collision becomes higher.
ජාලය තුළ දත්ත සම්ප්‍රේෂණය කරන උපාංග ගණන ඉහළ යත්ම, Offered Load (G) අගයද ඉහළ යන අතර දත්ත එකිනෙක ගැටීමේ සම්භාවිතාව වැඩි වේ.

A higher collision probability results in a lower success rate and reduced Throughput.
දත්ත ගැටීමේ සම්භාවිතාව වැඩි වීම, සාර්ථකත්වයේ ප්‍රතිශතය අඩු වීමට සහ දත්ත සම්ප්‍රේෂණ වේගය/කාර්යක්ෂමතාව අඩු වීමට හේතු වේ.

When only a few devices transmit, collisions are rare and the success rate remains high.
උපාංග කිහිපයක් පමණක් දත්ත සම්ප්‍රේෂණය කරන විට, දත්ත එකිනෙක ගැටීම ඉතා කලාතුරකින් සිදු වන අතර සාර්ථකත්වයේ ප්‍රතිශතය ඉහළ මට්ටමක පවතී.

Slotted ALOHA has twice the maximum Throughput of Pure ALOHA because transmissions are restricted to slot boundaries, reducing the vulnerable period from 2T to T and significantly decreasing packet collisions.
Slotted ALOHA සතු උපරිම Throughput අගය Pure ALOHA මෙන් දෙගුණයක් වන්නේ එහි දත්ත සම්ප්‍රේෂණයන් කාල පරිච්ඡේද වල ආරම්භයට පමණක් සීමා කර ඇති බැවිනි. එමඟින් දත්ත ගැටීමට ලක්විය හැකි අවදානම් කාල සීමාව 2T සිට T දක්වා අඩු වී, පැකට් එකිනෙක ගැටීම සැලකිය යුතු ලෙස පහත වැටේ.

2. CSMA/CD

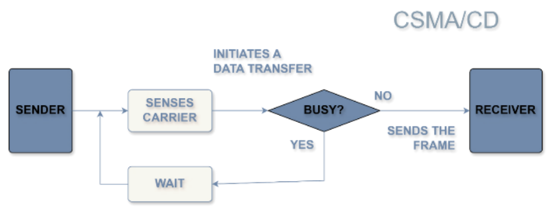
Ethernet uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection) to manage how multiple devices share a common communication channel.
උපාංග කිහිපයක් පොදු සන්නිවේදන නාලිකාවක් බෙදා ගන්නා ආකාරය කළමනාකරණය කිරීමට Ethernet විසින් CSMA/CD (Carrier Sense Multiple Access with Collision Detection) භාවිත කරයි.

This protocol ensures orderly data transmission and minimizes data collisions in a shared network.
මෙම නියමාවලිය විධිමත් දත්ත සම්ප්‍රේෂණය සහතික කරන අතර හවුල් ජාලයක දත්ත ගැටුම් අවම කරයි.

Carrier Sense (CS)

Before sending data, a device listens to the network to check if another device is already transmitting.
දත්ත යැවීමට පෙර, වෙනත් උපාංගයක් දැනටමත් සම්ප්‍රේෂණය කරන්නේ දැයි පරීක්ෂා කිරීමට උපාංගයක් ජාලයට සවන් දෙයි.

If the channel is busy, it waits before sending its data. This helps avoid immediate collisions.
නාලිකාව කාර්යබහුල නම්, එය එහි දත්ත යැවීමට පෙර බලා සිටී. මෙය ක්ෂණික ගැටුම් වළක්වා ගැනීමට උපකාරී වේ.



Multiple Access (MA)

Multiple Access (MA) is the ability of multiple devices to share and use the same communication medium (network cable or wireless channel).
Multiple Access (MA) යනු උපාංග කිහිපයකට එකම සන්නිවේදන මාධ්‍යයක් (ජාල කේබලයක් හෝ රැහැන් රහිත නාලිකාවක්) බෙදාහදා ගනිමින් භාවිත කිරීමට ඇති හැකියාවයි.

A multiple access protocol controls how devices access the shared medium, helping to reduce data transmission conflicts and improve network efficiency.
බහු ප්‍රවේශ නියමාවලිය මඟින් උපාංග පොදු මාධ්‍යයට ප්‍රවේශ වන ආකාරය පාලනය කරනු ලබයි. එමඟින් දත්ත සම්ප්‍රේෂණය කිරීමේදී සිදුවන ගැටුම් අවම කිරීමට සහ ජාලයේ කාර්යක්ෂමතාව වැඩි කිරීමට උදවු වේ.

Collision Detection (CD)

Despite checking, collisions can still occur if two devices start transmitting at nearly the same time.
පරීක්ෂා කළද, උපාංග දෙකක් ආසන්න වශයෙන් එකම වේලාවක සම්ප්‍රේෂණය කිරීමට පටන් ගන්නේ නම් ගැටීම් තවමත් සිදුවිය හැක.

To handle this, devices monitor the network while transmitting. If a collision is detected (when signal interference is noticed), both devices stop transmitting immediately.
මෙය හැසිරවීමට, සම්ප්‍රේෂණය කරන අතරතුර උපාංග ජාලය නිරීක්ෂණය කරයි. ගැටුමක් අනාවරණය වුවහොත් (සංඥා බාධාවන් නිරීක්ෂණය වූ විට), උපාංග දෙකම වහාම සම්ප්‍රේෂණය කිරීම නතර කරයි.

Collision Avoidance (CA)

Collision Avoidance (CA) is a technique used to reduce the chance of data collisions before transmission occurs.
Collision Avoidance (CA) යනු දත්ත සම්ප්‍රේෂණය වීමට පෙර, දත්ත එකිනෙක ගැටීමේ සම්භාවිතාව අඩු කිරීම සඳහා භාවිත කරන තාක්ෂණයකි.

Before sending data, a device listens to the communication medium. If the medium is busy, it waits for a random period before checking again and transmitting only when the medium is free.

Backoff and Retry

After a collision, devices wait for a random **backoff period** before resending data, helping to prevent repeated collisions.
දත්ත එකිනෙක ගැටීමකින් පසුව, නැවත නැවතත් ගැටීම් සිදුවීම වැළැක්වීම සඳහා, උපාංග නැවත දත්ත යැවීමට පෙර අහඹු පසුබැසීමේ කාල සීමාවක් රැඳී සිටියි.

Feature ලක්ෂණය	Pure ALOHA	Slotted ALOHA	CSMA/CD
Transmission Method සම්ප්‍රේෂණ ක්‍රමය	Devices transmit at any time. උපාංග ඕනෑම වේලාවක දත්ත සම්ප්‍රේෂණය කරයි	Devices transmit only at the beginning of a time slot. උපාංගවලට දත්ත සම්ප්‍රේෂණය කළ හැක්කේ කාල සීමාවක ආරම්භයේදීම පමණි	Devices listen before transmitting. උපාංග දත්ත සම්ප්‍රේෂණය කිරීමට පෙර මාධ්‍යයට සවන් දෙයි.
Carrier Sensing වාහක සංවේදනය	No/නැත	No/නැත	Yes/ ඇත
Collision Detection ගැටුම් හඳුනාගැනීම	No/නැත	No/නැත	Yes/ ඇත
Collision Probability ගැටුම් සම්භාවිතාව	Very High ඉතා ඉහළයි	Lower than Pure ALOHA Pure ALOHA වලට වඩා අඩුයි	Low/ අඩුයි
Time Synchronization කාල සමකාලීනකරණය	Not Required අවශ්‍ය නොවේ	Required අවශ්‍ය වේ	Not Required අවශ්‍ය නොවේ
Efficiency කාර්යක්ෂමතාව	Low අඩුයි (≈18%)	Moderate මධ්‍යස්ථයි (≈37%)	High/ ඉහළයි
Collision Handling ගැටුම් කළමනාකරණය	Waits a random time and retransmits. අහඹු වේලාවක් රැඳී සිට නැවත සම්ප්‍රේෂණය කරයි	Waits a random time and retransmits. අහඹු වේලාවක් රැඳී සිට නැවත සම්ප්‍රේෂණය කරයි	Detects collision, stops transmission immediately, then retransmits after a random backoff time. ගැටුමක් හඳුනාගත් සැනින් සම්ප්‍රේෂණය නවතා අහඹු පසුබැසීමේ කාලයකට පසු නැවත සම්ප්‍රේෂණය කරයි
Typical Network ප්‍රායෝගික ජාලකරණ භාවිතය	Early radio communication මුල්කාලීන රේඩියෝ සන්නිවේදනය	Synchronized satellite communication සමකාලීන චන්ද්‍රිකා සන්නිවේදනය	Wired Ethernet (Half-duplex) රැහැන් සහිත Ethernet

Transport Layer Protocols (TCP and UDP)

Both TCP and UDP are transport-layer protocols that define how data is sent across a network. They serve different purposes and suit different use cases.
TCP සහ UDP යන දෙකම ජාලයක් හරහා දත්ත යවනු ලබන ආකාරය නිර්වචනය කරන ප්‍රවාහන ස්ථර නියමාවලි වේ. ඒවා විවිධ අරමුණු ඉටු කරන අතර විවිධ භාවිත අවස්ථා සඳහා සුදුසු වේ.

TCP (Transmission Control Protocol)

A connection-oriented protocol, meaning that a reliable connection is established between the sender and receiver before any data is transferred.
සම්බන්ධතා-නැඹුරු නියමාවලියකි, එයින් අදහස් කරන්නේ ඕනෑම දත්තයක් හුවමාරු කිරීමට පෙර යවන්නා සහ ග්‍රාහකයා අතර විශ්වාසනීය සම්බන්ධතාවයක් ස්ථාපිත කර ගන්නා බවයි.

How a TCP connection is established (3-Way Handshake)

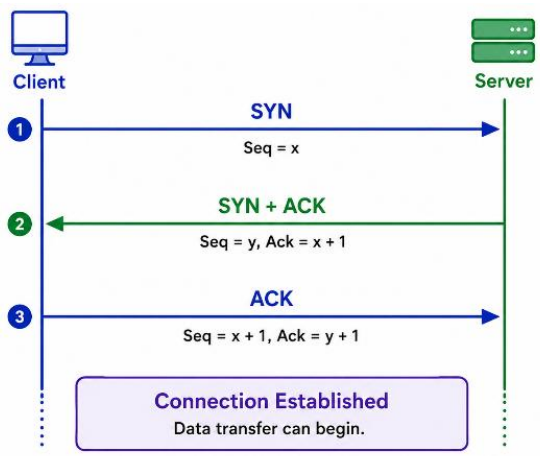
1. SYN
The sender sends a synchronize (SYN) request to initiate the connection.
සම්බන්ධතාවය ආරම්භ කිරීම සඳහා යවන්නා විසින් සමමුහුර්තකරණ (SYN) ඉල්ලීමක් යවයි.

2. SYN-ACK
The receiver responds with a synchronize-acknowledge (SYN-ACK).
ලබන්නා විසින් සමමුහුර්තකරණ-පිළිගැනීමේ (SYN-ACK) පණිවිඩයක් මඟින් ප්‍රතිචාර දක්වයි.

3. ACK
The sender replies with an acknowledgment (ACK), completing the connection setup.
යවන්නා විසින් පිළිගැනීමේ (ACK) පණිවිඩයක් මඟින් පිළිතුරු සපයන අතර, එමඟින් සම්බන්ධතාවය පිහිටුවීම සම්පූර්ණ වේ.

Three steps are needed because both sides must independently confirm they can send and receive.
පියවර තුනක් අවශ්‍ය වන්නේ දෙපාර්ශවයටම තමන්ට දත්ත යැවීමට සහ ලැබීමට හැකි බව ස්වාධීනව තහවුරු කර ගත යුතු බැවිනි.

Two steps would leave one side's readiness unverified.
පියවර දෙකක් පමණක් තිබුනේ නම්, එක් පාර්ශවයක සූදානම තහවුරු නොවී පවතිනු ඇත.



Characteristics of TCP
TCP හි ලක්ෂණ

Connection-Oriented / සම්බන්ධතා-නැඹුරු
Requires a handshake before data transmission.
දත්ත සම්ප්‍රේෂණයට පෙර අතට අත දීමක් (handshake) අවශ්‍ය වේ.

Reliable / විශ්වසනීය වේ
Guarantees error-free, ordered delivery. Lost packets are retransmitted.
දෝෂ රහිත, අනුපිළිවෙලින් යුත් බෙදාහැරීමක් සහතික කරයි. මඟ හැරුණු දත්ත පැකට්ටු නැවත සම්ප්‍රේෂණය කරනු ලැබේ.

Congestion Control / තදබදය පාලනය
Monitors network traffic and reduces transmission speed if congestion is detected.
ජාල ගමනාගමනය නිරීක්ෂණය කරන අතර තදබදයක් අනාවරණය වුවහොත් සම්ප්‍රේෂණ වේගය අඩු කරයි.

Sequencing / අනුක්‍රමණය
Assigns sequence numbers to packets so they can be reassembled in the correct order.
දත්ත පැකට්ටු නිවැරදි අනුපිළිවෙලට නැවත සැකසිය හැකි වන පරිදි ඒවාට අනුක්‍රමික අංක ලබා දෙයි.

Acknowledgment (ACK) / පිළිගැනීම
The receiver confirms every packet received. If no ACK is received, the sender retransmits.
ලබන්නා විසින් ලැබුණු සෑම පැකට්ටුවක්ම තහවුරු කරයි. කිසිදු ACK පණිවිඩයක් නොලැබුනේ නම්, ප්‍රේරකයා විසින් එය නැවත සම්ප්‍රේෂණය කරයි.

Header Size / ශීර්ෂ ප්‍රමාණය
20–60 bytes
A header is a block of metadata prepended to each packet that tells the network how to handle and deliver it.
ශීර්ෂයක් යනු ජාලය විසින් එය හසුරුවන සහ බෙදාහරින ආකාරය පවසන, එක් එක් දත්ත පැකට්ටුවකට කලින් එක් කරනු ලබන පාරදත්ත කොටසකි.

Common Use Cases / භාවිතා වන අවස්ථා
Any scenario where data accuracy matters more than speed.
වේගයට වඩා දත්තවල නිරවද්‍යතාවය වැදගත් වන ඕනෑම අවස්ථාවක්.

- Web browsing (HTTP/HTTPS)
- Email (SMTP, IMAP, POP3)
- File transfers (FTP, SFTP)
- SSH connections

UDP (User Datagram Protocol)

A connectionless protocol. Data is sent directly without establishing a connection first.
සම්බන්ධතාවලින් තොර (connectionless) නියමාවලියකි. පළමුව සම්බන්ධතාවයක් පිහිටුවීමකින් තොරව දත්ත සෘජුවම යවනු ලැබේ.

Characteristics of UDP
UDP හි ලක්ෂණ

Faster than TCP / TCP වලට වඩා වේගවත්ය
UDP skips connection setup, acknowledgments, retransmissions, and ordering reducing latency and processing cost significantly.
UDP විසින් සම්බන්ධතාවය පිහිටුවීම, පිළිගැනීම්, නැවත සම්ප්‍රේෂණය කිරීම් සහ අනුපිළිවෙලකට සැකසීම් මගහරින බැවින් ප්‍රමාද කාලය සහ සැකසුම් පිරිවැය සැලකිය යුතු ලෙස අඩු කරයි.

Connectionless / සම්බන්ධතා නොමැත
No handshake or setup required. Data is sent immediately.
අතට අත දීමක් (handshake) හෝ පිහිටුවීමක් අවශ්‍ය නොවේ. දත්ත වහාම යවනු ලැබේ.

Unreliable / විශ්වසනීය නොවන
No guarantee of delivery. Lost packets are not retransmitted.
බෙදාහැරීම පිළිබඳ සහතිකයක් නොමැත. මඟ හැරුණු දත්ත පැකට්ටු නැවත සම්ප්‍රේෂණය නොකෙරේ.

No Sequencing / අනුක්‍රමණයක් නොමැත
Packets may arrive out of order; UDP does not reorder them.
දත්ත පැකට්ටු අනුපිළිවෙලින් බැහැරව පැමිණිය හැකිය; UDP මඟින් ඒවා නැවත අනුපිළිවෙලකට සකස් නොකරයි.

No Flow Control / ප්‍රවාහ පාලනයක් නොමැත
Data is sent at whatever rate the application generates it.
යෙදුම (application) මඟින් ජනනය කරන ඕනෑම වේගයකින් දත්ත යවනු ලැබේ.

No Congestion Control / තදබදය පාලනයක් නොමැත
Does not slow down when the network is congested.
ජාලය තදබදයක් ඇති විට දී ද වේගය අඩු නොකරයි.

No Acknowledgment / පිළිගැනීමක් නොමැත
The sender never knows if the data arrived.
දත්ත ලැබුණේද නැද්ද යන්න යවන්නා කිසිවිටෙක නොදනී.

Low Overhead / අඩු ශීර්ෂ ප්‍රමාණය
Header is only 8 bytes, making it faster and more lightweight than TCP.
ශීර්ෂය බයිට 8 ක් පමණක් වන බැවින්, එය TCP වලට වඩා වේගවත් සහ සැහැල්ලු වේ.

Common Use Cases / භාවිතා වන අවස්ථා

Any scenario where speed matters more than perfect delivery.
පරිපූර්ණ බෙදාහැරීමට වඩා වේගය වැදගත් වන ඕනෑම අවස්ථාවක්.

- Live video and audio streaming
- Online gaming
- VoIP (Voice over IP)
- DNS queries
- IoT sensor data

TCP vs UDP **(Summary)**

Property / ලක්ෂණය	**TCP**	**UDP**
Connection සම්බන්ධතාව	Connection-oriented සම්බන්ධතා-නැඹුරු	Connectionless සම්බන්ධතා-රහිත
Reliability විශ්වසනීයත්වය	Guaranteed delivery දත්ත ලැබෙන බවට සහතික කරයි	No guarantee දත්ත ලැබෙන බවට සහතිකයක් නැත
Ordering පිළිවෙළ සකස් කිරීම	Packets reordered පැකට්ටු නිසි පිළිවෙළට සකස් කෙරේ	Packets may arrive out of order පැකට්ටු අක්‍රමවත්ව ලැබිය හැක
Speed වේගය	Slower (due to overhead) මන්දගාමීයි (Overhead නිසා)	Faster (minimal overhead) වේගවත් (අවම overhead)
Header Size ශීර්ෂයේ ප්‍රමාණය	20–60 bytes බයිට (20–60)	8 bytes බයිට 8
Error Checking දෝෂ පරීක්ෂාව	Yes (with retransmission) ඔව් (නැවත සම්ප්‍රේෂණය කිරීම් ද සහිතව)	Basic checksum only මූලික චෙක්සම් එකක් පමණි

ictfromabc.com

Multiplexing
බහුපථකරණය

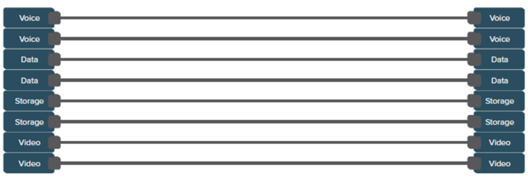
Multiplexing is the process of sending multiple signals or data streams over a single communication channel, such as a wire or a radio frequency at the same time.
බහුපථකරණය යනු වයරයක් හෝ රේඩියෝ සංඛ්‍යාතයක් වැනි තනි සන්නිවේදන නාලිකාවක් හරහා එකම අවස්ථාවේදී සංඥා හෝ දත්ත ප්‍රවාහ කිහිපයක් යැවීමේ ක්‍රියාවලියයි.

A Multiplexer (MUX) combines the signals at the sender.
බහුපථකරණය මඟින් යවන්නාගේ පාර්ශවයේදී මෙම සංඥා එකිනෙක ඒකාබද්ධ කරනු ලබයි.

A Demultiplexer (DEMUX) separates the signals at the receiver.
ප්‍රති-බහුපථකරණය මඟින් ලබන්නාගේ පාර්ශවයේදී එම සංඥා එකිනෙක වෙන් කරනු ලබයි.

There are four types of multiplexing
බහුපථකරණයෙහි ආකාර හතරක් තිබේ

- Time Division Multiplexing(TDM)
  කාලය බෙදීමේ බහුපථකරණය
- Frequency Division Multiplexing(FDM)
  සංඛ්‍යාතය බෙදීමේ බහුපථකරණය
- Wavelength Division Multiplexing(WDM)
  තරංග ආයාමය බෙදීමේ බහුපථකරණය
- Code Division Multiplexing(CDM/CDMA)
  කේතය බෙදා ගැනීමේ බහුපථකරණය



Individual fibers per channel

Multiplexing combines multiple channels on a single dark fiber

Advantages of multiplexing
බහුපථකරණයේ වාසි

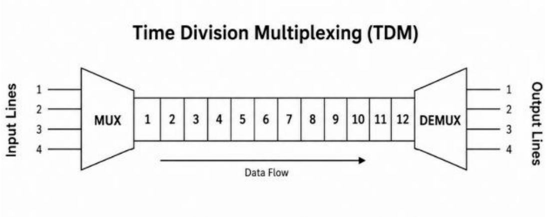
- Efficient utilization of bandwidth
  කලාප පළල කාර්යක්ෂමව භාවිත කරයි
- Allows multiple users to share one communication channel
  බහුවිධ පරිශීලකයන්ට එක් සන්නිවේදන නාලිකාවක් බෙදා ගැනීමට ඉඩ සලසයි
- Reduces communication cost
  සන්නිවේදන පිරිවැය අඩු කරයි
- Increases channel capacity
  නාලිකා ධාරිතාව වැඩි කරයි
- Simplifies network infrastructure
  ජාල යටිතල පහසුකම් සරල කරයි
- Supports many users simultaneously
  එකවර පරිශීලකයින් විශාල ප්‍රමාණයකට සහය දක්වයි
- Simplifies network expansion
  ජාල ව්‍යාප්තිය සරල කරයි
- Communication medium is used at all times more and more effectively by someone
  සන්නිවේදන මාධ්‍යය සෑම විටම වඩ වඩාත් ඵලදායී ලෙස කවුරුන් හෝ භාවිත කරනු ලබයි

Disadvantages of multiplexing
බහුපථකරණයේ අවාසි

- Failure of the shared channel affects all users
  හවුල් නාලිකාවේ බිඳවැටීම සියලුම පරිශීලකයින්ට බලපායි
- Requires additional hardware (mux and demux)
  අමතර දෘඩාංග (mux සහ demux) අවශ්‍ය වේ
- Communication becomes more complex
  සන්නිවේදනය වඩාත් සංකීර්ණ වේ

ictfromabc.com

Time Division Multiplexing (TDM)
කාලය බෙදීමේ බහුපථකරණය



Time Division Multiplexing transmits multiple signals over a single communication channel by dividing the transmission time into slots.
කාලය බෙදාගැනීමේ බහුපථකරණය මගින් සම්ප්‍රේෂණ කාලය slot වලට බෙදා තනි සන්නිවේදන නාලිකාවක් හරහා බහු සංඥා සම්ප්‍රේෂණය කරයි.

Time Slots
The total transmission time is divided into small segments called time slots. Each signal or data stream gets a specific time slot to transmit its information.
සම්පූර්ණ සම්ප්‍රේෂණ කාලය time slots ලෙස හැඳින්වෙන කුඩා කොටස් වලට බෙදා ඇත. සෑම සංඥාවක්ම හෝ දත්ත ප්‍රවාහයක්ම එහි තොරතුරු සම්ප්‍රේෂණය කිරීමට නිශ්චිත time slot එකක් ලබා ගනී.

Frames
A frame is one complete set of time slots, with one slot assigned to each input channel. Are transmitted repeatedly to allow all channels to share the same communication link.
රාමුවක් යනු සම්පූර්ණ කාල පරාසයන්කට්ටලයකි. මෙහිදී එක් එක් ආදාන නාලිකාව සඳහා එක් කාල පරාසය බැගින් වෙන්කර ඇත. සියලුම නාලිකාවලට එකම සන්නිවේදන සබැඳිය බෙදාහදා ගැනීමට ඉඩ සැලසීම සඳහා මේවා නැවත නැවතත් සම්ප්‍රේෂණය කරනු ලැබේ.

Round-Robin Fashion
The time slots are allocated to each signal in a sequential, round-robin manner. After all signals have transmitted their data in their respective time slots, the cycle repeats.
එක් එක් සංඥා සඳහා අනුක්‍රමික, රවුන්ඩ් රොබින් ආකාරයෙන් time slots වෙන් කරනු ලැබේ. සියලුම සංඥා ඒවායේ දත්ත නියමිත time slot එක තුළ සම්ප්‍රේෂණය කළ පසු, මෙම චක්‍රය නැවත සිදුවේ.

Synchronization
Both the sender and receiver must be synchronized to ensure that each signal transmits and receives data in the correct time slot.
සෑම සංඥාවක්ම නිවැරදි time slot එක තුළ දත්ත සම්ප්‍රේෂණය කිරීම සහ ලබා ගැනීම සහතික කිරීම සඳහා යවන්නා සහ ලබන්නා යන දෙකම සමමුහුර්ත කළ යුතුය.

Guard Time
Guard time is a small unused interval inserted between consecutive time slots to prevent overlapping caused by synchronization errors.
ආරක්ෂක කාලය යනු සමමුහුර්තකරණ දෝෂ හේතුවෙන් සිදුවන එකිනෙක මත අතිච්ඡාදනය වීම් වැළැක්වීම සඳහා, අනුගාමික කාල පරාසයන් අතරට ඇතුළත් කරනු ලබන භාවිතයට නොගන්නා කුඩා කාල පරතරයකි.

Advantages of TDM
TDMහි වාසි

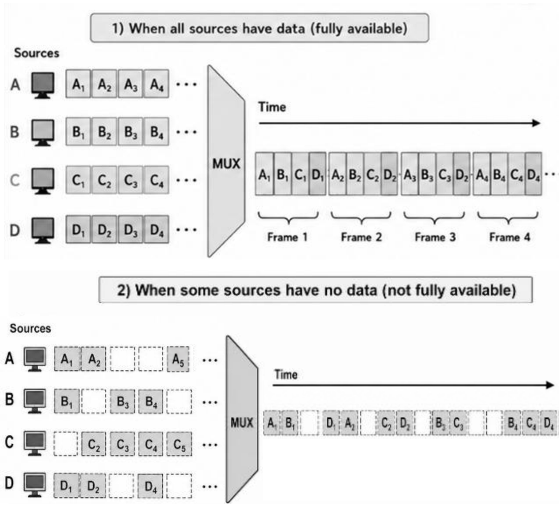
- Efficient channel utilization.
  කාර්යක්ෂම නාලිකා භාවිතය.
- No signal interference.
  සංඥා බාධා කිරීම් නොමැති වීම.
- Reliable digital transmission.
  විශ්වසනීය අංකිත සම්ප්‍රේෂණය.
- Cost-effective communication.
  පිරිවැය-ඵලදායී සන්නිවේදනය.

Disadvantages of TDM
TDMහි අවාසි

- Requires precise synchronization.
  නිවැරදි සමමුහුර්තකරණයක් අවශ්‍ය වේ.
- Time slots may be wasted.
  කාල පරාසයන් අපතේ යා හැක.
- Transmission delay may occur.
  සම්ප්‍රේෂණ ප්‍රමාදයන් සිදුවිය හැක.
- Higher implementation complexity.
  ක්‍රියාත්මක කිරීමේ සංකීර්ණත්වය වැඩි වීම.

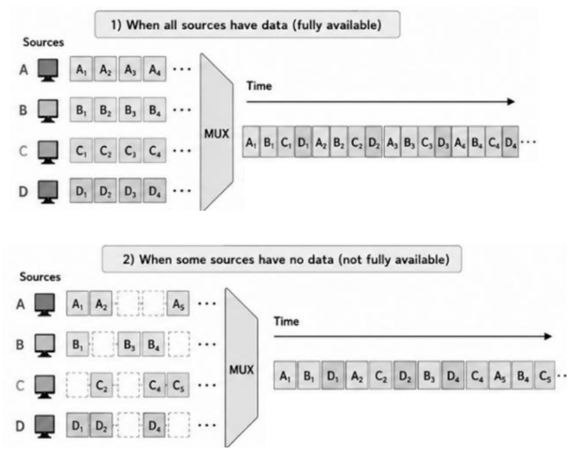
Types of TDM
TDM වර්ග

Synchronous TDM
සමමුහුර්ත TDM



Each input device is assigned a fixed time slot in every transmission cycle regardless of whether it has data to send. As a result, time slots remain reserved even when no data is transmitted, which can lead to inefficient bandwidth utilization**.**
සෑම ආදානයට ම සෑම ප්‍රසාරණ වාරයකදීම ස්ථාවර කාල පරාසයක් වෙන් කරනු ලැබේ. දත්ත සම්ප්‍රේෂණය නොකළද එම කාල පරාසයන් වෙන් කර ඇති බැවින් කලාප පළලයෙන් යම් අපාතේ යෑමක් සිදු විය හැකිය.

Statistical (Asynchronous) TDM
සංඛ්‍යානමය / අසමමුහුර්ත TDM

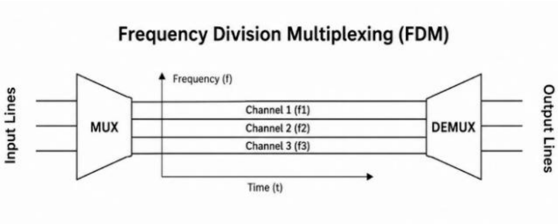


Time slots are allocated dynamically only to devices that have data to transmit. Since unused slots are not reserved, the available bandwidth is utilized more efficiently and channel capacity is improved.
කාල පරාසයන් වෙන් කරනු ලබන්නේ දත්ත පවතින ආදායන සඳහා පමණි. භාවිත යෝජනා නොකරන කාල පරාසයන් අපාතේ නොයන බැවින් කලාප පළලය වඩා කාරයක්ෂම ලෙස භාවිතා කළ හැකිය.

Common Applications
පොදු භාවිතයන්

- Digital Telephone Networks (PSTN): Multiple voice calls share a single communication line.
  ඩිජිටල් දුරකථන ජාල (PSTN): බහුවිධ හඬ ඇමතුම් තනි සන්නිවේදන මාර්ගයක් බෙදාහදා ගනී.
- GSM Cellular Networks (TDMA): Multiple users communicate over the same frequency using assigned time slots.
  GSM සෙලියුලර් ජාල (TDMA): පරිශීලකයින් කිහිප දෙනෙකු තමන්ට වෙන් කරන ලද කාල පරාසයන් භාවිතයෙන් එකම සංඛ්‍යාතය හරහා සන්නිවේදනය කරයි
- Fiber Optic Networks (SONET/SDH): Multiple digital signals are transmitted through a single optical fiber.
  ප්‍රකාශ තන්තු ජාල (SONET/SDH): බහුවිධ අංකිත සංඥා ප්‍රකාශ තන්තුවක් හරහා සම්ප්‍රේෂණය වේ.
- Satellite Communication: Several ground stations share the same satellite channel using time-slot allocation.
  චන්ද්‍රිකා සන්නිවේදනය: භූමිස්ථාන කිහිපයක් කාල පරාස වෙන් කිරීම් භාවිතයෙන් එකම චන්ද්‍රිකා නාලිකාව බෙදාහදා ගනී.
- Industrial Automation: Data from multiple sensors and controllers is transmitted over a common communication link.
  කාර්මික ස්වයංක්‍රීයකරණය:සංවේදක සහ පාලක කිහිපයකින් ලැබෙන දත්ත පොදු සන්නිවේදන සබැඳියක් හරහා සම්ප්‍රේෂණය වේ.

Frequency Division Multiplexing (FDM)
සංඛ්‍යාතය බෙදීමේ බහුපථකරණය



FDM transmit multiple signals over a single communication channel by assigning each signal a different frequency band within the given bandwidth.

FDM මගින් දී ඇති කලාප පළල තුළ එක් එක් සංඥාවට එකිනෙකට වෙනස් සංඛ්‍යාත පරාසයන් බැගින් ලබා දීමෙන්, තනි සන්නිවේදන නාලිකාවක් ඔස්සේ බහුවිධ සංඥා සම්ප්‍රේෂණය කරනු ලබයි.

Dividing the Frequency Spectrum
The available bandwidth is divided into multiple frequency bands, and each signal is assigned to a specific band.

පවතින කලාප පළල බහු සංඛ්‍යාත කලාපවලට බෙදා, සෑම සංඥාවක්ම නිශ්චිත කලාපයකට පවරා ඇත.

Simultaneous Transmission
All signals are transmitted simultaneously, but each occupies its own frequency range.

සියලුම සංඥා එකවර සම්ප්‍රේෂණය වේ, නමුත් සෑම එකක්ම තමන්ගේම සංඛ්‍යාත පරාසයක් ගනී.

Bandpass Filters
At the receiver end, filters are used to separate the signals based on their frequency bands, ensuring that each signal is correctly decoded without interference from others.

ග්‍රාහක අන්තයේදී, ඒවායේ සංඛ්‍යාත පරාස මත පදනම්ව සංඥා වෙන් කිරීමට පෙරහන් භාවිතා කරනු ලැබේ, එමගින් සෑම සංඥාවක්ම අනෙක් ඒවාගෙන් බාධාවකින් තොරව නිවැරදිව විකේතනය කරන බව සහතික කරයි.

Guard Bands
Guard bands are small unused frequency ranges placed between adjacent channels to prevent interference.

ආරක්ෂක කලාප යනු මැදිහත්වීම් වැළැක්වීම සඳහා යාබද නාලිකා අතර පිහිටුවා ඇති, භාවිතයට නොගන්නා කුඩා සංඛ්‍යාත පරාසයන් වේ

Examples of FDM
FDM පිළිබඳ උදාහරණ

AM/FM Radio Broadcasting
AM/FM රේඩියෝ විකාශනය

Each radio station is assigned a different frequency.

සෑම රේඩියෝ නාලිකාවකටම එකිනෙකට වෙනස් වූ සංඛ්‍යාතයක් බැගින් ලබා දී ඇත.

Cable Television (CATV)
කේබල් රූපවාහිනී සේවා

Multiple TV channels are transmitted simultaneously on different frequency bands through the same coaxial cable.

එකම සමාක්ෂ කේබලයක් හරහා එකිනෙකට වෙනස් සංඛ්‍යාත පරාසයන් ඔස්සේ රූපවාහිනී නාලිකා කිහිපයක් එකවර සම්ප්‍රේෂණය කරනු ලබයි.

Satellite Communication
උපග්‍රහණ සන්නිවේදනය

Different communication channels use separate frequency bands on the same satellite link.

එකම උපග්‍රහණ සබැඳියක් තුළ, විවිධ සන්නිවේදන නාලිකා සඳහා එකිනෙකට වෙනස් වූ සංඛ්‍යාත පරාසයන් භාවිතා කරනු ලබයි.

DSL (Digital Subscriber Line)
Voice and Internet data are transmitted simultaneously over the same telephone line using separate frequency bands.

එකම දුරකථන රැහැනක් හරහා එකිනෙකට වෙනස් සංඛ්‍යාත පරාසයන් භාවිතා කරමින් හඬ සහ අන්තර්ජාල දත්ත එකවර සම්ප්‍රේෂණය කරනු ලබයි.

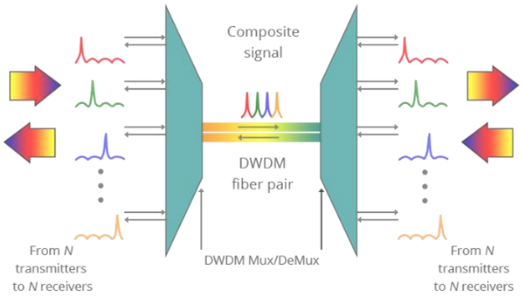
Advantages of FDM
FDM හි වාසි

- Simultaneous transmission allows all users to communicate without waiting for channel access.
  සමගාමී සම්ප්‍රේෂණය නාලිකාවට ප්‍රවේශ වීම සඳහා බලා සිටීමකින් තොරව සියලුම පරිශීලකයින්ට එකිනෙකා සමඟ සන්නිවේදනය කිරීමට ඉඩ සලසයි.
- Very low transmission delay (latency) due to dedicated frequency channels.
  සංඛ්‍යාත නාලිකා භාවිතය නිසා සම්ප්‍රේෂණ ප්‍රමාදය ඉතා අවම වේ.
- Continuous data transfer is possible because each user is assigned a fixed frequency band.
  එක් එක් පරිශීලකයා සඳහා ස්ථාවර සංඛ්‍යාත කලාපයක් පවරා ඇති බැවින් අඛණ්ඩව දත්ත හුවමාරු කිරීමේ හැකියාව පවතී.
- Suitable for real-time applications, such as radio and television broadcasting.
  ගුවන්විදුලි සහ රූපවාහිනී විකාශනය වැනි තත්කාලීන යෙදුම් සඳහා වඩාත් සුදුසු වේ

Disadvantages of FDM
FDM හි අවාසි

- Bandwidth utilization is inefficient, as an allocated frequency band remains.
  දත්ත සම්ප්‍රේෂණය නොවන විට පවා වෙන් කරන ලද සංඛ්‍යාත කලාපයක් එලෙසම රඳවා තබා ගන්නා බැවින්, කලාප පළල භාවිතය අකාර්යක්ෂම වේ.
- Unused frequency bands cannot be shared with other users during communication.
  සන්නිවේදනය අතරතුර භාවිතයට නොගත් සංඛ්‍යාත කලාප අනෙකුත් පරිශීලකයන් සමඟ බෙදා ගත නොහැක.
- Guard bands are required between adjacent frequency channels to minimize interference, reducing the effective bandwidth.
  බාධා අවම කිරීම සඳහා යාබද සංඛ්‍යාත නාලිකා අතර ආරක්ෂක කලාප අවශ්‍ය වන අතර, එමඟින් ඵලදායී කලාප පළල අඩු වේ.
- Susceptible to crosstalk and adjacent-channel interference if channels are not adequately separated.
  නාලිකා ප්‍රමාණවත් ලෙස වෙන් කර නොමැති නම්, ඒවා crosstalk සහ යාබද නාලිකා බාධාවලට ගොදුරු වීමේ ඉඩකඩ වැඩිය.

Wavelength division multiplexing (WDM)
තරංග ආයාමය බෙදීමේ බහුපථකරණය



Used only with optic fiber (same as FDM using light)
ප්‍රකාශ තන්තු සමඟ පමණක් භාවිතා වේ (ආලෝකය භාවිතා කරන FDM ක්‍රියාවලියට සමාන වේ).

Wavelength Division Multiplexing is a technique that allows multiple data streams to be transmitted simultaneously over a single optical fiber by using different wavelengths (or colors) of light for each data stream.
තරංග ආයාමය බෙදීමේ බහුපථකරණය යනු එක් එක් දත්ත ප්‍රවාහය සඳහා ආලෝකයේ විවිධ තරංග ආයාම (හෝ වර්ණ) භාවිතා කරමින් එක් ප්‍රකාශ තන්තුවක් හරහා බහු දත්ත ප්‍රවාහයන් එකවර සම්ප්‍රේෂණය කිරීමට ඉඩ සලසන තාක්ෂණයකි.

Each wavelength carries its own data signal, and since these wavelengths do not interfere with each other, they can travel together on the same fiber.
සෑම තරංග ආයාමයක්ම එයට වෙන්වූ දත්ත සංඥාවක් රැගෙන යන අතර, මෙම තරංග ආයාම එකිනෙකට බාධා නොකරන බැවින්, එකම තන්තුවක් තුළින් එකට ගමන් කළ හැක.

There are two main types
ප්‍රධාන වර්ග දෙකකි

Dense Wavelength Division Multiplexing (DWDM)
Uses closely spaced wavelengths, allowing more channels to be transmitted over the same fiber.
එකම තන්තුව හරහා වැඩි නාලිකා සම්ප්‍රේෂණය කිරීමට ඉඩ සලසමින් සමීප පරතරයන් සහිත තරංග ආයාම භාවිතා කරයි.

Coarse Wavelength Division Multiplexing (CWDM)
Uses fewer wavelengths with wider spacing between them, typically for shorter-distance communication.සාමාන්‍යයෙන් කෙටි දුර සන්නිවේදනය සඳහා, අඩු තරංග ආයාම ඒවා අතර පුළුල් පරතරයක් සහිත භාවිතා කරයි.

How WDM works
WDM ක්‍රියා කරන ආකාරය

Optical multiplexer
At the transmitting end, an optical multiplexer combines multiple signals from different sources onto a single fiber, each at a different wavelength.
සම්ප්‍රේෂණ අන්තයේ දී, දෘශ්‍ය බහුපථකරණයක් විවිධ ප්‍රභව වලින් ලැබෙන සංඥා කිහිපයක්, සෑම එකක්ම වෙනස් තරංග ආයාමයකින් එක් තන්තුවක් මතට ඒකාබද්ධ කරයි.

Optical fiber transmission
The multiplexed signals are transmitted over the optical fiber.
බහු සංඥා ප්‍රකාශ තන්තු හරහා සම්ප්‍රේෂණය වේ.

Optical demultiplexer
At the receiving end, an optical demultiplexer separates the individual signals based on their wavelength.
ග්‍රාහක අන්තයේ දී, ප්‍රකාශ ප්‍රති බහුපථකරණයක් මඟින් ඒවායේ තරංග ආයාමය මත පදනම්ව තනි තනි සංඥා වෙන් කරයි.

Applications of WDM
WDM හි යෙදුම්

Long-haul optical networks
WDM is widely used in long-haul optical networks to transmit large amounts of data over long distances.(Ex:Submarine cables)
WDM දිගු දුර ප්‍රකාශ ජාල වල විශාල දත්ත ප්‍රමාණයක් දිගු දුරකට සම්ප්‍රේෂණය කිරීමට බහුලව භාවිතා වේ.(උදා: සබ්මැරීන් කේබල්)

Data centers
WDM can be used to interconnect servers and storage devices in data centers.
දත්ත මධ්‍යස්ථානවල සේවාදායක සහ ගබඩා උපාංග අන්තර් සම්බන්ධ කිරීමට උෟව භාවිතා කළ හැක.

Optical Fiber Backbone Networks
ප්‍රකාශ තන්තු බැක්බෝන් ජාල
Enables multiple wavelengths to carry large volumes of data over a single optical fiber, increasing network capacity and efficiency.
ජාලයේ ධාරිතාව සහ කාර්යක්ෂමතාව ඉහළ නංවමින්, තනි ප්‍රකාශ තන්තුවක් හරහා විශාල දත්ත ප්‍රමාණයක් රැගෙන යාමට තරංග ආයාම කිහිපයකට ඉඩ සලසයි.

Advantages of WDM
WDM හි වාසි

- **Extremely High Capacity**
  ඉතා ඉහළ ධාරිතාව
  Multiple signals are transmitted simultaneously over a single optical fiber.
  තනි ප්‍රකාශ තන්තු කේබලයක් ඔස්සේ එකවර සංඥා කිහිපයක් සම්ප්‍රේෂණය කළ හැකිය.
- **Efficient Fiber Utilization**
  කාර්යක්ෂම ප්‍රකාශ තන්තු භාවිතය
  Maximizes the capacity of existing optical fiber infrastructure.
  දැනට පවතින ප්‍රකාශ තන්තු යටිතල පහසුකම්වල ධාරිතාව උපරිම ලෙස භාවිතයට ගනී.
- **Scalable**
  පහසුවෙන් පුළුල් කළ හැකි වීම
  Capacity can be increased by adding more wavelengths.
  තරංග ආයාම වැඩි ප්‍රමාණයක් එකතු කිරීම මඟින් ධාරිතාව තවදුරටත් ඉහළ නැංවිය හැකිය.
- **Low Transmission Loss**
  අඩු සම්ප්‍රේෂණ හානිය
  Supports reliable long-distance communication with minimal signal loss.
  අවම සංඥා හානියක් සහිතව, විශ්වාසදායක ලෙස දිගු දුර සන්නිවේදනයන් සිදු කිරීමට සහය දක්වයි.

Disadvantages of WDM
WDM හි අවාසි

- Requires specialized and expensive equipment
  විශේෂිත සහ මිල අධික උපකරණ අවශ්‍ය වේ
- Can be complex to install and manage
  ස්ථාපනය සහ කළමනාකරණය කිරීම සංකීර්ණ විය හැකිය

ictfromabc.com

Code division multiplexing (CDM)
කේතය බෙදා ගැනීමේ බහුපථකරණය

In CDM, multiple data signals are transmitted over the same frequency band at the same time, but each signal is encoded with a unique code.
CDM හි, බහු දත්ත සංඥා එකම සංඛ්‍යාත කලාපයක් හරහා එකවර සම්ප්‍රේෂණය වේ, නමුත් සෑම සංඥාවක්ම අනන්‍ය කේතයකින් කේතනය කර ඇත

This process spreads the signal across a wider frequency band.
මෙම ක්‍රියාවලිය පුළුල් සංඛ්‍යාත කලාපයක් හරහා සංඥාව විහිදුවයි.

Receiver Operation
ග්‍රාහක ක්‍රියාකාරිත්වය

- The receiver extracts only the signal encoded with its matching spreading code.
ග්‍රාහකය මගින් උකහා ගනු ලබන්නේ එහි ගැලපෙන විහිදුම් කේතය මගින් කේතනය කරන ලද සංඥාව පමණි.

- Signals using different codes are treated as background noise and ignored.
වෙනත් කේත භාවිතා කරන සංඥා, පසුබිම් ශබ්ද ලෙස සලකා නොසලකා හරිනු ලැබේ.

- Similar to several groups of people speaking simultaneously in different languages within the same room.
මෙය එකම කාමරයක් තුළ පුද්ගලයින් කණ්ඩායම් කිහිපයක් එකිනෙකට වෙනස් භාෂාවලින් එකවර කතා කරනවා හා සමාන වේ.

- Each listener understands only the language they know and ignores the others.
සෑම සවන්දෙන්නෙකුටම තේරුම් ගත හැක්කේ තමන් දන්නා භාෂාව පමණක් වන අතර ඔවුන් අනෙක් භාෂාවන් නොසලකා හරියි.

CDM is primarily used in wireless networks, while wired networks typically use TDM, FDM, or WDM, however, CDM is also applicable to wired communication systems.
CDM ප්‍රධාන වශයෙන්ම රැහැන් රහිත ජාල සඳහා භාවිතා වන අතර, රැහැන් සහිත ජාල සාමාන්‍යයෙන් TDM, FDM, හෝ WDM භාවිතා කරයි. කෙසේ වුවද, කෑළු රැහැන් සහිත සන්නිවේදන පද්ධති සඳහාද අදාළ කර ගත හැක.

Applications of CDM
CDM හි යෙදුම්

CDMA cellular networks
CDM is widely used in Code Division Multiple Access (CDMA) cellular networks.
CDM බහුලව භාවිතා වන්නේ Code Division Multiple Access (CDMA) සෙලියුලර් ජාල වලයි.

Wireless local area networks (WLANs) CDM can be used in WLANs to improve capacity and reduce interference.
CDM, ධාරිතාව වැඩි දියුණු කිරීමට සහ මැදිහත්වීම් අඩු කිරීමට WLAN වල භාවිතා කළ හැක.

Satellite communications
CDM is used in satellite communication systems to allow multiple users to share the same frequency band.
එකම සංඛ්‍යාත කලාපය බෙදා ගැනීමට බහු පරිශීලකයින්ට ඉඩ දීම සඳහා CDM චන්ද්‍රිකා සන්නිවේදන පද්ධතිවල භාවිතා වේ.

Military Communications
හමුදා සන්නිවේදනය
Secure, anti-jamming communication systems.
ආරක්ෂිත, ජෑම්-විරෝධී සන්නිවේදන පද්ධති.

GPS (Global Positioning System)
GPS (ගෝලීය ස්ථාන නිර්ණායක පද්ධතිය)
Uses unique spreading codes for satellite signals.
චන්ද්‍රිකා සංඥා සඳහා අනන්‍ය වූ විහිදුම් කේත භාවිතා කරයි.

Wireless Sensor Networks
රැහැන් රහිත සංවේදක ජාල
Enables simultaneous communication among multiple sensor nodes.
බහු සංවේදක නෝඩ් අතර එකවර සන්නිවේදනය කිරීමට ඉඩ සලසයි.

ictfromabc.com

Advantages
වාසි

CDM can support a large number of users on a single frequency channel.
CDM හට තනි සංඛ්‍යාත නාලිකාවක පරිශීලකයින් විශාල සංඛ්‍යාවක් සඳහා සහය විය හැක.

The spread spectrum technique makes CDM more resistant to interference from other signals.
පැතිරීමේ වර්ණාවලි තාක්ෂණය මගින් CDM වෙනත් සංඥා වලින් බාධා වීම වලක්වයි.

CDM can provide a degree of security, as the spreading code can be kept secret.
පැතිරීමේ කේතය රහසිගතව තබා ගත හැකි බැවින් CDM හට යම් මට්ටමක ආරක්ෂාවක් සැපයිය හැක.

Disadvantages
අවාසි

CDM is more complex to implement because encoding and decoding requires significant computation.
කේතනය කිරීම සහ විකේතනය කිරීම සඳහා සැලකිය යුතු පරිගණකමය ගණනය කිරීම් අවශ්‍ය වන බැවින්, CDM ක්‍රියාත්මක කිරීම වඩාත් සංකීර්ණ වේ.

CDM can have lower data rates compared to other multiplexing techniques, especially for a given bandwidth.
CDM හට අනෙකුත් මල්ටිප්ලෙක්සිං ශිල්පීය ක්‍රම හා සසඳන විට අඩු දත්ත අනුපාත තිබිය හැක, විශේෂයෙන්ම දී ඇති කලාප පළලක් සඳහා.

Performance decreases as the number of simultaneous users increases.
එකවර සම්බන්ධ වන පරිශීලකයින් සංඛ්‍යාව වැඩි වන විට කාර්ය සාධනය අඩු වේ.

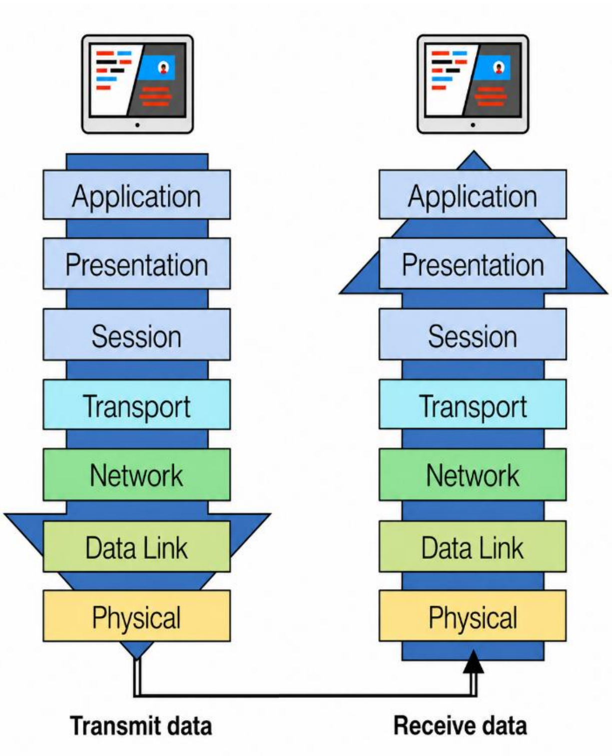
Comparison of Multiplexing Techniques
බහුපථකරණ ශිල්පීය ක්‍රම සංසන්දනය

Feature ලක්ෂණය	TDM	FDM	WDM	CDM
Division බෙදීම	Time කාලය	Frequency සංඛ්‍යාතය	Wavelength තරංග ආයාමය	Code කේතය
Medium මාධ්‍යය	Digital අංකිත	Analog ප්‍රතිසම	Optical Fiber ප්‍රකාශ තන්තු	Wireless රැහැන් රහිත
Simultaneous සමකාලීන බව	No නැත	Yes ඔව්	Yes ඔව්	Yes ඔව්
Synchronization සමමුහුර්තකරණය	Required අවශ්‍ය වේ	Not Required අවශ්‍ය නොවේ	Not Required අවශ්‍ය නොවේ	Required අවශ්‍ය වේ
Example උදාහරණ	Telephone	Radio	Fiber	CDMA
Bandwidth Efficiency කලාප පළල භාවිතය	Medium මධ්‍යස්ථ	Medium මධ්‍යස්ථ	Very High ඉතා ඉහළ	High ඉහළ

OSI Reference Model
OSI විමර්ශන ආකෘතිය

The OSI (Open Systems Interconnection) Model is a seven-layer conceptual reference model developed by the International Organization for Standardization (ISO) that describes how data is transmitted between two devices over a network.
OSI ආකෘතිය යනු ජාලයක් හරහා උපාංග දෙකක් අතර දත්ත සම්ප්‍රේෂණය වන ආකාරය විස්තර කිරීම සඳහා ප්‍රමිතිකරණය සඳහා වූ ජාත්‍යන්තර සංවිධානය (ISO) මඟින් සකස් කරන ලද, ස්ථර හතකින් යුත් සංකල්පීය විමර්ශන ආකෘතියකි.

It divides the communication process into seven layers, where each layer performs a specific function and provides services to the layer above while receiving services from the layer below.
එය සන්නිවේදන ක්‍රියාවලිය ස්ථර හතකට බෙදා දක්වන අතර, එහිදී එක් එක් ස්ථරය මඟින් නිශ්චිත කාර්යයක් ඉටු කරමින් තමාට ඉහළින් ඇති ස්ථරයට සේවාවන් සපයන අතරම තමාට පහළින් ඇති ස්ථරයෙන් සේවාවන් ලබා ගනී.



Purpose of the OSI Reference Model
OSI ආකෘතියේ අරමුණ

- Enables interoperability between different hardware and software vendors.
  විවිධ දෘඩාංග සහ මෘදුකාංග නිෂ්පාදකයින් අතර අන්තර් ක්‍රියාකාරීත්වය සක්‍රිය කරයි.
- Simplifies network design, implementation, and maintenance.
  ජාල සැලසුම්කරණය, ක්‍රියාත්මක කිරීම සහ නඩත්තු කිරීම සරල කිරීම.
- Makes network troubleshooting easier by isolating problems to a specific layer.
  ගැටලු පවතින නිශ්චිත ස්ථරය වෙන්කර හඳුනා ගැනීම මඟින් ජාලයන්හි දෝෂ නිරාකරණය පහසු කිරීම.
- Provides a common reference model for learning and developing networking technologies.
  ජාලකරණ තාක්ෂණයන් ඉගෙනීම සහ සංවර්ධනය කිරීම සඳහා පොදු විමර්ශන ආකෘතියක් සැපයීම.

Data Transmission in the OSI Model
OSI ආකෘතිය තුළ දත්ත සම්ප්‍රේෂණය

At the Sender (Transmit Data)
යවන්නාගේ පාර්ශවයේදී

The data is created at the Application Layer and moves downward through each layer to the දත්ත මුලින්ම යෙදුම් ස්ථරය තුළ නිර්මාණය වන අතර, එතැන් සිට භෞතික ස්ථරය දක්වා එක් එක් ස්ථරය ඔස්සේ පහළට ගමන් කරයි.

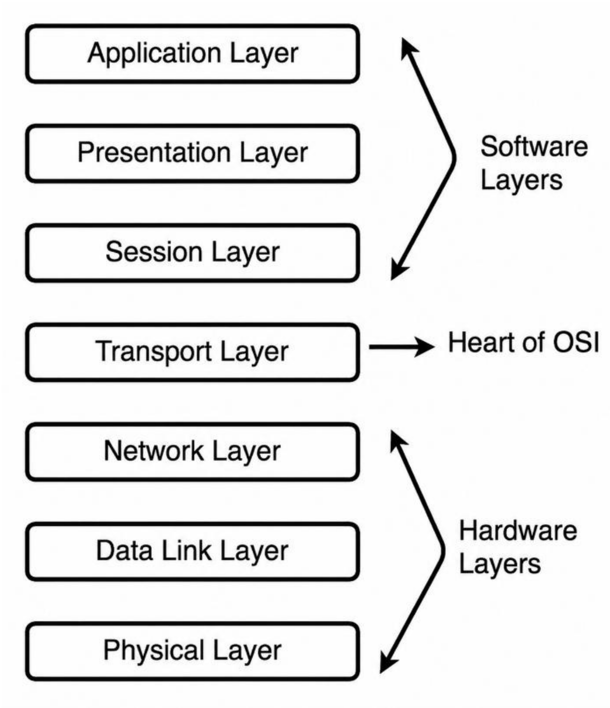
As data passes through each layer, protocol information is added. This process is called Encapsulation.
දත්ත එක් එක් ස්ථරය හරහා ගමන් කිරීමේදී, ප්‍රොටොකෝල තොරතුරු ඒ වෙත එකතු කරනු ලැබේ. මෙම ක්‍රියාවලිය කැප්සියුලකරණය ලෙස හඳුන්වයි.

At the Receiver (Receive Data)
ලබන්නාගේ පාර්ශවයේදී

The received signal enters through the Physical Layer and moves upward to the Application Layer.
ලැබෙන සංඥාව මුලින්ම භෞතික ස්ථරය හරහා පද්ධතියට ඇතුළු වන අතර, එතැන් සිට යෙදුම් ස්ථරය දක්වා එක් එක් ස්ථරය ඔස්සේ ඉහළට ගමන් කරයි.

Each layer removes its protocol information from the data before passing it to the next layer. This process is called Decapsulation.
එක් එක් ස්ථරය මඟින් දත්ත ඊළඟ ස්ථරයට යොමු කිරීමට ප්‍රථම, ඒ වෙත එකතු කර තිබූ තමාට අදාළ ප්‍රොටොකෝල තොරතුරු ඉවත් කරනු ලබයි. මෙම ක්‍රියාවලිය ප්‍රතිකැප්සියුලකරණය ලෙස හඳුන්වයි.

Software and Hardware Layers
මෘදුකාංග සහ දෘඩාංග ස්ථර



The OSI model is divided into Software Layers and Hardware Layers based on their primary functions.
OSI ආකෘතිය එහි මූලික කාර්යයන් පදනම් කරගෙන මෘදුකාංග ස්ථර සහ දෘඩාංග ස්ථර ලෙස කොටස් දෙකකට බෙදා දක්වයි.

The Transport Layer acts as the heart of the OSI model because it connects the software layers with the hardware layers and provides end-to-end communication.
ප්‍රවාහන ස්ථරය මෘදුකාංග ස්ථර සහ දෘඩාංග ස්ථර එකිනෙකා සමඟ සම්බන්ධ කරමින්, end-to-end සන්නිවේදනය සපයන බැවින් එය OSI ආකෘතියේ හෘදය ලෙස හැඳින්වේ.

Software Layers: / මෘදුකාංග ස්ථර:
Application, Presentation, Session
යෙදුම් ස්ථරය, නිරූපණ ස්ථරය, සැසි ස්ථරය

Heart of OSI: / OSI හි හෘදය වස්තුව:
Transport Layer
ප්‍රවාහන ස්ථරය

Hardware Layers: / දෘඩාංග ස්ථර:
Network, Data Link, Physical
ජාල ස්ථරය, දත්ත සබැඳි ස්ථරය, භෞතික ස්ථරය

Application layer
යෙදුම් ස්ථරය

The topmost layer of the OSI model.
මෙය OSI ආකෘතියේ ඉහළින්ම පිහිටි ස්ථරය වේ.

It provides network services directly to end-user applications, allowing users to communicate over a network.
එය පරිශීලකයාගේ යෙදුම් (end-user applications) වෙත සෘජුවම ජාල සේවාවන් සපයන අතර, එමඟින් පරිශීලකයින්ට ජාලයක් හරහා සන්නිවේදනය කිරීමට අවස්ථාව සලසා දෙයි.

Functions / කාර්යයන්

Provides an interface between user applications and the network.
පරිශීලක යෙදුම් සහ ජාලය අතර අතුරු මුහුණතක් ලබා දීම.

Enables applications to access network services.
යෙදුම් මෘදුකාංගවලට ජාල සේවාවන් වෙත ප්‍රවේශ වීමට ඉඩ සැලසීම.

Identifies communication partners and checks the availability of network resources.
සන්නිවේදනය සිදු කරන අනෙක් පාර්ශවය හඳුනා ගැනීම සහ ජාල සම්පත්වල පවතින සූදානම පරීක්ෂා කිරීම.

Common Services / පොදු සේවාවන්

- Web browsing / වෙබ් සැරිසරණය
- File transfer / ගොනු හුවමාරු කිරීම
- Email communication / විද්‍යුත් තැපැල් සන්නිවේදනය
- Remote login / දුරස්ථ පරිගණක වෙත පිවිසීම
- Domain name resolution / වසම් නාම නිරාකරණය

Protocols / නියමාවලි

- HTTP / HTTPS
- FTP
- SMTP
- POP3 / IMAP
- DNS
- Telnet / SSH

Examples / උදාහරණ
- Opening a website using a web browser.
  වෙබ් අතිරික්සුවක් භාවිතයෙන් වෙබ් අඩවියක් විවෘත කිරීම.
- Sending or receiving an email.
  විද්‍යුත් තැපෑලක් යැවීම හෝ ලැබීම.
- Uploading or downloading files.
  ගොනු උඩුගත කිරීම හෝ බාගත කිරීම.
- Accessing a remote computer using SSH.
  SSH තාක්ෂණය භාවිතයෙන් දුරස්ථ පරිගණකයකට සම්බන්ධ වීම.

Presentation Layer
සමර්පණ ස්ථරය

It is responsible for preparing data for the Application Layer by ensuring that it is in a format suitable for transmission and interpretation by the receiving system.
ලබන්නාගේ පද්ධතියට දත්ත පහසුවෙන් අර්ථකථනය කරගත හැකි සහ සම්ප්‍රේෂණයට සුදුසු ආකෘතියකින් පවතින බව තහවුරු කරමින්, යෙදුම් ස්ථරය සඳහා දත්ත සකස් කර දීම මෙහි වගකීම වේ.

Functions / කාර්යයන්

Translates data between different data formats.
විවිධ දත්ත ආකෘති අතර දත්ත පරිවර්තනය කිරීම.

Encrypts data before transmission.
සම්ප්‍රේෂණයට පෙර දත්ත ගුප්තකේතනය කිරීම.

Decrypts received encrypted data.
ලැබුණු ගුප්තකේතනය කළ දත්ත ප්‍රතිකේතනය කිරීම.

Compresses data to reduce its size before transmission.
සම්ප්‍රේෂණයට පෙර දත්තවල ප්‍රමාණය අඩු කිරීම සඳහා දත්ත සංකෝචනය කිරීම.

Decompresses received compressed data.
ලැබුණු සංකෝචිත දත්ත ප්‍රසාරණය කිරීම.

Ensures data is presented in a format compatible with the receiving system.
ලැබෙන පද්ධතිය සමඟ ගැළපෙන ආකෘතියකින් දත්ත ඉදිරිපත් වන බව තහවුරු කිරීම.

Syntax conversation.
වාක්‍ය වින්‍යාස පරිවර්තනය.

Character code conversation.
අක්ෂර කේත පරිවර්තනය.

Protocols / නියමාවලි

- SSL / TLS
- MIME
- ASCII – Character encoding
- Unicode – Character encoding

Examples / උදාහරණ

- Converting text between ASCII and Unicode.
  ASCII සහ Unicode අතර පෙළ පරිවර්තනය කිරීම.
- Encrypting data during secure web communication (HTTPS).
  ආරක්ෂිත වෙබ් සන්නිවේදනයේදී (HTTPS) දත්ත ගුප්තකේතනය කිරීම.
- Compressing image or video files before transmission.
  සම්ප්‍රේෂණයට පෙර රූප හෝ වීඩියෝ ගොනු සංකෝචනය කිරීම.
- Decompressing received compressed files.
  ලැබුණු සංකෝචිත ගොනු නැවත ප්‍රසාරණය කිරීම.

Session Layer
සැසි ස්ථරය

It is responsible for managing communication sessions between applications running on different devices.
විවිධ උපාංගවල ක්‍රියාත්මක වන යෙදුම් මෘදුකාංග අතර පවතින සන්නිවේදන සැසි කළමනාකරණය කිරීම මෙහි වගකීම වේ.

Session Management
සැසි කළමනාකරණය

Session Establishment / සැසියක් ආරම්භ කිරීම

Creates a communication session between two applications before data transmission begins.
දත්ත සම්ප්‍රේෂණය ආරම්භ කිරීමට ප්‍රථම, යෙදුම් මෘදුකාංග දෙක අතර සන්නිවේදන සැසියක් නිර්මාණය කරයි.

Session Maintenance / සැසිය පවත්වාගෙන යෑම

Keeps the communication session active and manages the exchange of data throughout the communication process.
සන්නිවේදන ක්‍රියාවලිය පුරාවටම සන්නිවේදන සැසිය සක්‍රියව තබා ගන්නා අතර දත්ත හුවමාරු වීම් පාලනය කරයි.

Session Synchronization / සැසි සමමුහුර්තකරණය

Places synchronization checkpoints during data transmission, allowing communication to resume from the last checkpoint if an interruption occurs.
දත්ත සම්ප්‍රේෂණය වන අතරතුර සමමුහුර්ත සලකුණු ඇතුළත් කරයි. එමඟින් සන්නිවේදනයට කිසියම් බාධාවක් ඇති වුවහොත්, අවසන් වරට සලකුණු කළ ස්ථානයේ සිට නැවත සන්නිවේදනය ආරම්භ කිරීමට අවස්ථාව ලැබේ.

Session Restoration (Recovery) / සැසිය නැවත යථා තත්ත්වයට පත් කිරීම

Recovers an interrupted communication session by continuing data transfer from the last synchronization checkpoint instead of restarting the entire session.
බාධා ඇති වූ සන්නිවේදන සැසියක් මුල සිටම ආරම්භ කරනවා වෙනුවට, අවසන් වරට තැබූ සමමුහුර්ත සලකුණේ සිට දත්ත හුවමාරුව ඉදිරියට කරගෙන යමින් සැසිය යථා තත්ත්වයට පත් කරයි.

Session Termination / සැසිය අවසන් කිරීම

Closes the communication session and releases all associated resources after communication is completed.
සන්නිවේදනය සම්පූර්ණයෙන්ම අවසන් වූ පසු, සන්නිවේදන සැසිය වසා දමා ඒ සඳහා වෙන් කර තිබූ සියලුම සම්පත් නිදහස් කරයි.

Functions / කාර්යයන්

Establishes communication sessions between applications.
යෙදුම් මෘදුකාංග අතර සන්නිවේදන සැසි ආරම්භ කිරීම.

Maintains active communication sessions.
සක්‍රිය සන්නිවේදන සැසි බිඳ වැටීමට නොදී පවත්වාගෙන යෑම.

Synchronizes data exchange between communicating devices.
සන්නිවේදනය සිදු කරන උපාංග අතර දත්ත හුවමාරුව සමමුහුර්තකරනය කිරීම.

Controls dialog between devices (full-duplex or half-duplex).
උපාංග අතර සිදුවන සංවාද පාලනය කිරීම (පූර්ණ ද්විපථ හෝ අර්ධ ද්විපථ ලෙස).

Terminates communication sessions after data transfer is complete.
දත්ත හුවමාරුව අවසන් වූ පසු සන්නිවේදන සැසි නිමාවට පත් කිරීම.

Restores interrupted sessions from synchronization checkpoints.
බාධා ඇති වූ සැසි, සමමුහුර්ත සලකුණුවල සිට නැවත යථා තත්ත්වයට පත් කිරීම.

Protocols / නියමාවලි

- RPC (Remote Procedure Calls)
- NetBIOS
- PPTP (Point-to-Point Tunneling Protocol)
- Socks
- ASP
- NFS

Examples / උදාහරණ

- A video conference maintaining an active communication session.
  වීඩියෝ සම්මන්ත්‍රණයකදී සන්නිවේදන සැසිය සක්‍රියව පවත්වාගෙන යෑම.
- Resuming a large file transfer after a temporary network interruption.
  තාවකාලික ජාල බිඳ වැටීමකින් පසු, විශාල ගොනුවක් බාගත කිරීම නැවතුණු තැන සිට නැවත ආරම්භ කිරීම.
- Keeping a remote desktop session active until the user disconnects.
  පරිශීලකයා සම්බන්ධතාවය විසන්ධි කරන තෙක් දුරස්ථ ඩෙස්ක්ටොප් සැසියක් සක්‍රියව තබා ගැනීම.
- Logging out of an online banking session after completing transactions.
  ගනුදෙනු අවසන් වූ පසු අන්තර්ජාල බැංකු සැසියකින් ස්වයංක්‍රීයව පිටවීම.

Applications That Support Session Restoration
සැසි නැවත යථා තත්ත්වයට පත් කිරීමට සහය දක්වන යෙදුම්

These applications support resuming interrupted sessions.
මෙම යෙදුම් බාධා වූ සැසි නැවත නැවතුණු තැන සිට ආරම්භ කිරීමට සහය දක්වයි.

- Web browsers / වෙබ් අතිරික්සු
- Cloud services / වලාකුළු සේවාවන්
- E-commerce platforms
  විද්‍යුත් වාණිජ්‍ය වේදිකා
- Social media applications/ සමාජ මාධ්‍ය යෙදුම්
- Streaming services / ප්‍රවාහ සේවාවන්

Applications That Usually Do Not Support Session Restoration
සැසි නැවත යථා තත්ත්වයට පත් කිරීමට සාමාන්‍යයෙන් සහය නොදක්වන යෙදුම්

These applications do not support session restoration to enhance security.
ආරක්ෂාව වැඩි දියුණු කිරීම සඳහා මෙම යෙදුම් සැසි නැවත යථා තත්ත්වයට පත් කිරීමට සහය නොදක්වයි.

- Online banking and financial services
  මාර්ගගත බැංකුකරණය සහ මූල්‍ය සේවාවන්
- Government services / රාජ්‍ය සේවාවන්
- High-security applications
  ඉහළ ආරක්ෂාවක් සහිත යෙදුම්

NOTE:
In modern networks, the functions of the Application, Presentation, and Session layers are usually combined into a single Application Layer in the TCP/IP model.
නූතන ජාලකරණයේදී, OSI ආකෘතියේ පවතින යෙදුම්, සමර්පණ, සහ සැසි යන ස්ථර තුනෙහිම කාර්යයන් සාමාන්‍යයෙන් TCP/IP ආකෘතිය තුළ එකම යෙදුම් ස්ථරයක් ලෙස ඒකාබද්ධ කර ඇත.

However, in the OSI model, they are studied as three separate layers, each with specific responsibilities.
කෙසේ වෙතත්, OSI ආකෘතිය තුළදී, මෙම එක් එක් ස්ථරයට පැවරුණු නිශ්චිත වගකීම් වෙන් වෙන්ව හඳුනා ගැනීම සහ අධ්‍යයනය කිරීම සඳහා ඒවා එකිනෙකට වෙනස් ස්ථර තුනක් ලෙස සලකා සාකච්ඡා කරනු ලබයි.

Transport Layer
ප්‍රවාහ ස්ථරය

The Transport Layer is the fourth layer of the OSI model.
ප්‍රවාහ ස්ථරය යනු OSI ආකෘතියේ හතරවන ස්ථරයයි.

It provides end-to-end communication between the sender and receiver by ensuring that data is delivered reliably, accurately, and in the correct order.
එය දත්ත විශ්වාසදායක ලෙස, නිවැරදිව සහ නිසි අනුපිළිවෙළින් බෙදා හැරීම තහවුරු කරමින්, යවන්නා සහ ලබන්නා අතර අන්තයේ සිට අන්තයටම (end-to-end) සන්නිවේදනය සපයයි.

Functions / කාර්යයන්

Provides end-to-end communication between devices.
උපාංග අතර අන්තයේ සිට අන්තයටම සන්නිවේදනය ලබා දීම.

Segments data into smaller units before transmission.
සම්ප්‍රේෂණයට පෙර දත්ත කුඩා කොටස්වලට (segments) වෙන් කිරීම.

Reassembles received segments into the original data.
ලැබුණු දත්ත කොටස් නැවත එකතු කර මුල් දත්ත බවට ප්‍රතිසංවිධානය කිරීම.

Performs error detection and recovery.
දෝෂ හඳුනා ගැනීම සහ ඒවා යථා තත්ත්වයට පත් කිරීම සිදු කිරීම.

Controls data flow between sender and receiver.
යවන්නා සහ ලබන්නා අතර දත්ත ගලා යාමේ වේගය පාලනය කිරීම.

Ensures reliable and ordered data delivery.
විශ්වාසදායක මෙන්ම නිසි අනුපිළිවෙළින් යුත් දත්ත බෙදා හැරීමක් තහවුරු කිරීම.

Protocols / නියමාවලි

1.TCP (Transmission Control Protocol)

A connection-oriented transport layer protocol that provides reliable, ordered, and error-checked delivery of data between devices.
උපාංග අතර දත්ත විශ්වාසවන්තව, අනුපිළිවෙළින් සහ දෝෂ පරීක්ෂාවකට ලක් කරමින් බෙදා හරින සම්බන්ධතා-අභිමුඛ (connection-oriented) ප්‍රවාහන ස්ථර නියමාවලියකි.

Characteristics / ලක්ෂණ:

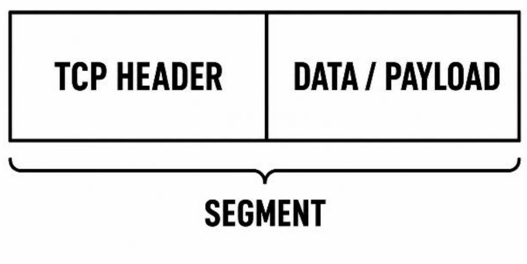
- Connection-oriented communication.
  සම්බන්ධතා-අභිමුඛ සන්නිවේදනය.
- Provides reliable data delivery.
  විශ්වාසවන්ත දත්ත බෙදාහැරීමක් සපයයි.
- Ensures data is delivered in the correct order.
  දත්ත නිවැරදි අනුපිළිවෙලට ලැබීම සහතික කරයි.
- Performs error detection and retransmission of lost data.
  දෝෂ හඳුනාගැනීම සහ අහිමි වූ දත්ත නැවත සම්ප්‍රේෂණය කිරීම සිදු කරයි.
- Supports flow control and congestion control.
  ප්‍රවාහ පාලනය සහ තදබද පාලනය සඳහා සහය දක්වයි.
- Suitable for applications that require high reliability.
  ඉහළ විශ්වාසවන්තභාවයක් අවශ්‍ය යෙදුම් සඳහා සුදුසු වේ.

2.UDP (User Datagram Protocol)

A connectionless transport layer protocol that provides fast, low-overhead data transmission without guaranteeing reliable delivery.
විශ්වාසවන්තව දත්ත ලැබීම සහතික නොකරන, වේගවත් සහ අඩු පොදුකාර්ය පිරිවැයක් සහිත දත්ත සම්ප්‍රේෂණයක් සපයන සම්බන්ධතා-විරහිත ප්‍රවාහන ස්ථර නියමාවලියකි.

Characteristics / ලක්ෂණ:

- Connectionless communication.
  සම්බන්ධතා-විරහිත සන්නිවේදනය.
- Provides fast data transmission.
  වේගවත් දත්ත සම්ප්‍රේෂණයක් සපයයි.
- Does not guarantee reliable data delivery.
  විශ්වාසවන්ත දත්ත බෙදාහැරීමක් සහතික නොකරයි.
- Does not ensure data is delivered in the correct order.
  දත්ත නිවැරදි අනුපිළිවෙලට ලැබීම සහතික නොකරයි.
- Does not perform retransmission of lost data.
  අහිමි වූ දත්ත නැවත සම්ප්‍රේෂණය නොකරයි.
- Suitable for real-time applications where speed is more important than reliability.
  විශ්වාසවන්තභාවයට වඩා වේගය වැදගත් වන තත්කාලීන යෙදුම් සඳහා සුදුසු වේ.



Network layer
ජාල ස්ථරය

The Network Layer is the Layer 3 of the OSI model.
ජාල ස්තරය යනු OSI ආකෘතියේ 3 වන ස්තරයයි

At this layer, the data received from the Transport Layer is given source and destination IP addresses.
ප්‍රවාහන ස්ථරයෙන් ලැබෙන දත්තයට යවන්නාගේ සහ ලබන්නාගේ IP ලිපින එකතු කරයි.

After this, the data unit is called a packet.
එවිට එම දත්ත ඒකකය පැකට් ලෙස හැඳින්වේ.

Functions/ කාර්යයන්

Performs logical addressing using source and destination IP addresses.
ප්‍රභව සහ ගමනාන්ත IP ලිපින භාවිතයෙන් තාර්කික ලිපිනකරණය සිදු කරයි.

Selects the best path for data to travel through the network.
ජාලය හරහා දත්ත ගමන් කිරීම සඳහා හොඳම මාර්ගය තෝරා ගනී.

Performs routing to send packets from one network to another.
එක් ජාලයක සිට තවත් ජාලයකට පැකට්ටු යැවීම සඳහා මාර්ගගත කිරීම සිදු කරයි.

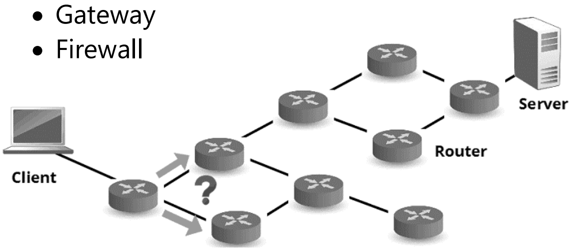
Handles packet forwarding through routers.
මාර්ගගතය හරහා පැකට්ටු ඉදිරියට යැවීම හසුරුවයි.

Protocols/ නියමාවලි

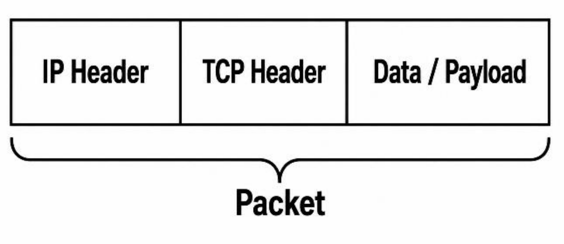
- IP (Internet Protocol)
- ICMP(Internet Control Message Protocol)
- RIP (Routing Information Protocol)
- IGMP

Devices operating at the network layer
ජාල ස්ථරය තුළ භාවිත කරන උපාංග

- Router
- Layer 3 switch
- Gateway
- Firewall



The network layer adds a header to the data from the transport layer to create a packet, and the receiver removes that header before passing the data upward.
ජාල ස්තරය මඟින් පැකට්ටුවක් නිර්මාණය කිරීම සඳහා ප්‍රවාහන ස්තරයෙන් ලැබෙන දත්තවලට ශීර්ෂයක් එකතු කරන අතර, ලබන්නා එම දත්ත ඉහළට යැවීමට පෙර එම ශීර්ෂය ඉවත් කරයි.



Data Link layer
දත්ත සම්බන්ධක ස්ථරය

The Data Link Layer is the Layer 2 of the OSI model
දත්ත සබැඳි ස්ථරය යනු OSI ආකෘතියේ 2 වන ස්තරයයි.

It is responsible for reliable data transfer between two directly connected devices over a physical communication link.
එය භෞතික සන්නිවේදන සබැඳියක් හරහා සෘජුවම සම්බන්ධ කර ඇති උපාංග දෙකක් අතර විශ්වාසදායක දත්ත හුවමාරුවක් සිදු කිරීම සඳහා වගකියනු ලබයි.

MAC addresses for data packets coming from the network layer are aggregated into data frames.
ජාල ස්ථරයේ සිට පැමිණි දත්ත පැකට්ටු සඳහා MAC ලිපින එකතු වී දත්ත රාමු බවට පත්වේ.

Functions/ කාර්යයන්

Reliable data transmission across a single physical network segment.
තනි භෞතික ජාල කොටසක් හරහා විශ්වසනීය දත්ත සම්ප්‍රේෂණයයි.

Handles node-to-node data transmission.
නෝඩ් එකක සිට තවත් නෝඩ් එකක් වෙත සිදුවන දත්ත සම්ප්‍රේෂණය හසුරුවයි.

Performs error detection and correction.
දෝෂ හඳුනා ගැනීම සහ ඒවා නිවැරදි කිරීම සිදු කරයි.

Performs framing by dividing data into frames.
දත්ත, රාමු වලට බෙදීම මඟින් රාමුගත කිරීම සිදු කරයි.

Performs flow control to regulate the rate of data transmission.

දත්ත සම්ප්‍රේෂණ වේගය පාලනය කිරීම සඳහා ප්‍රවාහ පාලනය සිදු කරයි.

There are two sub-layers here.
මෙහි උප ස්ථර දෙකක් පවතී.

1. Logical Link Control (LLC)
තාර්කික සබැඳි පාලනය
Handles error control, flow control, and multiplexing.
දෝෂ පාලනය, ප්‍රවාහ පාලනය සහ බහුවිධකරණය හසුරුවයි.

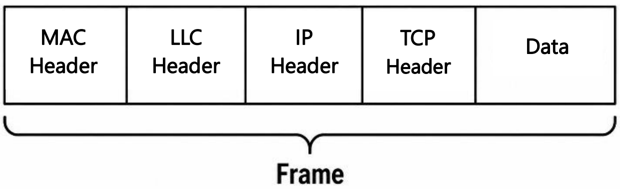
2. Media Access Control (MAC)
මාධ්‍ය ප්‍රවේශ පාලනය
Manages access to the physical medium.
භෞතික මාධ්‍යයට ප්‍රවේශය කළමනාකරණය කරයි.

Protocols/ නියමාවලි

- Ethernet
- Point-to-Point Protocol (PPP)
- Wi-Fi / IEEE 802.11
- Token Ring
- HDLC (High-Level Data Link Control)

Devices operating at the data link layer
දත්ත සම්බන්ධක ස්ථරය තුළ භාවිත කරන උපාංග

- Switch
- Bridge
- Network Interface Card (NIC)
- Repeater



Physical layer
භෞතික ස්ථරය

The Physical Layer is Layer 1 of the OSI model.
භෞතික ස්ථරය යනු OSI ආකෘතියේ 1 වන ස්තරයයි.

Physical data transmission takes place in the Physical Layer, where frames are converted into bits for transmission through the communication medium.
භෞතික දත්ත සම්ප්‍රේෂණය සිදුවන්නේ භෞතික ස්තරය තුළ වන අතර, එහිදී සන්නිවේදන මාධ්‍යය හරහා සම්ප්‍රේෂණය කිරීම සඳහා රාමු, බිටු බවට පරිවර්තනය කරනු ලබයි.

Functions/ කාර්යයන්

Transmits and receives raw bits over the communication medium.
සන්නිවේදන මාධ්‍යය හරහා දත්ත බිටු සම්ප්‍රේෂණය කිරීම සහ ලබා ගැනීම සිදු කරයි.

Defines the physical characteristics of transmission media and network devices.
සම්ප්‍රේෂණ මාධ්‍යයන්හි සහ ජාල උපාංගයන්හි භෞතික ලක්ෂණ නිර්වචනය කරයි.

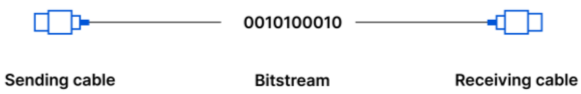
Converts bits into electrical, optical, or radio signals for transmission.
සම්ප්‍රේෂණය සඳහා බිටු, විද්‍යුත්, ප්‍රකාශ (ආලෝක) හෝ රේඩියෝ සංඥා බවට පරිවර්තනය කරයි.

Defines data transmission modes
දත්ත සම්ප්‍රේෂණ මාදිලි නිර්වචනය කරයි.

Defines data transmission methods
දත්ත සම්ප්‍රේෂණ ක්‍රම නිර්වචනය කරයි.

Defines the physical topology of the network.
ජාලයේ භෞතික ස්ථලකය නිර්වචනය කරයි.

Specifies signal timing, voltage levels, data rates, and connector types.
සංඥා කාලසන්නිවේදනය, වෝල්ටීයතා මට්ටම්, දත්ත සම්ප්‍රේෂණ වේගයන් සහ සම්බන්ධක වර්ග නිශ්චිතව දක්වයි.

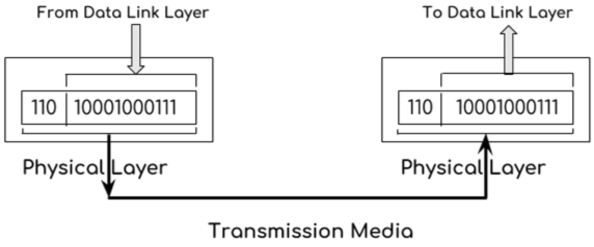


Protocols/ නියමාවලි

- DSL
- Ethernet
- WI-FI
- Bluetooth

Devices operating at the physical layer
භෞතික ස්ථරය තුළ භාවිත කරන උපාංග

- Network Interface Card(NIC)
- Cables
- Repeater
- Hub



Encapsulation

The process of adding protocol information to data as it moves down through the layers of the OSI model during transmission.
දත්ත සම්ප්‍රේෂණයේදී OSI ආකෘතියේ ස්ථර හරහා පහළට ගමන් කරන විට, එම දත්තවලට ප්‍රොටෝකෝල තොරතුරු එකතු කිරීමේ ක්‍රියාවලිය වේ.

Application Layer යෙදුම් ස්ථරය	Generates the data. දත්ත ජනනය කරයි.
Presentation Layer සමර්පණ ස්ථරය	Adds presentation information. නිරූපණ තොරතුරු එකතු කරයි.
Session Layer සැසි ස්ථරය	Adds session information. සැසි තොරතුරු එකතු කරයි.
Transport Layer ප්‍රවාහන ස්ථරය	Adds a transport header to create a Segment. Segment සෑදීම සඳහා ප්‍රවාහන ශීර්ෂකයක් එකතු කරයි.
Network Layer ජාල ස්ථරය	Adds an IP header to create a Packet. පැකට්ටුවක් සෑදීම සඳහා IP ශීර්ෂකයක් එකතු කරයි.
Data Link Layer දත්ත සබැඳි ස්ථරය	Adds a header and trailer to create a Frame. රාමුවක් සෑදීම සඳහා ශීර්ෂකයක් සහ වලිගයක් එකතු කරයි.
Physical Layer භෞතික ස්ථරය	Converts the frame into Bits for transmission. සම්ප්‍රේෂණය සඳහා රාමු බිටු බවට පරිවර්තනය කරයි.

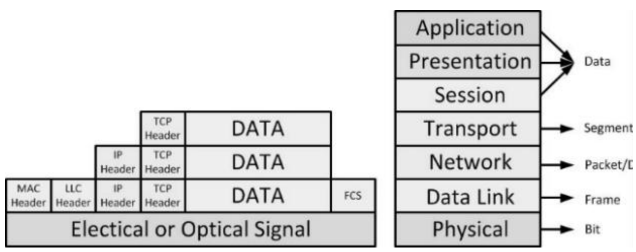
Decapsulation

The process of removing protocol information from data as it moves up through the layers of the OSI model at the receiving device.
ලබන්නාගේ උපාංගයේදී දත්ත OSI ආකෘතියේ ස්ථර හරහා ඉහළට ගමන් කරන විට, එම දත්තවලින් ප්‍රොටෝකෝල තොරතුරු ඉවත් කිරීමේ ක්‍රියාවලිය.

After removing and processing this information, the data is passed upward until it reaches the application layer, where the original message is delivered to the user.
මෙම තොරතුරු ඉවත් කර සකස් කිරීමෙන් පසු, දත්ත මුල් පණිවිඩය පරිශීලකයා වෙත ලැබෙන යෙදුම් ස්ථරය වෙත ළඟා වන තෙක් ඉහළට යොමු කරනු ලැබේ.

Data Units in OSI / දත්ත ඒකකය

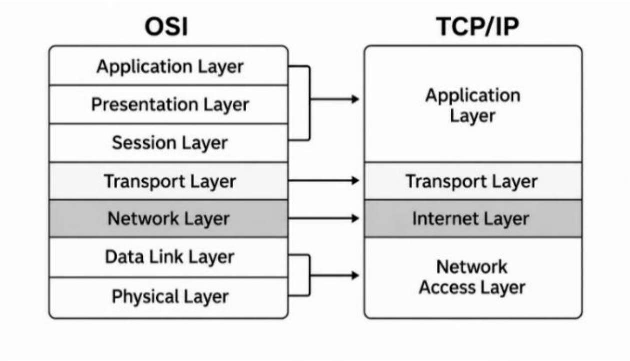
OSI Layer **OSI ස්තරය**	**Protocol Data Unit** **නියමාවලි දත්ත ඒකකය**
Application layer යෙදුම් ස්තරය	Data/ දත්ත
Presentation layer සමර්පණ ස්තරය	Data/ දත්ත
Session layer සැසි ස්තරය	Data/ දත්ත
Transport layer ප්‍රවාහන ස්තරය	Segment (TCP) / Datagram (UDP)
Network layer ජාල ස්තරය	Packet/ පැකට්ටුව
Data Link layer දත්ත සම්බන්ධක ස්ථරය	Frame රාමුව
Physical layer භෞතික ස්ථරය	Bit/ බිටුව



Addressing used in OSI layers:
OSI ස්තරයන්හි භාවිත වන ලිපිනකරණය

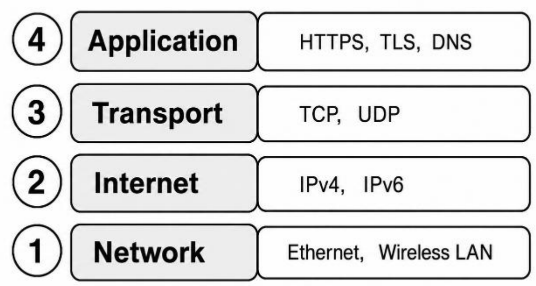
OSI Layer OSI ස්තරය	Address Used භාවිත වන ලිපිනය
Transport Layer ප්‍රවාහන ස්තරය	Port Number/ කෙවෙනි අංකය
Network Layer ජාල ස්තරය	IP Address/ IP ලිපිනය
Data Link Layer දත්ත සම්බන්ධකරණ ස්තරය	MAC Address MAC ලිපිනය

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



The TCP/IP Model is a four-layer networking model that defines how data is transmitted between devices over the Internet and TCP/IP-based networks.
TCP/IP ආකෘතිය යනු අන්තර්ජාලය සහ TCP/IP පාදක කරගත් ජාල හරහා උපාංග අතර දත්ත සම්ප්‍රේෂණය වන ආකාරය නිර්වචනය කරන ස්ථර හතරකින් යුත් ජාලකරණ ආකෘතියකි.

The TCP/IP model is the foundation of modern Internet communication and is widely used in computer networks.
TCP/IP ආකෘතිය යනු නවීන අන්තර්ජාල සන්නිවේදනයේ පදනම වන අතර එය පරිගණක ජාල තුළ බහුලව භාවිතා වේ.



Purpose of the TCP/IP Model
TCP/IP ආකෘතියේ අරමුණ

Standardizes Internet communication.
අන්තර්ජාල සන්නිවේදනය ප්‍රමිතිකරණය කරයි.

Defines how data is transmitted across interconnected networks.
අන්තර්-සම්බන්ධිත ජාල හරහා දත්ත සම්ප්‍රේෂණය වන ආකාරය නිර්වචනය කරයි.

Enables communication between different devices and network technologies.
විවිධ උපාංග සහ ජාල තාක්ෂණයන් අතර සන්නිවේදනය සක්‍රීය කරයි.

Provides the foundation for the Internet and modern computer networks.
අන්තර්ජාලය සහ නවීන පරිගණක ජාල සඳහා පදනම සපයයි.

Relationship Between the OSI and TCP/IP Models
OSI සහ TCP/IP ආකෘති අතර සම්බන්ධතාවය

The TCP/IP model performs the same communication functions as the OSI model, but it uses only four layers by combining some of the OSI layers.
TCP/IP ආකෘතිය මගින් OSI ආකෘතියට සමාන සන්නිවේදන කාර්යයන්ම සිදු කරන නමුත්, එය OSI ස්ථර කිහිපයක් එකිනෙක ඒකාබද්ධ කරමින් ස්ථර හතරක් පමණක් භාවිතා කරයි.

- The Application Layer combines the Application, Presentation, and Session layers of the OSI model.
  යෙදුම් ස්ථරය, OSI ආකෘතියේ යෙදුම්, නිරූපණ සහ සැසි ස්ථර ඒකාබද්ධ කරයි.
- The Transport Layer corresponds to the Transport Layer of the OSI model.
  ප්‍රවාහන ස්ථරය, OSI ආකෘතියේ ප්‍රවාහන ස්ථරයට අනුරූප වේ.
- The Internet Layer corresponds to the Network Layer of the OSI model.
  අන්තර්ජාල ස්ථරය, OSI ආකෘතියේ ජාල ස්ථරයට අනුරූප වේ.
- The Network Access (Link) Layer combines the Data Link and Physical layers of the OSI model.
  ජාල ප්‍රවේශ/සබැඳි ස්ථරය, OSI ආකෘතියේ දත්ත සබැඳි සහ භෞතික ස්ථර ඒකාබද්ධ කරයි.

ictfromabc.com

Data Encapsulation / දත්ත කැප්සියුලගත කිරීම

When data is sent over a network, it doesn't travel as-is. It gets wrapped in layers of headers as it moves down the network stack, from the application down to the physical wire.
ජාලයක් හරහා දත්ත යවන විට, එය ඒ ආකාරයෙන්ම ගමන් කරන්නේ නැත. එය යෙදුම් ස්තරයේ සිට භෞතික වයරය දක්වා ජාල ස්තර පෙළ ඔස්සේ පහළට යන විට, එය ශීර්ෂක ස්තරවලින් ඔතා ගනු ලැබේ.

Each layer adds its own header and renames the data unit. This process is called encapsulation.
සෑම ස්තරයක්ම තමන්ගේම ශීර්ෂකයක් එකතු කරන අතර දත්ත ඒකකය නැවත නම් කරයි. මෙම ක්‍රියාවලිය කැප්සියුලගත කිරීම ලෙස හැඳින්වේ.

The Process / ක්‍රියාවලිය

1. Data (Application Layer) / දත්ත
An application creates data
යෙදුමක් මඟින් දත්ත නිර්මාණය කරයි.

e.g., a browser building an HTTP request.
උදා: බ්‍රවුසරයක් මඟින් HTTP ඉල්ලීමක් ගොඩනැගීම.

2. Segment (Transport Layer) / සෙග්මන්ට්
TCP or UDP takes the data and adds a header with port numbers (and sequencing info for TCP). The data is now called a segment.
TCP හෝ UDP මඟින් දත්ත ලබාගෙන පෝට් අංක (port numbers) අඩංගු ශීර්ෂකයක් එක් කරයි (සහ TCP සඳහා අනුක්‍රමික තොරතුරු/sequencing info). දත්ත දැන් සෙග්මන්ට් එකක් ලෙස හැඳින්වේ.

Purpose / අරමුණ
Identifies which application or process the data belongs to.
දත්ත අයත් වන්නේ කුමන යෙදුමකට හෝ ක්‍රියාවලියකට (process) දැයි හඳුනා ගනී.

3. Packet (Network Layer) / පැකට්ටුව
IP adds a header with source and destination IP addresses. The segment is now called a packet.
IP මඟින් මූලාශ්‍ර සහ ගමනාන්ත IP ලිපිනයන් සහිත ශීර්ෂකයක් එක් කරයි. සෙග්මන්ට් එක දැන් පැකට්ටුවක් ලෙස හැඳින්වේ.

Purpose / අරමුණ
Allows the data to be routed across different networks to reach the right device.
නිවැරදි උපාංගය වෙත ළඟා වීම සඳහා විවිධ ජාල හරහා දත්ත රවුට් (route) කිරීමට ඉඩ සලසයි.

4. Frame (Data Link Layer) / ෆ්‍රේම්
Ethernet or Wi-Fi adds a header with source and destination MAC addresses, plus a trailer for error-checking. The packet is now called a frame.
Ethernet හෝ Wi-Fi මඟින් මූලාශ්‍ර සහ ගමනාන්ත MAC ලිපිනයන් සහිත ශීර්ෂකයක්, සහ දෝෂ සෙවීම සඳහා trailer එකක් කරයි. පැකට්ටුව දැන් ෆ්‍රේම් එකක් ලෙස හැඳින්වේ.

Purpose / අරමුණ
allows delivery across a single local link (e.g., PC to switch, router to router).
තනි දේශීය සබැඳියක් හරහා බෙදා හැරීමට ඉඩ සලසයි (උදා: පරිගණකයේ සිට ස්විචයට, රවුටරයේ සිට රවුටරයට).

5. Bits (Physical Layer) / බිටු
The frame is converted into a stream of bits (1s and 0s) and sent as electrical signals, light pulses, or radio waves.
ෆ්‍රේම් එක බිටු ප්‍රවාහයක් (1 සහ 0) බවට පරිවර්තනය කර විද්‍යුත් සංඥා, ආලෝක ස්පන්දන හෝ රේඩියෝ තරංග ලෙස යවනු ලැබේ.

Purpose / අරමුණ
Actual transmission across the physical medium.
භෞතික මාධ්‍යය හරහා සිදුවන සැබෑ සම්ප්‍රේෂණය.

Quick Summary
Data → Segment → Packet → Frame → Bits

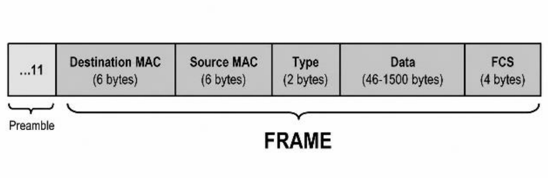
	Layer ස්තරය	**Unit Name** ඒකකයේ නම	**Key Addition** ප්‍රධාන එකතු කිරීම
1	Application / යෙදුම්	Data / දත්ත	App content / යෙදුම් අන්තර්ගතය
2	Transport / ප්‍රවාහන	Segment / සෙග්මන්ට්	Port numbers / කෙවෙණි අංක
3	Network / ජාල	Packet / පැකට්ටුව	IP addresses / IP ලිපිනයන්
4	Data Link / දත්ත සබැඳි	Frame / රාමුව	MAC addresses / MAC ලිපිනයන්
5	Physical / භෞතික	Bits / බිටු	Signal transmission / සංඥා සම්ප්‍රේෂණය

Frames / රාමු (The Unit of Transmission)

When data is generated by a device to be sent to another device over a communication network, it first goes through the OSI model's layers.
සන්නිවේදන ජාලයක් හරහා වෙනත් උපාංගයකට යැවීමට යම් උපාංගයක් මඟින් දත්ත උත්පාදනය කරන විට, එය මුලින්ම OSI ආකෘතියේ ස්ථර හරහා ගමන් කරයි.

By the time the data reaches the Data Link Layer (Layer 2), it is encapsulated into a unit called a frame.
එම දත්ත, දත්ත සම්බන්ධක ස්තරය (2 ස්ථරය) වෙත ළඟා වන විට, එය රාමුවක් ලෙස හැඳින්වෙන ඒකකයකට සංවෘත වේ.

Structure of a frame / රාමුවක ව්‍යුහය



Preamble
The preamble is a series of bits that helps synchronize communication between devices by indicating the start of a frame.
Preamble යනු රාමුවක ආරම්භය දැක්වීමෙන් උපාංග අතර සන්නිවේදනය සමමුහුර්ත කිරීමට උපකාර වන බිටු මාලාවකි.

It allows the receiving device to know when the frame is beginning.
රාමුව ආරම්භ වන විට එය ග්‍රාහක උපාංගයට දැන ගැනීමට ඉඩ සලසයි.

Destination MAC Address
This is the MAC address of the receiving device. It ensures that the frame is delivered to the correct device on the local network.
මෙය ග්‍රාහක උපාංගයේ MAC ලිපිනයයි. එය රාමුව ස්ථානීය ජාලයේ නිවැරදි උපාංගය වෙත ලබා දීම සහතික කරයි.

Source MAC Address
This is the MAC address of the sending device. It allows the recipient to know which device sent the frame, enabling responses or further communication.
මෙය දත්ත යවන උපාංගයේ MAC ලිපිනයයි. එමගින් ප්‍රතිචාර හෝ වැඩිදුර සන්නිවේදනය සක්‍රීය කරමින් රාමුව යැවූ උපාංගය කුමක්දැයි දැන ගැනීමට ග්‍රාහකයාට ඉඩ සලසයි.

EtherType/Length
This field either indicates the type of protocol used in the frame's payload (EtherType) or specifies the length of the payload data.
මෙම ක්ෂේත්‍රය මගින් රාමුවේ payload හී (EtherType) භාවිතා කරන නියමාවලි වර්ගය හෝ payload දත්තවල දිග සඳහන් කරයි.

It is essential for determining what kind of data is being transmitted (Ex. IPv4, IPv6, ARP).
සම්ප්‍රේෂණය වන්නේ කුමන ආකාරයේ දත්තද යන්න තීරණය කිරීම සඳහා එය අත්‍යවශ්‍ය වේ (උදා. IPv4, IPv6, ARP).

Payload (Data)
This is the actual data being transmitted from the source to the destination.
මූලාශ්‍රයෙන් ගමනාන්තයට සම්ප්‍රේෂණය වන සත්‍ය දත්ත මෙයයි.

It could be a network packet, such as an IP packet, or any other higher-layer data that is encapsulated inside the frame.
එය IP පැකට්ටුවක් වැනි ජාල පැකට්ටුවක් හෝ රාමුව තුළ කොටු කර ඇති වෙනත් ඉහළ ස්ථර දත්තයක් විය හැකිය.

The payload is typically limited to a certain size (e.g., Ethernet frames can carry a maximum of 1500 bytes of data in the payload).
Payload එක සාමාන්‍යයෙන් යම් ප්‍රමාණයකට සීමා වේ (උදා. ඊතර්නෙට් රාමු වලට උපරිම බයිට 1500ක දත්ත payload එකක් රැගෙන යා හැක).

Frame Check Sequence (FCS)
The FCS is used for error detection. It contains a cyclic redundancy check (CRC) value, which is a mathematical calculation based on the frame's content.
දෝෂ හඳුනාගැනීම සඳහා FCS භාවිතා වේ. එහි චක්‍රීය අතිරික්ත පරීක්ෂාව (CRC) අගයක් අඩංගු වේ, එය රාමුවේ අන්තර්ගතය මත පදනම් වූ ගණිතමය ගණනය කිරීමකි.

The receiving device recalculates the CRC to check for transmission errors.
සම්ප්‍රේෂණ දෝෂ සඳහා පරීක්ෂා කිරීමට ග්‍රාහක උපාංගය මගින් CRC නැවත ගණනය කරයි.

If the values don't match, the frame is considered corrupted and discarded.
අගයන් නොගැලපේ නම්, රාමුව වෙනස් වී ඇත ලෙස සලකා ඉවතලනු ලැබේ.

Frame Creation
රාමු නිර්මාණය

Each frame is created based on the specific characteristics and quality of the link between the two devices.
උපාංග දෙක අතර සම්බන්ධකයේ නිශ්චිත ලක්ෂණ සහ ගුණාත්මකභාවය මත පදනම්ව සෑම රාමුවක්ම නිර්මාණය කරයි.

For example, if the devices are connected by a high-speed link, the frame may carry more data; if the link is less reliable, the frame may be smaller to minimize the impact of errors.
උදාහරණයක් ලෙස, උපාංග අධිවේගී සබැඳියක් මගින් සම්බන්ධ කර ඇත්නම්, රාමුවට වැඩි දත්ත රැගෙන යා හැක; සබැඳිය අඩු විශ්වසනීය නම්, දෝෂ වල බලපෑම අවම කිරීම සඳහා රාමුව කුඩා විය හැක.

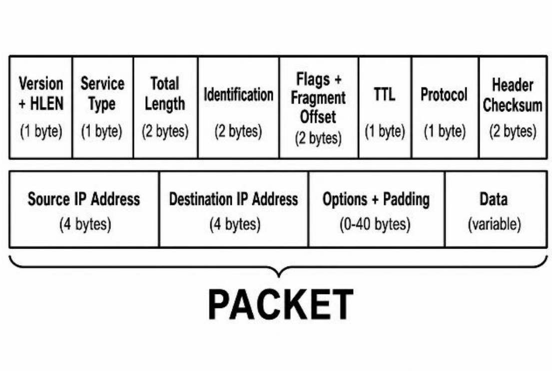
Packets **(The Unit of Transmission)**

When data is generated by a device to be sent to another device over a communication network, it first passes through the OSI model's layers.
සන්නිවේදන ජාලයක් හරහා වෙනත් උපාංගයකට යැවීම සඳහා උපාංගයක් මඟින් දත්ත ජනනය කරන විට, එය මුලින්ම OSI මාදිලියේ ස්තර හරහා ගමන් කරයි.

By the time the data reaches the Network Layer (Layer 3), it is encapsulated into a unit called a packet.
දත්ත ජාල ස්තරය (3 වන ස්තරය) වෙත ළඟා වන විට, එය පැකට්ටුවක් ලෙස හැඳින්වෙන ඒකකයකට කැප්සියුලගත කරනු ලැබේ.

A packet is mainly used to carry data from one network to another network. It helps the data travel across different networks until it reaches the correct destination device.
පැකට්ටුවක් ප්‍රධාන වශයෙන් භාවිතා කරන්නේ එක් ජාලයක සිට තවත් ජාලයකට දත්ත රැගෙන යාම සඳහාය. එය නිවැරදි ගමනාන්ත උපාංගය වෙත ළඟා වන තෙක් විවිධ ජාල හරහා දත්ත වලට ගමන් කිරීමට උපකාරී වේ.

Structure of a Packet / පැකට්ටුවක ව්‍යුහය



Header / ශීර්ෂකය
The header contains important control information needed to deliver the packet correctly.
පැකට්ටුව නිවැරදිව බෙදා හැරීමට අවශ්‍ය වැදගත් පාලන තොරතුරු ශීර්ෂකය තුළ අඩංගු වේ.

It includes details such as the source IP address, destination IP address, packet length, protocol type, and other routing-related information.
මූලාශ්‍ර IP ලිපිනය, ගමනාන්ත IP ලිපිනය, පැකට් දිග, නියමාවලි වර්ගය සහ රවුටින් වලට අදාළ වෙනත් තොරතුරු වැනි විස්තර මෙයට ඇතුළත් වේ.

Source IP Address / මූලාශ්‍ර IP ලිපිනය
This is the IP address of the device that sends the packet.
මෙය පැකට්ටුව එවනු ලබන උපාංගයේ IP ලිපිනයයි.

It allows the receiving device to know where the packet came from and where to send a reply if needed.
මෙය පැකට්ටුව පැමිණියේ කොහෙන්ද සහ අවශ්‍ය නම් පිළිතුරක් එවිය යුත්තේ කොතැනටද යන්න දැන ගැනීමට ලබන්නාගේ උපාංගයට ඉඩ සලසයි.

Destination IP Address / ගමනාන්ත IP ලිපිනය
This is the IP address of the device that should receive the packet.
මෙය පැකට්ටුව ලැබිය යුතු උපාංගයේ IP ලිපිනයයි.

Routers use the destination IP address to decide the best path for forwarding the packet across networks.
ජාල හරහා පැකට්ටුව ඉදිරියට යැවීම සඳහා හොඳම මාර්ගය තීරණය කිරීමට රවුටර (routers) විසින් ගමනාන්ත IP ලිපිනය භාවිතා කරයි.

Protocol Field / නියමාවලි ක්ෂේත්‍රය
This field identifies the type of data being carried in the packet.
මෙම ක්ෂේත්‍රය මගින් පැකට්ටුව තුළ රැගෙන යන දත්ත වර්ගය හඳුනා ගනී.

For example, it may indicate whether the packet contains TCP data, UDP data, or another type of higher-layer data.
උදාහරණයක් ලෙස, පැකට්ටුවේ TCP දත්ත, UDP දත්ත හෝ වෙනත් ඉහළ ස්තරයක දත්ත අඩංගු දැයි එයින් පෙන්නුම් කළ හැක.

Time To Live (TTL) / ජීවන කාලය
TTL is used to prevent packets from moving around the network forever.
පැකට්ටු සදහටම ජාලය පුරා සංසරණය වීම වැලැක්වීම සඳහා TTL භාවිතා කරයි.

Each time a packet passes through a router, the TTL value is reduced by one.
පැකට්ටුවක් රවුටරයක් හරහා ගමන් කරන සෑම අවස්ථාවකම, TTL අගය එකකින් අඩු වේ.

If the TTL reaches zero before the packet reaches its destination, the packet is discarded.
පැකට්ටුව එහි ගමනාන්තයට ළඟා වීමට පෙර TTL අගය බිංදුව වුවහොත්, පැකට්ටුව ඉවතලනු ලැබේ.

Payload (Data) / දත්ත
This is the actual data being carried inside the packet.
මෙය පැකට්ටුව තුළ රැගෙන යන සැබෑ දත්ත වේ.

The payload may contain data from higher layers, such as a TCP segment or UDP datagram.
පේලෝඩ් එකෙහි TCP සෙග්මන්ට් එකක් හෝ UDP ඩේටාග්‍රෑම් එකක් වැනි ඉහළ ස්තරවල දත්ත අඩංගු විය හැක.

The size of the payload depends on the network and the maximum transmission size supported by the link.
පේලෝඩ් හි ප්‍රමාණය ජාලය සහ එම සන්නිවේදන සබැඳිය (link) මගින් සහය දක්වන උපරිම සම්ප්‍රේෂණ ප්‍රමාණය මත රඳා පවතී.

Header Checksum / ශීර්ෂක චෙක්සම්
The header checksum is used to detect errors in the packet header.
පැකට් ශීර්ෂකයේ ඇති දෝෂ හඳුනා ගැනීමට ශීර්ෂක චෙක්සම් භාවිතා කරයි.

The receiving device or router checks this value to make sure the header has not been corrupted during transmission.
සම්ප්‍රේෂණයේදී ශීර්ෂකයට හානියක් සිදුවී නොමැති බව තහවුරු කර ගැනීම සඳහා ලබන්නාගේ උපාංගය හෝ රවුටරය මෙම අගය පරීක්ෂා කරයි.

If an error is detected, the packet may be discarded.
දෝෂයක් අනාවරණය වුවහොත්, පැකට්ටුව ඉවතලනු ලැබිය හැක.

Packet Creation / පැකට්ටු නිර්මාණය කිරීම

Each packet is created based on the data being sent and the network path it must travel through.
සෑම පැකට්ටුවක්ම නිර්මාණය වන්නේ යවනු ලබන දත්ත සහ එය ගමන් කළ යුතු ජාල මාර්ගය මත පදනම්ව ය.

For example, if the data is large, it may be divided into multiple smaller packets before transmission.
උදාහරණයක් ලෙස, දත්ත විශාල නම්, සම්ප්‍රේෂණයට පෙර එය කුඩා පැකට්ටු කිහිපයකට බෙදිය හැකිය.

Each packet can travel independently through the network and may take different routes to reach the destination.
සෑම පැකට්ටුවකටම ජාලය හරහා ස්වාධීනව ගමන් කළ හැකි අතර ගමනාන්තය වෙත ළඟා වීමට විවිධ මාර්ග ඔස්සේ යා හැක.

At the destination, the packets are reassembled to form the original data.
ගමනාන්තයේදී, මුල් දත්ත නැවත සකස් කිරීම සඳහා මෙම පැකට්ටු නැවත එකලස් කරනු ලැබේ.

Best Effort Delivery

A communication model in computer networks where the network attempts to deliver data packets without guaranteeing delivery, timing, order, or reliability.
පරිගණක ජාලවල පවතින සන්නිවේදන ආකෘතියක් වන අතර, බෙදා හැරීම, නියමිත වේලාවට, නිසි පිළිවෙළට ලැබීම හෝ විශ්වසනීයත්වය යනාදිය සහතික නොකර, ජාලය දත්ත පැකට් බෙදා හැරීමට උත්සාහ කරයි.

It is called Best Effort because the network makes its best attempt to deliver packets.
ජාලය විසින් පැකට් බෙදා හැරීමට තමන්ට හැකි උපරිම උත්සාහය දරන බැවින් මෙය Best Effort ලෙස හැඳින්වේ.

However, it does not promise speed, order, or error recovery.
කෙසේ වෙතත්, එය වේගය, නිසි පිළිවෙළ හෝ දෝෂ නිවැරදි කිරීම පිළිබඳව පොරොන්දු නොවේ.

What Best-Effort Does Not Guarantee
Best-Effort මඟින් සහතික නොකරන දේවල්

Delivery / බෙදාහැරීම
A packet may or may not reach the destination.
පැකට්ටුවක් ගමනාන්තයට ලැබීමට හෝ නොලැබීමට ඉඩ ඇත.

Delivery Time / බෙදාහරින කාලය
Packets may arrive quickly or slowly. There is no fixed delay guarantee.
පැකට් වේගයෙන් හෝ සෙමින් පැමිණිය හැක. ස්ථාවර ප්‍රමාද කාල සීමාවක් සහතික නොකරයි.

Packet Order / පැකට්වල පිළිවෙළ
Packets may arrive in a different order from the order in which they were sent.
පැකට් එවන ලද පිළිවෙළට වඩා වෙනස් පිළිවෙළකින් ගමනාන්තයට ලැබීමට ඉඩ ඇත.

Packet Loss / පැකට් අහිමි වීම
Packets may be dropped during transmission.
දත්ත සම්ප්‍රේෂණය වන අතරතුර පැකට් ගිලිහී යාමට ඉඩ ඇත.

Duplicate Packets / අනුපිටපත් පැකට්
In some cases, duplicate packets may be received.
සමහර අවස්ථාවලදී, එකම පැකට්ටුවේ පිටපත් කිහිපයක් ලැබීමට ඉඩ ඇත.

Simple Analogy
සරල උදාහරණය

Similar to sending postcards through a normal postal service.
මෙය සාමාන්‍ය තැපැල් සේවයක් හරහා තැපැල්පත් යැවීමට සමානය.

The postal service tries to deliver the postcards.
තැපැල් සේවය තැපැල්පත් බෙදා හැරීමට උපරිම උත්සාහයක් ගනියි.

However, it cannot guarantee that:
කෙසේ වෙතත්, එයට පහත දෑ සහතික කළ නොහැක:

- Every postcard will arrive.
  සෑම තැපැල්පතක්ම ලැබෙනු බව.
- The postcards will arrive on time.
  තැපැල්පත් නියමිත වේලාවට ලැබෙනු බව.
- The postcards will arrive in the order.
  තැපැල්පත් පිළිවෙළට ලැබෙනු බව.
- No postcard will be lost.
  කිසිදු තැපැල්පතක් අතරමඟදී නැති නොවන බව.

What's happening here is simply trying to send data somehow, not making sure it arrives correctly.
මෙහිදී සිදුවන්නේ දත්ත නිවැරදිව ලැබුණාදැයි තහවුරු කරගැනීම නොව, කෙසේ හෝ යැවීමට උත්සාහ කිරීම පමණි.

How it works
ක්‍රියා කරන ආකාරය

When a router receives a packet, it follows a simple forwarding process.
මාර්ගකයකට දත්ත පැකට්ටුවක් ලැබුණු විට, එය සරල ඉදිරියට යැවීමේ ක්‍රියාවලියක් අනුගමනය කරයි:

1. Checking the Destination Address
   ගමනාන්ත ලිපිනය පරීක්ෂා කිරීම

The router checks the destination IP address in the packet.
මාර්ගකය විසින් පැකට්ටුවේ ඇති ගමනාන්ත IP ලිපිනය පරීක්ෂා කරයි.

2. Finding the Next Hop
   ඊළඟ පියවර (Hop) සෙවීම

The router uses its routing table to find the next router or destination path.
මාර්ගකය තම Routing වගුව භාවිතයෙන් ඊළඟ මාර්ගකය හෝ ගමනාන්ත මාර්ගය සොයා ගනියි.

3. Forwarding the Packet
   පැකට්ටුව ඉදිරියට යැවීම

The router forwards the packet if network resources are available.
ජාලයේ සම්පත් පවතී නම් මාර්ගකය පැකට්ටුව ඉදිරියට යවයි.

4. Handling Congestion
තදබදය පාලනය කිරීම

If the router is congested, packets may be delayed.
ජාලය තුළ අධික තදබදයක් ඇත්නම්, පැකට් ප්‍රමාද විය හැක.

Some packets may wait in a queue.
සමහර පැකට් පෝලිමක රැඳී සිටියි.

Some packets may be dropped.
සමහර පැකට් හැලී (dropped) යා හැකියි.

The router usually does not retransmit dropped packets.
සාමාන්‍යයෙන් මාර්ගකය විසින් මෙලෙස හැලී ගිය පැකට් නැවත සම්ප්‍රේෂණය නොකරයි.

Best-Effort Service in the Internet
අන්තර්ජාලය තුළ Best-Effort සේවාව

The Internet mainly uses a best-effort delivery model.
අන්තර්ජාලය ප්‍රධාන වශයෙන්ම ක්‍රියා කරන්නේ best-effort බෙදාහැරීමේ ආකෘතිය මතය.

The Internet Protocol (IP) is a best-effort delivery.
Internet Protocol (IP) යනු Best-effort බෙදාහැරීමකි.

IP does not guarantee:
IP මඟින් පහත දෑ සහතික නොකරයි:

- Successful delivery / සාර්ථක බෙදාහැරීම
- Correct packet order / නිවැරදි පැකට් පිළිවෙළ
- Reliability / විශ්වසනීයත්වය
- Error recovery / දෝෂ නිවැරදි කිරීම
- Fixed delay / ස්ථාවර ප්‍රමාද කාලය
- Reserved bandwidth / වෙන්කළ කලාප පළල

Those responsibilities are handled by higher-layer protocols if needed.
අවශ්‍යතාවයක් වුවහොත් එම වගකීම් ඉහළ ස්ථරවල නියමාවලි මඟින් පාලනය කරනු ලබයි:

TCP - Adds reliability by retransmitting lost packets and ensuring they arrive in order.
TCP - අහිමි වූ පැකට් නැවත යැවීමෙන් සහ ඒවා නිසි පිළිවෙළට ලැබෙන බව සහතික කිරීමෙන් විශ්වසනීයත්වයක් එක් කරයි.

UDP - Simply relies on IP's best-effort service and sends packets without recovery.
UDP - IP හි ඇති best-effort සේවාව මතම පමණක් රඳා පවතින අතර, දෝෂ නිවැරදි කිරීමකින් තොරව පැකට් සෘජුවම යවයි.

Advantages
වාසි

1. Simple Design / සරල සැලසුම
The network does not need complex control mechanisms.
ජාලය සඳහා සංකීර්ණ පාලන යාන්ත්‍රණ අවශ්‍ය නොවේ.

2. Fast Packet Forwarding
වේගවත් පැකට් සම්ප්‍රේෂණය
Routers can forward packets quickly because they do not need to check many guarantee conditions.
මාර්ගකවලට සහතික කිරීමේ කොන්දේසි රැසක් පරීක්ෂා කිරීමට අවශ්‍ය නොවන බැවින් පැකට් ඉක්මනින් ඉදිරියට යැවිය හැක.

3. Low Overhead / අඩු පාලන දත්ත පිරිවැය
Less control information in the network.
ජාලය තුළ ගමන් කරන පාලන තොරතුරු ප්‍රමාණය අවමය.

4. High Scalability / ඉහළ පරිමාණ්‍යතාව
Best-effort service supports a very large number of users and devices. This is one reason why the Internet can scale globally.
Best-effort සේවාවට අතිවිශාල පරිශීලකයින් සහ උපාංග සංඛ්‍යාවකට සහය දිය හැක. අන්තර්ජාලය ගෝලීය වශයෙන් ව්‍යාප්ත වීමට එකම හේතුවක් වන්නේ මෙයයි.

5. Efficient Resource Usage
කාර්යක්ෂම සම්පත් භාවිතය
Network resources are shared among users. Bandwidth is used whenever it is available.
ජාල සම්පත් පරිශීලකයින් අතර බෙදාගැනේ. කලාප පළල පවතින ඕනෑම අවස්ථාවක එය ප්‍රයෝජනයට ගනු ලබයි.

Disadvantages
අවාසි

1. Packet Loss / පැකට් අහිමි වීම
Packets can be lost during transmission.
සම්ප්‍රේෂණය අතරතුර පැකට් නැති විය හැක.

2. Variable Delay / වෙනස් වන ප්‍රමාද කාලය
Packets may experience different delays. This is also called Variable Latency.
පැකට් එකිනෙකට වෙනස් ප්‍රමාදයන්ට ලක්විය හැක. මෙයට Variable Latency යැයිද කියනු ලැබේ.

3. Jitter

Jitter means variation in packet delay. It can affect real-time communication.
පැකට් ප්‍රමාද වීමේ කාල පරාසයන් අතර සිදුවන විචලනයයි. මෙය සජීවී සන්නිවේදනයට බාධා කරයි.

4. No Bandwidth Guarantee
කලාප පළල සහතික නොකිරීම

Applications cannot assume that a fixed amount of bandwidth will always be available.
යෙදුම් සඳහා ස්ථාවර කලාප පළල ප්‍රමාණයක් සැමවිටම පවතිනු ඇතැයි උපකල්පනය කළ නොහැක.

5. Reliability Must Be Added Separately
විශ්වසනීයත්වය වෙනම එකතු කළ යුතු වීම

Applications that require reliability must use protocols such as TCP. Otherwise, they must implement reliability by themselves.
විශ්වසනීයත්වය අවශ්‍ය වන යෙදුම් සඳහා TCP වැනි නියමාවලි භාවිතා කළ යුතුය. නැතහොත් ඔවුන් විසින්ම විශ්වසනීයත්වය ගොඩනගා ගත යුතුය.

Examples / උදාහරණ

Suitable for / වඩාත් සුදුසු වන්නේ

- Web browsing / වෙබ් අඩවි පරිශීලනය.
- Email / විද්‍යුත් තැපෑල
- File downloads / ගොනු බාගත කිරීම්
- General Internet traffic
  සාමාන්‍ය අන්තර්ජාල දත්ත ගමනාගමනය
- Cloud-based applications
  වලාකුළු ආශ්‍රිත යෙදුම්

Less suitable for / වඩාත් සුදුසු නොවන්නේ

- Voice over IP
- Live video conferencing
  සජීවී වීඩියෝ සම්මන්ත්‍රණ
- Online gaming / මාර්ගගත ක්‍රීඩා
- Remote surgery / දුරස්ථ සැත්කම්
- Industrial control systems
  කාර්මික පාලන පද්ධති

These applications often use Quality of Service (QoS) mechanisms to give their traffic higher priority and more predictable performance.
මෙවැනි යෙදුම්, තම දත්ත ගමනාගමනයට ඉහළ ප්‍රමුඛතාවයක් සහ පුරෝකථනය කළ හැකි කාර්යසාධනයක් ලබා දීම සඳහා බොහෝ විට Quality of Service (QoS) යාන්ත්‍රණයන් භාවිතා කරයි.

Guaranteed Service

A network model that provides absolute mathematical guarantees for bandwidth and delay bounds.
කලාප පළල සහ ප්‍රමාද සීමාවන් සඳහා නිරපේක්ෂ ගණිතමය සහතිකයන් ලබා දෙන ජාල ආකෘතියකි.

Ensures that conforming data packets arrive within a guaranteed delay bound and are not dropped due to network queue congestion.
අනුකූල දත්ත පැකට්ටු සහතික කරන ලද උපරිම කාල ප්‍රමිතියක් තුළ ලැබෙන බව තහවුරු කරන අතර, ජාල පෝලිම් තදබදය හේතුවෙන් ඒවා මඟහැරී යාම වළක්වයි.

Feature **ලක්ෂණය**	**Best-Effort Service**	**Guaranteed Service**
Delivery බෙදාහැරීම	No delivery guarantee බෙදාහැරීම පිළිබඳ සහතිකයක් නැත	Delivery may be guaranteed or negotiated බෙදාහැරීම සහතික කර ඇත නැතහොත් එකඟතාවයකට යටත් වේ
Packet Loss පැකට් අහිමි වීම	Packets may be lost පැකට් අහිමි විය හැක	Packet loss is minimized or compensated පැකට් අහිමි වීම අවම කර හෝ වන්දි ගෙවා ඇත
Delay ප්‍රමාදය	Delay is unpredictable ප්‍රමාදය පුරෝකථනය කළ නොහැක	Delay bounds may be guaranteed ප්‍රමාද සීමාවන් සහතික කළ හැක
Packet Order පැකට් පිළිවෙළ	Order is not guaranteed පිළිවෙළ සහතික කර නැත	Order may be controlled පිළිවෙළ පාලනය කළ හැක
Bandwidth කලාප පළල	No bandwidth guarantee කලාප පළල සහතික නොකරයි	Bandwidth may be reserved කලාප පළල වෙන් කර තැබිය හැක
Complexity සංකීර්ණත්වය	Simple සරලයි	More complex වඩාත් සංකීර්ණයි

Confidentiality and Authentication
රහස්‍යභාවය සහ සත්‍යාපනය

Confidentiality
රහස්‍යභාවය

Confidentiality ensures that information is only accessible to those authorized to view it.
රහස්‍යභාවය මඟින් තොරතුරු ප්‍රවේශ විය හැක්කේ එය බැලීමට බලය ලත් අයට පමණක් බව සහතික කරයි.

Without confidentiality, sensitive data could be intercepted and read by unauthorized parties, leading to potential misuse or loss of privacy.
රහස්‍යභාවයකින් තොරව, අනවසර පාර්ශ්වයන් විසින් සංවේදී දත්ත ග්‍රහණය කර කියවීමට හැකි වන අතර, එමඟින් අනිසි භාවිතයට හෝ පෞද්ගලිකත්වය අහිමි වීමට හේතු විය හැක.

For instance, if personal health records or financial information are not kept confidential, they could be accessed and exploited by cybercriminals or unauthorized individual
නිදසුනක් වශයෙන්, පුද්ගලික සෞඛ්‍ය වාර්තා හෝ මූල්‍ය තොරතුරු රහසිගතව තබා නොගන්නේ නම්, සයිබර් අපරාධකරුවන් හෝ අනවසර පුද්ගලයින් විසින් ඒවාට ප්‍රවේශ වී සූරාකෑමට ලක් කළ හැක.

Authentication
සත්‍යාපනය

Authentication verifies the identity of the sender or the source of information.
සත්‍යාපනය යවන්නාගේ අනන්‍යතාවය හෝ තොරතුරු මූලාශ්‍රය සත්‍යාපනය කරයි.

It ensures that the message or data comes from a legitimate and trusted source, preventing impersonation or fraudulent communications.
පුද්ගලාරෝපණය හෝ වංචනික සන්නිවේදනයන් වළක්වමින් පණිවිඩය හෝ දත්ත නීත්‍යානුකූල සහ විශ්වාසදායක මූලාශ්‍රයකින් පැමිණෙන බව සහතික කරයි.

Without proper authentication, an attacker could impersonate a trusted entity, such as a bank or service provider, to deceive individuals or gain unauthorized access to sensitive information.
නිසි සත්‍යාපනයකින් තොරව, ප්‍රහාරකයෙකුට පුද්ගලයන් රැවටීමට හෝ සංවේදී තොරතුරු වෙත අනවසරයෙන් ප්‍රවේශ වීමට බැංකුවක් හෝ සේවා සපයන්නෙකු වැනි විශ්වාසදායක ආයතනයක් ලෙස පෙනී සිටිය හැක.

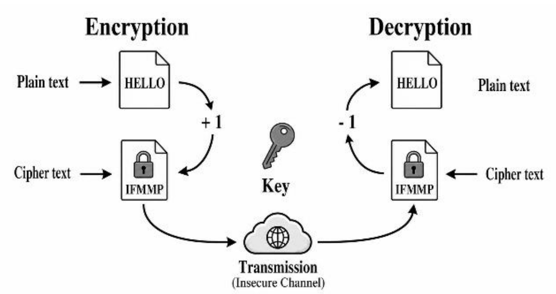
Cryptography
ගුප්තකේතනය

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it.
ගුප්තකේතනය යනු පණිවිඩයක් අදහස් කරන පුද්ගලයාට පමණක් එය කියවිය හැකි වන ලෙස තොරතුරු සැඟවීම හෝ කේතනය කිරීමේ ක්‍රියාවලියයි.

Encryption and Decryption
කේතනය සහ විකේතනය

Encryption is the process of converting plaintext (readable data) into ciphertext (encoded data) to protect it from unauthorized access.
කේතනය යනු සරල පෙළ (කියවිය හැකි දත්ත) අනවසර ප්‍රවේශයෙන් ආරක්ෂා කිරීම සඳහා කේතිත පෙළ (කේතගත දත්ත) බවට පරිවර්තනය කිරීමේ ක්‍රියාවලියයි.

Decryption is the reverse process, converting ciphertext back into plaintext so that authorized users can read it.
විකේතනය යනු එහි ප්‍රතිලෝම ක්‍රියාවලිය වන අතර, බලයලත් පරිශීලකයින්ට කියවිය හැකි පරිදි කේතිත පෙළ නැවත සාමාන්‍ය පෙළ බවට පරිවර්තනය කරයි.



Cryptographic Keys
ගුප්තකේතන යතුරු

Keys are secret pieces of information used in encryption and decryption. The security of the encrypted data depends on keeping the key confidential.
යතුරු යනු කේතනය සහ විකේතනය කිරීමේදී භාවිතා කරන රහස් තොරතුරු කොටස් වේ. කේතාත්මක දත්තවල ආරක්ෂාව රඳා පවතින්නේ යතුර රහසිගතව තබා ගැනීම මතය.

Encryption types
ගේතන වර්ග

There are two main types of encryptions:
ප්‍රධාන කේතන වර්ග දෙකක් පවතී:

- Symmetric key encryption
(Private key encryption)
සමමිතික යතුරු කේතනය
(පෞද්ගලික යතුරු ගුප්තකේතනය)

- Asymmetric key encryption
(Public key encryption)
අසමමිතික යතුරු කේතනය
(පොදු යතුරු කේතනය)

Symmetric key encryption
සමමිතික යතුරු කේතනය

Symmetric key encryption, also known as private-key encryption, uses the same key for both encryption and decryption.
පුද්ගලික යතුරු කේතනය ලෙසද හැඳින්වෙන සමමිතික යතුරු කේතනය, කේතනය සහ විකේතනය යන දෙකටම එකම යතුර භාවිතා කරයි.

How It Works
එය ක්‍රියා කරන ආකාරය

The sender uses the symmetric key to encrypt the plaintext into ciphertext.
යවන්නා සරල පෙළ කේතනය කිරීමට සමමිතික යතුර භාවිත කරයි.

The receiver uses the same symmetric key to decrypt the ciphertext back into plaintext.
ග්‍රාහකයා කේතිත පෙළ නැවත සරල පෙළට විකේතනය කිරීමට එම සමමිතික යතුරම භාවිතා කරයි.

This means that the same key is used to encode for both.
මෙයින් අදහස් කරන්නේ දෙකම කේතනය කිරීම සඳහා එකම යතුර භාවිතා කරන බවයි.

NOTE: Key Management
The symmetric key must be shared between the sender and the receiver securely. If the key is intercepted or compromised, the security of the communication is at risk.
සමමිතික යතුර යවන්නා සහ ලබන්නා අතර ආරක්ෂිතව බෙදා ගත යුතුය. යතුර සොරා ගතහොත් හෝ සම්මුතියකට ලක් වුවහොත්, සන්නිවේදනයේ ආරක්ෂාව අවදානමට ලක් වේ.

Advantages and Disadvantages of Symmetric Key Encryption
සමමිතික යතුරු කේතනයේ වාසි සහ අවාසි

Advantages වාසි

- Faster than asymmetric encryption
අසමමිතික කේතනයට වඩා වේගවත් වේ.

- Requires less computational power
අඩු පරිගණක බලයක් අවශ්‍ය වේ.

- Uses a single key, making encryption and decryption simple
එක් යතුරක් පමණක් භාවිතා වන බැවින් ක්‍රියාවලිය සරල වේ.

Disadvantages අවාසි

- Secure key sharing is difficult
යතුර ආරක්ෂිතව හුවමාරු කර ගැනීම අපහසුය.

- Risk if the key is intercepted
යතුර වෙනත් අයෙකු අතට පත්වුවහොත් අවදානමක් ඇත.

- Key management becomes complex with many users
පරිශීලකයින් වැඩි වන විට යතුරු කළමනාකරණය සංකීර්ණ වේ

Asymmetric Key Encryption
අසමමිතික කේතනය

No secret key is shared here
මෙහිදී රහස් යතුරු හුවමාරු කරගැනීමක් සිදු නොවේ.

How It Works
එය ක්‍රියා කරන ආකාරය

Key Pair Generation
යතුරු යුගලය නිර්මාණය කිරීම
Each person participating in the communication generates pair of keys consisting of a Public Key and a Private Key.
සන්නිවේදනයට සම්බන්ධ වන සෑම අයෙකුම තමන්ටම ආවේණික වූ පොදු සහ පෞද්ගලික යතුරු යුගලයක් නිර්මාණය කරගනී.

Key Management

Public Key/පොදු යතුර
Can be shared openly and is used to encrypt data or verify signatures.
විවෘතව බෙදා ගත හැකි අතර දත්ත කේතනය කිරීමට හෝ අත්සන් සත්‍යාපනය කිරීමට භාවිතා කරයි.

Private Key/පෞද්ගලික යතුර
Must be kept secret and secure; it is used to decrypt data or create signatures.
රහසිගතව සහ ආරක්ෂිතව තබා ගත යුතුය; එය දත්ත විකේතනය කිරීමට හෝ අත්සන් සෑදීමට භාවිතා කරයි

These keys are mathematically related, meaning that the encryption performed with one key can only be decrypted with the corresponding key.
මෙම යතුරු ගණිතමය වශයෙන් සම්බන්ධ වේ, එනම් එක් යතුරකින් සිදු කරන කේතනය විකේතනය කළ හැක්කේ එයට අදාළ අනෙක් යතුරෙන් පමණි.

Ensuring Confidentiality
රහස්‍යභාවය තහවුරු කිරීම

When Person A wants to ensure that only Person B can read the message:
Bට පමණක් කියවිය හැකි පරිදි පණිවිඩයක් යැවීමට Aට අවශ්‍ය වූ විට:

- Person A encrypts the message using Person B's Public Key.
  පුද්ගලයා A විසින් පුද්ගලයා B ගේ පොදු යතුර භාවිතයෙන් පණිවිඩය කේතනය කරයි.

- Only Person B can decrypt it using Person B's Private Key.
  පුද්ගලයා B ට පමණක් ඔහුගේ පෞද්ගලික යතුර භාවිතයෙන් එය විකේතනය කළ හැකිය.

This ensures that no one except the intended receiver can read the message.
මෙමඟින් අදහස් කරන ලද ලබන්නාට හැර වෙනත් කිසිවෙකුට පණිවිඩය කියවිය නොහැකි බව සහතික කරයි.

Ensuring Authentication
සත්‍යාපනය තහවුරු කිරීම

When Person B wants to verify that the message was actually sent by Person A:
පුද්ගලයා Bට, පණිවිඩය සැබවින්ම එවා ඇත්තේ පුද්ගලයා A විසින්ම බව තහවුරු කර ගැනීමට අවශ්‍ය වූ විට:

- Person A encrypts (signs) the message using Person A's Private Key.
  පුද්ගලයා A විසින් පුද්ගලයා A ගේ පෞද්ගලික යතුර භාවිතයෙන් පණිවිඩය ජ්කේතනය කරයි.
- Person B verifies it using Person A's Public Key.
  පුද්ගලයා B විසින් පුද්ගලයා A ගේ පොදු යතුර භාවිතයෙන් එය තහවුරු කරගනියි.

This proves the identity of the sender and provides authentication and non-repudiation.
මෙය මඟින් පණිවිඩය එවන්නාගේ අනන්‍යතාවය ඔප්පු වන අතර, සත්‍යාපනය සහ ප්‍රතික්ෂේප කළ නොහැකි බව (non-repudiation) තහවුරු කරයි.

NOTE: Encrypting the total message require additional computational operations. Therefore, digital signatures are used to provide authentication and integrity, which will be discussed later.
සම්පූර්ණ පණිවිඩයම කේතනය කිරීම සඳහා අතිරේක ගණනීය මෙහෙයුම් අවශ්‍ය වේ. එබැවින්, විශ්වසනීයත්වය සහ අඛණ්ඩතාව සැපයීම සඳහා ඩිජිටල් අත්සන් භාවිතා කරනු ලබන අතර, ඒ පිළිබඳව පසුව සාකච්ඡා කරනු ඇත.

Advantages and Disadvantages of Asymmetric Key Encryption
අසමමිතික යතුරු කේතනයේ වාසි සහ අවාසි

Advantages
වාසි

Public keys can be shared openly
ප්‍රසිද්ධ යතුරු ඕනෑම අයෙකු සමඟ බෙදා ගත හැක.

No need for a secure key exchange channel
ආරක්ෂිත යතුරු හුවමාරු නාලිකාවක් අවශ්‍ය නොවේ.

Ensures authentication and data integrity
දත්තවල සත්‍යතාව සහ අඛණ්ඩතාව සහතික කරයි.

Supports digital signatures
ඩිජිටල් අත්සන් සඳහා සහාය දක්වයි.

ictfromabc.com

Disadvantages අවාසි

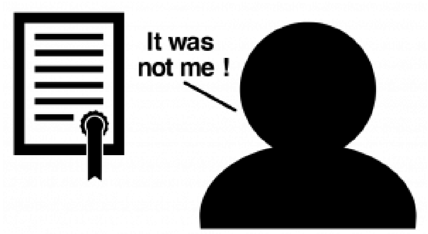
Slower than symmetric encryption
සමමිතික කේතනයට වඩා වේගය අඩුය.

Requires high computational power
වැඩි පරිගණක බලයක් අවශ්‍ය වේ.

Not suitable for large data encryption
විශාල දත්ත කේතනය කිරීමට එතරම් සුදුසු නොවේ.

Complex key generation and management
යතුරු නිර්මාණය සහ කළමනාකරණය සංකීර්ණ වේ.

Non-Repudiation
Digital signatures confirm the sender's identity and prevent them from denying their involvement.
ඩිජිටල් අත්සන් යවන්නාගේ අනන්‍යතාවය තහවුරු කරන අතර ඔවුන්ගේ සම්බන්ධය ප්‍රතික්ෂේප කිරීමෙන් වළක්වයි.



It is commonly achieved using Digital Signatures and Public Key Cryptography.
මෙය සාමාන්‍යයෙන් අංකිත අත්සන් සහ පොදු යතුරු කේතන භාවිතයෙන් ලබා ගනී.

Digital Signatures
අංකිත අත්සන්

The authenticity of digital documents or messages is verified using digital signatures, establishing trust in electronic communication.
අංකිත අත්සන් මඟින් විද්‍යුත් ලේඛනවල විශ්වාසවන්තභාවය සහ සත්‍යතාව තහවුරු කරයි.

The origin of the message is verified.
පණිවිඩයේ මූලාශ්‍රය සත්‍යාපනය කරයි.

Any unauthorized modification of the message is detected.
පණිවිඩය වෙනස් කර ඇත්දැයි හඳුනාගත හැකිය.

The author, as well as the date and time of signing, are verified.
අත්සන් කළ පුද්ගලයා, දිනය සහ වේලාව තහවුරු කරයි.

The integrity of the message content are ensured.
පණිවිඩ අන්තර්ගතයේ අඛණ්ඩතාව සහතික කෙරේ.

How to create a digital signature
අංකිත අත්සනක් නිර්මාණය කරන ආකාරය

Hash functions
හෑෂ් ශ්‍රිත

A hash function is a mathematical algorithm that takes an input (or message) and produces a fixed-size string of bytes, typically represented as a hexadecimal number.
හෑෂ් ශ්‍රිතයක් යනු ගණිතමය ඇල්ගොරිතමයක් වන අතර එය ආදානයක් (හෝ පණිවිඩයක්) ලබා ගෙන සාමාන්‍යයෙන් ෂඩ්දශමය සංඛ්‍යාවක් ලෙස නිරූපිත බයිට වල ස්ථාවර ප්‍රමාණයේ string නිපදවයි.

The output, known as the hash value or digest, is unique to each input.
හෑෂ් අගය හෝ ලෙස හඳුන්වන මෙම ප්‍රතිදානය එක් එක් ආදානයට අනන්‍ය වේ.

Even a small change in the input results in a completely different hash value, making hash functions ideal for verifying data integrity.
ආදානයේ කුඩා වෙනසක් පවා සම්පූර්ණයෙන්ම වෙනස් හැෂ් අගයක් ඇති කරයි, දත්ත අඛණ්ඩතාව තහවුරු කිරීම සඳහා හැෂ් ශ්‍රිතයන් වඩාත් සුදුසු වේ.

A one-way function, meaning the original input cannot be reconstructed from the hash value.
එක් මාර්ග (One-Way) ශ්‍රිතයක් වන අතර, හැෂ් අගයෙන් මුල් ආදානය නැවත ලබා ගත නොහැකි ය.

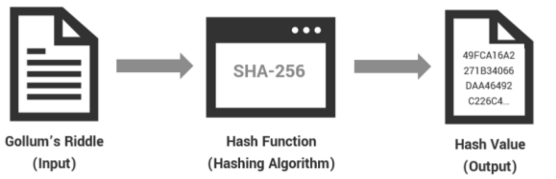
The output hash has a fixed length regardless of the input size. For example, SHA-256 always produces a 256-bit hash.
ආදානයේ ප්‍රමාණය කුමක් වුවද, හැෂ් අගයේ ප්‍රමාණය ස්ථාවර වේ. උදාහරණයක් ලෙස SHA-256 සමවිටම 256-bit හැෂ් අගයක් නිපදවයි.

Hash functions are deterministic, meaning the same input always produces the same hash value.
එකම ආදානය සමවිටම එකම හැෂ් අගය නිපදවන බැවින් හැෂ් ශ්‍රිතයන් නිශ්චිත වේ.

NOTE:
The security of a digital signature does not depend on the secrecy of the hash value, as anyone can compute it.
ඩිජිටල් අත්සනක ආරක්ෂාව රඳා පවතින්නේ එහි හැෂ් අගයේ රහස්‍යභාවය මත නොවේ, මන්ද ඕනෑම අයෙකුට එය ගණනය කළ හැකි බැවිනි.

Instead, it depends on the sender's private key, which is exclusively capable of generating a valid digital signature by encrypting a specific hash value of the message.
ඒ වෙනුවට, එය රඳා පවතින්නේ පණිවිඩයේ නිශ්චිත හැෂ් අගයක් කේතනය කිරීම මඟින් වලංගු ඩිජිටල් අත්සනක් උත්පාදනය කිරීමට අනන්‍ය ලෙස හැකියාව ඇති, යවන්නාගේ පුද්ගලික යතුර මත ය.

Therefore, any unauthorized modification of the message will result in a signature verification failure because the attacker cannot generate a matching signature.
එබැවින්, පණිවිඩයට කිසියම් අනවසර වෙනස් කිරීමක් සිදු කළහොත්, අත්සන සත්‍යාපනය කිරීම අසාර්ථක වනු ඇත. මන්දයත්, ප්‍රහාරකයාට ඊට ගැළපෙන අත්සනක් නිර්මාණය කිරීමට නොහැකි බැවිනි.



1. **Hashing the Message**
   පණිවිඩය හැෂ් කිරීම

A hash function (such as SHA-256) is applied to the message or document you want to sign.
ඔබට අත්සන් කිරීමට අවශ්‍ය පණිවිඩයට හෝ ලේඛනයට හැෂ් ශ්‍රිතයක් (SHA-256වැනි) යොදනු ලැබේ.

This hash produces a fixed-length value, a unique representation of the original message.
මෙම හැෂ් ශ්‍රිතය මගින් ස්ථාවර දිග අගයක් වන මුල් පණිවිඩයේ අනන්‍ය නිරූපණයක් නිපදවයි.

2. **Encrypting the Hash**
   හැෂ් එක කේතනය කිරීම

The message hash is encrypted using the sender's private key. This encrypted hash forms the digital signature.
හැෂ් පණිවිඩ යවන්නාගේ පුද්ගලික යතුර භාවිතයෙන් කේතනය කරනු ලබයි. මෙම කේතිත හැෂ් එක අංකිත අත්සන සාදයි.

The encryption ensures that only the sender, who holds the private key, could have created this signature.
කේතනය මගින් පුද්ගලික යතුර තබාගෙන සිටින යවන්නාට පමණක් මෙම අත්සන නිර්මාණය කළ හැකි බව සහතික කරයි.

3. **Attaching the Signature**
   අත්සන ඇමිණීම

The digital signature (the encrypted hash) is attached to the original message or document.
අංකිත අත්සන (කේතනය කළ හැෂ්) මුල් පණිවිඩයට හෝ ලේඛනයට අමුණා ඇත.

Along with the signature, the sender's public key is also shared so the recipient can verify it.
අත්සන සමඟින්, ග්‍රාහකායට එය සත්‍යාපනය කළ හැකි වන පරිදි යවන්නාගේ පොදු යතුර ද බෙදා ගනු ඇත.

4. **Sending the Signed Document**
   අත්සන් කරන ලද ලේඛනය යැවීම

The sender sends the signed document (message + digital signature + public key) to the recipient.
යවන්නා විසින් අත්සන් කරන ලද ලේඛනය (පණිවිඩය + අංකිත අත්සන + පොදු යතුර) ග්‍රාහකයා වෙත යවයි.

5. **Decrypting the Signature**
   අත්සන විකේතනය කිරීම

The receiver uses the sender's public key to decrypt the digital signature. This decrypted value is the hash that was generated from the original message by the sender.
අංකිත අත්සන විකේතනය කිරීමට ග්‍රාහකයා යවන්නාගේ පොදු යතුර භාවිතා කරයි. මෙම විකේතනය කළ අගය යවන්නා විසින් මුල් පණිවිඩයෙන් උත්පාදනය කරන ලද හැෂ් වේ.

6. **Generating a Hash from the Received Message**
   ලැබුණු පණිවිඩයෙන් හැෂ් එකක් උත්පාදනය කිරීම

The receiver generates their own hash from the received message using the same hash algorithm the sender used.
ග්‍රාහකයා විසින් ලැබුණු පණිවිඩයෙන් තමන්ගේම හැෂ් උත්පාදනය කරන්නේ යවන්නා භාවිතා කළ එකම හැෂ් ඇල්ගොරිතම භාවිතා කරමිනි.

7. Comparing the Two Hashes
හැෂ් අගයන් දෙක සැසඳීම

The receiver compares the hash they just generated from the message with the decrypted hash that was sent. If the two hash values match, it confirms that:
ග්‍රාහකයා පණිවිඩයෙන් ඔහු විසින් ජනනය කරන ලද හැෂ් එවා ඇති විකේතනය කළ හැෂ් සමඟ සංසන්දනය කරයි. හැෂ් අගයන් දෙක ගැලපෙන්නේ නම්, එය පහත දෑ තහවුරු කරයි:

- The message has not been altered.
  පණිවිඩය වෙනස් කර නැත.

- The message is indeed from the sender.
  පණිවිඩය ඇත්ත වශයෙන්ම යවන්නාගෙන් පැමිණ ඇත.

NOTE: Any change to the message produces a different hash value, causing signature verification to fail.
පණිවිඩයට සිදු කරන ඕනෑම වෙනස් කිරීමක් මඟින් වෙනස් හැෂ් අගයක් නිපදවන අතර, එමඟින් අත්සන තහවුරු කිරීමේ ක්‍රියාවලිය අසාර්ථක වේ.

Because only the sender possesses the private key, an attacker cannot generate a valid signature for the modified message
පුද්ගලික යතුර සතු වන්නේ යවන්නාට පමණක් බැවින්, ප්‍රහාරකයෙකුට වෙනස් කරන ලද පණිවිඩයක් සඳහා වලංගු ඩිජිටල් අත්සනක් නිර්මාණය කළ නොහැක.

Digital signatures solve the inefficiency of double encryption required to ensure both authentication and confidentiality.
සත්‍යතාව තහවුරු කිරීම සහ රහස්‍යභාවය යන දෙකම සහතික කිරීම සඳහා අවශ්‍ය වන ද්විත්ව කේතන ක්‍රියාවලියේ ඇති අකාර්යක්ෂමතාවයට ඩිජිටල් අත්සන් මඟින් විසඳුම් ලබා දෙයි.

By signing only, the message hash and encrypting the message once, they provide strong security with reduced processing time.
පණිවිඩයේ හැෂ් අගය පමණක් අත්සන් කිරීමෙන් සහ පණිවිඩය එක් වරක් පමණක් කේතනය කිරීමෙන්, ඒවා මඟින් අඩු සැකසුම් කාලයකින් ඉහළ ආරක්ෂාවක් සපයයි.

Uses of Digital Signatures
ඩිජිටල් අත්සන්වල භාවිතයන්

- Online Banking and Financial Transactions
  ඔන්ලයින් බැංකුකරණය සහ මූල්‍ය ගනුදෙනු

  Authenticates users and secures electronic financial transactions.
  පරිශීලකයින් සත්‍යාපනය කිරීම සහ ඉලෙක්ට්‍රොනික මූල්‍ය ගනුදෙනුවල ආරක්ෂාව තහවුරු කිරීම සිදු කරයි.

- E-Government Services
  විද්‍යුත් රාජ්‍ය සේවා

  Secures electronic forms, tax filings, licenses, and other government documents.
  ඉලෙක්ට්‍රොනික පෝරම, බදු ගොනු කිරීම්, බලපත්‍ර සහ අනෙකුත් රාජ්‍ය ලේඛනවල ආරක්ෂාව තහවුරු කරයි.

- Blockchain and Cryptocurrency Transactions
  බ්ලොක්චේන් සහ ක්‍රිප්ටෝකරන්සි

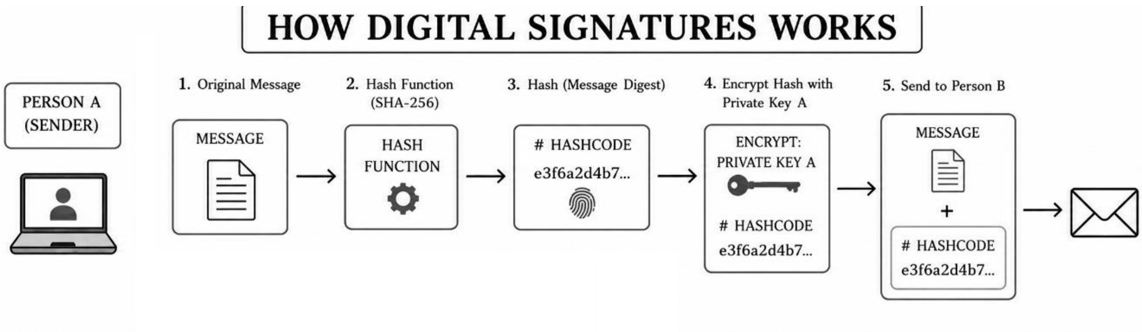
  Authorizes transactions and verifies ownership of digital assets.
  ගනුදෙනු ගනුදෙනු සඳහා අවසර ලබා දීම සහ ඩිජිටල් වත්කම්වල හිමිකාරිත්වය සත්‍යාපනය කිරීම සිදු කරයි.

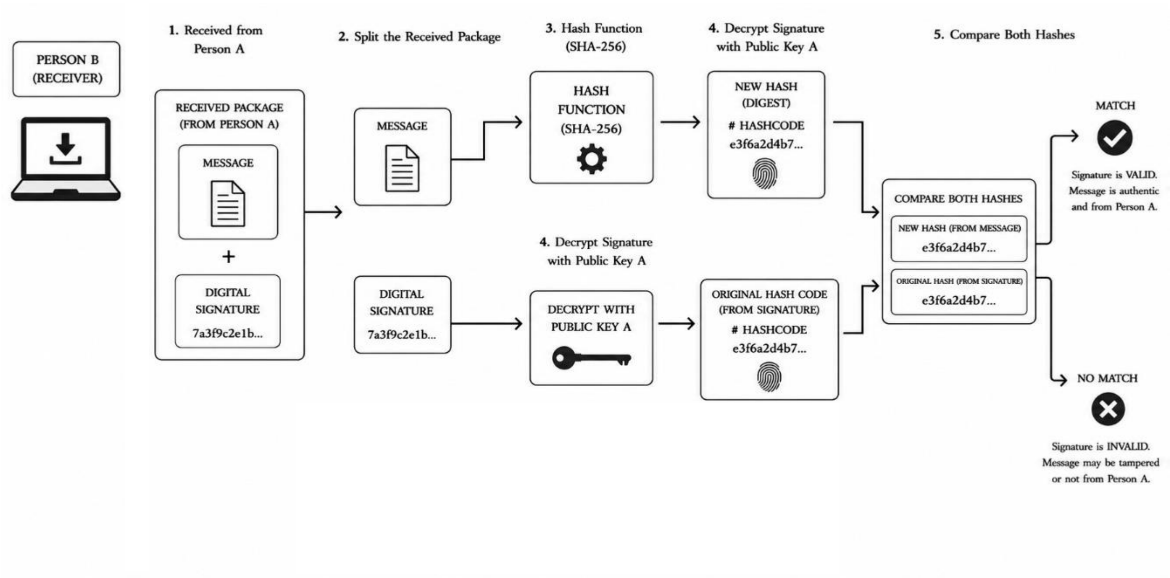
- Cryptocurrency Mining

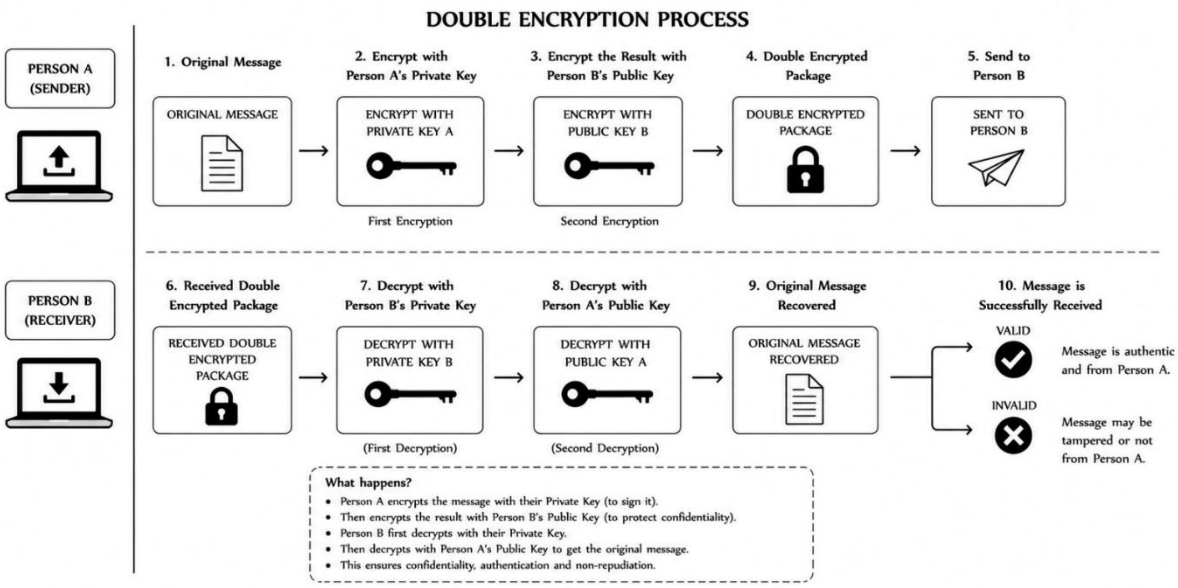
  Used to authenticate transaction ownership before transactions are validated and included in newly mined blocks.
  ගනුදෙනු වලංගු කර අලුතින් නිපදවන බ්ලොක්වලට ඇතුළත් කිරීමට පෙර, එම ගනුදෙනුවල හිමිකාරිත්වය සත්‍යාපනය කිරීමට භාවිතා කරයි.

- HTTPS (SSL/TLS Certificates)

  Used in SSL/TLS certificates to authenticate the identity of websites and establish secure HTTPS connections.
  වෙබ් අඩවිවල අනන්‍යතාවය සත්‍යාපනය කිරීමට සහ ආරක්ෂිත HTTPS සම්බන්ධතා ගොඩනැගීමට SSL/TLS සහතික තුළ භාවිතා වේ.


HOW DIGITAL SIGNATURES WORKS
PERSON A (SENDER)
1. Original Message
2. Hash Function (SHA-256)
3. Hash (Message Digest)
4. Encrypt Hash with Private Key A
5. Send to Person B
MESSAGE
HASH FUNCTION
HASHCODE e3f6a2d4b7...
ENCRYPT: PRIVATE KEY A
HASHCODE e3f6a2d4b7...
MESSAGE
+
HASHCODE e3f6a2d4b7...


PERSON B (RECEIVER)
1. Received from Person A
2. Split the Received Package
3. Hash Function (SHA-256)
4. Decrypt Signature with Public Key A
5. Compare Both Hashes
RECEIVED PACKAGE (FROM PERSON A)
MESSAGE
+
DIGITAL SIGNATURE 7a3f9c2e1b...
MESSAGE
DIGITAL SIGNATURE 7a3f9c2e1b...
HASH FUNCTION (SHA-256)
NEW HASH (DIGEST)
HASHCODE e3f6a2d4b7...
4. Decrypt Signature with Public Key A
DECRYPT WITH PUBLIC KEY A
ORIGINAL HASH CODE (FROM SIGNATURE)
HASHCODE e3f6a2d4b7...
COMPARE BOTH HASHES
NEW HASH (FROM MESSAGE) e3f6a2d4b7...
ORIGINAL HASH (FROM SIGNATURE) e3f6a2d4b7...
MATCH
Signature is VALID. Message is authentic and from Person A.
NO MATCH
Signature is INVALID. Message may be tampered or not from Person A.


DOUBLE ENCRYPTION PROCESS
PERSON A (SENDER)
1. Original Message
2. Encrypt with Person A's Private Key
3. Encrypt the Result with Person B's Public Key
4. Double Encrypted Package
5. Send to Person B
ORIGINAL MESSAGE
ENCRYPT WITH PRIVATE KEY A
ENCRYPT WITH PUBLIC KEY B
DOUBLE ENCRYPTED PACKAGE
SENT TO PERSON B
First Encryption
Second Encryption
PERSON B (RECEIVER)
6. Received Double Encrypted Package
7. Decrypt with Person B's Private Key
8. Decrypt with Person A's Public Key
9. Original Message Recovered
10. Message is Successfully Received
RECEIVED DOUBLE ENCRYPTED PACKAGE
DECRYPT WITH PRIVATE KEY B
DECRYPT WITH PUBLIC KEY A
ORIGINAL MESSAGE RECOVERED
VALID
Message is authentic and from Person A.
INVALID
Message may be tampered or not from Person A.
(First Decryption)
(Second Decryption)
What happens?
• Person A encrypts the message with their Private Key (to sign it).
• Then encrypts the result with Person B's Public Key (to protect confidentiality).
• Person B first decrypts with their Private Key.
• Then decrypts with Person A's Public Key to get the original message.
• This ensures confidentiality, authentication and non-repudiation.

Security of Communication and Internet-Connected Devices
සන්නිවේදන සහ අන්තර්ජාලයට සම්බන්ධ උපාංගවල ආරක්ෂාව

Network security is essential for protecting sensitive data such as personal information, financial transactions, and business operations.
පුද්ගලික තොරතුරු, මූල්‍ය ගනුදෙනු සහ ව්‍යාපාරික කටයුතු වැනි සංවේදී දත්ත ආරක්ෂා කිරීම සඳහා ජාල ආරක්ෂණය අත්‍යවශ්‍ය වේ.

Without adequate security, networks are vulnerable to threats including hacking, malware, data theft, and unauthorized access.
නිසි ආරක්ෂාවක් නොමැති විට, හැකර්වරුන් අනිෂ්ට මෘදුකාංග සහ දත්ත සොරකම් කිරීම් වැනි තර්ජනවලට ජාලයන් ගොදුරු විය හැකිය.

These threats may result in data breaches, financial loss, and loss of privacy.
මෙම තර්ජන හේතුවෙන් දත්ත කාන්දු වීම්, මූල්‍ය පාඩු සහ පුද්ගලිකත්වය අහිමි වීම සිදු විය හැක.

Malware
අනිෂ්ට මෘදුකාංග

Malware refers to malicious software designed to damage systems, disrupt services, steal data, or gain unauthorized access.
පද්ධතිවලට හානි කිරීමට, සේවාවන් අඩාල කිරීමට හෝ දත්ත සොරකම් කිරීමට නිර්මාණය කර ඇති හානිකර මෘදුකාංග මෙලෙස හැඳින්වේ.

Common types of malwares include viruses, worms, ransomware, and spyware.
සාමාන්‍යයෙන් දක්නට ලැබෙන අනිෂ්ට මෘදුකාංග වර්ග අතරට වයිරස් වර්ම්ස්, රැන්සම්වෙයාර් සහ ස්පයිවෙයාර් ඇතුළත් වේ.

Virus

A virus attaches itself to legitimate files or programs and is activated when executed.
වයිරස් නීත්‍යානුකූල ගොනු හෝ වැඩසටහන් සමඟ සම්බන්ධ වී ක්‍රියාත්මක වේ. ක්‍රියාත්මක වූ පසු දත්ත විනාශ කිරීම හෝ වෙනත් පද්ධතිවලට පැතිරීම සිදු කරයි.

Once activated, data corruption, deletion, and spread to other systems may occur.
එය ක්‍රියාත්මක වූ පසු, දත්ත දත්ත විකෘති වීම දත්ත මැකී යාම සහ අනෙකුත් පද්ධති කරා පැතිරී යාම සිදු විය හැකිය.

Viruses are commonly transmitted through infected files or email attachments.
වයිරස් සාමාන්‍යයෙන් ආසාදිත ගොනු හෝ විද්‍යුත් තැපැල් ඇමුණුම් හරහා ව්‍යාප්ත වේ.

Worms

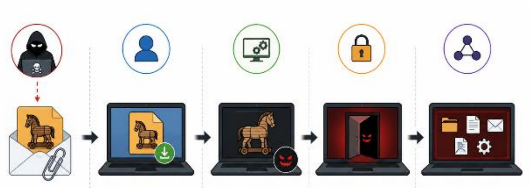
Worms are malicious programs that do not require attachment to other files or programs.
Worms වෙනත් ගොනු මත රඳා නොපවතින, ස්වයංව ප්‍රතිනිර්මාණය වෙමින් ජාලය හරහා ස්වාධීනව පැතිරෙන හානිකර වැඩසටහන් වේ.

Software or network vulnerabilities are exploited to enable self-replication and independent spreading.
ස්වයං-ප්‍රතිනිර්මාණය සහ ස්වාධීනව පැතිරීම සිදු කිරීම සඳහා මෘදුකාංග හෝ ජාල පද්ධතිවල පවතින දුර්වලතාවන් ප්‍රයෝජනයට ගනු ලබයි.

Network connections are commonly used to propagate from one system to another.
එක් පද්ධතියක සිට තවත් පද්ධතියකට ව්‍යාප්ත වීම සඳහා සාමාන්‍යයෙන් ජාල සම්බන්ධතා භාවිතා කරයි.

Large-scale infections may occur when security flaws in network protocols are exploited.\
ජාල නියමාවලි පවතින ආරක්ෂක දෝෂ ප්‍රයෝජනයට ගත් විට, මහා පරිමාණයේ ආසාදනයන් සිදු විය හැකිය.

Trojans (Trojan Horses)



Trojans are malicious programs that are disguised as legitimate software to deceive users into installing them.
ට්‍රෝජන් (Trojans) පෙනුමෙන් ආරක්ෂිත මෘදුකාංග ලෙස පෙනී සිටිමින් පරිශීලකයා රවටා පද්ධතියට ඇතුළු වේ.

Once installed, unauthorized system access may be granted, and data theft or system damage may occur.
ස්ථාපනය කළ පසු, පද්ධතියට අනවසරයෙන් පිවිසීමට ඉඩ ලැබිය හැකි අතර, දත්ත සොරකම් කිරීම හෝ පද්ධතියට හානි සිදු විය හැකිය.

Unlike viruses and worms, Trojans do not self-replicate.
වයිරස් සහ වර්ම්ස් මෙන් නොව, ට්‍රෝජන් මෘදුකාංග ස්වයංව ප්‍රතිනිර්මාණය (self-replicate) නොවේ.

Fake software updates are commonly used as a method of Trojan distribution.
ව්‍යාජ මෘදුකාංග යාවත්කාලීන කිරීම් (fake software updates) ට්‍රෝජන් ව්‍යාප්ත කිරීමේ පොදු ක්‍රමයක් ලෙස භාවිතා කරයි

Ransomware

Ransomware is a type of malware that encrypts files or locks systems, making data or systems inaccessible.
රැන්සම්වෙයාර් යනු ගොනු කේතනය (encrypt) කරන හෝ පද්ධති අගුළු දමන අනිෂ්ට මෘදුකාංග වර්ගයකි, එමඟින් දත්ත හෝ පද්ධති වෙත ප්‍රවේශ වීමට නොහැකි වේ

Victims are demanded to pay a ransom in order to restore access to data or systems.
දත්ත හෝ පද්ධති වෙත ප්‍රවේශය නැවත ලබා ගැනීම සඳහා වින්දිතයන්ගෙන් කප්පම් මුදලක් ගෙවන ලෙස ඉල්ලා සිටියි.

Significant data loss, financial damage, and operational disruption may result from ransomware attacks
රැන්සම්වෙයාර් ප්‍රහාර මඟින් සැලකිය යුතු දත්ත අහිමි වීමක්, මූල්‍ය හානි සහ මෙහෙයුම් කටයුතු අඩාල වීම් සිදු විය හැකිය.

Cyberattacks (සයිබර් ප්‍රහාර)

Cyberattacks are illegal attempts to steal data, damage systems, or disrupt networks.
සයිබර් ප්‍රහාර යනු දත්ත සොරකම් කිරීමට, පද්ධතිවලට හානි කිරීමට හෝ ජාල ක්‍රියාකාරිත්වය අඩාල කිරීමට ගනු ලබන නීතිවිරෝධී උත්සාහයන් වේ.

Phishing
තතුබෑම

Phishing is defined as a social engineering attack in which legitimate organizations are impersonated to obtain sensitive information such as login credentials or credit card details.
තතුබෑම යනු පිවිසුම් තොරතුරු හෝ ක්‍රෙඩිට් කාඩ් විස්තර වැනි සංවේදී තොරතුරු ලබා ගැනීම සඳහා පිළිගත් ආයතනයක් ලෙස පෙනී සිටිමින් සිදුකරන සමාජ ඉංජිනේරු ප්‍රහාරයකි.

Malicious emails or messages are commonly used to direct users to harmful links.
පරිශීලකයින් හානිකර සබැඳි වෙත යොමු කිරීම සඳහා සාමාන්‍යයෙන් අනිෂ්ට ඊමේල් හෝ පණිවිඩ භාවිතා කරයි.

Denial of Service (DoS) Attacks

Denial of Service attacks are carried out by overwhelming a network or server with excessive requests.
සේවා ප්‍රතික්ෂේප කිරීමේ ප්‍රහාර සිදු කරනු ලබන්නේ ජාලයක් හෝ සේවාදායකයක් වෙත දරාගත නොහැකි තරම් ඉල්ලීම් ප්‍රමාණයක් එවීමෙනි.

As a result, systems may crash or become unavailable to legitimate users.
මෙහි ප්‍රතිඵලයක් ලෙස, පද්ධති බිඳ වැටීමට හෝ නීත්‍යානුකූල පරිශීලකයින්ට භාවිතා කළ නොහැකි තත්ත්වයට පත් විය හැකිය.

Botnets

Botnets are networks of compromised devices controlled remotely.
බොට්නෙට් යනු දුරස්ථව පාලනය කරනු ලබන, ආසාදිත (compromised) උපාංග ජාලයකි.

These are often used to launch large-scale DDoS attacks or spread malware.
මේවා බොහෝ විට මහා පරිමාණ (DDoS) ප්‍රහාර එල්ල කිරීමට හෝ අනිෂ්ට මෘදුකාංග පැතිරවීමට භාවිතා කරයි.

Man-in-the-Middle (MitM) Attacks

Communication between two parties is secretly intercepted and altered.
පාර්ශවයන් දෙකක් අතර සිදුවන සන්නිවේදනය රහසිගතව බාධා කර (intercepted) වෙනස් කරනු ලැබේ.

Consequences
අහිතකර ඵල

An attacker can modify messages during transmission, causing misunderstandings and incorrect actions.
පණිවිඩ හුවමාරු වන අතරතුර ප්‍රහාරකයෙකුට ඒවා වෙනස් කළ හැකි අතර, එමඟින් වැරදි වැටහීම් සහ වැරදි ක්‍රියාමාර්ග ඇති විය හැක.

The receiver cannot be sure that the received data is identical to what the sender originally sent.
ලැබුණු දත්ත, යවන්නා මුලින්ම එවූ දත්තවලට සම්පූර්ණයෙන්ම සමාන බව පිළිගන්නා පාර්ශවයට ස්ථිරවම ප්‍රකාශ කළ නොහැක.

The attacker can insert, delete, or alter information, leading to confusion or misinformation.
ප්‍රහාරකයාට තොරතුරු ඇතුළත් කිරීමට, මැකීමට හෝ වෙනස් කිරීමට හැකි අතර, එමඟින් ව්‍යාකූලත්වයක් හෝ වැරදි තොරතුරු පැතිරීමක් සිදුවිය හැක.

Sensitive information such as passwords, banking details, and personal messages can be intercepted and read.
මුරපද, බැංකු තොරතුරු සහ පෞද්ගලික පණිවිඩ වැනි රහසිගත තොරතුරු අතරමගදී සොරාගෙන කියවීමට ලක්විය හැක.

The attacker can pretend to be either the sender or the receiver, making both parties believe they are communicating directly.
ප්‍රහාරකයාට යවන්නා හෝ ලබන්නා ලෙස පෙනී සිටිය හැකි අතර, දෙපාර්ශවයම තමන් සෘජුවම එකිනෙකා සමඟ සන්නිවේදනය කරන බව විශ්වාස කිරීමට සලස්වයි.

Altered transactions, fake instructions, or manipulated communications can result in financial losses and disrupted operations.
වෙනස් කරන ලද ගනුදෙනු, ව්‍යාජ උපදෙස් හෝ විකෘති කරන ලද සන්නිවේදනයන් හේතුවෙන් මූල්‍යමය පාඩු සහ මෙහෙයුම් කටයුතු අඩාල වීම් සිදු විය හැක.

Zero-Day Exploits

Zero-day exploits occur when unknown vulnerabilities in software or hardware are exploited before a security patch is developed.
මෘදුකාංගයක හෝ දෘඩාංගයක පවතින නොදන්නා දුර්වලතාවක්, ඒ සඳහා ආරක්ෂක පිළියම් (patch) සෑදීමට පෙර ප්‍රයෝජනයට ගැනීම Zero-day exploits ලෙස හැඳින්වේ.

Attackers take advantage of newly discovered flaws prior to vendor awareness or remediation.
නිෂ්පාදකයා ඒ පිළිබඳව දැනුවත් වීමට හෝ පිළියම් යෙදීමට පෙර ප්‍රහාරකයින් අලුතින් සොයාගත් දෝෂවලින් ප්‍රයෝජනය ලබා ගනී.

Insider Threats

Insider threats originate from within an organization, typically involving individuals with authorized access to sensitive data.
අභ්‍යන්තර තර්ජන ඇතිවන්නේ ආයතනයක් තුළිනි. සාමාන්‍යයෙන් මෙයට සංවේදී දත්ත වෙත ප්‍රවේශ වීමට අවසර ඇති පුද්ගලයින් සම්බන්ධ වේ.

Data theft or misuse may occur due to malicious or negligent internal actors.
ද්වේෂසහගත හෝ නොසැලකිලිමත් අභ්‍යන්තර ක්‍රියාකාරීන් නිසා දත්ත සොරකම් කිරීම හෝ අවභාවිතය සිදු විය හැකිය.

Password Attacks

Password attacks are carried out by guessing, stealing, or cracking user passwords.
පරිශීලක මුරපද අනුමාන කිරීම, සොරකම් කිරීම හෝ බිඳ දැමීම (cracking) මඟින් මුරපද ප්‍රහාර සිදු කරනු ලැබේ

Techniques such as brute-force attacks and credential stuffing are commonly used.
මේ සඳහා brute-force attacks සහ credential stuffing වැනි තාක්ෂණික ක්‍රම බහුලව භාවිතා වේ.

Spoofing

Attacker impersonates a trusted user, device, or system.
ප්‍රහාරකයෙකු විශ්වාසවන්ත පරිශීලකයෙකු, උපාංගයක් හෝ පද්ධතියක් ලෙස ව්‍යාජව පෙනී සිටියි.

Uses fake identity information (IP, MAC, Email, DNS, Website, Caller ID).
ව්‍යාජ (IP, MAC, ඊමේල්, DNS, වෙබ් අඩවි හෝ දුරකථන අංක භාවිතා කරයි.)

Deceives users or security systems into trusting the attacker.
පරිශීලකයන් හෝ ආරක්ෂක පද්ධති නොමැති විශ්වාසයක් ඇති කරයි.

Bypasses security controls to gain unauthorized access.
ආරක්ෂක පාලනයන් මඟ හැරී අනවසර ප්‍රවේශය ලබා ගනී.

Steals sensitive information or intercepts communications.
සංවේදී තොරතුරු සොරකම් කරයි හෝ සන්නිවේදන අනුගමනය කරයි.

Commonly used with phishing and Man-in-the-Middle (MitM) attacks.
Phishing සහ Man-in-the-Middle (MitM) ප්‍රහාරයන් සමග බහුව භාවිතා වේ.

Prevented using authentication, encryption, and digital certificates.
Authentication, Encryption සහ Digital Certificates භාවිතයෙන් අවරණය කළ හැක.

SQL Injection (SQLi)

SQL Injection is a cyberattack where malicious SQL code is inserted into input fields to manipulate a database.
SQL Injection යනු වෙබ් අඩවියක දත්ත ඇතුළත් කරන ස්ථාන හරහා අනිෂ්ට කේත ඇතුළත් කර දත්ත ගබඩාව හැසිරවීම සඳහා කරනු ලබන සයිබර් ප්‍රහාරයකි.

This technique is used by attackers to bypass security measures, view sensitive data, or modify database records without authorization.
ප්‍රහාරකයින් මෙම උපක්‍රමය භාවිතා කරන්නේ ආරක්ෂක පියවරයන් මඟහැරීමට, සංවේදී දත්ත බැලීමට හෝ අවසරයකින් තොරව දත්ත ගබඩාවේ වාර්තා වෙනස් කිරීමටයි.

Vulnerabilities
මෘදුකාංග දුර්වලතා

Security weaknesses or flaws within a system, software, or network that may be exploited by attackers to gain unauthorized access or cause harm are defined as vulnerabilities.
පද්ධතියක්, මෘදුකාංගයක් හෝ ජාලයක් තුළ පවතින, අනවසර ප්‍රවේශයක් ලබා ගැනීමට හෝ හානි සිදු කිරීමට ප්‍රහාරකයින් විසින් ප්‍රයෝජනයට ගත හැකි ආරක්ෂක දුර්වලතා හෝ දෝෂ මෙලෙස හැඳින්වේ.

Data Leakage

Data leakage occurs when sensitive information is exposed unintentionally or through misconfiguration.
නොදැනුවත්ව හෝ වැරදි සැකසුම් නිසා සංවේදී තොරතුරු නිරාවරණය වීම දත්ත කාන්දු වීමක් ලෙස හැඳින්වේ.

Confidential data may be leaked via unsecured cloud storage or removable media.
ආරක්ෂිත නොවන වලාකුළු ආචයන හෝ ඉවත් කළ හැකි මාධ්‍ය (උදා:USB) හරහා රහසිගත දත්ත කාන්දු විය හැකිය.

Unsecured Wi-Fi Networks

Unsecured wireless networks allow unauthorized users to intercept data or gain network access.
ආරක්ෂිත නොවන රැහැන් රහිත ජාල මඟින් අනවසර පරිශීලකයින්ට දත්ත බාධා කිරීමට හෝ ජාලයට ඇතුළු වීමට ඉඩ ලැබිය හැකිය.

Sensitive information may be captured through packet sniffing techniques.
packet sniffing තාක්ෂණයන් හරහා සංවේදී තොරතුරු ලබා ගත හැකිය.

Software Vulnerabilities

Security weaknesses in outdated or unpatched software may be exploited by attackers.
යාවත්කාලීන නොකළ හෝ පිළියම් (patch) නොයෙදූ මෘදුකාංගවල පවතින ආරක්ෂක දුර්වලතා ප්‍රහාරකයින් විසින් ප්‍රයෝජනයට ගත හැකිය.

Regular updates and patch management are required to reduce this risk.
මෙම අවදානම අවම කිරීම සඳහා නිතිපතා යාවත්කාලීන කිරීම් සහ පිළියම් කළමනාකරණය අවශ්‍ය වේ.

Antivirus

Software designed to detect, prevent, and remove malicious software (malware).
අනිෂ්ට මෘදුකාංග හඳුනා ගැනීමට, වැළැක්වීමට සහ ඉවත් කිරීමට සකසා ඇති මෘදුකාංග.

Core functions / මූලික කාර්යයන්

- Real-time/on-access scanning (checks files as they're opened/downloaded)
  තියුණු කාලීන පරිලෝකනය කිරීම (ගොනු විවෘත කරන විට/බාගත කරන විට ඒවා පරීක්ෂා කිරීම)
- Scheduled full-system scans
  සැලසුම්ගත සම්පූර්ණ පද්ධති පරිලෝකන
- Quarantine (isolates infected files instead of deleting immediately)
  නිරෝධායනය (ආසාදිත ගොනු වහාම මකා දැමීම වෙනුවට හුදකලා කිරීම)
- Automatic signature/database updates
  ස්වයංක්‍රීය අත්සන්/දත්ත සමුදාය යාවත්කාලීන කිරීම්
- Email and web protection (blocks phishing links, malicious attachments)
  විද්‍යුත් තැපෑල සහ වෙබ් ආරක්ෂණය (පිෂිං සබැඳි, අනිෂ්ට ඇමුණුම් අවහිර කිරීම)

Types of malware it targets
ඉලක්ක කරන අනිෂ්ට මෘදුකාංග වර්ග

Viruses	Worms
Trojans	Ransomware
Spyware/Adware	Rootkits

How it works / එය ක්‍රියා කරන ආකාරය

Signature-based detection
අත්සන් මත පදනම් වූ හඳුනාගැනීම

Compares files against a database of known malware "signatures" (hashes). Fast but can't catch brand-new threats.
දන්නා අනිෂ්ට මෘදුකාංගවල hashes දත්ත සමුදායක් සමඟ ගොනු සංසන්දනය කරයි. වේගවත් නමුත් හාත්පසින්ම අලුත් තර්ජන හඳුනාගත නොහැක.

Heuristic analysis / හියුරිස්ටික් විශ්ලේෂණය

Examines code behavior/structure for suspicious patterns, even if no exact signature exists.
නිවැරදිම අත්සනක් නොමැති වුවද, සැක සහිත රටාවන් සඳහා කේතයේ හැසිරීම/ව්‍යුහය පරීක්ෂා කරයි.

Behavioral/real-time monitoring
හැසිරීම්/තථ්‍ය කාලීන නිරීක්ෂණය

Watches running processes for malicious actions (e.g., encrypting files rapidly, modifying system files) and blocks them on the fly.
අනිෂ්ට ක්‍රියා (උදා. ගොනු වේගයෙන් සංකේතනය කිරීම, පද්ධති ගොනු වෙනස් කිරීම) සඳහා ක්‍රියාත්මක වන ක්‍රියාවලීන් නිරීක්ෂණය කරන අතර ඒවා එසැනින් අවහිර කරයි.

Sandboxing

Runs suspicious files in an isolated environment (inside the actual OS) to observe behavior safely.
හැසිරීම් ආරක්ෂිතව නිරීක්ෂණය කිරීම සඳහා හුදකලා පරිසරයක (සැබෑ මෙහෙයුම් පද්ධතිය තුළ) සැක සහිත ගොනු ධාවනය කරයි.

Key limitations / ප්‍රධාන සීමාවන්

- Zero-day attacks (unknown threats) can slip past signature-based detection
  සීරෝ-ඩේ ප්‍රහාර (නොදන්නා තර්ජන) අත්සන් මත පදනම් වූ හඳුනාගැනීම් මඟ හැර යා හැක
- Can't stop social engineering (e.g., user willingly giving up a password)
  සමාජ ඉංජිනේරු විද්‍යාව වැළැක්විය නොහැක (උදා. පරිශීලකයා කැමැත්තෙන්ම මුරපදයක් ලබා දීම)
- May slow down system performance during scans
  පරිලෝකනය කිරීමේදී පද්ධතියේ ක්‍රියාකාරීත්වය මන්දගාමී විය හැක

Best practices / හොඳම භාවිතයන්

- Keep antivirus and OS updated
  ඇන්ටිවෛරස් සහ මෙහෙයුම් පද්ධතිය යාවත්කාලීනව තබා ගන්න
- Don't rely on antivirus alone (pair with firewalls, backups, and safe browsing habits)
  ඇන්ටිවෛරස් මත පමණක් විශ්වාසය නොතබන්න (ෆයර්වෝල්, උපස්ථ සහ ආරක්ෂිත බ්‍රවුසින් පුරුදු සමඟ ඒකාබද්ධව භාවිත කරන්න)
- Regularly run full scans, not just real-time protection
  තථ්‍ය කාලීන ආරක්ෂාව පමණක් නොව, නිතිපතා සම්පූර්ණ පරිලෝකන ක්‍රියාත්මක කරන්න

Examples
උදාහරණ

- Windows Defender
- Norton
- Bitdefender
- Kaspersky
- Malwarebytes

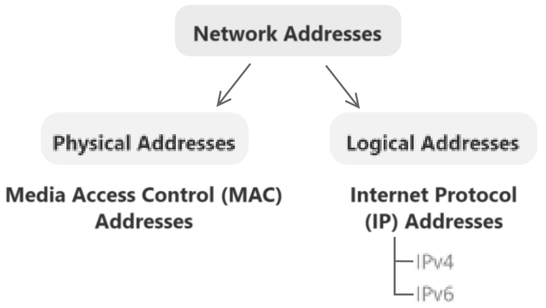
IP addressing
IP ලිපිනකරණය

Network addresses
ජාල ලිපින

A network address is an identifier used to identify a network or a device on a network. It enables devices to locate, communicate, and exchange data with each other.
ජාල ලිපිනයක් යනු ජාලයක් හෝ ජාලයක ඇති උපාංගයක් හඳුනා ගැනීමට භාවිතා කරන හඳුන්වනයකි. එමඟින් උපාංගවලට එකිනෙකා සොයා ගැනීමට, සන්නිවේදනය කිරීමට සහ දත්ත හුවමාරු කර ගැනීමට හැකියාව ලැබේ.

There are two types of network addresses.
ජාල ලිපින ප්‍රධාන වශයෙන් වර්ග දෙකකි.

MAC Address identifies what the device is by providing its unique hardware identity, while an IP Address identifies where the device is by indicating its logical location on a network.
MACලිපිනය භාවිතා කරන්නේ උපාංගය කුමක්ද යන්න හඳුනා ගැනීමට වන අතර, IP ලිපිනය භාවිතා කරන්නේ උපාංගය කොතැනද යන්න ජාලයක් තුළ හඳුනා ගැනීමටයි.



Media Access Control (MAC) Address

A MAC Address is a unique physical address assigned to a device's Network Interface Card (NIC) by the manufacturer. It is used to identify devices and enable communication within a Local Area Network (LAN).
MAC ලිපිනයක් යනු උපාංගයක නිෂ්පාදකයා විසින් එහි ඇති ජාල අතුරුමුහුණත් කාඩ්පතට ලබා දෙන සුවිශේෂී, භෞතික ලිපිනයකි. මෙය ස්ථානීය ජාලයක් තුළ උපාංග හඳුනා ගැනීමට සහ ඒවා අතර සන්නිවේදනය සිදු කිරීමට භාවිතා කරයි.

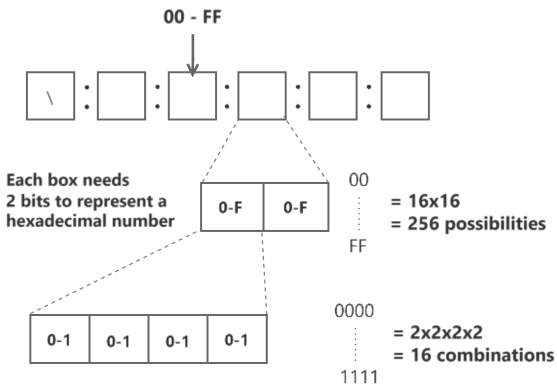
MAC addresses operate at the Data Link Layer (Layer 2) of the OSI Model.
MAC ලිපින, OSI ආකෘතියේ දත්ත සම්බන්ධක ස්තරය තුළ ක්‍රියාත්මක වේ.

It's permanent and does not change, as it is hard-coded into the device’s Network Interface Card (NIC) by the manufacturer during production.
නිෂ්පාදනය අතරතුර නිෂ්පාදකයා විසින් උපාංගයේ ජාල අතුරුමුහුණත් කාඩ්පතට එය තදින් කේතනය කර ඇති බැවින් එය ස්ථිර වන අතර වෙනස් නොවේ.

A MAC Address uniquely identifies a network interface, not the entire device. Therefore, a single device can have multiple MAC addresses if it has multiple network interfaces, such as Ethernet, Wi-Fi, or Bluetooth.
MAC ලිපිනයක් මඟින් සම්පූර්ණ උපාංගය නොව ජාල අතුරුමුහුණතක් අනන්‍ය ලෙස හඳුනා ගනී. එබැවින්, Ethernet, Wi-Fi හෝ Bluetooth වැනි බහු ජාල අතුරුමුහුණත් තිබේ නම්, තනි උපාංගයකට බහු ඒක ලිපින තිබිය හැකිය.

A MAC address consists of 48 bits in binary.
MAC ලිපිනයක් ද්විමය බිටු 48 කින් සමන්විත වේ.

For human convenience, it is written as six groups of two hexadecimal digits separated by colons (:) or hyphens (-).
මිනිසාගේ පහසුව සඳහා, එය තිත් දෙකකින් (:) හෝ කෙටි ඉරකින් (-) වෙන් කරන ලද, ෂඩ් දශමය පාදයේ සංඛ්‍යා දෙක බැගින් වූ කාණ්ඩ හයක් ලෙස ලියා දක්වනු ලැබේ.



Each of the above 6 groups can have 256 different options from 0 (00_{16}) to 256 (FF_{16})

The maximum number of MAC addresses
= 16 x 16 x ….. x 16 (16^{12})
= 2^{48}
= 281,474,976,710,656
= Approximately 281 Trillion

Minimum possible MAC address
පැවතිය හැකි අවම MAC ලිපිනය
00:00:00:00:00:00

Maximum possible MAC address
පැවතිය හැකි උපරිම MAC ලිපිනය
FF:FF:FF:FF:FF:FF

A random MAC address
අහඹු MAC ලිපිනයක්
4C:70:17:AB:BC:AC

IP Addresses

IPv4 (version 4)

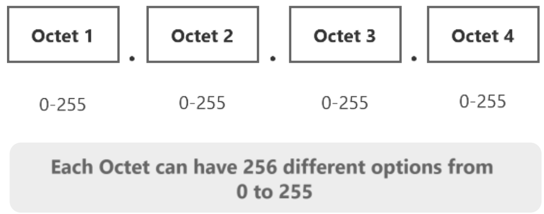
IPv4 uses a 32-bit binary address scheme.
IPv4 මගින් ද්විමය බිටු 32ක ලිපින ක්‍රමයක් භාවිතා කරයි.

For human convenience, the IPv4 address is written in dotted decimal notation. In this format, the 32-bit binary IP address is divided into four 8-bit (**octet** or byte) sections.
මිනිසුන්ගේ පහසුව සඳහා, IPv4 ලිපින තිත් දශමය අංකනයකින් ලියා ඇත. මෙම ආකෘතියේ දී, බිටු 32 ද්විමය IP ලිපිනය බිටු 8 (**අෂ්ටක** හෝ බයිට) කොටස් හතරකට බෙදා ඇත.

Each section is converted into a decimal number, and these four decimal numbers are separated by periods (dots).
සෑම කොටසක්ම දශම සංඛ්‍යාවක් බවට පරිවර්තනය කරන අතර, මෙම දශම සංඛ්‍යා හතර නැවතීමේ ලකුණු (තිත්) මගින් වෙන් කරනු ලැබේ.

For example, the binary IP address 11000000 10101000 00000000 00000001 becomes 192.168.0.1 in dotted decimal notation.
උදාහරණයක් ලෙස, ද්විමය IP ලිපිනය වන 11000000.10101000.00000000.00000001 තිත් දශම අංකනය තුළ 192.168.0.1 බවට පත් වේ.

Dotted Decimal Notation



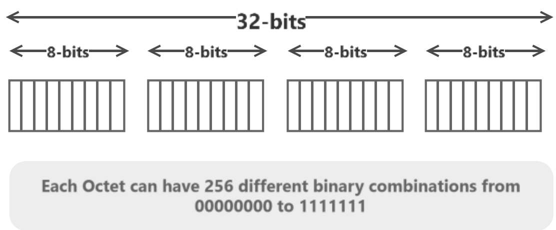
So, the maximum number of IPv4 addresses
එබැවින්, පැවතිය හැකි උපරිම IPb4 ලිපින ගණන
= 256 x 256 x 256 x 256
= 4,294,967,296
= Approximately 4.3 Billion

Minimum possible IPv4 address
පැවතිය හැකි අවම IPv4 ලිපිනය
0.0.0.0

Maximum possible IPv4 address
පැවතිය හැකි උපරිම IPv4 ලිපිනය
255.255.255.255

Random IPv4 address
අහඹු IPv4 ලිපිනයක්
192.168.0.1

Binary Notation



So, the maximum number of IPv4 addresses
එබැවින්, පැවතිය හැකි උපරිම IPb4 ලිපින ගණන
= 2^{32}
= 2 x 2 x 2 x ….. x 2
= 4,294,967,296
= Approximately 4.3 Billion

Minimum possible IPv4 address
පැවතිය හැකි අවම IPv4 ලිපිනය
00000000 00000000 00000000 00000000

Maximum possible IPv4 address
පැවතිය හැකි උපරිම IPv4 ලිපිනය
11111111 11111111 11111111 11111111

Random IPv4 address
අහඹු IPv4 ලිපිනයක්
11000000 10101000 00000000 0000000

Private IP Address
පුද්ගලික IP ලිපිනය

A Private IP Address is an IP address used within a local network and is not directly accessible from the Internet.
පුද්ගලික IP ලිපිනයක් යනු දේශීය ජාලයක් තුළ පමණක් භාවිතා වන ලිපිනයක් වන අතර, අන්තර්ජාලයේ සිට සෘජුවම එය වෙත ප්‍රවේශ විය නොහැක.

These addresses are assigned and managed by a Network Administrator or a router and are used for communication between devices within the same network.
මෙම ලිපින ජාල පරිපාලකයෙකු හෝ රවුටරයක් මඟින් පවරනු ලබන අතර පාලනය කරනු ලැබේ. මේවා භාවිතා කරනු ලබන්නේ එකම ජාලය තුළ ඇති උපාංග අතර සන්නිවේදනය සඳහාය.

Devices in different private networks can have the same private IP address, because private IP addresses are only unique within their own local network.
විවිධ පුද්ගලික ජාල වල උපාංගවලට එකම පුද්ගලික IP ලිපිනයක් තිබිය හැකිය, මන්ද පුද්ගලික IP ලිපින ඒවායේ දේශීය ජාලය තුළ පමණක් අද්විතීය වේ.

Private IP ranges
පුද්ගලික IP පරාසයන්

- Class A → 10.0.0.0 - 10.255.255.255
- Class B → 172.16.0.0 - 172.31.255.255
- Class C → 192.168.0.0 - 192.168.255.255

Public IP Address
පොදු IP ලිපිනය

A Public IP Address is a globally unique IP address that is assigned by an Internet Service Provider (ISP) and is accessible over the Internet.
පොදු IP ලිපිනයක් යනු අන්තර්ජාල සේවා සපයන්නෙකු විසින් පවරනු ලබන, අන්තර්ජාලය හරහා සෘජුවම ප්‍රවේශ විය හැකි, ලොව පුරා අනන්‍ය වූ IP ලිපිනයකි.

It allows devices or networks to communicate with external networks worldwide. Since public IP addresses must be unique across the Internet, no two devices can use the same public IP address at the same time.
එය මඟින් උපාංගවලට හෝ ජාලවලට ලොව පුරා ඇති බාහිර ජාල සමඟ සන්නිවේදනය කිරීමට ඉඩ සලසයි. පොදු IP ලිපින මුළු අන්තර්ජාලය පුරාම එකිනෙකට වෙනස් විය යුතු බැවින්, එකම අවස්ථාවකදී උපාංග දෙකකට එකම පොදු IP ලිපිනය භාවිතා කළ නොහැක.

Static IP Address
ස්ථාවර IP ලිපිනය

A Static IP Address is a permanent IP address that remains the same unless it is manually changed by a network administrator.
ස්ථාවර IP ලිපිනයක් යනු ජාල පරිපාලකයෙකු විසින් එය හස්තීයව වෙනස් කරන තුරු නොවෙනස්ව පවතින ස්ථිර IP ලිපිනයකි.

Static IP addresses are commonly used for servers, websites, and network devices that need a fixed location on the network.
ජාලය තුළ ස්ථිර පිහිටීමක් අවශ්‍ය වන සේවාදායක පරිගණක, වෙබ් අඩවි සහ ජාල උපාංග සඳහා සාමාන්‍යයෙන් ස්ථාවර IP ලිපින භාවිතා කරනු ලැබේ.

Domain names (such as www.google.com) are often linked to static IP addresses so that users can consistently access the same server or service.
පරිශීලකයන්ට නිරන්තරයෙන්ම එකම සේවාදායකය හෝ සේවාව වෙත පිවිසීමට හැකි වන පරිදි, වසම් නාම (උදාහරණයක් ලෙස www.google.com) බොහෝ විට මෙම ස්ථාවර IP ලිපින සමඟ සම්බන්ධ කර ඇත.

Dynamic IP Address
ගතික IP ලිපිනය

A Dynamic IP Address is a temporary IP address that is automatically assigned to a device and may change over time.
ගතික IP ලිපිනයක් යනු උපාංගයකට ස්වයංක්‍රීයව පවරනු ලබන සහ කාලයත් සමඟ වෙනස් විය හැකි තත්කාලීන IP ලිපිනයකි.

Dynamic IP addresses are managed by a Dynamic Host Configuration Protocol (DHCP) server, which automatically allocates available IP addresses to devices when they connect to a network.
ගතික IP ලිපින පාලනය කරනු ලබන්නේ DHCP සේවාදායකයක් මඟිනි. එමඟින් උපාංගයක් ජාලයකට සම්බන්ධ වන විට, භාවිතයට ගත හැකිව ඇති IP ලිපින ස්වයංක්‍රීයව එම උපාංගය වෙත වෙන් කර දෙයි.

This method simplifies network management and is commonly used in home and office networks.
මෙම ක්‍රමය මඟින් ජාල කළමනාකරණය පහසු කරවන අතර, නිවාස සහ කාර්යාලීය ජාලවල බහුලවම භාවිතා වන්නේ මෙම ක්‍රමයයි.

Network Address Translation (NAT)
ජාල ලිපින පරිවර්තනය

Network Address Translation (NAT) is a technique used by routers to translate private IP addresses used within a local network into a public IP address used on the Internet, and vice versa.
ජාල ලිපින පරිවර්තනය යනු ස්ථානීය ජාලයක් තුළ භාවිතා වන පුද්ගලික IP ලිපින, අන්තර්ජාලය තුළ භාවිතා වන පොදු IP ලිපිනයක් බවට පරිවර්තනය කිරීම සඳහා සහ එහි ප්‍රතිලෝම ක්‍රියාවලිය සඳහා රවුටර විසින් භාවිතා කරනු ලබන තාක්ෂණයකි.

NAT allows multiple devices on a private network to share a single public IP address when accessing the Internet.
NAT මඟින් පුද්ගලික ජාලයක ඇති උපාංග කිහිපයකට අන්තර්ජාලයට පිවිසීමේදී එකම පොදු IP ලිපිනයක් හවුලේ භාවිතා කිරීමට අවස්ථාව ලබා දෙයි.

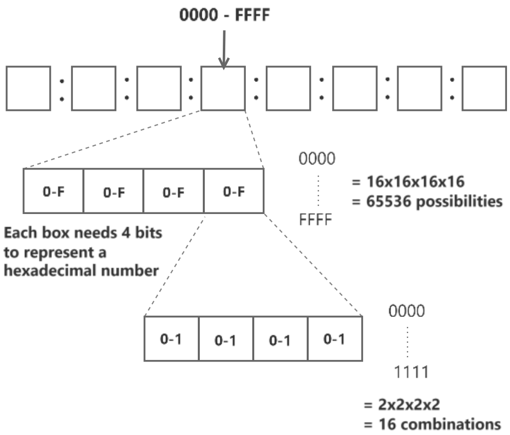
NAT is performed by routers and will be discussed in more detail in the Router lesson.
NAT රවුටර මගින් සිදු කරනු ලබන අතර එය රවුටර් පාඩමේදී වඩාත් විස්තරාත්මකව සාකච්ඡා කෙරේ.

IPv6 (version 6)

IPv6 was introduced mainly to solve IPv4 address exhaustion and provide a much larger address space, ensuring the continued growth and scalability of the Internet.
IPv4 ලිපින හිඟවීමට විසඳුමක් ලෙස සහ වඩාත් විශාල ලිපින අවකාශයක් ලබා දීම වෙනුවෙන් ප්‍රධාන වශයෙන්ම IPv6 හඳුන්වා දෙන ලද අතර, එමඟින් අන්තර්ජාලයේ අඛණ්ඩ වර්ධනය සහ පරිමාණ්‍යතාව සහතික කරයි.

They use a 128-bit binary addressing system, massively increasing the number of unique addresses available compared to IPv4's 32-bit system.
ඒවා බිටු 128ක ද්විමය ලිපින පද්ධතියක් භාවිතා කරයි, IPv4 හි බිටු 32හි පද්ධතියට සාපේක්ෂව පවතින අනන්‍ය ලිපින ගණන විශාල වශයෙන් වැඩි කරයි.

IPv6 addresses are written in hexadecimal and are represented in eight groups of four hexadecimal digits, separated by colons for the easy use of humans.
IPv6 ලිපින ෂඩ්දශමය ආකාරයෙන් ලියා ඇති අතර colons වලින් වෙන් කරන ලද ෂඩ්දශම ඉලක්කම් හතරක කාණ්ඩ අටකින් මිනිසුන්ගේ පහසු භාවිතය සඳහා නිරූපණය කෙරේ.



Each of the above 8 groups can have 65536 different options from 0 (0000_{16}) to 65535 ($FFFF_{16}$)

The maximum number of IPv6 addresses
පැවතිය හැකි උපරිම IPv6 ලිපින ගණන
= 65536 x 65536 x ….. x 65536 (65536^8)
= 2^{128}
= 340,282,366,920,938,463
= Approximately 340 Undecillion

Minimum possible IPv6 address
පැවතිය හැකි අවම IPv6 ලිපිනය
0000:0000:0000:0000:0000:0000:0000:0000

Maximum possible IPv6 address
පැවතිය හැකි උපරිම IPv6 ලිපිනය
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

A random IPv6 address
අහඹු IPv6 ලිපිනයක්
3F4B:00A2:7C1D:3A8B:002F:AC11:BB99:E776

From this point, the syllabus focuses only on IPv4 addresses which used to identify a device in a network.
මෙතැන් සිට, විෂය නිර්දේශය අවධානය යොමු කරන්නේ ජාලයක් තුළ උපාංගයක් හඳුනා ගැනීමට භාවිතා කරන (IPv4) ලිපින පිළිබඳව පමණි.

Classful addressing
පන්ති සහිත ලිපින

In the early days of the Internet, organizations required networks of different sizes. Some needed very large networks with millions of host addresses, while others required only medium-sized or small networks.
අන්තර්ජාලයේ මුල් අවධියේදී, සංවිධාන සඳහා විවිධ ප්‍රමාණවලින් යුත් ජාල අවශ්‍ය විය. සමහරුන්ට ධාරක ලිපින මිලියන ගණනක් සහිත ඉතා විශාල ජාල අවශ්‍ය වූ අතර, තවත් සමහරුන්ට අවශ්‍ය වූයේ මධ්‍යම ප්‍රමාණයේ හෝ කුඩා ජාල පමණි.

The concept of dividing IPv4 addresses into classes was introduced to manage IP address allocation efficiently.
IP ලිපින බෙදා හැරීම කාර්යක්ෂමව කළමනාකරණය කිරීම සඳහා IPv4 ලිපින පන්තිවලට බෙදීමේ සංකල්පය හඳුන්වා දෙන ලදී.

To simplify IP address allocation and support these varying requirements, IPv4 addresses were divided into several predefined classes.
IP ලිපින වෙන් කිරීම සරල කිරීමට සහ මෙම විවිධ අවශ්‍යතාවලට සහය දැක්වීම සඳහා, IPv4 ලිපින පූර්වයෙන් අර්ථ දක්වන ලද පංති කිහිපයකට බෙදා වෙන් කරන ලදී.

Each class provided a different number of network and host addresses, allowing organizations to choose a class that best matched the size of their network.
සෑම පංතියක්ම එකිනෙකට වෙනස් ජාල සහ ධාරක ලිපින සංඛ්‍යාවක් ලබා දුන් අතර, එමඟින් සංවිධානවලට ඔවුන්ගේ ජාලයේ ප්‍රමාණයට වඩාත්ම ගැළපෙන පංතියක් තෝරා ගැනීමට ඉඩ සැලසිනි.

The class system helped distribute IP addresses based on the number of hosts a network required.
ජාලයකට අවශ්‍ය ධාරක සංඛ්‍යාව මත පදනම්ව IP ලිපින බෙදා හැරීමට පන්ති පද්ධතිය උදවු විය.

This approach, known as classful addressing, made IP address allocation straightforward and easier to manage during the early growth of the Internet.
පංති සහිත ආමන්ත්‍රණය ලෙස හැඳින්වෙන මෙම ප්‍රවේශය, අන්තර්ජාලයේ මුල්කාලීන වර්ධනය අතරතුරදී ෂඡ ලිපින වෙන් කිරීම සෘජු මෙන්ම කළමනාකරණය කිරීමට පහසු එකක් බවට පත් කළේය.

There are two parts of an IP address
IP ලිපිනයක කොටස් දෙකක් ඇත

1. **Network part** ජාල කොටස
2. **Host part** ධාරක කොටස

Network part
ජාල කොටස

The network part of an IP address identifies the network to which a device belongs.
IP ලිපිනයක ජාල කොටස උපාංගයක් අයත් ජාලය හඳුනා ගනී.

All devices on the same network share the same network part in their IP addresses.
එකම ජාලයේ ඇති සියලුම උපාංග එවාගේ IP ලිපිනවල එකම ජාල කොටස බෙදා ගනී.

This is similar to how a postal code helps identify a general location for a group of houses.
මෙය තැපැල් කේතයක් නිවාස සමූහයක් සඳහා පොදු ස්ථානයක් හඳුනා ගැනීමට උපකාර වන ආකාරය හා සමාන වේ.

The length of the network part is determined by the IP address class.
ජාල කොටසෙහි දිග තීරණය කරනු ලබන්නේ IP ලිපින පන්තිය මගිනි.

Note:
The network portion of an IP address is fixed based on the subnet and cannot be changed, as it is used to identify the specific network to which the device belongs.
IP ලිපිනයක ජාල කොටස උපජාලය මත පදනම්ව නියතව පවතින අතර එය උපාංගය අයත් වන නිශ්චිත ජාලය හඳුනා ගැනීමට භාවිතා කරන බැවින් එය වෙනස් කළ නොහැක.

Host part
ධාරක කොටස

The host part of an IP address identifies the individual device (host) within the network.
IP ලිපිනයක ධාරක කොටස ජාලය තුළ ඇති තනි උපාංගයක් (ධාරක) හඳුනා ගනී.

Each device in the network has a unique host part.
ජාලයේ සෑම උපාංගයකටම අනන්‍ය ධාරක කොටසක් ඇත.

If the network part is like a postal code, the host part is like a house number that identifies each house within that postal area.
ජාල කොටස තැපැල් කේතයක් වැනි නම්, ධාරක කොටස එම තැපැල් ප්‍රදේශය තුළ ඇති සෑම නිවසක්ම හඳුනා ගන්නා නිවාස අංකයක් වැනිය.

The host part length is also determined by the IP address class. The remaining bits after the network part are used for the host part.
ධාරක කොටසෙහි දිග තීරණය කරනු ලබන්නේ IP ලිපින පන්තිය මගිනි. ජාල කොටසෙන් පසු ඉතිරි වන බිටු ධාරක කොටස සඳහා භාවිතා වේ.

Network Address
ජාල ලිපිනය
The network address is the first address in any given IP network. It identifies the specific network itself. It is used to refer to the entire network when routing traffic between networks.
ජාල ලිපිනය යනු ඕනෑම IP ජාලයක පළමු ලිපිනයයි. එමගින් එම නිශ්චිත ජාලයම හඳුනා ගනී. ජාල අතර ගමනාගමනය මෙහෙයවීමේදී එය මුළු ජාලයටම යොමු කිරීමට භාවිතා කරයි.

Broadcast Address
විකාශන ලිපිනය
The broadcast address is the last address in any IP network. It is used to send messages to all devices within a particular network. When a packet is sent to the broadcast address, all hosts on that network will receive the message.
විකාශන ලිපිනය ඕනෑම IP ජාලයක අවසාන ලිපිනය වේ. එය නිශ්චිත ජාලයක් තුළ ඇති සියලුම උපාංග වෙත පණිවිඩ යැවීමට භාවිතා කරයි. විකාශන ලිපිනයට පැකට්ටුවක් යැවූ විට, එම ජාලයේ සියලුම ධාරකයන්ට පණිවිඩය ලැබෙනු ඇත.

Note:
Since two addresses have to be reserved for the network and broadcast addresses, these two addresses cannot be assigned to hosts.
ජාලය සහ විකාශන ලිපින සඳහා ලිපින දෙකක් වෙන් කළ යුතු බැවින්, මෙම ලිපින දෙක ධාරකයන් වෙත පැවරිය නොහැක.

Therefore, the number of IP addresses that can assigned to hosts in a network is always less than the total number of IP address by 2.
එබැවින්, ජාලයක ධාරක වෙත පැවරිය හැකි IP ලිපින ගණන සෑම විටම මුළු ෂජ ලිපින ගණනට වඩා 2 කින් අඩු වේ

The address space is divided into five classes.
ලිපින අවකාශය පන්ති පහකට බෙදා ඇත.

1. **Class A**
Used by large organizations that require very large networks with a huge number of hosts.
අතිවිශාල පරිගණක සංඛ්‍යාවක් සහිත ඉතා විශාල ජාල අවශ්‍ය වන මහා පරිමාණ සංවිධාන/ආයතන විසින් භාවිතා කරයි.

2. **Class B**
Used by universities and medium-to-large organizations that need a moderate number of hosts and networks.
මධ්‍යස්ථ ජාල සහ පරිගණක සංඛ්‍යාවක් අවශ්‍ය වන විශ්වවිද්‍යාල සහ මධ්‍යම හෝ මහා පරිමාණයේ ආයතන විසින් භාවිතා කරයි.

3. **Class C**
Used by homes, offices, and small businesses that require small networks with fewer hosts.
අඩු පරිගණක සංඛ්‍යාවක් සහිත කුඩා ජාල අවශ්‍ය වන නිවාස, කාර්යාල සහ කුඩා ව්‍යාපාර විසින් භාවිතා කරයි.

4. **Class D**
Used for multicast communication, where data is sent to multiple devices simultaneously.
එක්වර උපාංග කිහිපයකට දත්ත යැවීම සඳහා වන බහු-ප්‍රචාරණය සන්නිවේදනය වෙනුවෙන් භාවිතා කරයි.

5. **Class E**
Reserved for research, development, and experimental networking purposes.
පර්යේෂණ, සංවර්ධන සහ පරීක්ෂණාත්මක ජාලකරණ කටයුතු සඳහා වෙන් කර ඇත.

Class A
The first bit of the 32 bits is fixed as 0.
බිටු 32 න් පළමු බිටුව 0 ලෙස නියත කර ඇත.

The first octet (8 bits) identifies the network, meaning the first octet is reserved for network identification.
පළමු අෂ්ටකය (බිටු 8) ජාලය හඳුනා ගනී, එනම් පළමු අෂ්ටකය ජාලය හඳුනාගැනීම සඳහා වෙන් කර ඇත.

The last three octets (24 bits) are used for the host portion, which identifies devices (hosts) on that network.
එම ජාලයේ උපාංග (ධාරක) හඳුනා ගන්නා ධාරක කොටස සඳහා අවසාන අෂ්ටක තුන (බිටු 24) භාවිතා වේ.

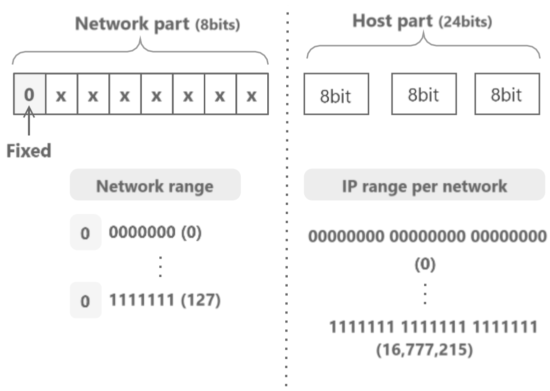
This division determines the number of networks of a particular type and the device count in each network.
මෙම බෙදීම මඟින් නිශ්චිත වර්ගයකට අයත් ජාල සංඛ්‍යාව සහ එක් එක් ජාලය තුළ ඇති උපාංග සංඛ්‍යාව තීරණය කරයි.

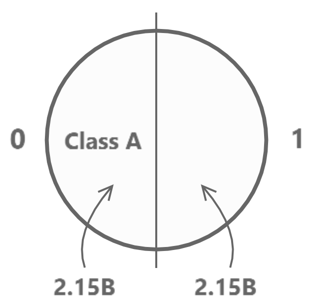
Smaller number of class A networks and a huge number of devices per network is available.
පංති A වර්ගයේ ජාල කුඩා සංඛ්‍යාවක් සහ ජාලයක් සඳහා ඉතා විශාල උපාංග සංඛ්‍යාවක් පවතී.

Every classful IPv4 address that starts with a 0 as the first bit, belongs to class A.
පළමු බිටුව ලෙස 0 කින් ආරම්භ වන සෑම පන්ති සහිත IPv4 ලිපිනයක්ම A පන්තියට අයත් වේ.

Since the first bit is set to 0, the total set of 4.3 million IPv4 addresses is divided into two equal parts.
පළමු බිට් එක 0 ලෙස සවි කර ඇති බැවින්, මිලියන 4.3 ක් වන මුළු IPv4 ලිපින කුලකය සමාන කොටස් දෙකකට බෙදේ.

Class A owns one of those two parts which contains approximately 2.1million IP addresses.
IP ලිපින ආසන්න වශයෙන් මිලියන 2.1ක් පමණ අඩංගු එම කොටස් දෙකෙන් එකක් A පන්තිය සතු වේ.





The circle represents the total number of IPv4 addresses (4.3B)

After fixing the first bit as 0, there are 7 remaining bits for the network part. Therefore, the number of unique combinations that 7 bits can form will be the number of class A networks.
පළමු බිටුව 0 ලෙස සවි කළ පසු ජාල කොටස සඳහා ඉතිරි බිටු 7ක් ඇත. එබැවින්, බිටු 7 කට සෑදිය හැකි අනන්‍ය සංයෝජන ගණන A පන්තියේ ජාල ගණන වනු ඇත.

After reserving 8 bits for the network part, we are left with 24 remaining bits out of 32, for the host part.
ජාල කොටස සඳහා බිටු 8ක් වෙන් කිරීමෙන් පසුව, ධාරක කොටස සඳහා 32න් ඉතිරි බිටු 24ක් අපට ඉතිරි වේ.

So, the number of unique combinations that 24 bits can form will be the maximum number of IP addresses in a class A network.
එබැවින්, බිටු 24 කට සෑදිය හැකි අනන්‍ය සංයෝජන ගණන A පන්තියේ ජාලයක උපරිම IP ලිපින ගණන වනු ඇත.

The total number of IP addresses that can be assigned to hosts in a class A network is less than that maximum number of IP addresses by two.
A පන්තියේ ජාලයක ධාරකයන්ට පැවරිය හැකි මුළු IP ලිපින ගණන එම උපරිම IP ලිපින ගණනට වඩා දෙකකින් අඩුය.

The maximum number of Class A networks
උපරිම A පන්තියේ ජාල ගණන
= 2^7 = 128

The maximum no. of IP addresses in a class A network
A පන්තියේ ජාලයක ඇති උපරිම IP ලිපින ගණන
= 2^{24} = 16,777,216

The maximum no. of possible hosts in a class A network
A පන්තියේ ජාලයක පැවතිය හැකි උපරිම ධාරක ගණන
= $2^{24} - 2$
= 16,777,216 – 2
= 16,777,214

The total no. of class A IP addresses
A පන්තියේ පවතින මුළු IP ලිපින ගණන
= 128 x 16,777,216 or 2^{31} (32-1)
= 2,147,483,648
= Approximately 2.1 billion

Note:

$2^{\text{network part bits}}$ = No. of maximum networks

$2^{\text{ජාල කොටසේ බිටු}}$ = මුළු ජාල ගණන

$2^{\text{host part bits}}$ = Maximum no. of addresses

$2^{\text{සත්කාරක කොටසේ බිටු}}$ = උපරිම ලිපින ගණන

Usable host count = Maximum no. of addresses – 2

භාවිත කල හැකි සත්කාරක ගණන = උපරිම ලිපින ගණන – 2

Note:

From 0.0.0.0 to 0.255.255.255

This block is reserved and is not assigned for public use. The address 0.0.0.0 is often used to indicate an unknown or unspecified network, or during initial system setup.

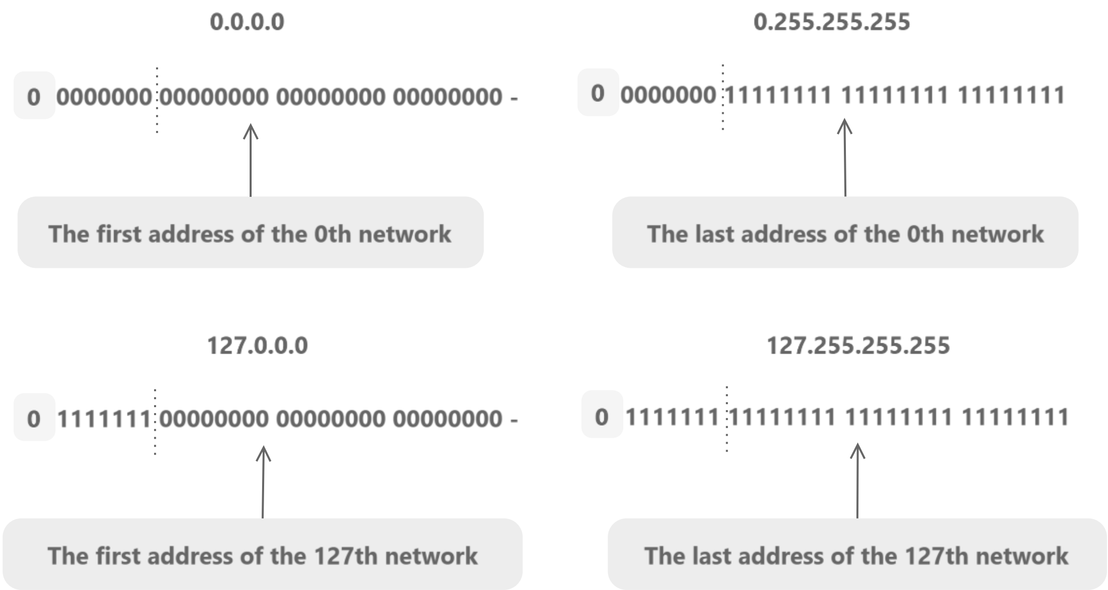
මෙම කොටස වෙන් කර ඇති අතර පොදු භාවිතය සඳහා පවරා නැත. 0.0.0.0 ලිපිනය බොහෝ විට නොදන්නා හෝ නිශ්චිත නොවන ජාලයක් දැක්වීමට හෝ මූලික පද්ධති සැකසුමේදී භාවිතා වේ.

From 127.0.0.0 to 127.255.255.255

This block is reserved for loopback and testing purposes. The address 127.0.0.1 is commonly used as the loopback address for local testing on the host machine.

මෙම කොටස ලූප්බැක් සහ පරීක්ෂණ අරමුණු සඳහා වෙන් කර ඇත. 127.0.0.1 ලිපිනය ධාරක යන්ත්‍රයේ ස්ථානීය පරීක්ෂාව සඳහා ලූප්බැක් ලිපිනය ලෙස බහුලව භාවිතා වේ.

These reservations lead to the wastage of millions of IP addresses.
මෙම වෙන් කිරීම් මිලියන ගණනක IP ලිපින නාස්තියට තුඩු දෙයි.



0th network contains approximately 16.7 million IP addresses and vast majority of them are not used and wasted.

0 වන ජාලයේ IP ලිපින මිලියන 16.7 ක් පමණ අඩංගු වන අතර ඒවායින් අතිමහත් බහුතරයක් භාවිතා නොකරන අතර අපතේ යයි.

127th network also contains another 16.7 million IP addresses, but in practice, only one address which is 127.0.0.1 is commonly used for the loopback function. The remaining addresses in this range are almost never used, resulting in significant wastage.

127 වන ජාලයේ තවත් IP ලිපින මිලියන 16.7 ක් අඩංගු වේ, නමුත් ප්‍රායෝගිකව, ලූප්බැක් ශ්‍රිතය සඳහා බහුලව භාවිතා වන්නේ 127.0.0.1 වන එක් ලිපිනයක් පමණි. මෙම පරාසයේ ඉතිරි ලිපින බොහෝ විටෙක භාවිතා නොකරන අතර, සැලකිය යුතු නාස්තියක් ඇති කරයි.

Class B

In class B addresses, the second bit of the 32 bits is fixed as 0 while the first bit is 1.

B පන්තියේ ලිපින වලදී, බිටු 32 න් පළමු බිටුව 1 පවතින අතරතුර දෙවන බිටුව 0 ලෙස නියත කෙරේ.

The first two octets (16 bits) identify the network, meaning the first two octets are reserved for network identification.

පළමු අෂ්ටක දෙක (බිටු 16) ජාලය හඳුනා ගනී, එනම් පළමු අෂ්ටක දෙක ජාලය හඳුනාගැනීම සඳහා වෙන් කර ඇත.

The last two octets (16 bits) are used for the host portion, which identifies devices (hosts) on that network.

එම ජාලයේ උපාංග (ධාරක) හඳුනා ගන්නා ධාරක කොටස සඳහා අවසාන අෂ්ටක දෙක (බිටු 16) භාවිතා වේ.

This addressing scheme provides a moderate number of networks while allowing a moderate number of hosts within each network, making it suitable for medium sized organizations.

මෙම ලිපින ක්‍රමය මඟින් මධ්‍යස්ථ ජාල ප්‍රමාණයක් ලබා දෙන අතරම, එක් එක් ජාලය තුළ මධ්‍යස්ථ ධාරක පරිගණක ප්‍රමාණයක් පවත්වා ගැනීමට ඉඩ සලසයි, එමඟින් මෙය මධ්‍යම ප්‍රමාණයේ සංවිධාන සඳහා වඩාත් සුදුසු වේ.

Every classful IPv4 address that starts with 10 as the first two bits, belongs to class B.

පළමු බිටු දෙක 10 කින් ආරම්භ වන සෑම පන්ති සහිත IPv4 ලිපිනයක්ම B පන්තියට අයත් වේ.

When the first bit is 1, it includes half of the total IPv4 addresses which is approximately 2.15 billion.

පළමු බිට් එක 1 විට, එයට ආසන්න වශයෙන් බිලියන 2.15 වන මුළු IPv4 ලිපිනවලින් අඩක් ඇතුළත් වේ.

Since all B, C, D, and E classes have to share these 2.15 billion addresses, it again has to be divided.

සියලුම B, C, D, සහ E පන්ති මෙම බිලියන 2.15 ලිපින බෙදා ගත යුතු බැවින්, එය නැවත බෙදිය යුතුය.

Therefore, the second bit is fixed as 0 such that the remaining set of IP addresses can be divided into two equal parts.

එබැවින්, ඉතිරි IP ලිපින කුලකය සමාන කොටස් දෙකකට බෙදිය හැකි පරිදි දෙවන බිටුව 0 ලෙස නියත කරනු ලැබේ.

Class B owns one of those two parts which contains approximately one billion IP addresses.

IP ලිපින ආසන්න වශයෙන් බිලියන 1ක් පමණ අඩංගු එම කොටස් දෙකෙන් එකක් B පන්තිය සතු වේ.

After fixing the first two bits as 10, there are 14 remaining bits for the network part. Therefore, the number of unique combinations that 14 bits can form will be the number of class B networks.

පළමු බිටු දෙක 10 ලෙස සවි කළ පසු ජාල කොටස සඳහා ඉතිරි බිටු 14ක් ඇත. එබැවින්, බිටු 14 කට සෑදිය හැකි අනන්‍ය සංයෝජන ගණන B පන්තියේ ජාල ගණන වනු ඇත.

After reserving 16 bits for the network part, we are left with another 16 remaining bits out of 32, for the host part.

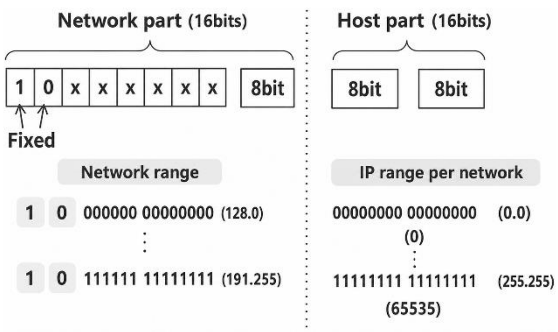
ජාල කොටස සඳහා බිටු 16ක් වෙන් කිරීමෙන් පසුව, ධාරක කොටස සඳහා 32න් තවත් ඉතිරි බිටු 16ක් අපට ඉතිරි වේ.

So, the number of unique combinations that 16 bits can form will be the maximum number of IP addresses in a class B network.

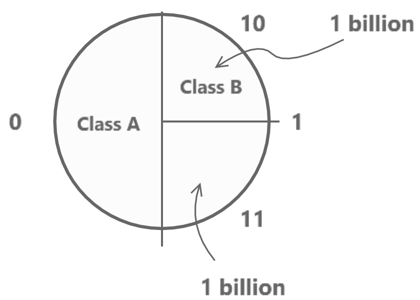
එබැවින්, බිටු 16 කට සෑදිය හැකි අනන්‍ය සංයෝජන ගණන B පන්තියේ ජාලයක උපරිම IP ලිපින ගණන වනු ඇත.

The total number of IP addresses that can be assigned to hosts in a class B network is less than that maximum number of IP addresses by two.

B පන්තියේ ජාලයක ධාරකයන්ට පැවරිය හැකි මුළු IP ලිපින ගණන එම උපරිම IP ලිපින ගණනට වඩා දෙකකින් අඩුය.



The remaining 2.15 billion IP addresses are now divided into two equal parts, and class B owns one of those two.



The maximum number of Class B networks
උපරිම B පන්තියේ ජාල ගණන
= 2^{14} = 16,384

The maximum no. of IP addresses in a class B network
B පන්තියේ ජාලයක ඇති උපරිම IP ලිපින ගණන
= 2^{16} = 65,536

The maximum no. of possible hosts in a class B network
B පන්තියේ ජාලයක පැවතිය හැකි උපරිම ධාරක ගණන
= $2^{16} - 2$
= 65,536 – 2
= 65,534

The total no. of class B IP addresses
B පන්තියේ පවතින මුළු IP ලිපින ගණන
= 16,384 x 65,536 or 2^{30} (32-2)
= 1,073,741,824
= Approximately 1 billion

NOTE:
Private Class B Range (172.16.0.0)
The range from 172.16.0.0 to 172.31.255.255 is reserved for private use, containing 1,048,576 IP addresses.
172.16.0.0 සිට 172.31.255.255 දක්වා පරාසය පුද්ගලික භාවිතය සඳහා වෙන් කර ඇත, එහි IP ලිපින 1,048,576 අඩංගු වේ.

These addresses are typically used within private networks and cannot be routed on the public internet.
මෙම ලිපින සාමාන්‍යයෙන් පුද්ගලික ජාල තුළ භාවිතා වන අතර පොදු අන්තර්ජාලයට යොමු විය නොහැක.

Link-Local Address (169.254.0.0)
This range is reserved for link-local addressing, used when a device cannot obtain an IP address via DHCP.
මෙම පරාසය සම්බන්ධක-ස්ථානීය ලිපින සඳහා වෙන් කර ඇත, උපාංගයකට DHCP හරහා IP ලිපිනයක් ලබා ගත නොහැකි විට භාවිතා වේ.

This range contains 65,536 addresses and is used only within a local segment, not for communication over the internet.
මෙම පරාසයේ ලිපින 65,536 ක් අඩංගු වන අතර අන්තර්ජාලය හරහා සන්නිවේදනය සඳහා නොව, ස්ථානීය අංශයක් තුළ පමණක් භාවිතා වේ

Class C
In class C addresses, the third bit of the 32 bits is fixed as 0 while both the first two bits are 1.
C පන්තියේ ලිපින වලදී, බිටු 32 න් පළමු බිටු දෙකම 1 ලෙස පවතින අතරේදී තුන්වන බිටුව 0 ලෙස නියත කෙරේ.

The first three octets (24 bits) identify the network, meaning the first three octets are reserved for network identification.
පළමු අෂ්ටක තුන (බිටු 24) ජාලය හඳුනා ගනී, එනම් පළමු අෂ්ටක තුන ජාලය හඳුනාගැනීම සඳහා වෙන් කර ඇත.

The last octet (8 bits) is used for the host portion, which identifies devices (hosts) on that network.
එම ජාලයේ උපාංග (ධාරක) හඳුනා ගන්නා ධාරක කොටස සඳහා අවසාන අෂ්ටකය (බිටු 8) භාවිතා වේ.

This makes the number of networks huge and number of devices per network smaller.
මෙය මඟින් ජාල සංඛ්‍යාව විශාල කරන අතර එක් ජාලයකට ඇති උපාංග සංඛ්‍යාව කුඩා කරයි.

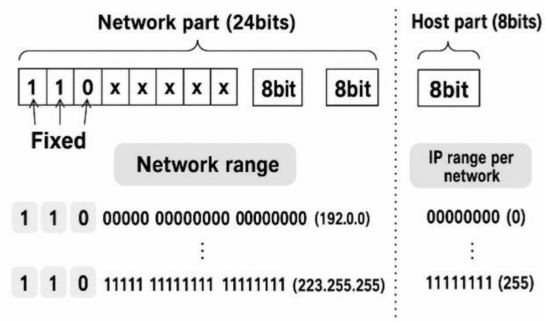
Every classful IPv4 address that starts with 110 as the first three bits, belongs to class C.
පළමු බිටු තුන 110 කින් ආරම්භ වන සෑම පන්ති සහිත IPv4 ලිපිනයක්ම C පන්තියට අයත් වේ.

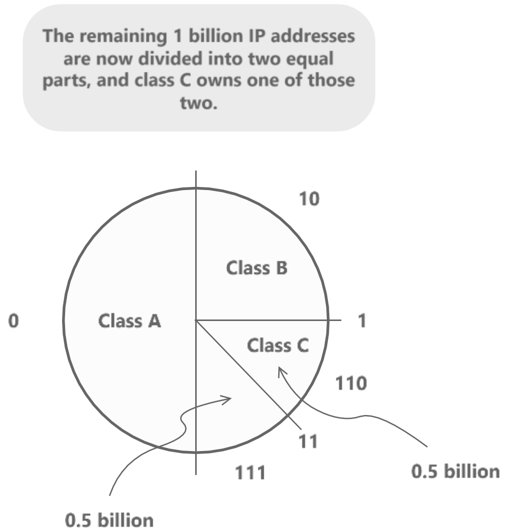
When the first two bits are fixed as 11, it includes half of the 2.1 billion addresses which is approximately 1 billion.
පළමු බිටු එක 1 ලෙස සවි කළ විට, එයට ආසන්න වශයෙන් බිලියන 1 වන බිලියන 2.1 IPv4 ලිපිනවලින් අඩක් ඇතුළත් වේ.

Since all C, D, and E classes have to share these 1billion addresses, it again has to be divided.
සියලුම C, D, සහ E පන්ති මෙම බිලියන 1 ලිපින බෙදා ගත යුතු බැවින්, එය නැවත බෙදිය යුතුය.

Therefore, the third bit is fixed as 0 such that the remaining set of IP addresses can be divided into two equal parts.
එබැවින්, ඉතිරි IP ලිපින කුලකය සමාන කොටස් දෙකකට බෙදිය හැකි පරිදි දෙවන බිටුව 0 ලෙස නියත කරනු ලැබේ.

Class C owns one of those two parts which contains approximately half of a billion IP addresses.
IP ලිපින බිලියනයකින් අඩක් පමණ අඩංගු එම කොටස් දෙකෙන් එකක් C පන්තිය සතුය.





After fixing the first three bits as 110, there are 21 remaining bits for the network part. Therefore, the number of unique combinations that 21 bits can form will be the number of class C networks.
පළමු බිටු තුන 110 ලෙස සවි කළ පසු ජාල කොටස සඳහා ඉතිරි බිටු 21ක් ඇත. එබැවින්, බිටු 21 කට සෑදිය හැකි අනන්‍ය සංයෝජන ගණන C පන්තියේ ජාල ගණන වනු ඇත.

After reserving 24 bits for the network part, we are left with 8 remaining bits out of 32, for the host part.
ජාල කොටස සඳහා බිටු 24ක් වෙන් කිරීමෙන් පසුව, ධාරක කොටස සඳහා 32න් තවත් ඉතිරි බිටු 8ක් අපට ඉතිරි වේ.

So, the number of unique combinations that 8 bits can form will be the maximum number of IP addresses in a class C network.
එබැවින්, බිටු 8 කට සෑදිය හැකි අනන්‍ය සංයෝජන ගණන C පන්තියේ ජාලයක උපරිම IP ලිපින ගණන වනු ඇත.

The total number of IP addresses that can be assigned to hosts in a class C network is less than that maximum number of IP addresses by two.
C පන්තියේ ජාලයක ධාරකයන්ට පැවරිය හැකි මුළු IP ලිපින ගණන එම උපරිම IP ලිපින ගණනට වඩා දෙකකින් අඩුය.

The maximum number of Class C networks
උපරිම C පන්තියේ ජාල ගණන
= 2^{21} = 2,097,152

The maximum no. of IP addresses in a class C network
C පන්තියේ ජාලයක ඇති උපරිම IP ලිපින ගණන
= 2^{8}= 256

The maximum no. of possible hosts in a class C network
C පන්තියේ ජාලයක පැවතිය හැකි උපරිම ධාරක ගණන
= $2^{8} - 2$
= 256 – 2
= 254

The total no. of class C IP addresses
C පන්තියේ පවතින මුළු IP ලිපින ගණන
= 2,097,152 x 256 or 2^{29} (32-3)
= 536,870,912
= Approximately 530 million

Note:
There are some reserved Class C networks that we don't use for public internet traffic
පොදු අන්තර්ජාල ගමනාගමනය සඳහා භාවිතා නොකරන වෙන් කර ඇති Class C ජාල කිහිපයක් තිබේ

Private IP addresses
192.168.0.0 - 192.168.255.255
These are reserved for private network use (Ex. home LANs) and are not routed on the internet.
මේවා පුද්ගලික ජාල සඳහා වෙන් කර ඇත (උදා. කාර්යාල LANs) සහ අන්තර්ජාලය හරහා ගමන් නොකෙරේ.

Reserved for special purposes
192.0.0.0
Reserved by IANA for special use.
විශේෂ භාවිතය සඳහා IANA විසින් වෙන් කර ඇත.

192.88.99.0
Reserved for IPv6-to-IPv4 relay use.
IPv6-to-IPv4 රිලේ භාවිතය සඳහා වෙන් කර ඇත.

192.0.2.0, **198.51.100.0**, and **203.0.113.0**
Reserved for documentation and example use (TEST-NET).
ලේඛනගත කිරීම සහ උදාහරණ භාවිත සඳහා වෙන් කර ඇත (TEST-NET).

Class D

In class D addresses, the fourth bit of the 32 bits is fixed as 0 while all the first three bits are 1.

D පන්තියේ ලිපින වලදී, බිටු 32 න් පළමු බිටු තුනම 1 ලෙස පවතින අතරේදී හතරවන බිටුව 0 ලෙස නියත කෙරේ.

When the first three bits are fixed as 111, it includes half of the 1 billion addresses which is approximately 500 million.

පළමු බිට් එක 1 ලෙස සවි කළ විට, එයට ආසන්න වශයෙන් මිලියන 500 වන බිලියන 1ක ලිපිනවලින් අඩක් ඇතුළත් වේ.

Since there is only one class left, which is class E, these two classes can equally share these 500 million addresses.

ඉතිරිව ඇත්තේ E පන්තිය වන එක් පන්තියක් පමණක් බැවින්, මෙම පන්ති දෙකට මෙම මිලියන 500 ලිපින සමානව බෙදා ගත හැකිය.

Therefore, the fourth bit is fixed as 0 such that those 500 million addresses can be divided into two equal parts.

එමනිසා, එම ලිපින මිලියන 500 සමාන කොටස් දෙකකට බෙදිය හැකි වන පරිදි හතරවන බිටුව 0 ලෙස නියත කරනු ලැබේ.

Class D owns one of those two parts which contains approximately 250 million IP addresses.

IP ලිපින මිලියන 250ක් පමණ අඩංගු එම කොටස් දෙකෙන් එකක් D පන්තිය සතුය.

1 1 1 0 0000 00000000 00000000 00000000 (224.0.0.0)

⋮

1 1 1 0 1111 11111111 11111111 11111111 (239.255.255.255)

Class D addresses are needed for multicast communication. They allow one sender to send data to a group of selected devices at the same time, instead of sending separate copies to each device.

බහුප්‍රේක්ෂණ සන්නිවේදනය සඳහා Class D ලිපින අවශ්‍ය වේ. එමඟින් එක් එක් උපාංගය වෙත වෙන වෙනම පිටපත් යැවීම වෙනුවට, එකම අවස්ථාවකදී තෝරාගත් උපාංග සමූහයකට දත්ත යැවීමට එක් සම්ප්‍රේෂකයෙකුට ඉඩ සලසයි.

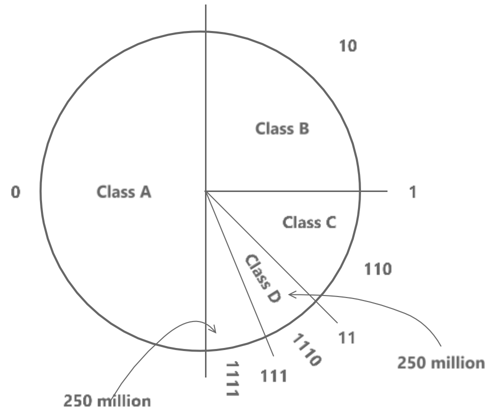
Class E

In class E addresses, the fourth bit of the 32 bits is fixed as 1 while all the first three bits are also 1.

E පන්තියේ ලිපින වලදී, බිටු 32 න් පළමු බිටු තුන ද 1 ලෙස පවතින අතරේදී හතරවන බිටුව ද 1 ලෙස නියත කෙරේ.

When the fourth bit is fixed as 1, class E includes the rest 250 million addresses

හතරවන බිටුව 1 ලෙස සවි කළ විට, E පන්තියට ඉතිරි මිලියන 250 ලිපින ඇතුළත් වේ



1 1 1 1 0000 00000000 00000000 00000000 (240.0.0.0)

⋮

1 1 1 1 1111 11111111 11111111 11111111 (255.255.255.255)

Class E addresses are reserved for experimental and research purposes. They are not used for normal device addressing in networks.

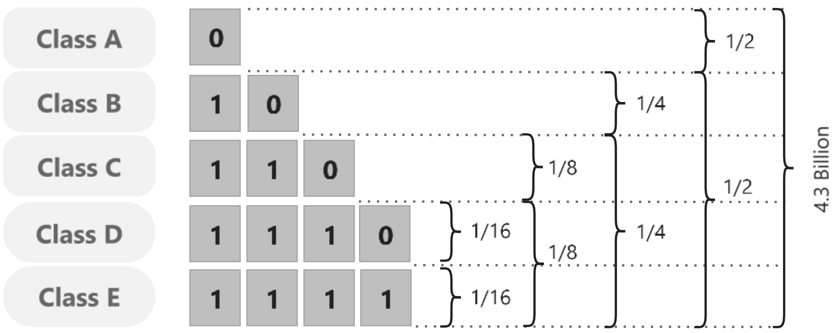
Class E ලිපින පර්යේෂණ සහ පරීක්ෂණාත්මක අරමුණු සඳහා වෙන් කර ඇත. ඒවා ජාල තුළ සාමාන්‍ය උපාංග ලිපිනකරණය සඳහා භාවිතා නොකෙරේ.

Summary – Network Part & Host Part of each class

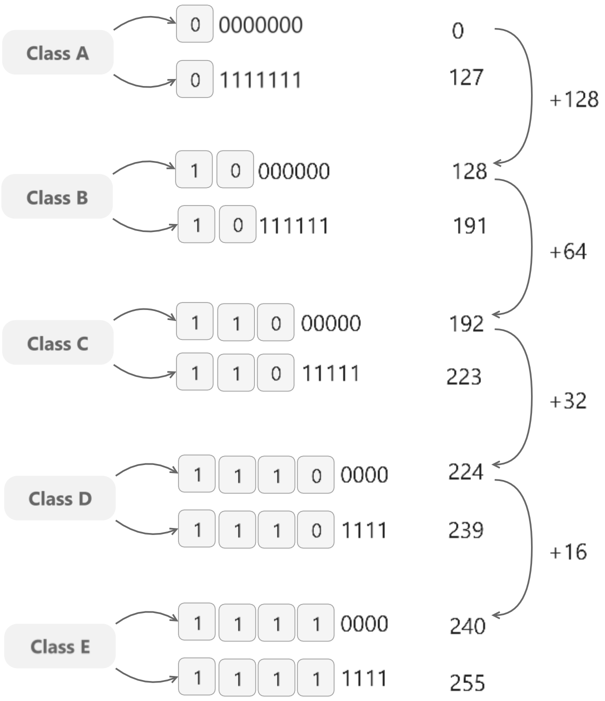
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host

Note:
Unlike Classes A, B, and C, Class D and Class E addresses are not allocated using network and host divisions.
A, B සහ C පන්ති මෙන් නොව, D සහ E පන්ති ලිපින, ජාල සහ ධාරක කොටස් භාවිතයෙන් වෙන් නොකෙරේ.

How 4.3 billion addresses are distributed among 5 classes
පන්තීන් 5 අතර IP ලිපින බිලියන 4.3 ක් බෙදී යන ආකාරය



Class of an IP address by looking at the first octet
පළමු අෂ්ටකය දෙස බැලීමෙන් IP ලිපිනයක් අයත් වන පන්තිය හඳුනා ගැනීම



Class A	0	-	127
Class B	128	-	192
Class C	192	-	223
Class D	224	-	239
Class E	240	-	255

Default mask
සම්මත ආවරණය

A default mask consists of binary 1s and 0s where the 1s represent the network portion, and the 0s represent the host portion of the IP address.
උපජාල ආවරණයක් ද්වීමය 1 සහ 0 වලින් සමන්විත වේ. 1 ඒවා ජාල කොටස නියෝජනය කරන අතර 0 ඒවා IP ලිපිනයේ ධාරක කොටස නියෝජනය කරයි.

A default mask is used to identify which network an IP address belongs to in internet routing, helping routers determine the network portion of the address.
අන්තර්ජාල ගමනාගමනයේදී IP ලිපිනයක් අයත් වන්නේ කුමන ජාලයටද යන්න හඳුනා ගැනීමට සම්මත ආවරණයක් භාවිතා කරයි, එය රවුටරවලට ලිපිනයේ ජාල කොටස තීරණය කිරීමට උපකාරී වේ.

Ex.
When a data packet with a random IP address arrives at a router, it performs the Bitwise AND operation between that IP address and its default mask to find the network that it belongs to.
අහඹු IP ලිපිනයක් සහිත දත්ත පැකට්ටුවක් රවුටරයකට පැමිණි විට, එය එම IP ලිපිනය සහ එහි සම්මත ආවරණය අතර බිටු අනුසාරිත AND මෙහෙයුම සිදු කර එය අයත් වන ජාලය සොයා ගනී.

The result of this operation will be the network address of the network that the data packet belongs to.
මෙම මෙහෙයුමේ ප්‍රතිඵලය වනුයේ දත්ත පැකට්ටුව අයත් වන ජාලයේ ජාල ලිපිනයයි.

Using this network address, the data packet is sent to the router which is connected to that destined network.
මෙම ජාල ලිපිනය භාවිතා කරමින් දත්ත පැකට්ටුව එම නියමිත ජාලයට සම්බන්ධ කර ඇති රවුටරය වෙත යවනු ලැබේ.

Default masks of classes
පන්තිවල සම්මත ආවරණ

A → 11111111 00000000 00000000 00000000
255.0.0.0

B → 11111111 11111111 00000000 00000000
255.255.0.0

C → 11111111 11111111 11111111 00000000
255.255.255.0

Example 01

192.168.16.32 ⟶ Class C

Default mask of class C ⟶ 255.255.255.0

```
     11000000 10101000 00010000 00100000 <-- Given IP
AND  11111111 11111111 11111111 00000000 <-- Default Mask
     -----------------------------------
     11000000 10101000 00010000 00000000
```

Network address = 192.168.16.0
Broadcasting address = 192.168.16.255

Usable minimum IP = 192.168.16.1
Usable maximum IP = 192.168.16.254
} 254 devices

Example 02

172.16.4.9 ⟶ Class B

Default mask of class B ⟶ 255.255.0.0

```
     10101100 00010000 00000100 00001001 <-- Given IP
AND  11111111 11111111 00000000 00000000 <-- Default Mask
     -----------------------------------
     10101100 00010000 00000000 00000000
```

Network address = 172.16.0.0
Broadcasting address = 172.16.255.255

Usable minimum IP = 172.16.0.1
Usable maximum IP = 172.16.255.254
} 65,534 devices

Example 03

10.1.5.7 ⟶ Class A

Default mask of class A ⟶ 255.0.0.0

```
     00001010 00000001 00000101 00000111 <-- Given IP
AND  11111111 00000000 00000000 00000000 <-- Default Mask
     -----------------------------------
     00001010 00000000 00000000 00000000
```

Network address = 10.0.0.0
Broadcasting address = 10.255.255.255

Usable minimum IP = 10.0.0.1
Usable maximum IP = 10.255.255.254
} 16,777,214 devices

ictfromabc.com

Classless IP addressing
පන්ති රහිත IP ලිපිනකරණය

Classless IP addressing, also known as Classless Inter-Domain Routing (CIDR) allows more flexible allocation of IP addresses compared to classful addressing.
Classless Inter-Domain Routing ලෙසද හැඳින්වෙන පන්ති රහිත IP ලිපින විසින් පන්ති සහිත ලිපිනවලට සාපේක්ෂව IP ලිපින වඩාත් නම්‍යශීලී ලෙස බෙදා හැරීමට ඉඩ සලසයි.

The problem with classful IP addressing
පන්ති සහිත IP ලිපිනයන්හි පවතින ගැටලුව

Before CIDR, IP addresses were divided into fixed classes (A, B, C) with fixed-size default masks (/8, /16, /24). This was rigid.
CIDR හඳුන්වා දීමට පෙර, IP ලිපිනයන් ස්ථාවර පෙරනිමි ආවරණ (/8, /16, /24) සහිත ස්ථාවර පන්තිවලට (A, B, C) බෙදා තිබුණි. මෙය ඉතා දැඩි (නම්‍යශීලී නොවන) ක්‍රමවේදයක් විය.

A Class A network gave 16 million+ host addresses, a Class C gave only 254, nothing in between.
A පන්තියේ ජාලයකින් ධාරක ලිපින මිලියන 16 කට වඩා ලබා දුන් අතර, C පන්තියකින් ලබා දුන්නේ ලිපින 254 ක් පමණි, ඒ අතරමැද කිසිවක් තිබුණේ නැත.

An organization needing, say, 1,000 addresses had to take a whole Class B (65,000+ addresses) and waste the rest, or use multiple Class Cs and waste routing table space.
උදාහරණයක් ලෙස, ලිපින 1,000 ක් අවශ්‍ය වූ සංවිධානයකට සම්පූර්ණ B පන්තියක්ම (Class B - ලිපින 65,000+) ලබාගෙන ඉතිරිය අපතේ හැරීමට සිදු විය, නැතහොත් C පන්ති කිහිපයක් භාවිත කර රවුටින් වගුවේ ඉඩ අපතේ හැරීමට සිදු විය.

This led to massive IP address wastage and rapid depletion of the available IPv4 address space, since address blocks couldn't be sized to actual need.
ලිපින කොටස් සැබෑ අවශ්‍යතාවයට අනුව ප්‍රමාණගත කිරීමට නොහැකි වූ බැවින්, මෙයින් විශාල වශයෙන් IP ලිපින අපතේ යාමක් සහ පවතින IPv4 ලිපින අවකාශය සීඝ්‍රයෙන් ක්ෂය වී යාමක් සිදු විය.

Why Classless IP addressing is used
පන්ති රහිත IP ලිපිනකරණය භාවිතා කිරීමට හේතු

Slow down the exhaustion of IPv4 address space by allocating only as many addresses as a network actually needs.
ජාලයකට සැබවින්ම අවශ්‍ය වන ලිපින ප්‍රමාණය පමණක් වෙන්කර දීම මගින් IPv4 ලිපින අවකාශය ක්ෂය වී යාම ප්‍රමාද කිරීම.

Reduce the size of global routing tables through route summarization/aggregation. Multiple smaller networks can be advertised as a single combined route (e.g., several /24s summarized into one /21), instead of the internet's routers needing to track each one separately.
මාර්ග සාරාංශකරණය/එකතු කිරීම මගින් ගෝලීය රවුටින් වගු වල ප්‍රමාණය අඩු කිරීම. අන්තර්ජාලයේ රවුටර වලට එක් එක් ජාලය වෙන වෙනම නිරීක්ෂණය කිරීමට අවශ්‍ය වීම වෙනුවට, කුඩා ජාල කිහිපයක් එකම ඒකාබද්ධ මාර්ගයක් ලෙස ප්‍රචාරය කළ හැක (උදාහරණයක් ලෙස, /24 ජාල කිහිපයක් එකම /21 ජාලයක් ලෙස සාරාංශ කිරීම).

Give ISPs and organizations flexibility to allocate address blocks that match real-world demand rather than forcing a class-based fit.
පන්ති මත පදනම් වූ ගැළපීමකට බල කිරීම වෙනුවට, සැබෑ ලෝකයේ ඉල්ලුමට ගැලපෙන පරිදි ලිපින කොටස් වෙන්කර දීමට අන්තර්ජාල සේවා සපයන්නන්ට (ISPs) සහ සංවිධානවලට නම්‍යශීලීභාවයක් ලබා දීම.

No fixed classes
ස්ථාවර පන්ති නොමැත
IP addresses are assigned based on network size.
ජාල ප්‍රමාණය මත පදනම්ව IP ලිපින පවරනු ලැබේ.

Flexible network masks
නම්‍යශීලී ජාල ආවරණ
Network administrators can use default masks of any length (Ex. /12, /20, /27) to suit the specific needs of the network.
ජාල පරිපාලකයින්ට ජාලයේ නිශ්චිත අවශ්‍යතාවලට සරිලන පරිදි ඕනෑම දිගකින් (උදා. /12,) /20, /27) සම්මත ආවරණ භාවිතා කළ හැක.

Efficient IP allocation
කාර්යක්ෂම IP වෙන්කිරීම්
Networks can be tailored to fit the exact number of hosts, reducing IP address wastage.
IP ලිපින නාස්තිය අවම කරමින්, නිවැරදි ධාරක සංඛ්‍යාවට ගැලපෙන පරිදි ජාල සකස් කළ හැක.

CIDR notation
(Classless Inter-Domain Routing)

CIDR notation is a compact way to represent an IP address along with its associated network prefix or default mask.
CIDR අංකනය යනු ජාල උපසර්ගය හෝ සම්මත ආවරණය සමඟ IP ලිපිනයක් නියෝජනය කිරීමට භාවිතා කරන සංයුක්ත ක්‍රමයකි.

It consists of the IP address followed by a slash (/) and a number that represents the number of bits used for the block part of the address.
එය IP ලිපිනයෙන් පසුව slash (/) එකක් සහ ලිපිනයේ කාණ්ඩ කොටස සඳහා භාවිතා කරන බිටු ගණන නියෝජනය කරන අංකයකින් සමන්විත වේ.

IP block
IP කාණ්ඩය

IP block refers to the network part and cannot be changed.
කාණ්ඩය යනු ජාල කොටස ලෙස හැඳින්විය හැකි අතර එය වෙනස් කළ නොහැක.

The number after the slash (Ex. /26) indicates how many bits are reserved for the block.
ස්ලෑෂ් (උදා. /26) එකට පසු අංකය කාණ්ඩය සඳහා කොපමණ බිටු ප්‍රමාණයක් වෙන් කර තිබේද යන්න දක්වයි.

The remaining bits represent the host part.
ඉතිරි බිටු ධාරක කොටස නියෝජනය කරයි.

Network Mask
ජාල ආවරණය

A network mask identifies which part of an IP address represents the network and which part represents the host.
ජාල ආවරණයක් මඟින් IP ලිපිනයක කුමන කොටසකින් ජාලය නිරූපණය කරන්නේද සහ කුමන කොටසකින් ධාරක නිරූපණය කරන්නේද යන්න හඳුනා ගනී.

In CIDR, the network mask is written using a slash (/) followed by the number of network bits.
CIDR ක්‍රමවේදයේදී, ජාල ආවරණය ලියනු ලබන්නේ ඇල ඉරක් (/) සහ ඉන් පසුව ජාල බිටු ගණන සඳහන් කිරීමෙනි.

Example 01

192.168.10.45/27

Network mask ⟶ 255.255.255.224

```
     11000000 10101000 00001010 00101101 <-- Given IP
AND  11111111 11111111 11111111 11100000 <-- Network Mask
     -----------------------------------
     11000000 10101000 00001010 00100000
```

Network address = 192.168.10.32
Broadcasting address = 192.168.10.63

Usable minimum IP = 192.168.10.33
Usable maximum IP = 192.168.10.62
} 30 devices

Example 02

172.20.150.200/20

Network mask ⟶ 255.255.255.224

```
     10101100 00010100 10010110 11001000 <-- Given IP
AND  11111111 11111111 11110000 00000000 <-- Network Mask
     -----------------------------------
     10101100 00010100 10010000 00000000
```

Network address = 172.20.144.0
Broadcasting address = 172.20.159.255

Usable minimum IP = 172.20.144.1
Usable maximum IP = 172.20.159.254
} 4094 devices

Example 03

10.100.200.150/13

Network mask ⟶ 255.248.0.0

```
     00001010 01100100 11001000 10010110 <-- Given IP
AND  11111111 11111000 00000000 00000000 <-- Network Mask
     -----------------------------------
     00001010 01100000 00000000 00000000
```

Network address = 10.96.0.0
Broadcasting address = 10.103.255.255

Usable minimum IP = 10.96.0.1
Usable minimum IP = 10.103.255.254
} 524,286 devices

ictfromabc.com

Subnetting
උපජාලකරණය

Subnetting is the process of dividing a larger network into smaller, more manageable subnetworks.
උපජාලකරණය යනු විශාල ජාලයක් කුඩා, වඩා කළමනාකරණය කළ හැකි උපජාල වලට බෙදීමේ ක්‍රියාවලියයි.

Why subnetting is used
උපජාලකරණය භාවිතය

Efficient IP address utilization
කාර්යක්ෂම IP ලිපින භාවිතය
Avoids wasting large blocks of addresses on small networks.
කුඩා ජාල සඳහා විශාල ලිපින කුට්ටි අපතේ යාම වළක්වයි.

Simplifies network management
ජාල කළමනාකරණය සරල කරයි
Departments/locations can be assigned their own subnet.
දෙපාර්තමේන්තු/ස්ථාන සඳහා ඒවාටම ආවේණික වූ උපජාල පැවරිය හැක.

Reduces broadcast traffic
ප්‍රචාරණ සංඥා ගමනාගමනය අඩු කරයි
Smaller broadcast domains mean less network congestion.
කුඩා ප්‍රචාරණ වසම් මගින් ජාල තදබදය අඩු වේ.

Improves network performance
ජාල ක්‍රියාකාරීත්වය වැඩි දියුණු කරයි
Isolates traffic within logical segments.
තර්කානුකූල කොටස් තුළ දත්ත ගමනාගමනය වෙන් කරයි.

Enhances security
ආරක්ෂාව ඉහළ නංවයි
Traffic between subnets can be controlled via routers/ACLs/firewalls.
උපජාල අතර ගමනාගමනය රවුටර/ACL/ගිනිපවුරු හරහා පාලනය කළ හැක.

Supports hierarchical addressing
ධුරාවලිගත ලිපිනකරණය සඳහා සහය දක්වයි
Enables structured, scalable network design (used heavily in routing summarization).
ව්‍යුහගත, පරිමාණය කළ හැකි ජාල සැලසුම්කරණයකට ඉඩ සලසයි (මාර්ග සාරාංශකරණයේදී බහුලව භාවිතා වේ).

Advantages / වාසි

- Reduces broadcast domain size
  ප්‍රචාරණ වසම් ප්‍රමාණය අඩු කිරීම
- Better security via segmentation
  ඛණ්ඩනය මගින් වඩා හොඳ ආරක්ෂාවක් සැලසීම
- Efficient IP address use
  කාර්යක්ෂම IP ලිපින භාවිතය
- Easier fault isolation/troubleshooting
  දෝෂ වෙන්කර හඳුනා ගැනීම/දෝෂ නිරාකරණය පහසු වීම
- Enables route summarization
  මාර්ග සාරාංශකරණයට ඉඩ සැලසීම
- Supports org/departmental separation
  ආයතනික/දෙපාර්තමේන්තුමය වෙන්කිරීම් සඳහා සහය වීම

Disadvantages / අවාසි

- Adds design/config complexity
  සැලසුම් කිරීමේ සංකීර්ණත්වය වැඩි වීම
- Needs careful planning (waste risk)
  ප්‍රවේශම් සහගත සැලසුම්කරණයක් අවශ්‍ය වීම (අපතේ යාමේ අවදානම)
- More admin overhead
  වැඩි පරිපාලන පිරිවැයක් පැවතීම
  (routes, DHCP, ACLs)
- Misconfiguration risk
  වැරදි වින්‍යාසගත වීමේ අවදානම
  (bad masks = outages)
  (වැරදි ආවරණ = බිඳවැටීම්)
- More routing overhead
  වැඩි රවුටින් පිරිවැයක් පැවතීම
- Cross-subnet troubleshooting harder
  උපජාල අතර දෝෂ නිරාකරණය වඩාත් අපහසු වීම

Subnet mask
උපජාල ආවරණය

A subnet mask is used to identify which subnetwork an IP address belongs to among multiple subnets within the same network.
එකම ජාලය තුළ ඇති උපජාල අතරින් IP ලිපිනයක් අයත් වන්නේ කුමන උපජාලයටදැයි හඳුනා ගැනීමට උපජාල ආවරණයක් භාවිතා කරයි.

Subnet mask also consists with binary 1s and 0s where the 1s represent all the network and subnet bits (host bits used to create subnets) and 0s represent the host bits.
උපජාල අවරණයද ද්විමය 1 සහ 0 වලින් සමන්විත වන අතර එහිදී 1 ඒවා මගින් සියලුම ජාල සහ උපජාල බිටු (උපජාල නිර්මාණය කිරීමට භාවිතා කරන ධාරක බිටු) සහ 0 ඒවා මගින් ධාරක බිටු නියෝජනය කරයි.

When that previous data packet with the random IP address arrives at the network it belongs to, the router performs bitwise AND operation between the IP address and the corresponding subnet mask to identify the exact subnetwork within the network that this data packet should be routed to.
අහඹු IP ලිපිනය සහිත පෙර දත්ත පැකට්ටුවම එය අයත් ජාලයට පැමිණි විට, එය මාර්ගගත කළ යුතු ජාලය තුළ ඇති නිශ්චිත උපජාලය හඳුනා ගැනීම සඳහා රවුටරය IP ලිපිනය සහ එම ලිපිනයට අදාල උපජාල ආවරණය අතර බිටු අනුසාරිත AND මෙහෙයුමක් සිදු කරයි.

The result will be network address of the subnet to which the data packet belongs.
එහි ප්‍රතිඵලය වනුයේ දත්ත පැකට්ටුව අයත් වන උපජාලයේ ජාල ලිපිනයයි.

How a subnet mask is made
උපජාල ආවරණයක් සෑදෙන ආකාරය

A subnet mask is built by dividing the 32 bits of an IPv4 address into three parts, network bits, subnet bits and host bits.
IPv4 ලිපිනවල ඇති බිටු 32 ප්‍රමාණය ජාල බිටු, උපජාල බිටු සහ ධාරක බිටු ලෙස කොටස් තුනකට බෙදීමෙන් උපජාල ආවරණයක් ගොඩනගනු ලැබේ.

Network bits → always set to 1
ජාල බිටු → සැමවිටම 1 ලෙස සකසයි
These come from the original class-based mask, like the first 24 bits in a /24.
මේවා /24 ක මුල් බිටු 24 මෙන්, මුල් පංති සහිත ආවරණයෙන් ලබා ගැනේ.

Subnet bits → also set to 1
උපජාල බිටු → මේවාද 1 ලෙස සකසයි
These are borrowed from the host portion to create additional subnets.
අතිරේක උපජාල සෑදීම සඳහා මේවා ධාරක කොටසෙන් ඉල්ලා ගනු ලැබේ.

Host bits → set to 0
ධාරක බිටු → 0 ලෙස සකසයි
Whatever bits are left over, used to number individual devices.
ඉතිරි වන ඕනෑම බිටු ප්‍රමාණයක්, තනි උපාංග අංකනය කිරීම සඳහා භාවිතා කරයි.

Example / උදාහරණය

Take 255.255.255.0/24 and borrow 2 bits to make subnets.
255.255.255.0/24 ගෙන උපජාල සෑදීම සඳහා බිටු 2ක් ලබා ගන්න.

11111111.11111111.11111111.11000000

The first 24 bits are network bits (always 1)
පළමු බිටු 24 ජාල බිටු වේ (සැමවිටම 1)

The next 2 bits are subnet bits (turned into 1 to create subnets)
ඊළඟ බිටු 2 උපජාල බිටු වේ (උපජාල සෑදීම සඳහා 1 බවට පත් කර ඇත)

The last 6 bits are host bits (left as 0 to number devices)
අවසාන බිටු 6 ධාරක බිටු වේ (උපාංග අංකනය කිරීම සඳහා 0 ලෙස ඉතිරි කර ඇත)

Converting the last octet gives 192, so the mask is 255.255.255.192
අවසාන අෂ්ටකය පරිවර්තනය කිරීමෙන් 192 ලැබෙන බැවින්, ආවරණය 255.255.255.192 වේ.

Classful and Classless addressing
පන්ති සහිත සහ පන්ති රහිත ලිපිණකරනය

Subnetting can be divided into two main types: Subnetting in classful and classless addressing.
උපජාල ප්‍රධාන වර්ග දෙකකට බෙදිය හැකිය: පන්ති සහිත සහ පන්ති රහිත ලිපිනවල උපජාලකරණය.

Classful addressing follows predefined IP address classes (A, B, C, etc.) with fixed boundaries for the network and host portions based on the class.
පන්ති සහිත ලිපිනකරණය පන්තිය මත පදනම් වූ ස්ථාවර මායිම් සමඟ ජාල සහ ධාරක කොටස් සඳහා පූර්ව නිශ්චිත IP ලිපින පන්ති (A, B, C,) ආදිය) අනුගමනය කරයි.

Classless addressing (CIDR) ignores traditional class boundaries and allows flexible division of the network (called block) and host portions using CIDR (Classless Inter Domain Routing) notation.
පන්ති රහිත (CIDR) ලිපිනකරණය සම්ප්‍රදායික පන්ති සීමාවන් නොසලකා හරින අතර CIDR (පන්ති රහිත අන්තර් වසම් මාර්ගගත කිරීම) අංකනය භාවිතයෙන් ජාලය සහ ධාරක කොටස් නම්‍යශීලී ලෙස බෙදීමට ඉඩ සලසයි.

Note:
When creating subnets, the network part must remain fixed, its bits cannot be changed.
උපජාල නිර්මාණය කිරීමේදී, ජාල කොටස ස්ථාවරව පැවතිය යුතුය, එහි බිටු වෙනස් කළ නොහැක.

The bits of the host portion is used to define the subnets.
උපජාල අර්ථ දැක්වීමට ධාරක කොටසෙහි බිටු භාවිතා වේ.

Fixed length vs Variable length subnets
ස්ථාවර දිග සහ විචල්‍ය දිග උපජාල

1. Classful FLSM
(Fixed-Length Subnet Mask)
All subnets have the same size and the same subnet mask, resulting in equal-sized subnets.
සියලුම උපජාල වලට එකම ප්‍රමාණයක් සහ එකම උපජාල ආවරණ ඇත, එහි ප්‍රතිඵලයක් ලෙස සමාන ප්‍රමාණයේ උපජාල ලැබේ.

2. Classless FLSM
Subnets don't adhere to class boundaries but still use a uniform subnet mask across all subnets.
උපජාල පන්ති සීමාවන්ට අනුගත නොවන නමුත් තවමත් සියලුම උපජාල හරහා ඒකාකාර උපජාල ආවරණයක් භාවිතා කරයි.

3. Classless VLSM
Subnets without class boundaries can have different sizes, using variable-length subnet masks for more efficient IP address allocation.
පන්ති මායිම් නොමැති උපජාලවලට විවිධ ප්‍රමාණ ඇත, IP ලිපින වඩාත් කාර්යක්ෂමව වෙන් කිරීමට විචල්‍ය-දිග උපජාල ආවරණ භාවිතා කරයි.

Note:
Classful VLSM doesn't exist because classful protocols use one fixed mask per network and can't carry varying subnet mask info between routers.
පංති සහිත නියමාවලි මගින් එක් ජාලයක් සඳහා එක් ස්ථාවර ආවරණයක් පමණක් භාවිතා කරන බැවින් සහ රවුටර අතර විවිධ උපජාල ආවරණ තොරතුරු රැගෙන යාමට නොහැකි බැවින් පංති සහිත VLSM නොපවතී.

Subnetting in classful IP addressing
පන්ති සහිත IP ලිපිනකරණයේ උපජාලකරණය

1. Fixed-Length Subnet mask (FLSM)

In FLSM, all subnets within a network use the same subnet mask.
FLSM හිදී, ජාලයක් තුළ ඇති සියලුම උපජාල එකම උපජාල ආවරණයක් භාවිතා කරයි.

This results in subnets of equal size, meaning each subnet can accommodate the same number of hosts.
මෙහි ප්‍රතිඵලයක් ලෙස සමාන ප්‍රමාණයේ උපජාල ලැබේ, එයින් අදහස් වන්නේ සෑම උපජාලයකටම එකම ධාරක සංඛ්‍යාවකට ඉඩ සැලසිය හැකි බවයි.

Advantages / වාසි

Simple to Understand and Implement
තේරුම් ගැනීමට සහ ක්‍රියාත්මක කිරීමට සරල වීම
Since every subnet uses the same mask, calculations are straightforward, good for beginners and quick manual configuration.
සෑම උපජාලයක්ම එකම ආවරණයක් භාවිතා කරන බැවින්, ගණනය කිරීම් සරල වේ, මෙය ආරම්භකයින්ට සහ ඉක්මන් අතින් වින්‍යාස කිරීමට සුදුසු වේ.

Easy to Manage / කළමනාකරණය කිරීමට පහසු වීම
Uniform subnet sizes make network documentation, troubleshooting, and administration simpler.
ඒකාකාරී උපජාල ප්‍රමාණයන් ජාල ලේඛනගත කිරීම, දෝශ නිරාකරණය සහ පරිපාලනය වඩාත් සරල කරයි.

Faster Design Process / වේගවත් සැලසුම් ක්‍රියාවලිය
No need to calculate different subnet sizes for different departments/segments, one formula fits all.
විවිධ දෙපාර්තමේන්තු හෝ කොටස් සඳහා විවිධ උපජාල ප්‍රමාණයන් ගණනය කිරීමට අවශ්‍ය නොවේ, එක් සූත්‍රයක් සැමට ගැලපේ.

Disadvantages / අවාසි

Wastage of IP Addresses / IP ලිපින අපතේ යාම
If one subnet needs only 10 hosts but the fixed subnet size allows 62 or 254, the remaining addresses go unused.
එක් උපජාලයකට අවශ්‍ය වන්නේ සත්කාරකයන් 10 ක් පමණක් වුවද ස්ථාවර උපජාල ප්‍රමාණය මඟින් 62 ක් හෝ 254 ක් සඳහා ඉඩ ලබා දෙන්නේ නම්, ඉතිරි ලිපින භාවිතයට නොගෙන ඉතිරි වේ.

Inefficient for Networks with Varying Host Requirements
විවිධ සත්කාරක අවශ්‍යතා සහිත ජාල සඳහා අකාර්යක්ෂම වීම
Real-world networks rarely have equal-sized segments (e.g., a WAN link needing 2 IPs vs. a LAN needing 100), but FLSM forces one-size-fits-all subnetting.
සැබෑ ලෝකයේ ජාල වල කලාතුරකින් සමාන ප්‍රමාණයේ කොටස් පවතී (උදාහරණයක් ලෙස, WAN සබැඳියකට IP ලිපින 2 ක් අවශ්‍ය වන අතර LAN එකකට 100 ක් අවශ්‍ය වේ), එහෙත් FLSM මඟින් සැමට එකම ප්‍රමාණයේ උපජාලකරණයක් බල කරයි.

Classful IP Addressing
පන්ති සහිත උපජාලකරණය

Question 01 – Fixed Length Subnet Masking (FLSM)

Suppose you are given the IP address 192.168.20.0 and need to divide the network into 2 subnets, labeled Subnet A and Subnet B, with an equal number of hosts.
ඔබට 192.168.20.0 යන IP ලිපිනය ලබා දී ඇති අතර, මෙම ජාලය සමාන සත්කාරක පරිගණක සංඛ්‍යාවක් සහිත උපජාල 2 කට, එනම් උපජාල A සහ උපජාල B ලෙස බෙදිය යුතු යැයි උපකල්පනය කරන්න.

Since the given IP address belongs to Class C, the first three octets are used for the network part, and the last octet is used for the host part.
ලබා දී ඇති IP ලිපිනය Class C ගණයට අයත් වන බැවින්, එහි මුල් අෂ්ටක තුන ජාල කොටස සඳහා ද, අවසාන අෂ්ටකය සත්කාරක කොටස සඳහා ද භාවිතා වේ.

So, in 192.168.20.0:
Network part = 192.168.20
Host part = last octet

Let us calculate the number of subnet bits required.
අවශ්‍ය උපජාල බිටු ගණන ගණනය කරමු:

$2^{\text{Subnet bits}}$= Number of subnets
$2^{\text{උපජාල බිටු}}$ = උපජාල ගණන
$2^{\text{Subnet bits}}$ =2
$2^{\text{Subnet bits}}$ =2^1

Subnet bits = 1
To create 2 subnets, we borrow 1 bit from the host part.
උපජාල 2 ක් නිර්මාණය කිරීම සඳහා, අප විසින් සත්කාරක කොටසෙන් බිටු 1 ක් ණයට ගනු ලබයි.

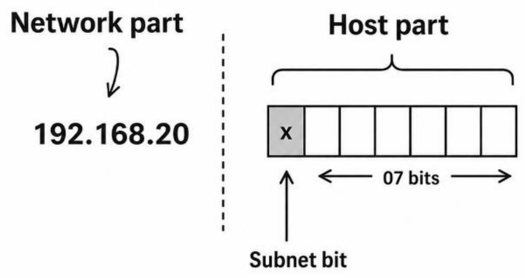
When we take 1 bit from the host part, only 7 bits remain for host addresses.
සත්කාරක කොටසෙන් බිටු 1 ක් ලබා ගත් විට, සත්කාරක ලිපින සඳහා ඉතිරි වන්නේ බිටු 7 ක් පමණි.

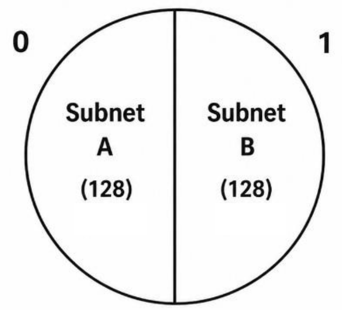
2^7=128

So, each subnet contains 128 IP addresses.
However, in each subnet:
එබැවින්, එක් එක් උපජාලය තුළ IP ලිපින 128 බැගින් අඩංගු වේ.කෙසේ වෙතත්, සෑම උපජාලයකම:

1 address is used as the network address
ලිපින 1 ක් ජාල ලිපිනය ලෙස භාවිතා වේ.
1 address is used as the broadcast address
ලිපින 1 ක් විකාශන ලිපිනය ලෙස භාවිතා වේ.

128−2=126





Subnet A
Network address = 192.168.20.0
Broadcast address = 192.168.20.127
Usable IP range = 192.168.20.1 -192.168.20.126

Subnet B
Network address = 192.168.20.128
Broadcast address = 192.168.20.255
Usable IP range =192.168.20.129 -192.168.20.254

Maximum IP addresses of each subnet
එක් එක් උපජාලයේ උපරිම IP ලිපින

=2^7=128
Maximum usable hosts
භාවිතා කළ හැකි උපරිම සත්කාරක ගණන

= 2^7−2=126

Subnet Mask / උපජාල ආවරණය
= 255.255.255.128

Question 02 – Fixed Length Subnet Mask (FLSM)

Suppose you are given the IP address 192.168.10.0 and need to divide the network into four subnets, labeled A, B, C, and D, with an equal number of hosts.
ඔබට 192.168.10.0 යන IP ලිපිනය ලබා දී ඇති බවත් එම ජාලය A, B, C සහ D ලෙසින් සමාන ධාරක සංඛ්‍යාවක් සහිත උපජාල හතරකට බෙදිය යුතු බවත් සිතන්න.

Since the given IP address belongs to Class C, the first three octets are used for the network part and the last octet is used for the host part.
දී ඇති IP ලිපිනය C පන්තියට අයත් වන බැවින්, පළමු අෂ්ටක තුන සහ අවසාන අෂ්ටකය පිළිවෙලින් ජාල කොටස සහ ධාරක කොටස සඳහා භාවිත වේ.

Let us calculate the number of subnet bits required.
අවශ්‍ය උපජාල බිටු ගණන ගණනය කරමු:

$2^{\text{Subnet bits}}$ = Number of subnets
$2^{\text{උපජාල බිටු}}$ = උපජාල ගණන

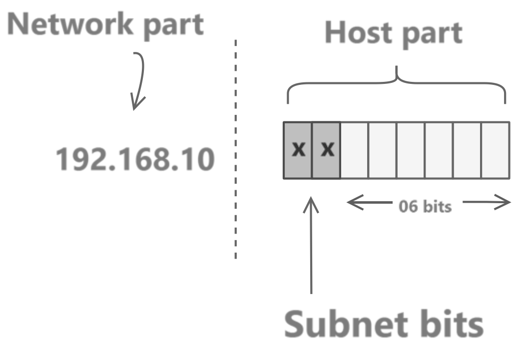
$2^{\text{Subnet bits / උපජාල බිටු}} = 4$
$2^{\text{Subnet bits / උපජාල බිටු}} = 2^2$

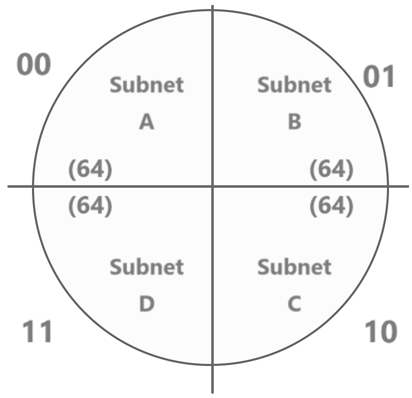
Subnet bits / උපජාල බිටු = 2

To achieve this, we can use the first two bits of the host part as the subnet bits and assign the values 00, 01, 10, and 11, thereby dividing the network into four equal subnets.
එය සිදු කිරීම සඳහා, අපට ධාරක කොටසෙහි පළමු බිටු දෙක උපජාල බිටු ලෙස ගෙන ඒවා 00, 01, 10 සහ 11 ලෙස නියත කර මෙම ජාලය සමාන සමාන උපජාල හතරකට බෙදිය හැකිය.

When we take 2 bits from the host part, only 6 bits remain for the host addresses.
අප විසින් ධාරක කොටසෙන් බිටු 2 ක් ලබා ගන්නා විට ධාරක ලිපින සඳහා බිටු 6 ක් ඉතිරි වේ.

Maximum IP addresses per subnet
උපජාලයකට තිබිය හැකි උපරිම IP ලිපින ගණන





Subnet A
Network address = 192.168.10.0
Broadcast address = 192.168.10.63
Usable IP range =192.168.10.1 - 192.168.10.62

Subnet B
Network address = 192.168.10.64
Broadcast address = 192.168.10.127
Usable IP range =192.168.10.65 – 192.168.10.126

Subnet C
Network address = 192.168.10.128
Broadcast address = 192.168.10.191
Usable IP range
=192.168.10.129 – 192.168.10.190

Subnet D
Network address = 192.168.10.192
Broadcast address = 192.168.10.255
Usable IP range
=192.168.10.193 – 192.168.10.254

Max IP addresses of each subnet
එක් එක් උපජාලයේ උපරිම IP ලිපින
= 2^6 = 64

Maximum usable hosts
භාවිතා කළ හැකි උපරිම සත්කාරක ගණන
= 2^6 - 2 = 62

Subnet Mask
උපජාල ආවරණය
= 255.255.255.192

Question 03 – Fixed Length Subnet Masking (FLSM)

Suppose you are given the IP address 172.16.0.0 and need to divide the network into 8 subnets, labeled A, B, C, D, E, F, G, and H, with an equal number of hosts.
ඔබට 172.16.0.0 යන IP ලිපිනය ලබා දී ඇති අතර, මෙම ජාලය සමාන සත්කාරක පරිගණක සංඛ්‍යාවක් සහිත උපජාල 8 කට, එනම් A, B, C, D, E, F, G සහ H ලෙස බෙදිය යුතු යැයි උපකල්පනය කරන්න.

Since the given IP address belongs to Class B, the first two octets are used for the network part, and the last two octets are used for the host part.
ලබා දී ඇති IP ලිපිනය Class B ගණයට අයත් වන බැවින්, එහි මුල් අෂ්ටක දෙක ජාල කොටස සඳහා ද, අවසාන අෂ්ටක දෙක සත්කාරක කොටස සඳහා ද භාවිතා වේ.

So, in 172.16.0.0:
Network part = 172.16
Host part = 0.0

Let us calculate the number of subnet bits required.
අවශ්‍ය උපජාල බිටු ගණන ගණනය කරමු:

$2^{\text{Subnet bits}}$ = Number of subnets
$2^{\text{උපජාල බිටු}}$ = උපජාල ගණන

$2^{\text{Subnet bits / උපජාල බිටු}} = 8$
$2^{\text{Subnet bits / උපජාල බිටු}} = 2^3$

Subnet bits / උපජාල බිටු = 3

To achieve this, we can use the first 3 bits of the host part as the subnet bits and assign the values 000, 001, 010, 011, 100, 101, 110, and 111, thereby dividing the network into 8 equal subnets.
මෙය සාක්ෂාත් කර ගැනීම සඳහා, අපට සත්කාරක කොටසේ මුල් බිටු 3 උපජාල බිටු ලෙස භාවිතා කළ හැකි අතර, ඒවා වෙත 000, 001, 010, 011, 100,101, 110, සහ 111 යන අගයන් ආදේශ කිරීම මඟින් ජාලය සමාන උපජාල 8 කට බෙදිය හැකිය.

When we take 3 bits from the host part, only 13 bits remain for host addresses.
සත්කාරක කොටසෙන් බිටු 3 ක් ලබා ගත් විට, සත්කාරක ලිපින සඳහා ඉතිරි වන්නේ බිටු 13 ක් පමණි.

Maximum IP addresses per subnet
එක් උපජාලයකට ලැබෙන උපරිම IP ලිපින සංඛ්‍යාව:

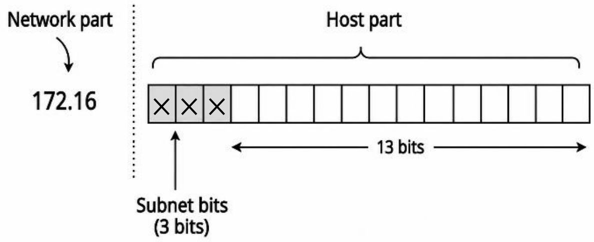
$2^{13}=8192$
So, each subnet contains 8192 IP addresses.
එබැවින්, එක් එක් උපජාලය තුළ IP ලිපින 8192 බැගින් අඩංගු වේ.

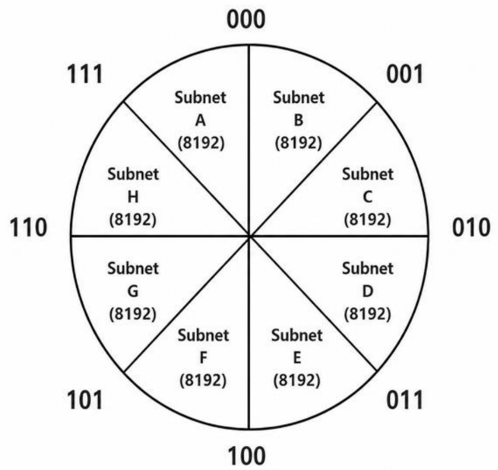
However, in each subnet: / කෙසේ වෙතත්, සෑම උපජාලයකම:

1 address is used as the network address
ලිපින 1 ක් ජාල ලිපිනය ලෙස භාවිතා වේ.
1 address is used as the broadcast address
ලිපින 1 ක් විකාශන ලිපිනය ලෙස භාවිතා වේ.

$8192-2=8190$

Therefore, each subnet can have 8190 usable host addresses.
එබැවින්, එක් එක් උපජාලය තුළ භාවිතා කළ හැකි සත්කාරක ලිපින 8190 ක් පැවතිය හැකිය.





Subnet A
Network address = 172.16.0.0
Broadcast address = 172.16.31.255
Usable IP range = 172.16.0.1 – 172.16.31.254

Subnet B
Network address = 172.16.32.0
Broadcast address = 172.16.63.255
Usable IP range = 172.16.32.1 – 172.16.63.254

Subnet C
Network address = 172.16.64.0
Broadcast address = 172.16.95.255
Usable IP range = 172.16.64.1 – 172.16.95.254

Subnet D
Network address = 172.16.96.0
Broadcast address = 172.16.127.255
Usable IP range = 172.16.96.1 – 172.16.127.254

Subnet E
Network address = 172.16.128.0
Broadcast address = 172.16.159.255
Usable IP range = 172.16.128.1 – 172.16.159.254

Subnet F
Network address = 172.16.160.0
Broadcast address = 172.16.191.255
Usable IP range = 172.16.160.1 – 172.16.191.254

Subnet G
Network address = 172.16.192.0
Broadcast address = 172.16.223.255
Usable IP range = 172.16.192.1 – 172.16.223.254

Subnet H
Network address = 172.16.224.0
Broadcast address = 172.16.255.255
Usable IP range = 172.16.224.1 – 172.16.255.254

Maximum IP addresses of each subnet = 2^{13}=8192
Maximum usable hosts = $2^{13}-2$=8190
Subnet Mask = 255.255.224.0

Question 04 – Fixed Length Subnet Masking (FLSM)

Suppose you are given the IP address 192.168.30.0 and need to divide the network into 3 subnets, labeled Subnet A, Subnet B, and Subnet C, with an equal number of hosts.
ඔබට 192.168.30.0 යන IP ලිපිනය ලබා දී ඇති අතර, මෙම ජාලය සමාන සත්කාරක පරිගණක සංඛ්‍යාවක් සහිත උපජාල 3 කට, එනම් උපජාල A, උපජාල B සහ උපජාල C ලෙස බෙදිය යුතු යැයි උපකල්පනය කරන්න.

Since the given IP address belongs to Class C, the first three octets are used for the network part, and the last octet is used for the host part.
ලබා දී ඇති IP ලිපිනය Class C ගණයට අයත් වන බැවින්, එහි මුල් අෂ්ටක තුන ජාල කොටස සඳහා ද, අවසාන අෂ්ටකය සත්කාරක කොටස සඳහා ද භාවිතා වේ.

So, in 192.168.30.0:
Network part = 192.168.30
Host part = last octet

Let us calculate the number of subnet bits required.
අවශ්‍ය උපජාල බිටු ගණන ගණනය කරමු:

$2^{\text{subnet bits}}$ ≥ The number of subnets
$2^{\text{subnet bits}} \geq 3$
$2^1 = 2$
1 subnet bit is not enough because it gives only 2 subnets. / උපජාල බිටු 1 ක් පමණක් ප්‍රමාණවත් නොවේ, මන්ද එයින් ලබාගත හැක්කේ උපජාල 2 ක් පමණි.

$2^2=4$
Therefore, Subnet bits = 2

Even though we need only 3 subnets, FLSM creates subnets in powers of 2. Therefore, borrowing 2 bits creates 4 equal subnets, and we can use 3 of them.
අපට අවශ්‍ය වන්නේ උපජාල 3ක් පමණක් වුවද, FLSM ක්‍රමවේදයේදී උපජාල නිර්මාණය වන්නේ 2 හි බලයන් ලෙසිනි. එබැවින්, බිටු 2 ක් ණයට ගැනීමෙන් සමාන උපජාල 4 ක් නිර්මාණය වන අතර, අපට ඒවායින් 3 ක් භාවිතා කළ හැකිය.

To achieve this, we can use the first 2 bits of the host part as the subnet bits and assign the values 00, 01, 10, and 11.
මෙය සාක්ෂාත් කර ගැනීම සඳහා, අපට සත්කාරක කොටසේ මුල් බිටු 2 උපජාල බිටු ලෙස භාවිතා කළ

හැකි අතර, ඒවා වෙත 00, 01, 10, සහ 11 යන අගයන් ආදේශ කළ හැකිය.

When we take 2 bits from the host part, only 6 bits remain for host addresses.
සත්කාරක කොටසෙන් බිටු 2 ක් ලබා ගත් විට, සත්කාරක ලිපින සඳහා ඉතිරි වන්නේ බිටු 6 ක් පමණි.

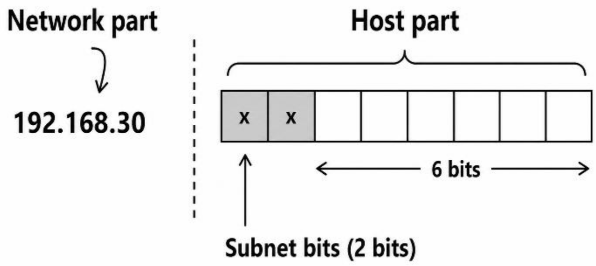
$2^6=64$

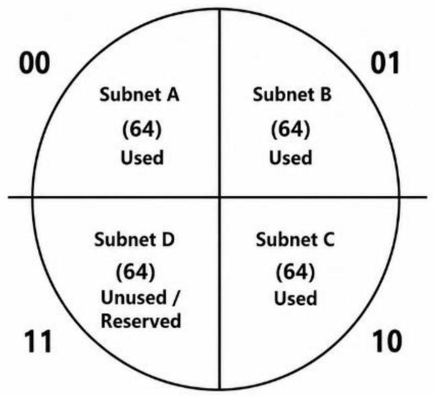
So, each subnet contains 64 IP addresses.
එබැවින්, එක් එක් උපජාලය තුළ IP ලිපින 64 බැගින් අඩංගු වේ.

However, in each subnet: / කෙසේ වෙතත්, සෑම උපජාලයකම:
1 address is used as the network address
ලිපින 1 ක් ජාල ලිපිනය ලෙස භාවිතා වේ.
1 address is used as the broadcast address
ලිපින 1 ක් විකාශන ලිපිනය ලෙස භාවිතා වේ.

64−2=62

Therefore, each subnet can have 62 usable host addresses.
එබැවින්, එක් එක් උපජාලය තුළ භාවිතා කළ හැකි සත්කාරක ලිපින 62 ක් පැවතිය හැකිය.





Subnet A
Network address = 192.168.30.0
Broadcast address = 192.168.30.63
Usable IP range = 192.168.30.1 – 192.168.30.62

Subnet B
Network address = 192.168.30.64
Broadcast address = 192.168.30.127
Usable IP range = 192.168.30.65 – 192.168.30.126

Subnet C
Network address = 192.168.30.128
Broadcast address = 192.168.30.191
Usable IP range = 192.168.30.129–192.168.30.190

Unused / Reserved Subnet
Network address = 192.168.30.192
Broadcast address = 192.168.30.255
Usable IP range = 192.168.30.193-192.168.30.254

This subnet is not used because the question asks only for 3 subnets.
මෙම උපජාලය භාවිතා නොකරනු ලබන්නේ, ප්‍රශ්නය මඟින් උපජාල 3ක් පමණක් විමසා ඇති බැවිනි.

Number of subnet bits borrowed
ණයට ගත් උපජාල බිටු සංඛ්‍යාව
= 2

Number of subnets created
නිර්මාණය වූ උපජාල සංඛ්‍යාව
= $2^2=4$

Number of required subnets
අවශ්‍ය උපජාල සංඛ්‍යාව
= 3

Maximum IP addresses of each subnet
එක් උපජාලයක ඇති උපරිම (IP) ලිපින සංඛ්‍යාව
= $2^6=64$

Maximum usable hosts
භාවිතා කළ හැකි උපරිම සත්කාරක පරිගණක සංඛ්‍යාව
= $2^6-2=62$

Subnet Mask / උපජාල ආවරණය = 255.255.255.192

Question 05 – Fixed Length Subnet Mask (FLSM)

Suppose you are given the IP address 131.10.0.0 and need to divide the network into four subnets, labeled A, B, C, and D, with an equal number of hosts.
ඔබට 131.10.0.0 යන IP ලිපිනය ලබා දී ඇති බවත් එම ජාලය A, B, C සහ D ලෙසින් සමාන ධාරක සංඛ්‍යාවක් සහිත උපජාල හතරකට බෙදිය යුතු බවත් සිතන්න.

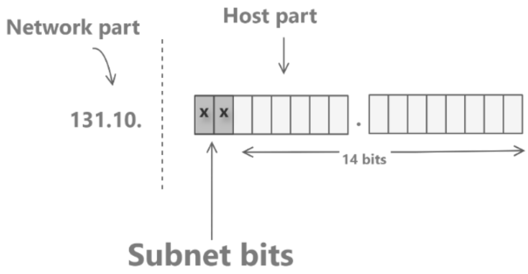
Since the given IP address belongs to class B, the first and the last two octets are used for the network and the host parts respectively.
දී ඇති IP ලිපිනය B පන්තියට අයත් වන බැවින්, පළමු සහ අවසාන අෂ්ටක දෙක පිළිවෙලින් ජාල කොටස සහ ධාරක කොටස සඳහා භාවිතා වේ.

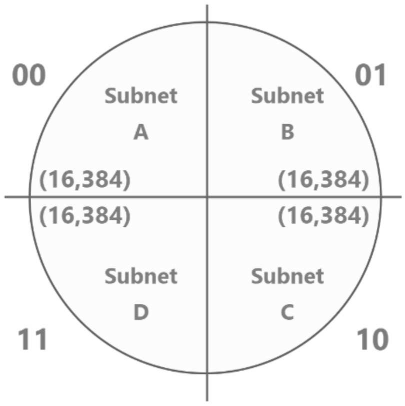
Let's calculate the number of Subnet bits required:
අවශ්‍ය උපජාල බිටු ගණන ගණනය කරමු:

$2^{\text{subnet bits}}$ = The number of subnets
$2^{\text{subnet bits}} = 4$
$2^{\text{subnet bits}} = 2^2$
$2^{\text{subnet bits}} = 2^2$
Subnet bits = 2

To achieve this, we can use the first two bits of the host part as the subnet bits and assign them values of 00, 01, 10, and 11, thereby dividing these addresses into four equal subnets.
එය සිදු කිරීම සඳහා, අපට ධාරක කොටසෙහි පළමු බිටු දෙක උපජාල බිටු ලෙස ගෙන ඒවා 00, 01, 10 සහ 11 ලෙස නියත කර මෙම ලිපින සමාන සමාන හතරකට බෙදිය හැකිය.

When we take two bits, there are only 14 remaining bits for the host part.
අප විසින් බිටු දෙකක් ලබා ගන්නා විට ධාරක කොටස සඳහා බිටු 14 ක් ඉතිරි වේ.





Subnet A
Network address = 131.10.0.0
Broadcast address = 131.10.63.255
Usable IP range = 131.10.0.1 – 131.10.63.254

Subnet B
Network address = 131.10.64.0
Broadcast address = 131.10.127.255
Usable IP range = 131.10.64.1 – 131.10.127.254

Subnet C
Network address = 131.10.128.0
Broadcast address = 131.10.191.255
Usable IP range = 131.10.128.1 – 131.10.191.254

Subnet D
Network address = 131.10.192.0
Broadcast address = 131.10.255.255
Usable IP range= 131.10.192.1 – 131.10.255.254

Max IP addresses of each subnet = 2^{14} = 16,384
Maximum usable hosts = 2^{14} - 2 = 16,382
Subnet mask = 255.255.192.0

ictfromabc.com

Classless IP Addressing

Question 01 – Fixed Length Subnet Mask (FLSM)

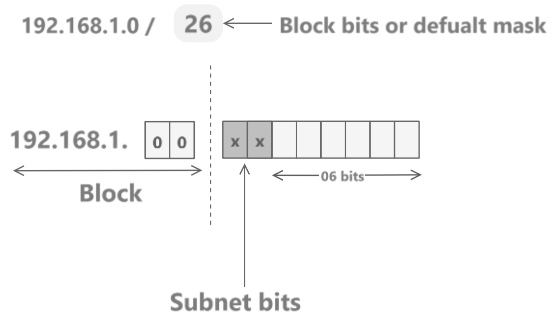
Suppose we are given the IP block 192.168.1.0/26 and asked to create four subnets as A, B, C, and D that contain an equal number of hosts.
අපට 192.168.1.0/(26) යන IP කොටස ලබා දී ඇති අතර, සමාන ධාරක සංඛ්‍යාවක් අඩංගු වන පරිදි A, B, C, සහ D ලෙස උප-ජාල හතරක් නිර්මාණය කිරීමට අවශ්‍ය යැයි උපකල්පනය කරමු.

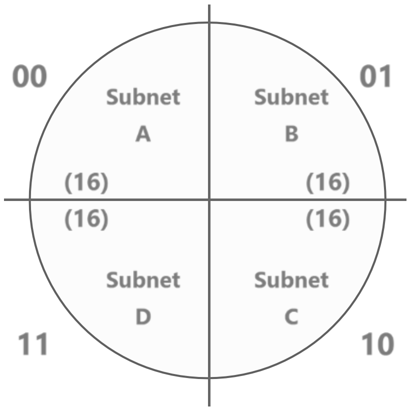
The block is given as /26, which means that the first 26 bits are reserved for the network portion and cannot be changed.
මෙම කොටස /26 ලෙස ලබා දී ඇත, එයින් අදහස් වන්නේ පළමු බිටු 26 ජාල කොටස සඳහා වෙන් කර ඇති බැවින් ඒවා වෙනස් කළ නොහැකි බවයි.

We need two bits from the host part to create these four subnets.
මෙම උප-ජාල හතර නිර්මාණය කිරීම සඳහා අපට ධාරක කොටසෙන් බිටු දෙකක් අවශ්‍ය වේ.

To achieve this, we can use the first two bits of the host part as subnet bits and assign the values 00, 01, 10, and 11, thereby dividing the host address space into four equal subnets.
මෙය සාක්ෂාත් කර ගැනීම සඳහා, අපට ධාරක කොටසේ පළමු බිටු දෙක උප-ජාල බිටු ලෙස භාවිතා කළ හැකි අතර, ඒවාට 00,01,10 සහ11 යන අගයන් ලබා දීමෙන් ධාරක ලිපින අවකාශය සමාන උප-ජාල හතරකට බෙදිය හැකිය.

When we take two bits, there are only 4 remaining bits for the host part.
අප බිටු දෙකක් ගත් විට, ධාරක කොටස සඳහා ඉතිරි වන්නේ බිටු 4ක් පමණි.





Subnet A
Network address = 192.168.1.0
Broadcast address = 192.168.1.15
Usable IP range = 192.168.1.1 – 192.168.1.14

Subnet B
Network address = 192.168.1.16
Broadcast address = 192.168.1.31
Usable IP range = 192.168.1.17 – 192.168.1.30

Subnet C
Network address = 192.168.1.32
Broadcast address = 192.168.1.47
Usable IP range = 192.168.1.33 – 192.168.1.46

Subnet D
Network address = 192.168.1.48
Broadcast address = 192.168.1.63
Usable IP range = 192.168.1.49 – 192.168.1.62

Max IP addresses of each subnet = 2^4 = 16
Maximum usable hosts = $2^4 - 2$ = 14
New subnet mask = 255.255.255.240 /28

ictfromabc.com

Question 02 – Fixed Length Subnet Mask (FLSM)

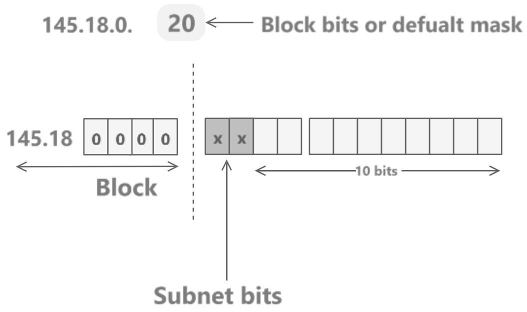
Suppose we are given the IP block 145.18.0.0/20 and asked to create four subnets as A, B, C, and D that contain an equal number of hosts.
145.18.0.0/20 යන IP කාණ්ඩය ලබා දී සමාන ධාරක සංඛ්‍යාවක් A, B, C සහ D ලෙස අඩංගු උපජාල හතරක් නිර්මාණය කිරීමට අපෙන් ඉල්ලා සිටී යැයි සිතමු.

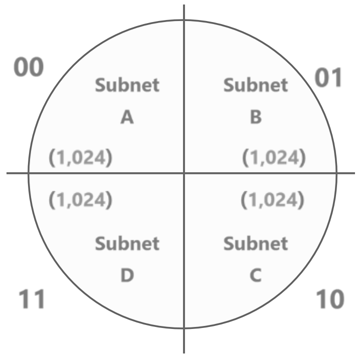
The block is given as 20 which means that the first 20 bits are reserved for the network portion and cannot be changed.
කාණ්ඩය 20 ලෙස දක්වා ඇති අතර එයින් අදහස් වන්නේ පළමු බිටු 20 ජාල කොටස සඳහා වෙන් කර ඇති බවත් එය වෙනස් කළ නොහැකි බවත්ය.

We need two bits from the host part to create these four subnets.
මෙම උපජාල හතර නිර්මාණය කිරීම සඳහා අපට සත්කාරක කොටසෙන් බිටු දෙකක් අවශ්‍ය වේ.

To achieve this, we can use the first two bits of the host part as the subnet bits and assign them values of 00, 01, 10, and 11, thereby dividing these addresses into four equal subnets.
එය සිදු කිරීම සඳහා, අපට ධාරක කොටසෙහි පළමු බිටු දෙක උපජාල බිටු ලෙස ගෙන ඒවා 00, 01, 10 සහ 11 ලෙස නියත කර මෙම ලිපින සමාන සමාන හතරකට බෙදිය හැකිය.

When we take two bits, there are only 10 remaining bits for the host part.
අප විසින් බිටු දෙකක් ලබා ගන්නා විට ධාරක කොටස සඳහා බිටු 10 ක් ඉතිරි වේ.





Subnet A
Network address = 145.18.0.0
Broadcast address = 145.18.3.255
Usable IP range = 145.18.0.1 – 145.18.3.254

Subnet B
Network address = 145.18.4.0
Broadcast address = 145.18.7.255
Usable IP range = 145.18.4.1 – 145.18.7.254

Subnet C
Network address = 145.18.8.0
Broadcast address = 145.18.11.255
Usable IP range = 145.18.8.1 – 145.18.11.254

Subnet D
Network address = 145.18.12.0
Broadcast address = 145.18.15.255
Usable IP range = 145.18.12.1 – 145.18.15.254

Max IP addresses of each subnet = 2^{10}= 1024
Maximum usable hosts = 2^{10} - 2 = 1022
Subnet mask = 255.255.252.0

ictfromabc.com

Question 01 – Variable Length Subnet Mask (VLSM)

Suppose you are asked to divide the IP block 192.168.10.0/25 into three subnets as shown below.

ඔබට 192.168.10.0/25 වන IP ලිපින කොටස පහත පරිදි උපජාල තුනකට (VLSM) බෙදීමට අවශ්‍ය බව සලකන්න.

Subnet A / උපජාල A
Half of the IP block (64 addresses)
IP කොටසෙන් අඩක් (ලිපින 64)

Subnet B / උපජාල B
Quarter of the IP block (32 addresses)
IP කොටසෙන් කාලක් (ලිපින 32)

Subnet C / උපජාල C
Quarter of the IP block (32 addresses)
IP කොටසෙන් කාලක් (ලිපින 32)

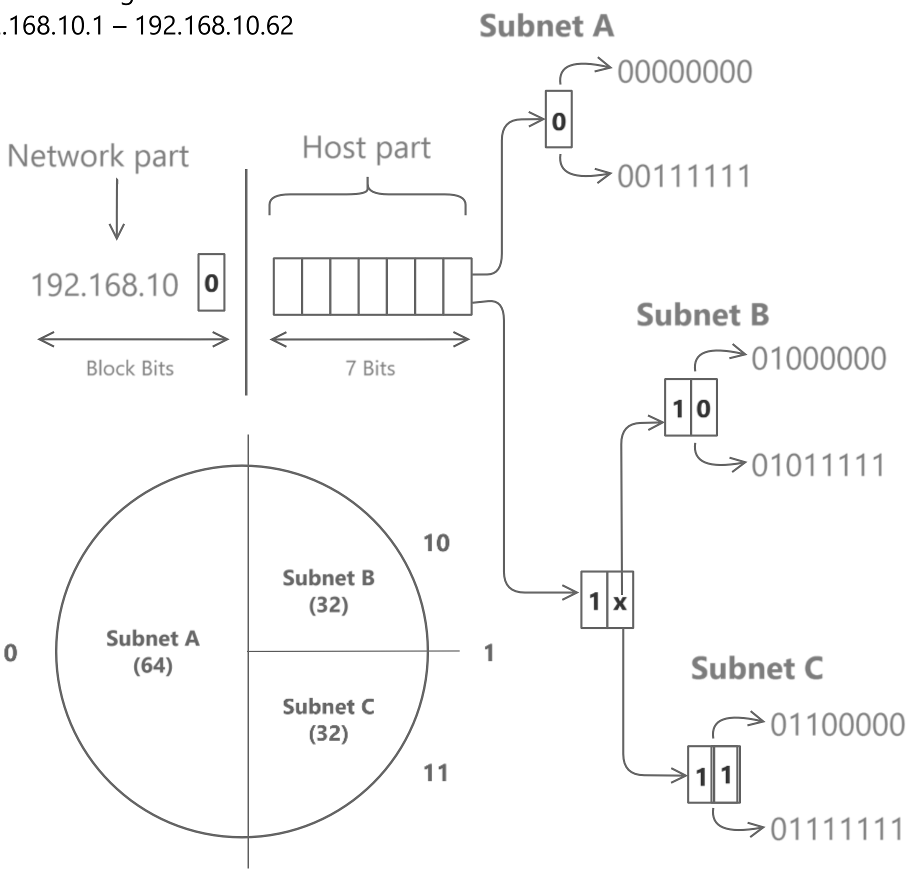
Subnet A / උපජාල A
Network address = 192.168.10.0
Broadcast address = 192.168.10.63
Subnet mask= 255.255.255.192
Usable IP range =
192.168.10.1 – 192.168.10.62

Subnet B / උපජාල B
Network address = 192.168.10.64
Broadcast address = 192.168.10.95
Subnet mask = 255.255.255.224
Usable IP range =
192.168.10.65 – 192.168.10.94

Subnet C / උපජාල C
Network address = 192.168.10.96
Broadcast address = 192.168.10.127
Subnet mask = 255.255.255.224
Usable IP range =
192.168.10.97 – 192.168.10.126

Maximum IP addresses in 192.168.10.0/25
= 2^7 = 128

Maximum usable hosts
= $2^7 - 2 = 128 - 2 = 126$



Question 02 – Variable Length Subnet Mask (VLSM)

Suppose you are asked to divide the IP block 192.168.0.0/20 into four VLSM subnets using the following allocation:
192.168.0.0/20 IP කොටස පහත දැක්වෙන වෙන්කිරීම් භාවිත කරමින් VLSM උපජාල හතරකට බෙදීමට ඔබට පවසන්නේ යැයි උපකල්පනය කරන්න:

- Subnet A – Half (1/2)
- Subnet B – Quarter (1/4)
- Subnet C – One Eighth (1/8)
- Subnet D – One Eighth (1/8)

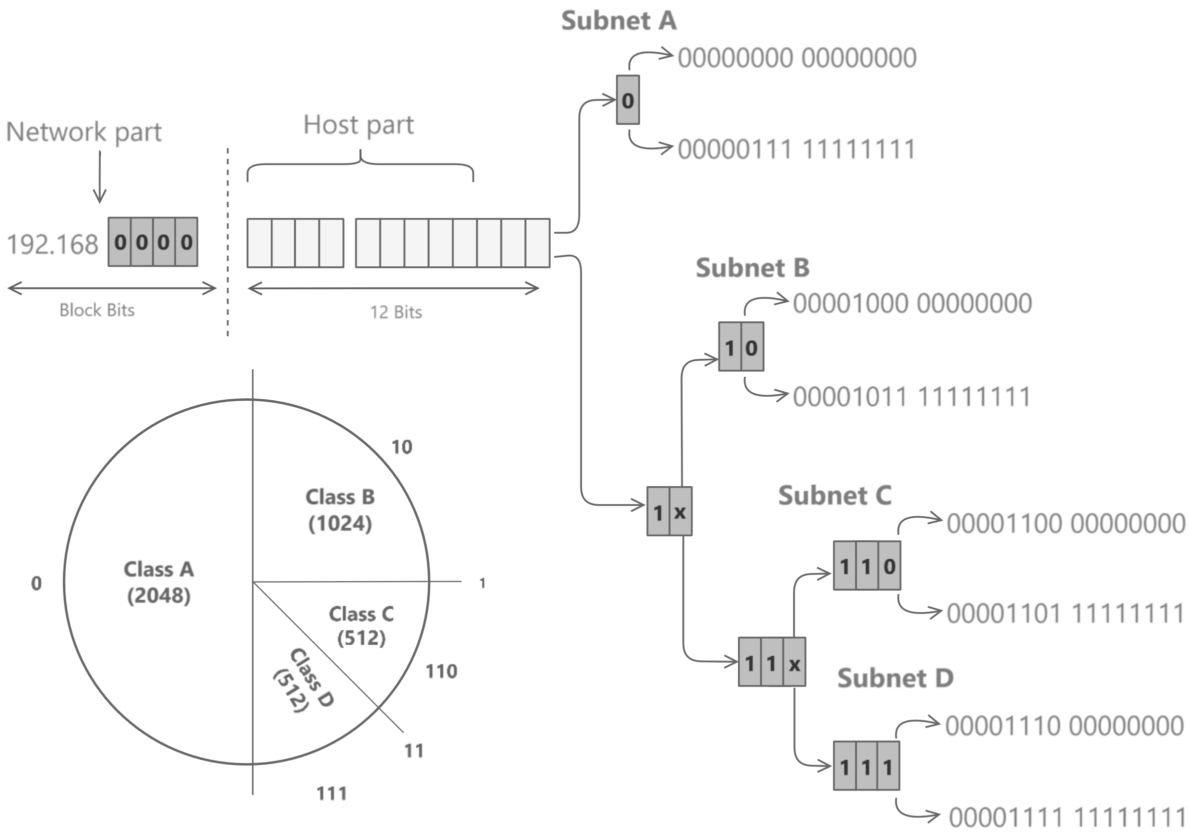
Subnet A (1/2 of /20) / උපජාල A
Network address = 192.168.0.0
Broadcast address = 192.168.7.255
Subnet mask = 255.255.248.0
Usable IP range = 192.168.0.1 – 192.168.7.254

Subnet B (1/4 of /20) / උපජාල B
Network address = 192.168.8.0
Broadcast address = 192.168.11.255
Subnet mask = 255.255.252.0
Usable IP range =192.168.8.1 – 192.168.11.254

Subnet C (1/8 of /20) / උපජාල C
Network address = 192.168.12.0
Broadcast address = 192.168.13.255
Subnet mask = 255.255.254.0 /23
Usable IP range = 192.168.12.1 –192.168.13.254

Subnet D (1/8 of /20) / උපජාල D
Network address = 192.168.14.0
Broadcast address = 192.168.15.255
Subnet mask = 255.255.254.0
Usable IP range =192.168.14.1 – 192.168.15.254

Maximum IP Addresses of the /20 Block
Maximum IP addresses = 2^{12} = 4096
Maximum usable hosts = 2^{12} − 2 = 4094



Additional question types

Question 01 / ප්‍රශ්නය 01

Determine the subnet range for the IP address 192.168.1.75/27.

192.168.1.75/27 IP ලිපිනය සඳහා උපජාල පරාසය නිර්ණය කරන්න.

Answer / පිළිතුර

The prefix length is /27

උපසර්ග දිග /27 වේ.

The subnet mask for /27 is 255.255.255.224

/27 සඳහා උපජාල වැස්ම 255.255.255.224 වේ.

B = 256 − N

Where; / මෙහි;

B = Block size / කොටස් ප්‍රමාණය

N = subnet mask value in the last octet

අවසාන අෂ්ටකයේ උපජාල වැස්මෙහි අගය

To find the block size 256 - 224 = 32

කොටස් ප්‍රමාණය සෙවීමට 256 - 224 = 32

So, the subnet ranges increase by 32.

එබැවින්, උපජාල පරාසයන් 32 බැගින් වැඩි වේ.

192.168.1.0 - 192.168.1.31
192.168.1.32 - 192.168.1.63
192.168.1.64 - 192.168.1.95
192.168.1.96 - 192.168.1.127

So, the subnet range that 192.168.1.75 belongs to is 192.168.1.64 - 192.168.1.95

එබැවින්, 192.168.1.75 අයත් වන උපජාල පරාසය 192.168.1.64 - 192.168.1.95 වේ.

Question 02 / ප්‍රශ්නය 02

Identify whether the subnet mask 255.255.255.250 is valid or invalid.

255.255.255.250 උපජාල වැස්ම වලංගු ද නැතහොත් අවලංගු ද යන්න හඳුනාගන්න.

Answer / පිළිතුර

A valid subnet mask must follow this pattern:

(A set of 1s followed by a set of 0s)

වලංගු උපජාල වැස්මක් මෙම රටාව අනුගමනය කළ යුතුය:

(1 කාණ්ඩයකට පසුව 0 කාණ්ඩයක් පැවතීම)

11111111.11111111.11111111.11111000

Convert 255.255.255.250 to binary.

255.255.255.250 ද්විමය ආකාරයට හරවන්න.

11111111.11111111.11111111.11111010

Since the 1s and 0s are mixed, the subnet mask is invalid.

මෙහි 1 සහ 0 මිශ්‍ර වී ඇති බැවින්, උපජාල වැස්ම අවලංගු වේ.

Question 03 / ප්‍රශ්නය 03

Determine whether 192.168.1.64/26 is a valid host address.

Answer / පිළිතුර

The subnet mask for /26 is 255.255.255.192

/26 සඳහා උපජාල වැස්ම 255.255.255.192 වේ.

Find the block size / කොටස් ප්‍රමාණය සොයන්න:

256 - 192 = 64

So, the subnet ranges increase by 64

එබැවින්, උපජාල පරාසයන් 64 බැගින් වැඩි වේ

192.168.1.0 - 192.168.1.63
192.168.1.64 - 192.168.1.127
192.168.1.128 - 192.168.1.191
192.168.1.192 - 192.168.1.255

The given IP address is 192.168.1.64

ලබා දී ඇති IP ලිපිනය 192.168.1.64 වේ

This is the first address in the subnet range

මෙය පහත උපජාල පරාසයේ පළමු ලිපිනයයි

192.168.1.64 - 192.168.1.127

The first address of a subnet is the network address.

උපජාලයක පළමු ලිපිනය ජාල ලිපිනය වේ.

Therefore, 192.168.1.64/26 is not a valid host address.

එබැවින්, 192.168.1.64/26 යනු වලංගු ධාරක ලිපිනයක් නොවේ.

Question 04 / ප්‍රශ්නය 04

A network administrator needs to create a subnet that can support at least 60 usable hosts. What subnet mask should be used?

ජාල පරිපාලකයෙකුට අවම වශයෙන් භාවිත කළ හැකි ධාරකයන් 60 කට සහය දැක්විය හැකි උපජාලයක් සෑදීමට අවශ්‍ය වේ. මේ සඳහා භාවිත කළ යුතු උපජාල වැස්ම කුමක්ද?

Answer / පිළිතුර

Use the formula, for no. of hosts

ධාරකයන් සංඛ්‍යාව සූත්‍රය භාවිත කරන්න.

$2^h - 2$ = no. of hosts

$2^5 - 2 = 30$, 30 usable hosts is not enough.

භාවිත කළ හැකි ධාරකයන් 30 ක් ප්‍රමාණවත් නොවේ.

$2^6 - 2 = 62$, 62 usable hosts is enough.

භාවිත කළ හැකි ධාරකයන් 62 ක් ප්‍රමාණවත් වේ.

So, we need 6 host bits.
එබැවින්, අපට ධාරක බිටු 6ක් අවශ්‍ය වේ.

Since IPv4 has 32 bits: 32 - 6 = 26
IPv4 සතුව බිටු 32 ක් ඇති බැවින්: 32 - 6 = 26

Therefore, the prefix length is 26
එබැවින්, උපසර්ග දිග 26 කි.

The subnet mask for /26 is 255.255.255.192
/26 සඳහා උපජාල වැස්ම 255.255.255.192 වේ.

Therefore, / එබැවින්,
The required subnet mask is 255.255.255.192
අවශ්‍ය උපජාල වැස්ම 255.255.255.192 වේ.

Question 05 / ප්‍රශ්නය 05

A Class C network must be divided into subnets where each subnet supports at least 50 usable hosts. Determine the number of borrowed bits.
C පංතියේ ජාලයක් උපජාලවලට බෙදිය යුතු අතර එහිදී එක් එක් උපජාලය අවම වශයෙන් භාවිත කළ හැකි ධාරකයන් 50 කට සහය දැක්විය යුතුය. ලබා ගත් බිටු සංඛ්‍යාව නිර්ණය කරන්න.

Answer / පිළිතුර

A Class C network has 8 host bits by default.
C පංතියේ ජාලයක පෙරනිමියෙන් ධාරක බිටු 8 ක් පවතී.

To support 50 usable hosts, $2^h - 2 \geq 50$
භාවිත කළ හැකි ධාරකයන් 50 කට සහය දැක්වීමට,
$2^h - 2 \geq 50$

$2^5 - 2 = 30$, 30 usable hosts is not enough.
භාවිත කළ හැකි ධාරකයන් 30 ක් ප්‍රමාණවත් නොවේ.

$2^6 - 2 = 62$, 62 usable hosts is enough.
භාවිත කළ හැකි ධාරකයන් 62 ක් ප්‍රමාණවත් වේ.

So, 6 host bits must remain.
එබැවින්, ධාරක බිටු 6 ක් ඉතිරි විය යුතුය.

Since a Class C network originally has 8 host bits, / C පංතියේ ජාලයක මුලින්ම ධාරක බිටු 8 ක් ඇති බැවින්,
8 - 6 = 2

Therefore, 2 bits are borrowed.
එබැවින්, බිටු 2 ක් ලබා ගෙන ඇත.

Question 06 / ප්‍රශ්නය 06

The network 192.168.1.0/24 is subnetted using the subnet mask 255.255.255.192. Determine the network address of the subnet which the IP address 192.168.1.130 belongs to.
192.168.1.0/24 ජාලය 255.255.255.192 උපජාල වැස්ම භාවිතයෙන් උපජාලකරණය කර ඇත. 192.168.1.130 IP ලිපිනය අයත් වන උපජාලයේ ජාල ලිපිනය නිර්ණය කරන්න.

Answer / පිළිතුර

The given subnet mask is, 255.255.255.192
ලබා දී ඇති උපජාල වැස්ම 255.255.255.192 වේ.

To find the block size, 256 - 192 = 64
කොටස් ප්‍රමාණය සෙවීමට, 256 - 192 = 64

So, the subnet ranges increase by 64
එබැවින්, උපජාල පරාසයන් 64 බැගින් වැඩි වේ

192.168.1.0 - 192.168.1.63
192.168.1.64 - 192.168.1.127
192.168.1.128 - 192.168.1.191
192.168.1.192 - 192.168.1.255

The given IP address is 192.168.1.130
ලබා දී ඇති IP ලිපිනය 192.168.1.130 වේ.

This IP address falls within the range
මෙම IP ලිපිනය පහත පරාසය තුළට වැටේ.
192.168.1.128 - 192.168.1.191

Therefore, it belongs to the subnet
එබැවින්, එය 192.168.1.128/26 උපජාලයට අයත් වේ.
192.168.1.128/26

Question 07 / ප්‍රශ්නය 07

Given the IP address 172.16.25.10/20, identify the network address and broadcast address.
172.16.25.10/20 IP ලිපිනය සලකා, එහි ජාල ලිපිනය සහ විකාශන ලිපිනය හඳුනාගන්න.

Answer / පිළිතුර

The prefix length is /20
උපසර්ග දිග /20 වේ.

This means the number of ones in the subnet mask is 20.
මින් අදහස් වන්නේ උපජාල වැස්මේ ඇති එකේ ඒවායේ සංඛ්‍යාව 20 ක් බවයි.

The subnet mask for /20 is 255.255.240.0
/20 සඳහා උපජාල වැස්ම 255.255.240.0 වේ.

To find the block size 256 - 240 = 16
කොටස් ප්‍රමාණය සෙවීමට 256 - 240 = 16

So, the subnets increase by 16 in the third octet.
එබැවින්, තෙවන අෂ්ටකය තුළ උපජාල 16 බැගින් වැඩි වේ.

172.16.0.0 - 172.16.15.255
172.16.16.0 - 172.16.31.255
172.16.32.0 - 172.16.47.255

The given IP address is 172.16.25.10
ලබා දී ඇති IP ලිපිනය 172.16.25.10 වේ.

This belongs to the subnet
මෙය පහත උපජාලයට අයත් වේ.
172.16.16.0 - 172.16.31.255

Therefore, / එබැවින්,
The network address is 172.16.16.0
ජාල ලිපිනය 172.16.16.0 වේ.

The broadcast address is the last address in that subnet, 172.16.31.255
විකාශන ලිපිනය යනු එම උපජාලයේ අවසාන ලිපිනය වන 172.16.31.255 වේ.

Question 08 / ප්‍රශ්නය 08
Determine whether the two hosts 192.168.1.70/26 and 192.168.1.130/26 are in the same network.
192.168.1.70/26 සහ 192.168.1.130/26 යන ධාරකයන් දෙදෙනා එකම ජාලයක සිටීද යන්න නිර්ණය කරන්න.

Answer / පිළිතුර

The given prefix length is /26
ලබා දී ඇති උපසර්ග දිග /26 වේ.

This means the subnet mask is 255.255.255.192
මින් අදහස් වන්නේ උපජාල වැස්ම 255.255.255.192 බවයි.

To find the block size 256 - 192 = 64
කොටස් ප්‍රමාණය සෙවීමට 256 - 192 = 64

So, the subnet ranges increase by 64
එබැවින්, උපජාල පරාසයන් 64 බැගින් වැඩි වේ.

192.168.1.0 - 192.168.1.63
192.168.1.64 - 192.168.1.127
192.168.1.128 - 192.168.1.191
192.168.1.192 - 192.168.1.255
192.168.1.70
This falls within 192.168.1.64 - 192.168.1.127
So, its network address is 192.168.1.64
මෙය 192.168.1.64 - 192.168.1.127 අතරට වැටේ.
එබැවින්, එහි ජාල ලිපිනය 192.168.1.64 වේ.

192.168.1.130
This falls within 192.168.1.128 - 192.168.1.191
So, its network address is 192.168.1.128
මෙය 192.168.1.128 - 192.168.1.191 අතරට වැටේ.
එබැවින්, එහි ජාල ලිපිනය 192.168.1.128 වේ.

Therefore, / එබැවින්,
192.168.1.70/26 and 192.168.1.130/26 are not in the same network.
192.168.1.70/26 සහ 192.168.1.130/26 එකම ජාලයක නොපවතී.

Question 09 / ප්‍රශ්නය 09
A company is given the network 192.168.10.0/24. It needs subnets for departments requiring 60 hosts, 30 hosts, 12 hosts, and 6 hosts. Use VLSM to allocate suitable subnets.
සමාගමකට 192.168.10.0/24 ජාලය ලබා දී ඇත. ධාරකයන් 60 ක්, ධාරකයන් 30 ක්, ධාරකයන් 12 ක් සහ ධාරකයන් 6 ක් අවශ්‍ය වන දෙපාර්තමේන්තු සඳහා ඊට උපජාල අවශ්‍ය වේ. සුදුසු උපජාල වෙන් කිරීම සඳහා VLSM භාවිත කරන්න.

Answer / පිළිතුර
In VLSM, always allocate subnets starting from the largest host requirement.
VLSM හි දී, සෑම විටම උපජාල වෙන් කිරීම විශාලතම ධාරක අවශ්‍යතාවයේ සිට ආරම්භ කරන්න.
60, 30, 12, 6

Find the suitable subnet size
සුදුසු උපජාල ප්‍රමාණය සොයන්න

Usable hosts = $2^n - 2$;
where n is the number of host bits.
මෙහි n යනු ධාරක බිටු සංඛ්‍යාවයි.

Subnets / උපජාල

192.168.10.0/26 - Used for 60 hosts

Network:	192.168.10.0
Usable:	192.168.10.1 - 192.168.10.62
Broadcast:	192.168.10.63

192.168.10.64/27 - Used for 30 hosts

Network:	192.168.10.64
Usable:	192.168.10.65 - 192.168.10.94
Broadcast:	192.168.10.95

192.168.10.96/28 - Used for 12 hosts

Network:	192.168.10.96
Usable:	192.168.10.97 - 192.168.10.110
Broadcast:	192.168.10.111

192.168.10.112/29 - Used for 6 hosts

Network:	192.168.10.112
Usable:	192.168.10.113 - 192.168.10.118
Broadcast:	192.168.10.119

Question 10 / ප්‍රශ්නය 10

The subnet 192.168.1.64/27 has already been allocated. Find the next available subnet.
192.168.1.64/27 උපජාලය දැනටමත් වෙන් කර ඇත. ඊළඟට ලබාගත හැකි උපජාලය සොයන්න.

Answer / පිළිතුර

The subnet mask for /27 is 255.255.255.224
/27 සඳහා උපජාල වැස්ම 255.255.255.224 වේ.

Find the block size: / කොටස් ප්‍රමාණය සොයන්න:
256 - 224 = 32

So, each subnet increases by 32 in the last octet.
එබැවින්, එක් එක් උපජාලය අවසාන අෂ්ටකය තුළ 32 බැගින් වැඩි වේ.

The subnet ranges are: / උපජාල පරාසයන් වන්නේ:

192.168.1.0 - 192.168.1.31
192.168.1.32 - 192.168.1.63
192.168.1.64 - 192.168.1.95
192.168.1.96 - 192.168.1.127

The given subnet is 192.168.1.64/27
ලබා දී ඇති උපජාලය 192.168.1.64/27 වේ.

Its range ends at 192.168.1.95
එහි පරාසය 192.168.1.95න් අවසන් වේ.

So, the next available subnet starts at 192.168.1.96
එබැවින්, ඊළඟට ලබාගත හැකි උපජාලය ආරම්භ වන්නේ 192.168.1.96න් ය.

Range: 192.168.1.96 – 192.168.1.127.

Question 11 / ප්‍රශ්නය 11

Given that the broadcast address of a subnet is 192.168.1.95/27, determine the network address.
උපජාලයක විකාශන ලිපිනය 192.168.1.95/27 ලෙස දී ඇති විට, එහි ජාල ලිපිනය නිර්ණය කරන්න.

Answer / පිළිතුර

The prefix length is /27
උපසර්ග දිග /27 වේ.

The subnet mask for /27 is 255.255.255.224
/27 සඳහා උපජාල වැස්ම 255.255.255.224 වේ.

256 - 224 = 32
So, each subnet has 32 addresses.
එබැවින්, එක් එක් උපජාලයකට ලිපින 32 ක් පවතී.

Since the broadcast address is the last address in the subnet, the network address can be found by subtracting 31 from the broadcast address, 95 - 31 = 64
විකාශන ලිපිනය උපජාලයේ අවසාන ලිපිනය වන බැවින්, විකාශන ලිපිනයෙන් 31 ක් අඩු කිරීමෙන් ජාල ලිපිනය සෙවිය හැක, 95 - 31 = 64

So, the network address is 192.168.1.64/27
එබැවින්, ජාල ලිපිනය 192.168.1.64/27 වේ.

Question 12 / ප්‍රශ්නය 12

Given the subnet 192.168.1.64/26, find the first usable host address and last usable host address.
192.168.1.64/26 උපජාලය සලකා, පළමු භාවිත කළ හැකි ධාරක ලිපිනය සහ අවසාන භාවිත කළ හැකි ධාරක ලිපිනය සොයන්න.

Answer / පිළිතුර

The prefix length is /26
උපසර්ග දිග /26 වේ.

The subnet mask for /26 is 255.255.255.192
/26 සඳහා උපජාල වැස්ම 255.255.255.192 වේ.

256 - 192 = 64

So, this subnet has 64 addresses.
එබැවින්, මෙම උපජාලයට ලිපින 64 ක් පවතී.

The network address is 192.168.1.64
ජාල ලිපිනය 192.168.1.64 වේ.

The subnet range is / උපජාල පරාසය වන්නේ
192.168.1.64 - 192.168.1.127

So, the broadcast address is 192.168.1.127
එබැවින්, විකාශන ලිපිනය 192.168.1.127 වේ.

The first usable host is one address after the network address 192.168.1.65
පළමු භාවිත කළ හැකි ධාරකයා වන්නේ ජාල ලිපිනයට පසුව ඇති එක් ලිපිනයක් වන 192.168.1.65 වේ.

The last usable host is one address before the broadcast address 192.168.1.126
අවසාන භාවිත කළ හැකි ධාරකයා වන්නේ විකාශන ලිපිනයට පෙර ඇති එක් ලිපිනයක් වන 192.168.1.126 වේ.

Question 13 / ප්‍රශ්නය 13
Given the subnet mask 255.255.255.224, find the prefix length.
255.255.255.224 උපජාල වැස්ම දී ඇති විට, උපසර්ග දිග සොයන්න.

Answer / පිළිතුර
The given subnet mask is 255.255.255.224
ලබා දී ඇති උපජාල වැස්ම 255.255.255.224 වේ.

Convert to binary: / ද්විමය ආකාරයට හරවන්න:

11111111. 11111111. 11111111. 11100000

Number of ones = 27 / එකේ ඒවායේ සංඛ්‍යාව = 27

So, the prefix length is /27
එබැවින්, උපසර්ග දිග /27 වේ.

Question 14 / ප්‍රශ්නය 14
Given the prefix length /28, find the subnet mask.
/28 උපසර්ග දිග දී ඇති විට, උපජාල වැස්ම සොයන්න.

Answer / පිළිතුර
This means the subnet mask has 28 ones.
මින් අදහස් වන්නේ උපජාල වැස්මට එකේ ඒවා 28 ක් ඇති බවයි.

IPv4 addresses have 32 bits in total.
IPv4 ලිපින සතුව සමස්තයක් ලෙස බිටු 32 ක් පවතී.

Write 28 ones followed by the remaining zeros:
එකේ ඒවා 28 ක් ලියා ඉන්පසු ඉතිරි බිටු සඳහා බිංදු ලියන්න:
11111111.11111111.11111111.11110000

Now convert each octet into decimal:
දැන් එක් එක් අෂ්ටකය දශම ආකාරයට හරවන්න:

11111111 = 255
11111111 = 255
11111111 = 255
11110000 = 240

So, the subnet mask is 255.255.255.240
එබැවින්, උපජාල වැස්ම 255.255.255.240 වේ.

Question 15 / ප්‍රශ්නය 15
How many total addresses and usable host addresses are available in the subnet 192.168.1.0/27?
192.168.1.0/27 උපජාලය තුළ සමස්ත ලිපින කීයක් සහ භාවිත කළ හැකි ධාරක ලිපින කීයක් පවතීද?

Answer / පිළිතුර
The given subnet is 192.168.1.0/27
ලබා දී ඇති උපජාලය 192.168.1.0/27 වේ.

IPv4 has 32 bits. / IPv4 සතුව බිටු 32 ක් පවතී.

The number of host bits is 32 - 27 = 5
ධාරක බිටු සංඛ්‍යාව වන්නේ 32 - 27 = 5

Total addresses: / මුළු ලිපින සංඛ්‍යාව:
$2^5 = 32$

Therefore, the subnet has 32 total addresses.
එබැවින්, උපජාලයට සමස්ත ලිපින 32 ක් පවතී.

However, two addresses cannot be assigned to devices:
කෙසේ වෙතත්, උපාංග සඳහා ලිපින දෙකක් පවරා දිය නොහැක:
Network address: 192.168.1.0
Broadcast address: 192.168.1.31

So, usable addresses are calculated using:
එබැවින්, භාවිත කළ හැකි ලිපින ගණනය කරනු ලබන්නේ, සූත්‍රය භාවිතයෙනි:
$2^h - 2$
$2^5 - 2 = 30$

Therefore, the subnet has 30 usable host addresses.
එබැවින්, උපජාලයට භාවිත කළ හැකි ධාරක ලිපින 30 ක් පවතී.

Total addresses: / මුළු ලිපින සංඛ්‍යාව: 32
Usable host addresses: 30
භාවිත කළ හැකි ධාරක ලිපින: 30

Question 16 / ප්‍රශ්නය 16
A Class C network 192.168.1.0/24 is subnetted using the prefix /27. How many subnets are created?
C පංතියේ ජාලයක් වන 192.168.1.0/24, /27 උපසර්ගය භාවිතයෙන් උපජාලකරණය කර ඇත. නිර්මාණය වන උපජාල සංඛ්‍යාව කොපමණද?

Answer / පිළිතුර
The original network is 192.168.1.0/24
මුල් ජාලය 192.168.1.0/24 වේ.

The new prefix is /27
නව උපසර්ගය /27 වේ.

To find the borrowed bits 27 - 24 = 3
ලබා ගත් බිටු සෙවීමට: 27 - 24 = 3

So, 3 bits have been borrowed from the host part.
එබැවින්, ධාරක කොටසෙන් බිටු 3 ක් ණයට ගෙන ඇත.

The number of subnets is calculated using 2^b
Where b is the number of borrowed bits.
උපජාල සංඛ්‍යාව 2^b භාවිතයෙන් ගණනය කරනු ලබයි මෙහි b යනු ණයට ගත් බිටු සංඛ්‍යාවයි.

$2^3 = 8$

Therefore, the network is divided into 8 subnets.
එබැවින්, ජාලය උපජාල 8 කට බෙදා ඇත.

Question 17 / ප්‍රශ්නය 17
A network 192.168.1.0/24 is subnetted using /27. Find the 5th subnet.
192.168.1.0/24 ජාලය /27 භාවිතයෙන් උපජාලකරණය කර ඇත. 5 වන උපජාලය සොයන්න.

Answer / පිළිතුර
The subnet mask for /27 is 255.255.255.224
/27 සඳහා උපජාල වැස්ම 255.255.255.224 වේ.

Block size: / කොටස් ප්‍රමාණය:
256 - 224 = 32

So, each subnet increases by 32 in the last octet.
එබැවින්, එක් එක් උපජාලය අවසාන අෂ්ටකය තුළ 32 බැගින් වැඩි වේ.

1st subnet:	192.168.1.0/27
2nd subnet:	192.168.1.32/27
3rd subnet:	192.168.1.64/27
4th subnet:	192.168.1.96/27
5th subnet:	192.168.1.128/27

Question 18 / ප්‍රශ්නය 18
A subnet starts at 192.168.1.96 and ends at 192.168.1.127. Find the CIDR prefix.

Answer / පිළිතුර
The subnet range is:
උපජාල පරාසය වන්නේ:
192.168.1.96 - 192.168.1.127

Count the total number of addresses:
සමස්ත ලිපින සංඛ්‍යාව ගණනය කරන්න:
127 - 96 + 1 = 32

So, the subnet has 32 total addresses.
එබැවින්, උපජාලයට සමස්ත ලිපින 32 ක් පවතී.

Since, $2^5 = 8$

There are 5 host bits. IPv4 has 32 bits in total:
මෙහි ධාරක බිටු 5 ක් පවතී. IPv4 සතුව සමස්තයක් ලෙස බිටු 32 ක් පවතී:

32 - 5 = 27

So, the prefix is: /27
එබැවින්, උපසර්ගය වන්නේ: /27

DMZ (Demilitarized Zone) / යුධමුක්ත කලාප

A DMZ is a separate network segment (subnet) placed between an internal (trusted) network and an external (untrusted) network, usually the internet.
DMZ යනු අභ්‍යන්තර (විශ්වාසදායක) ජාලයක් සහ බාහිර (අවිශ්වාසදායක) ජාලයක් (සාමාන්‍යයෙන් අන්තර්ජාලය) අතර පිහිටුවා ඇති වෙනම ජාල කොටසකි (උපජාලයකි).

It hosts servers that need to be reachable from outside, without exposing the internal LAN directly.
අභ්‍යන්තර LAN ජාලය සෘජුවම නිරාවරණය නොකර, බාහිරින් ප්‍රවේශ විය යුතු සේවාදායකයන් මෙහි රඳවා තබා ගනී.

Outsiders can reach services in the DMZ, but not walk straight into the internal network.
බාහිර පුද්ගලයින්ට DMZ හි ඇති සේවාවන් වෙත ප්‍රවේශ විය හැකි නමුත්, අභ්‍යන්තර ජාලයට සෘජුවම ඇතුළු විය නොහැක.

DMZ can never freely initiate connections into the internal LAN.
DMZ එකකට කිසිවිටකත් අභ්‍යන්තර LAN ජාලය වෙත ස්වේච්ඡාවෙන් සම්බන්ධතා ආරම්භ කළ නොහැක.

Why it's needed / එය අවශ්‍ය වීමට හේතුව

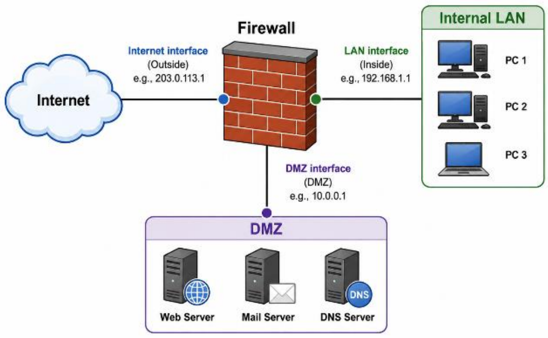
Public-facing servers (web, mail, DNS) must accept connections from the internet.
පොදු ජනතාවට විවෘත සේවාදායකයන් (වෙබ්, මේල්, DNS) අන්තර්ජාලයෙන් එන සබැඳි පිළිගත යුතුය.

If those servers sat directly on the internal LAN, a compromised server would give an attacker a direct foothold into internal systems.
එම සේවාදායකයන් සෘජුවම අභ්‍යන්තර LAN ජාලය තුළ තිබුණේ නම්, යම් සේවාදායකයක ආරක්ෂාව බිඳවැටුණු විට ප්‍රහාරකයෙකුට අභ්‍යන්තර පද්ධති වෙත සෘජුවම ප්‍රවේශ වීමේ අවස්ථාව ලැබේ.

The DMZ isolates that risk. If a DMZ server is breached, the attacker is still walled off from the internal network by another layer of firewall rules.
DMZ මඟින් එම අවදානම හුදකලා කරයි. DMZ සේවාදායකයක ආරක්ෂාව බිඳවැටුණද, ප්‍රහාරකයා තවමත් වෙනත් අග්නිපවුරු රීති ස්ථරයක් මඟින් අභ්‍යන්තර ජාලයෙන් වෙන් කර තබා ගනී.

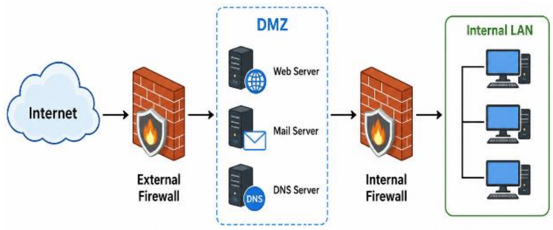
There are 2 ways to implement a DMZ
DMZ එකක් ක්‍රියාත්මක කිරීමට ක්‍රම 2 ක් ඇත

1. Single firewall (three-legged firewall)



Cheaper, simpler, but a single point of failure. One misconfiguration can expose the internal network.
ලාභදායී, සරල නමුත් එය තනි බිඳවැටීම් ලක්ෂ්‍යයකි. එක් වැරදි වින්‍යාස කිරීමකින් අභ්‍යන්තර ජාලය නිරාවරණය විය හැක

2. Dual firewall (back-to-back firewall)



More secure. An attacker who breaches FW1 and the DMZ still has to get past FW2. Preferred in production/enterprise setups.
වඩාත් ආරක්ෂිතයි. පළමු අග්නිපවුර සහ DMZ බිඳදමන ප්‍රහාරකයෙකුට දෙවන අග්නිපවුරද පසුකර යාමට සිදු වේ. නිෂ්පාදන/ව්‍යවසාය මට්ටමේ සැකසුම් සඳහා මෙය වඩාත් සුදුසු වේ.

What's typically stored in a DMZ
සාමාන්‍යයෙන් DMZ එකක ගබඩා කරන්නේ මොනවාද

Anything that must be internet-accessible goes here.
අන්තර්ජාලය හරහා ප්‍රවේශ විය යුතු ඕනෑම දෙයක් මෙහි ඇතුළත් වේ.

- Web servers / වෙබ් සේවාදායක
- Mail servers / මේල් සේවාදායක
- DNS servers / DNS සේවාදායක
- FTP servers / FTP සේවාදායක