🏠_Home_

🔗 CNS Short
🔗 IT Terminology
🔗CNS Lecture Slides

Computer Networking for Software Engineers

network

Data or Resources share කරගැනීමට, එකිනෙක connect කළ Computer 2ක් හෝ ඊට වැඩි ගණනක්.

Internet

worldwide system of computer networks
(ලෝකෙ පුරා තියෙන computer network එකතු කරල හදපු computer network එක)

Purpose of networking,

Data or Resources එකිනෙක share කරගැනීම.

Requirement for networking

Network එකකට connect වෙන devices සේරම
එකම rules set එකක්(Protocols) සහ standards අනුගමනය කරන්න ඕන.

Protocol

Internet එක හරහා, data යවන සහ ලැබෙන ආකාරය control කරන Rules set එකක්.

History

- Individual network systems

- Vendor-specific(වලෙන්දාට විශේෂිත) network models
  (ex: apple pc වලට එක network එකක්)

- Open and Vendor-neutral network models
  (වලෙන්දා මත රදානොපවතින network models)
  ex: OSI , TCP/IP

Network model

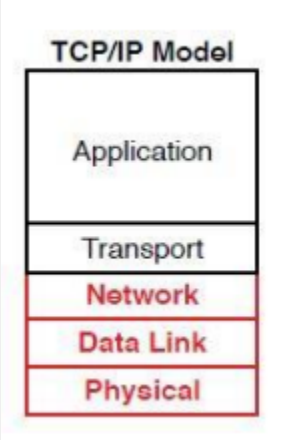
Network එකක devices එකිනෙක data share කරගනිද්දි අනුගමනය කරන protocols and standards සහිත predefined structure එකක්.
(network model = predefined structure + set of protocols and standards)

(also known as Networking Architecture or Networking Blueprint)

Requirement for networking
Network එකකට connect වෙන devices සේරම
එකම rules set එකක්(Protocols) සහ standards අනුගමනය කරන්න ඕන.

Network models :
- TCP/IP model
- OSI model

TCP/IP model

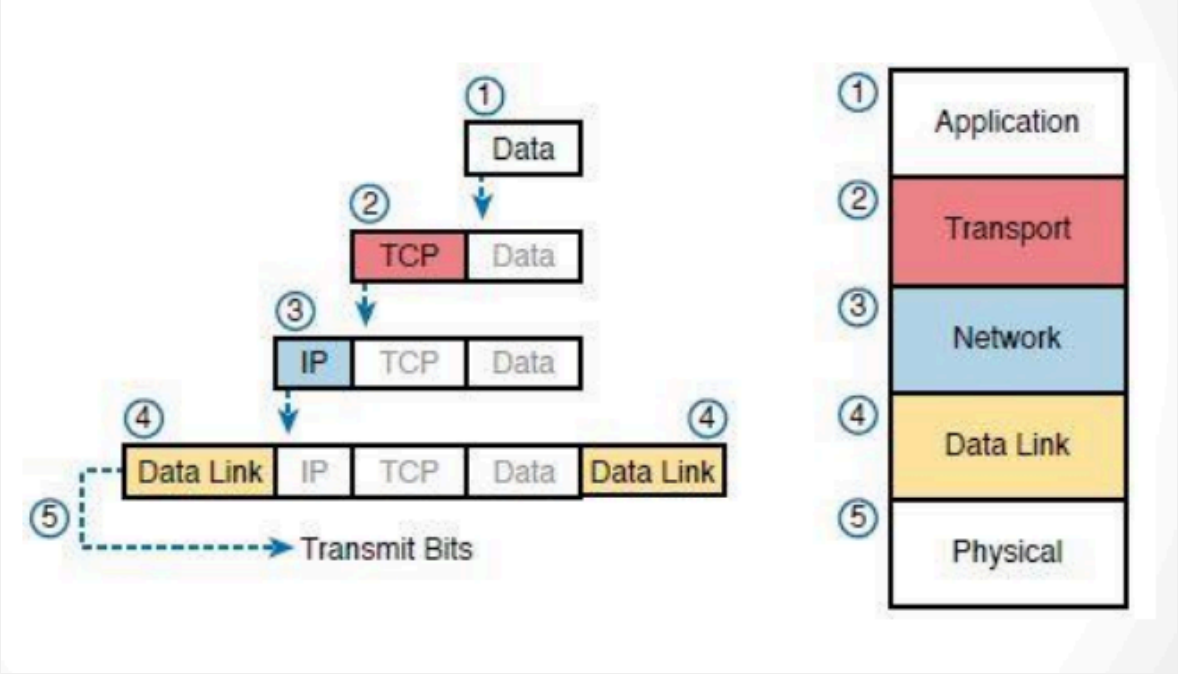


- Layers වලින් හැදිල තියෙන්නෙ.Layers trough data send වෙන්නෙ.

- හැම layer එකටම protocols & standards තියනෙවා.

(Each layer defines protocols, standards, and refers to third party protocols and standards.
ex: Ethernet standards define by IEEE)

Sending Data through TCP/IP



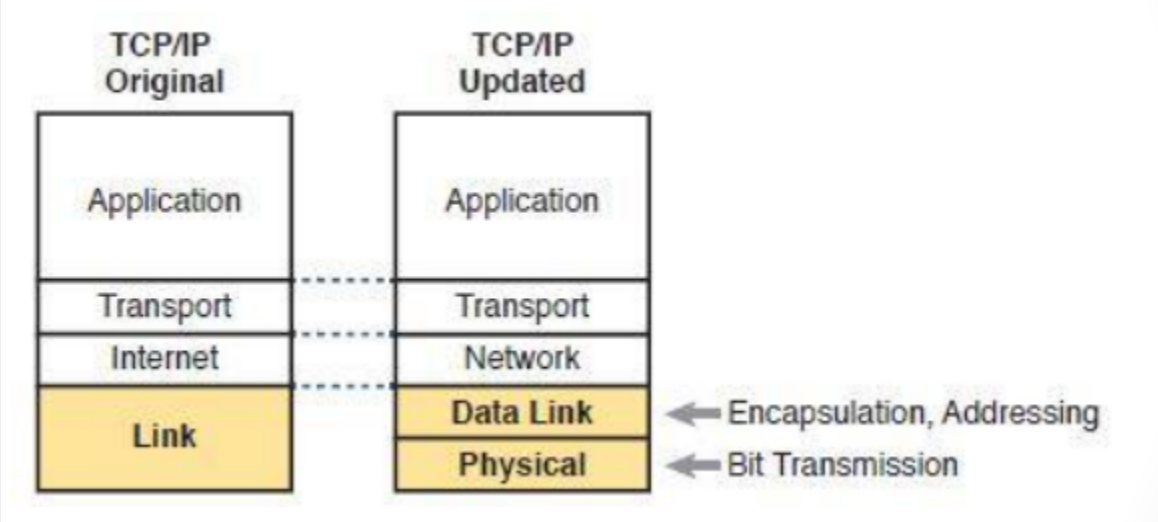
* යට ඉඳන් උඩට layer අංක කරන්නේ

Example protocols for each layer

TCP/IP Layer	Example Protocols
Application	HTTP, POP3, SMTP
Transport	TCP, UDP
Network	IP, ICMP
Data Link, Physical	Ethernet, 802.11 (Wi-Fi)

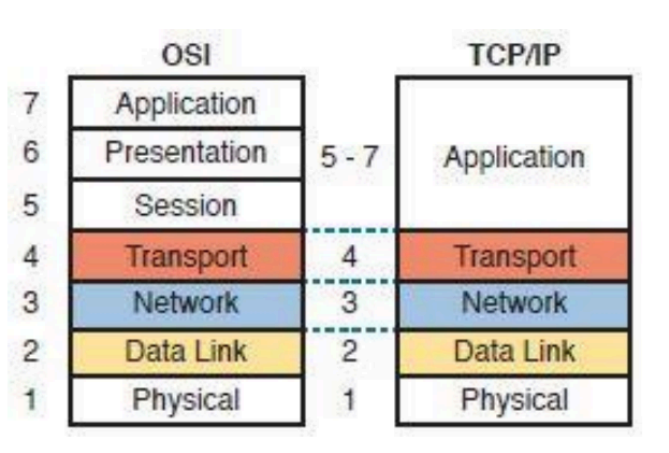
- පරණ TCP/IP model එකේ Link layer එක, updated model එකේ layer

2කට බෙදෙලා.

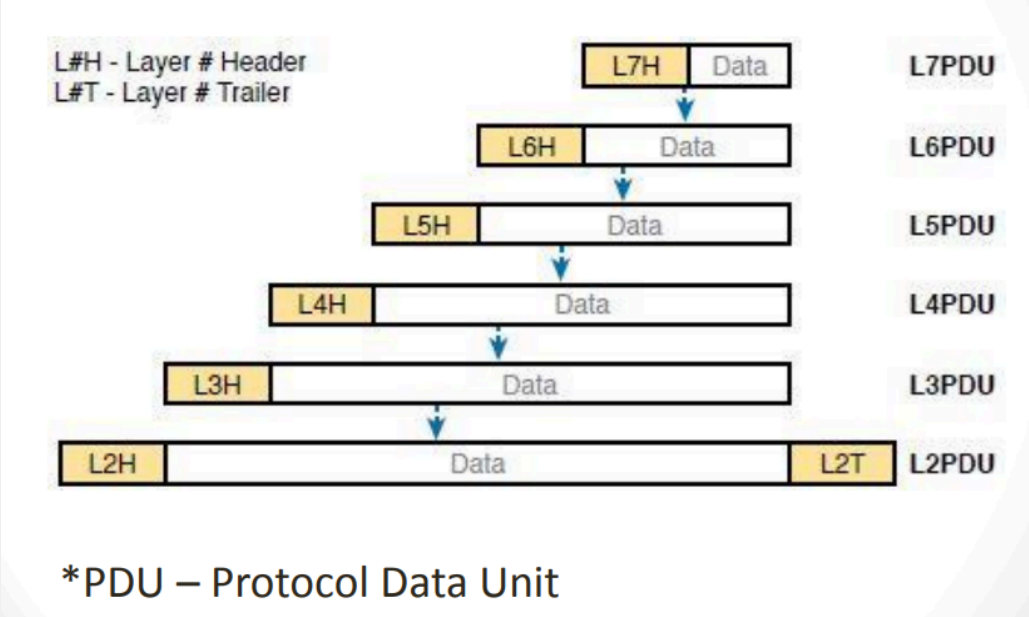


OSI model

- මුලින්ම ආපු standard Vendor-neutral network model එක.



* Networking වලදි OSI ආකෘතියේ ස්ථර අංකය හාවිතා කිරීම සිදුවේ.
(යට ඉදන් උඩට layer අංක කරන්නේ)



- OSI model එකේ data encapsulation තියෙනවා

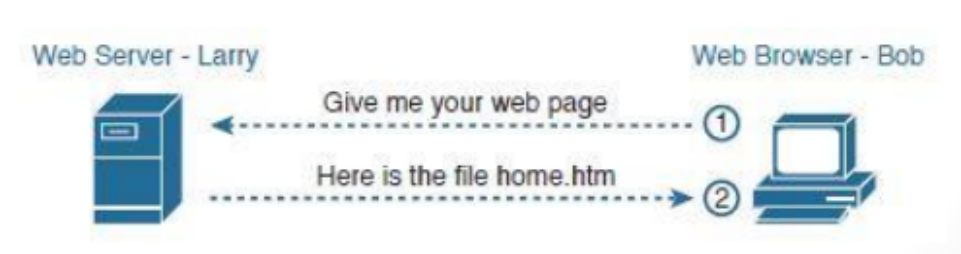
TCP/IP model Layers

* layer 5යි.
* හැම layer එකක්ම පාවිච්චි වෙන්නේ,
  - Top layer එකට service සපයන්න
  - Bottom layer එක මත depend වෙන්න

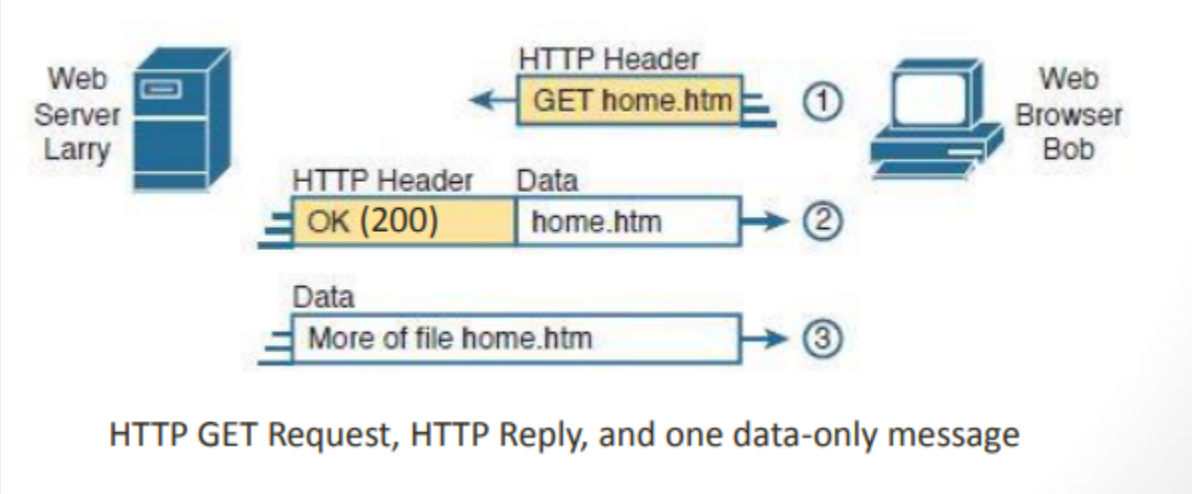
1. Application Layer

- Application Layer protocols මගින් Run වෙන Software එකට service සපයයි.
  ex: HTTP for web browsing

- Software එක සහ network එක අතර interface එක සාදයි.
- Software එක මේ layer එකට අයිති නෑ.



HTTP Protocol mechanism



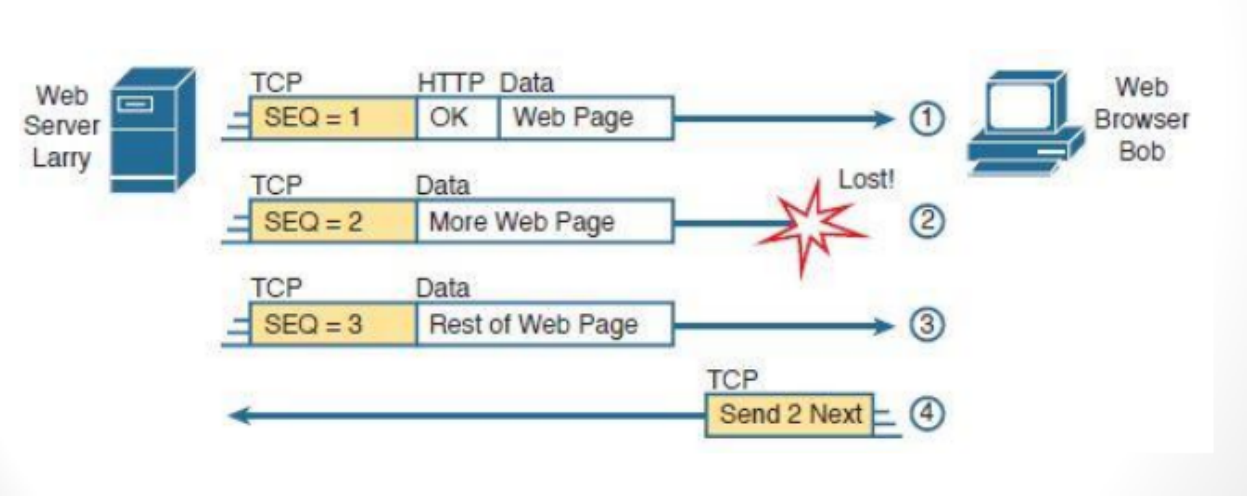
HTTP GET Request, HTTP Reply, and one data-only message

- Application වලට web page request කරන්න, ආයෙත් content එක return කරන්න, HTTP මගින් ඉඩසලසයි.
- HTTP Header එකේ තියෙන්නෙ, protocol වලට අවශ්‍ය information.

2. Transport Layer

- Application layer protocols වලට services සපයයි.
- Protocol 2යි,
    - TCP (Transmission Control Protocol)
    - UDP (User Datagram Protocol)
- Data transfer එක හරිවිදියට වුනාද කියල තහවුරු කරයි. ⇐ main task
- ඊට අමතරව Data recovery කරයි.

TCP Protocol Mechanism



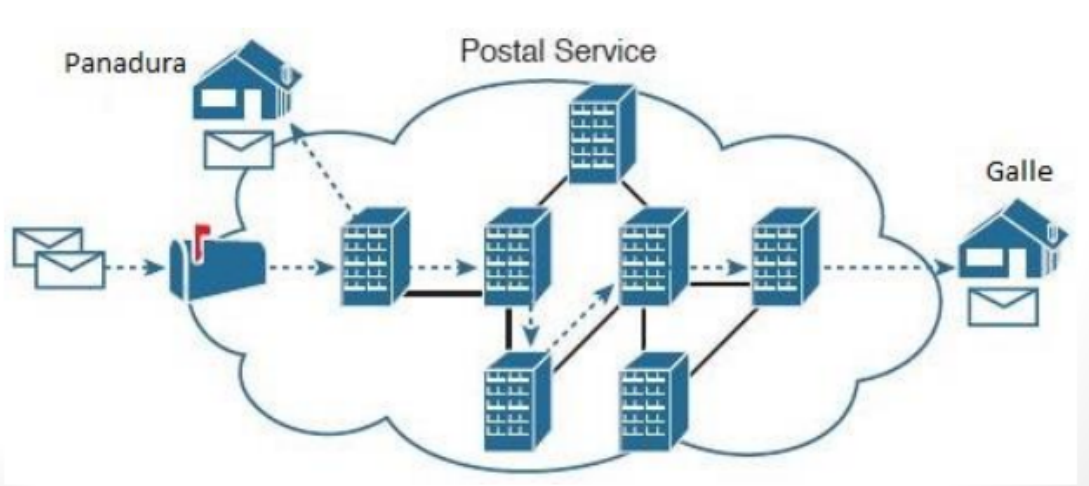
- Data segment විදියට යවන්නෙ.
- TCP Header එකේ Sequence number එකක් තියෙනෙ. Lost වෙන segment ආයෙ ගනේනගන්නෙ.

UDP ?

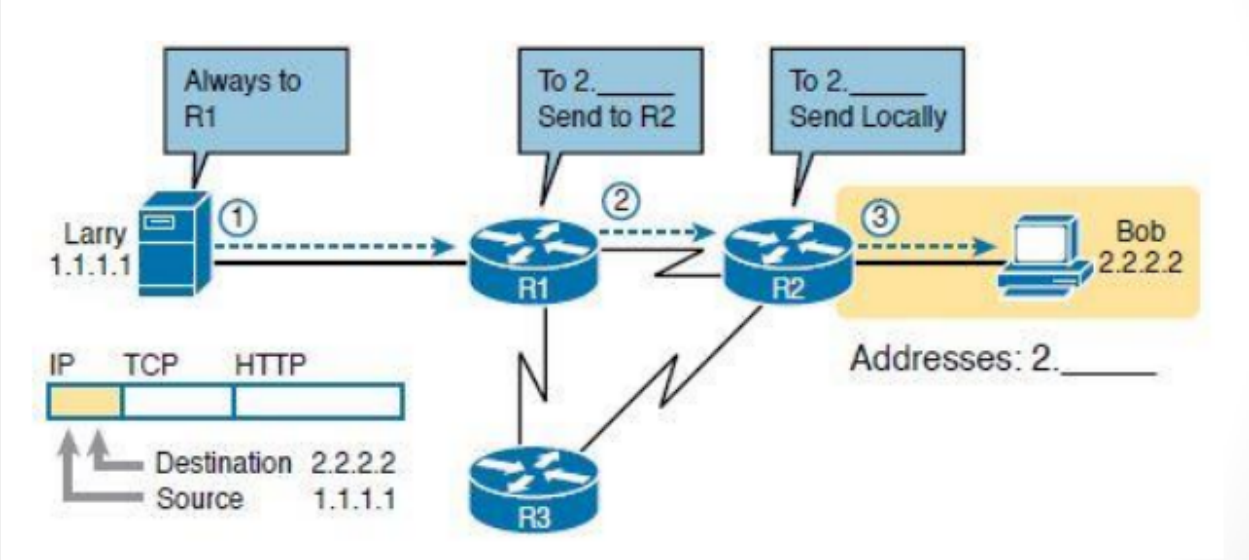
3. Network Layer

(most important layer)

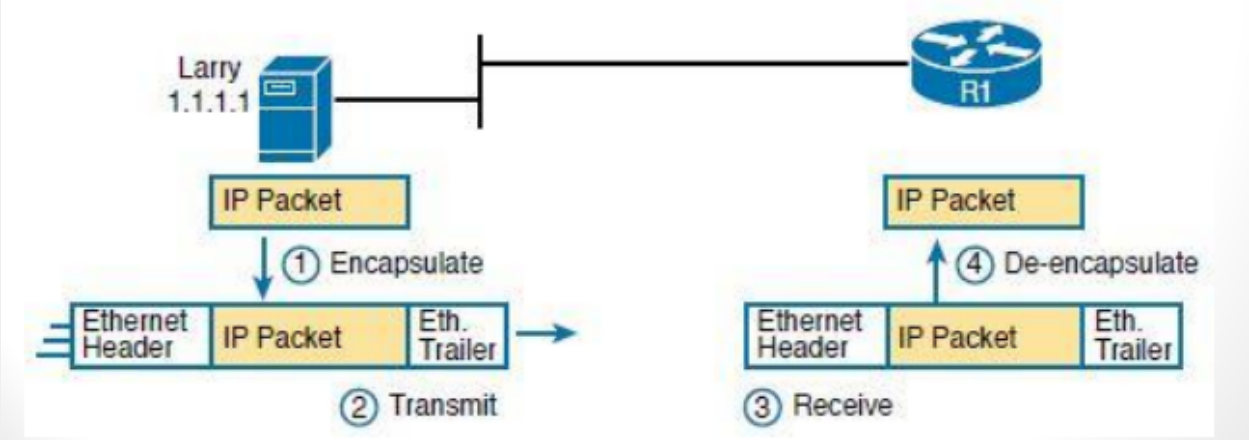
- IP (Internet Protocol) එක තියෙනෙ.
- Transport layer එකට service එක සපයයි. Data link layer එක මත depend වේ.
- Most important tasks ⇒ Addressing and routing
    - Addressing - Assigning unique identifiers (IP addresses) to devices on a network.
    - Routing - Network එකක් හරහා data packet අරන් යන්න ඕන සුදුසුම path එක (optimal path) තීරණය කරනෙ.



Network Layer Mechanism



Data Link layer & Physical layer



4. Data link layer

- prepare data to transmit (මාධ්‍යයට හරියන විදියට data ටික හදනවා.)
- heder එකට අමතරව මේ layer එකෙන් trailer එකක් දානවා.
- අන්තිමට data encapsulate කරන්නෙ මේකෙ.
  (Frames හදනවා)

5. physical layer

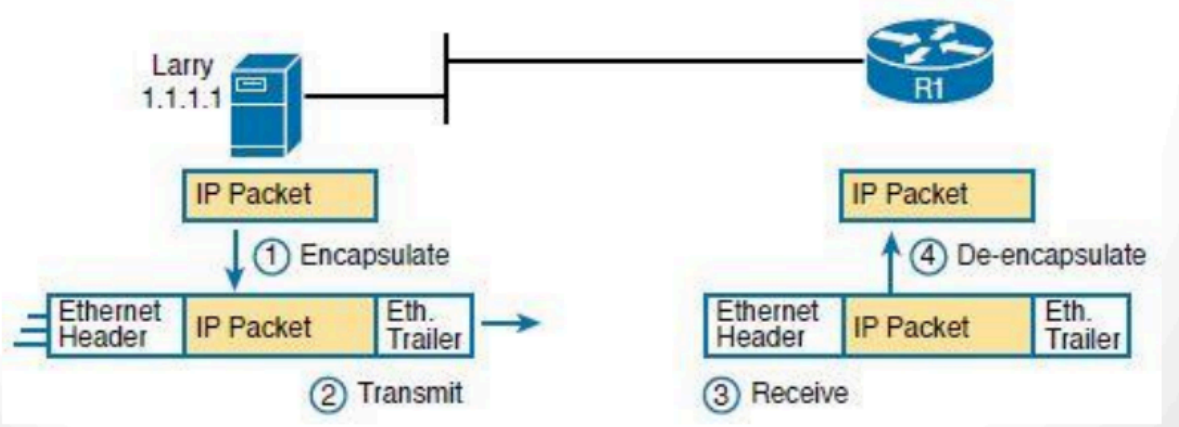
- Physical transmission එක ගැන බලනවා.
- මේ layer එකේ data encapsulate කරන්නෙ නෑ.
  (Frames යවනවා, physical connection එකක් හරහා)

Data Encapsulation

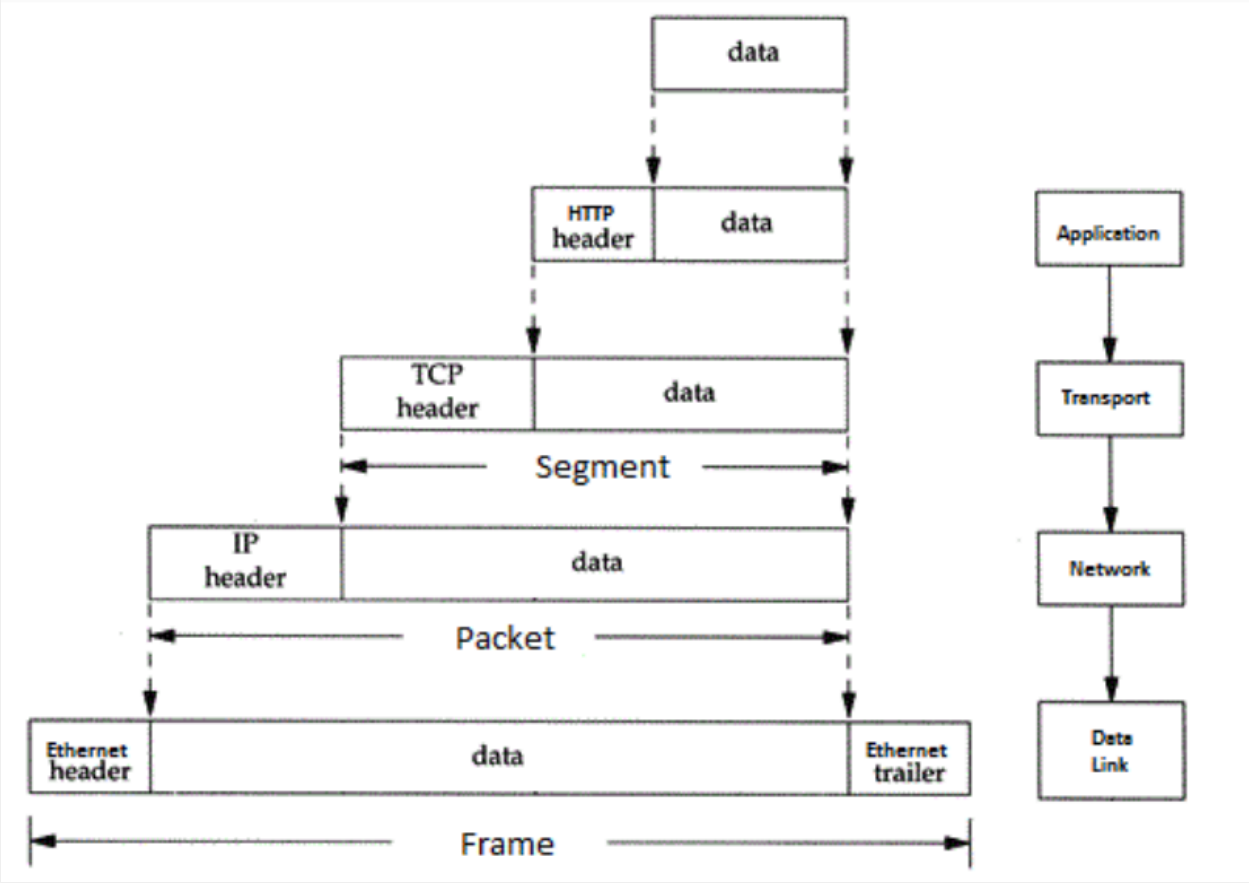
- TCP/IP model එකේ, එක් එක් layer එකේදී header එකක් add කිරීම අදහස් වේ.

- Task of the header
  Store information used by the protocol
  ex: “404 not found”

- Encapsulate කරපු data ආයෙ ගන්දදි de-encapsulate කරනවා.



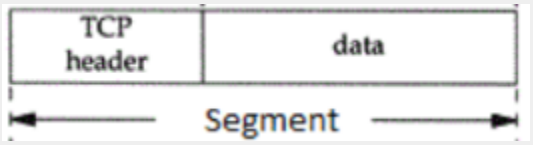
- data link layer එකේ Trailer එකතුත් add කරනෝ
- Physical layer එකේ data encapsulate කරන්නෙ නෑ.



Segment, packet, frame

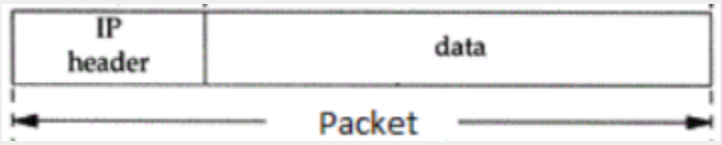
Segment

Segment = Application layer data + Transport layer header



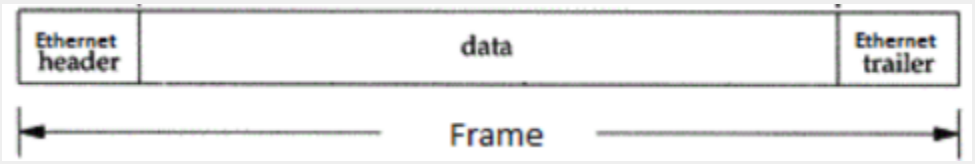
Packet

Packet = Transport layer data + Network layer header



Frame

Frame = Network layer data + Data link layer header & Trailer



Adjacent layer Vs Same layer interaction

Adjacent layer interaction - single device එකක යාබද layers අතර
Same layer interaction - multi device වල same layers අතර (ex: mis වුන data ඉල්ලගන්න එක)

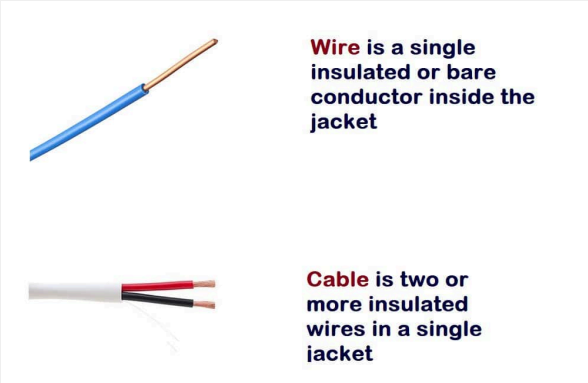
මේ 2ම හරි විදියට වෙනෙන ඕන.

Types of Communication Networks

Types of Computer Networks

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Enterprise Private Network (EPN)
- Virtual Private Network (VPN) etc.

Wire vs Cable



LAN vs WAN networks

	LAN (Local Area Network)	WAN (Wide Area Network)
Coverage	Small geographical area	Large geographical area or multiple sites
Size	Relatively smaller	Can be significantly larger
Speed	Higher data transfer speeds	Speeds can vary based on distance
Latency (ප්‍රමාදය)	Low latency	Higher latency due to longer distances
Connection Types	Wired (Ethernet), wireless (Wi-Fi)	Can include wired, wireless, and dedicated leased lines

Management	Easier to manage and maintain	More complex due to larger and distributed setup
Cost	Lower cost	Can be more expensive due to infrastructure
Security	Easier to secure and control	Requires additional security measures

LAN Technologies

Lan හදන්න පුලුවන් main technologies 2 කට

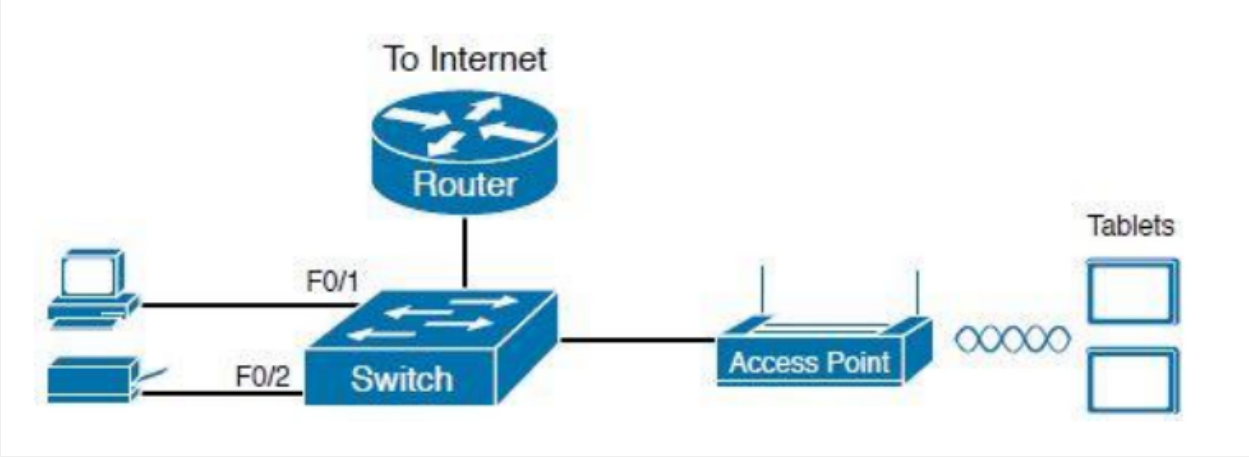
1. Wired (cabled) LANs
2. Wireless LANs

Transmission mediums

- Wired LANs - copper wires or fiber optic cables
  - *Copper wires use electrical circuitry and signals to transmit data*
  - *Fiber-optic cables use light pulses to transmit data*

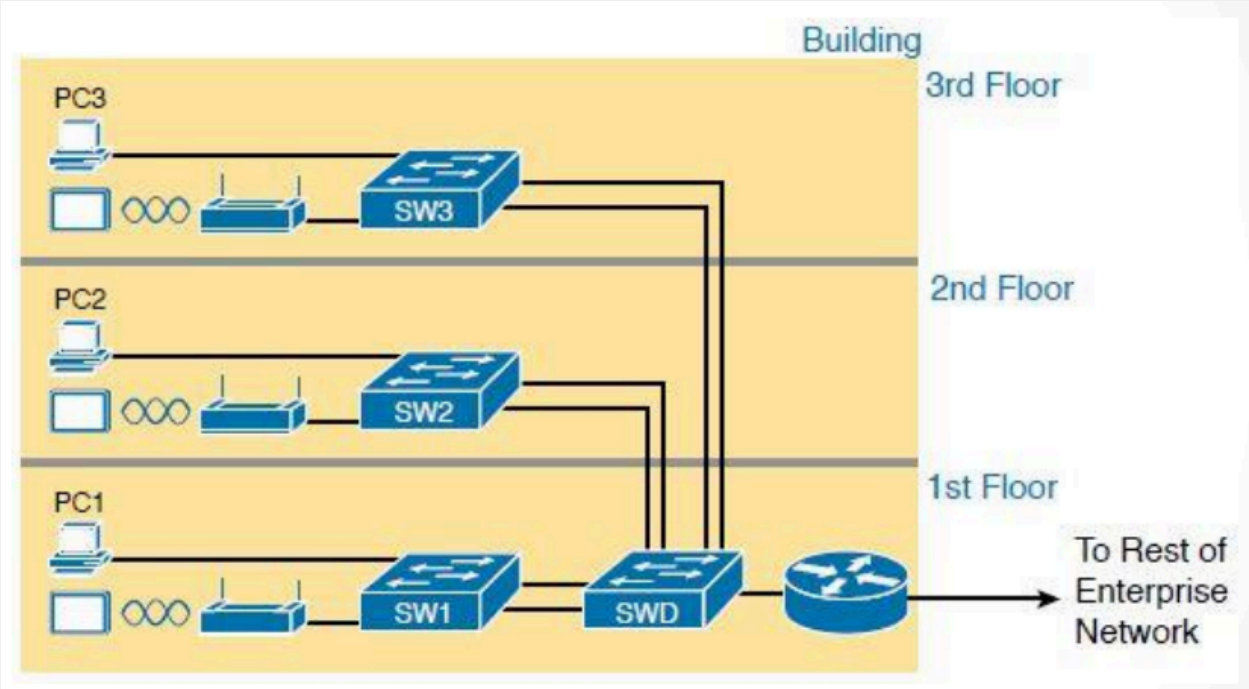
- Wireless LANs - radio waves

A typical SOHO network (Small Office Home Office network)



* Access point - switch එක වගේමයි, හැබැයි wireless

A typical Enterprise network



Ethernet LANs

- wired LAN technology එකේ **Physical** and **Data-Link layers** වලට තියනෙ family of LAN standards.

- local area networks (LANs) වල බහුලව භාවිතා වන technology එකක්.

- IEEE defines Ethernet standards for both DataLink and Physical layers. (IEEE -Institute of Electrical and Electronics Engineers)

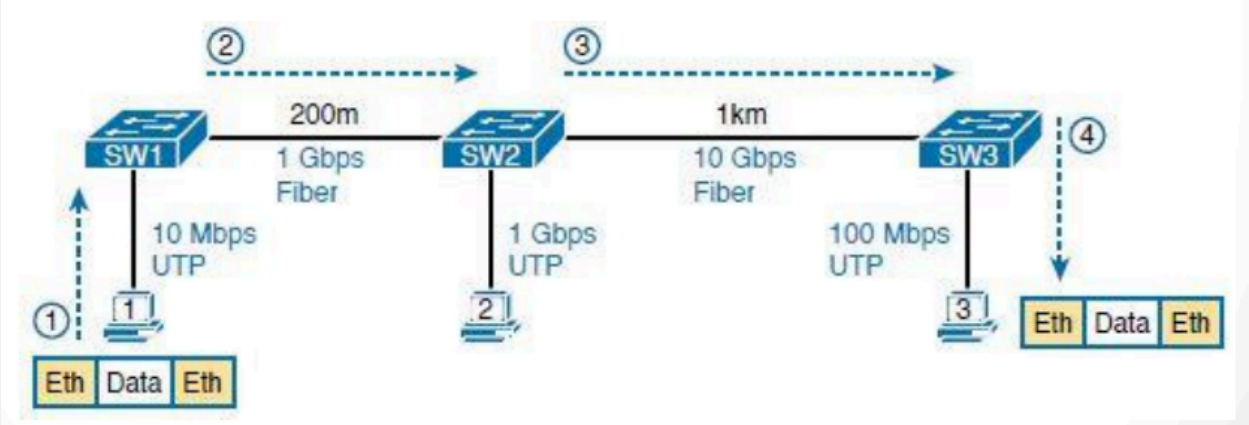
- Ethernet defines a range of standards depending on,
  - Distance
  - Speed
  - cable type

Common Types of Ethernet

Speed	Common Name	Informal IEEE Standard Name	Formal IEEE Standard Name	Cable Type, Maximum Length
10 Mbps	Ethernet	10BASE-T	802.3	Copper, 100m
100 Mbps	Fast Ethernet	100BASE-T	802.3u	Copper, 100m
1000 Mbps	Gigabit Ethernet	1000BASE-LX	802.3z	Fiber, 5000m
1000 Mbps	Gigabit Ethernet	1000BASE-T	802.3ab	Copper, 100m
10Gbps	10 Gig Ethernet	10GBASE-T	802.3an	Copper, 100m

T : Refers to Copper wires (UTP)
X : Refers to Fiber-optic cables

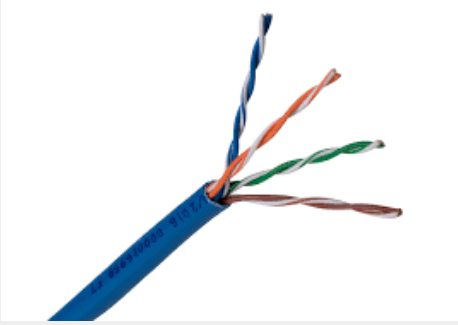
Consistent behavior on all Ethernet standards
Same Data-Link layers standards are used on all types of Ethernet Physical links.



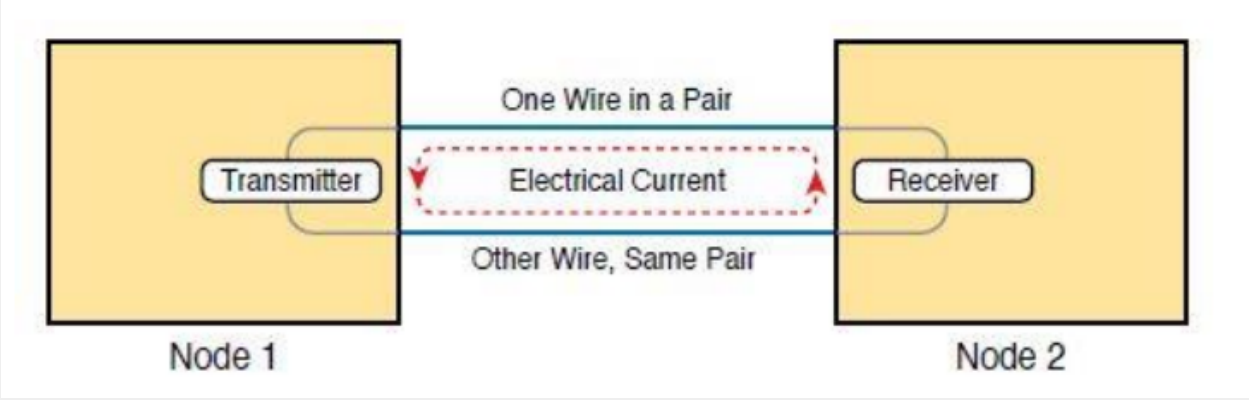
Building physical Ethernet Links

Using UTP Cables

UTP - Unshielded Twisted Pair



Use of UTP cables:

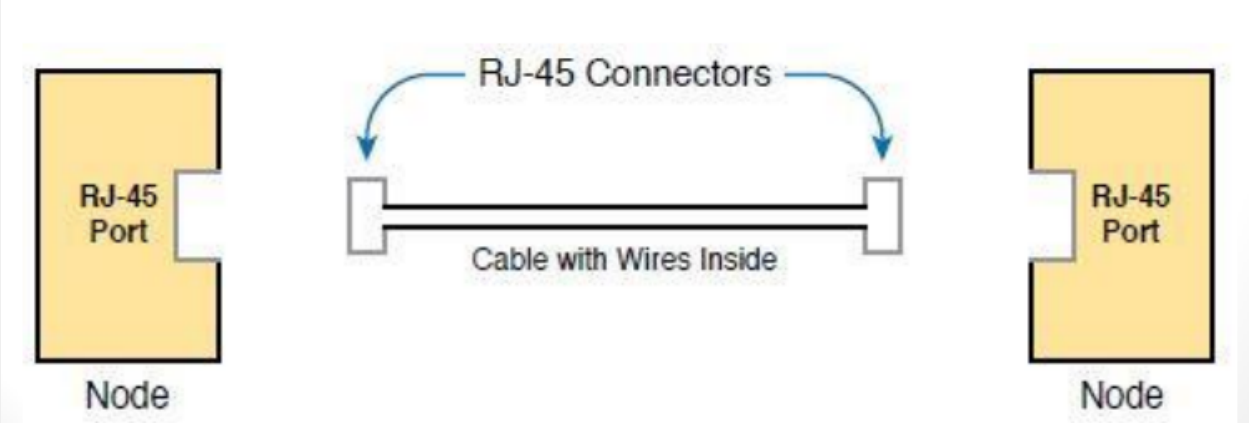


* Data convert කරනෙ 0 & 1 වලට
* Twisting - Electromagnetic Interference වලක්වයි

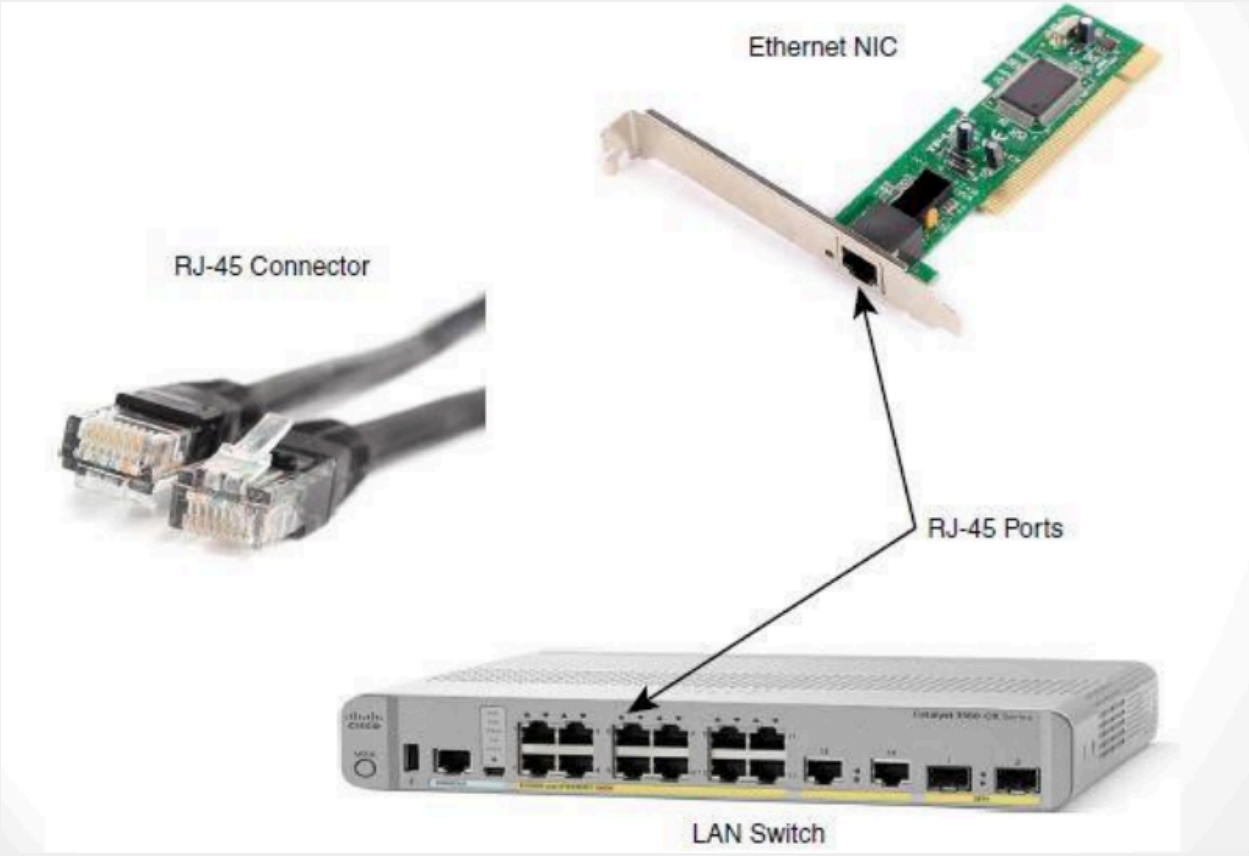
* Node - Network එකට connect වෙන ඕනම device එකක්

Building physical Ethernet Links

- Many Ethernet UTP cables use RJ-45 connectors to connect to devices
- RJ-45 connectors (jacks) has 8 pin positions or simply “pins”



Cables, Connectors and Ports

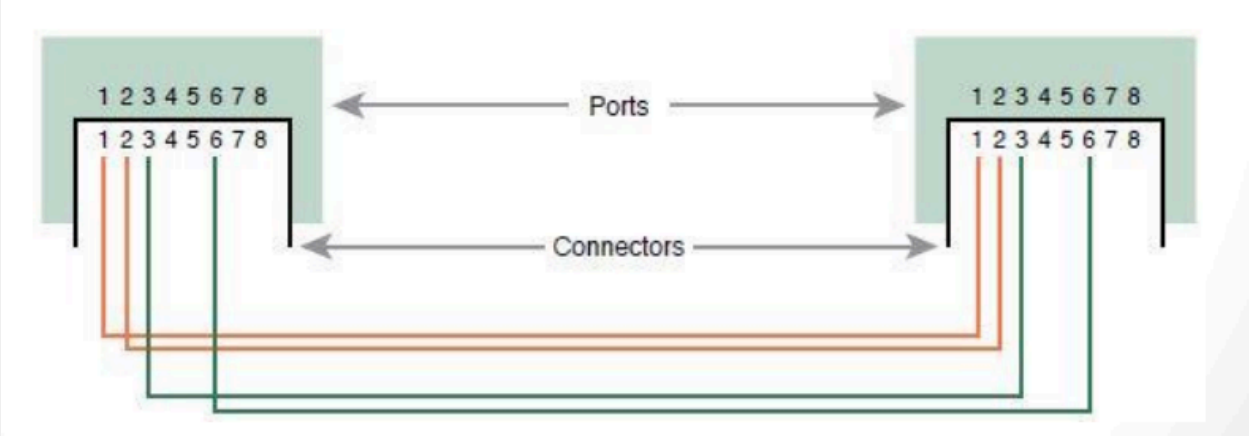


UTP Cabling pinout

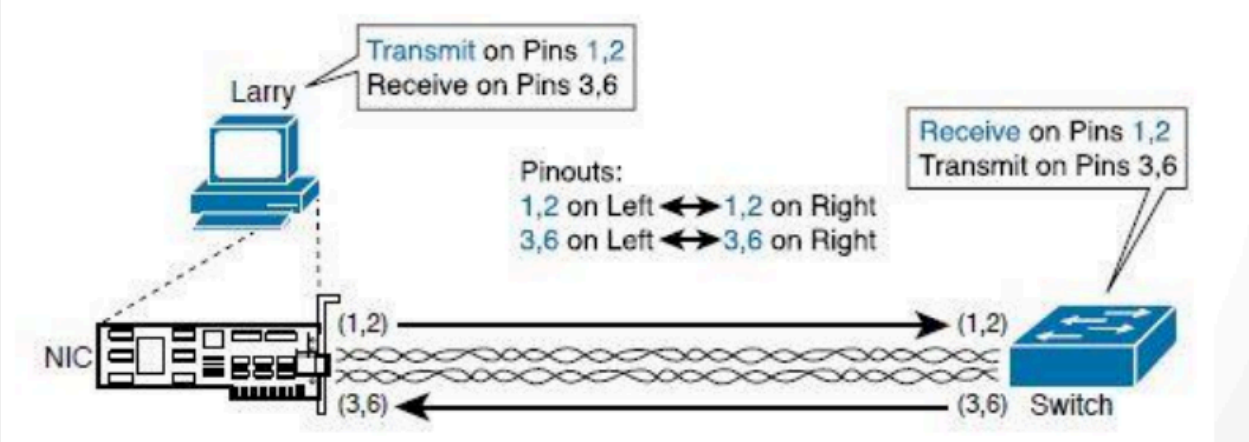
• 10BASE-T, 100BASE-T use 2 pairs, 1000BASE-T use 4 pairs to communicate.
• Between NIC and switch, UTP must use “straight through cable pinout”

UTP Straight-through cables

• Each connects to the same pin number on the other end.

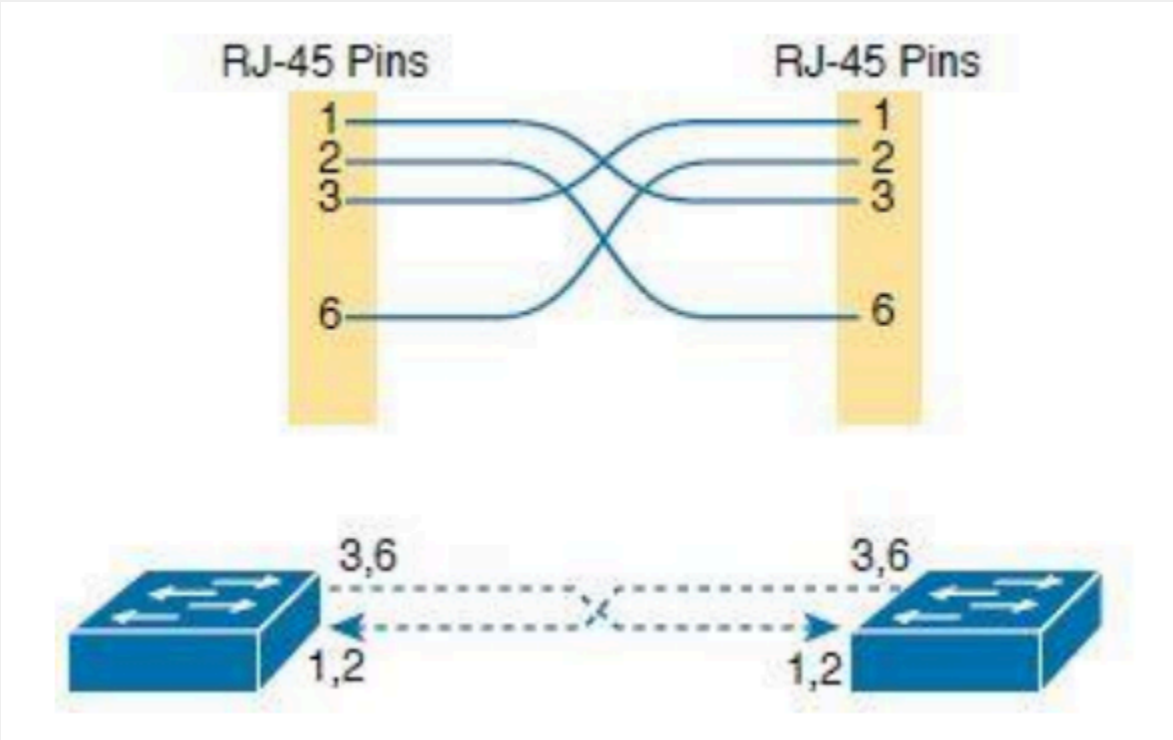


• In summary – A straight-through cable works correctly when the nodes use opposite pairs for transferring (sending and receiving) data
ex: PC & Switch



UTP crossover cables

• Crossover cables are needed to connect “like” devices (devices use the same pin pair for either sending or receiving)



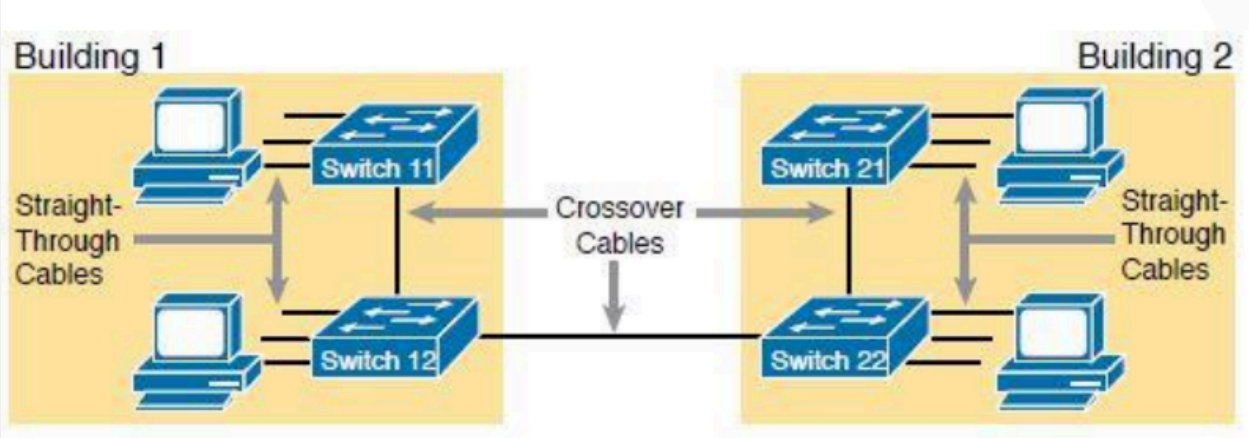
ex: Switch & Switch

Choosing right UTP cabling

• In summary,

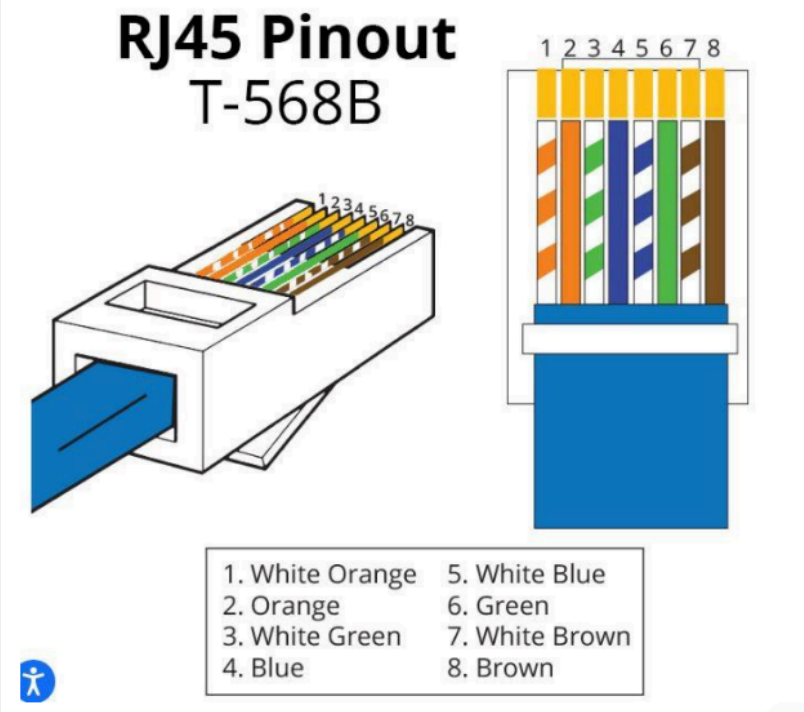
- Straight-through cable: If endpoints transmit on the different pin pairs
- Crossover cable: If endpoints transmit on same pin pairs

Transmits on Pins 1,2	Transmits on Pins 3,6
PC NICs	Hubs
Routers	Switches
Wireless Access Points (Ethernet Interface)	

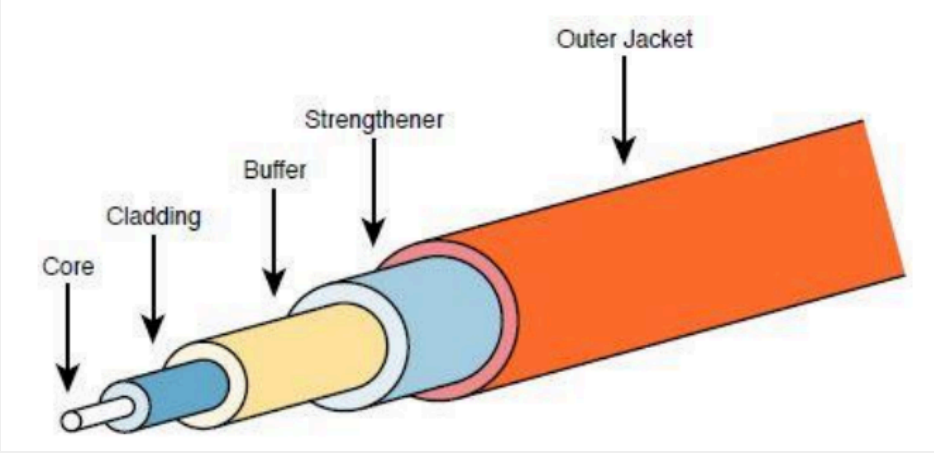


* “**Auto MDI-X**” feature resolves pinout jargon

UTP cabling pinout



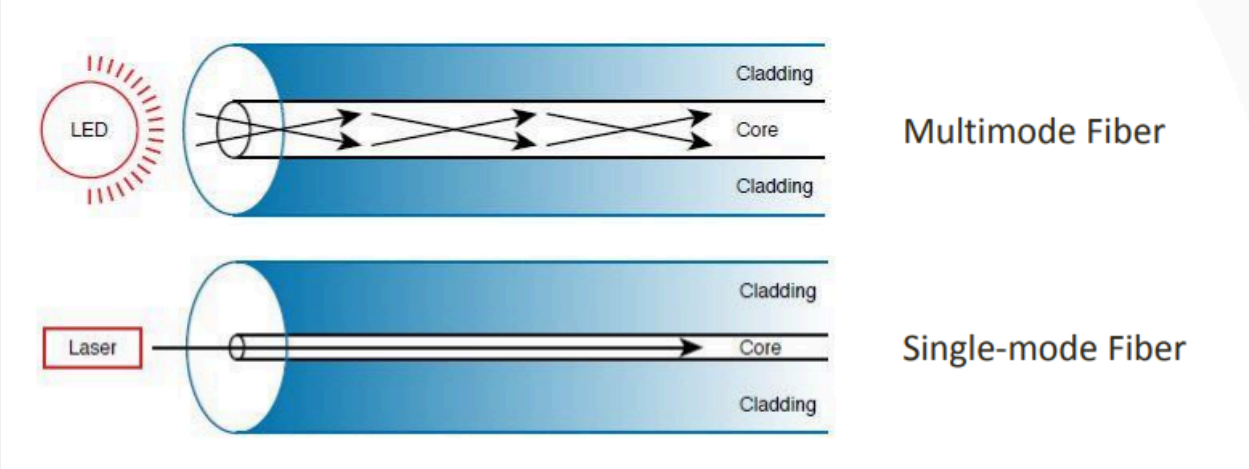
Using Fiber-optic Cables



• Three outer layers (Outer Jacket, Strengthener an Buffer) are for the protection of the cable

• Two inner layers (Cladding and Core) create the environment for transmission of light (data)

Multi-Mode vs. Single Mode Fiber



- SM uses more expensive “optical transmitters” and ports
- SM allows longer cable lengths

Comparison: MM vs. SM

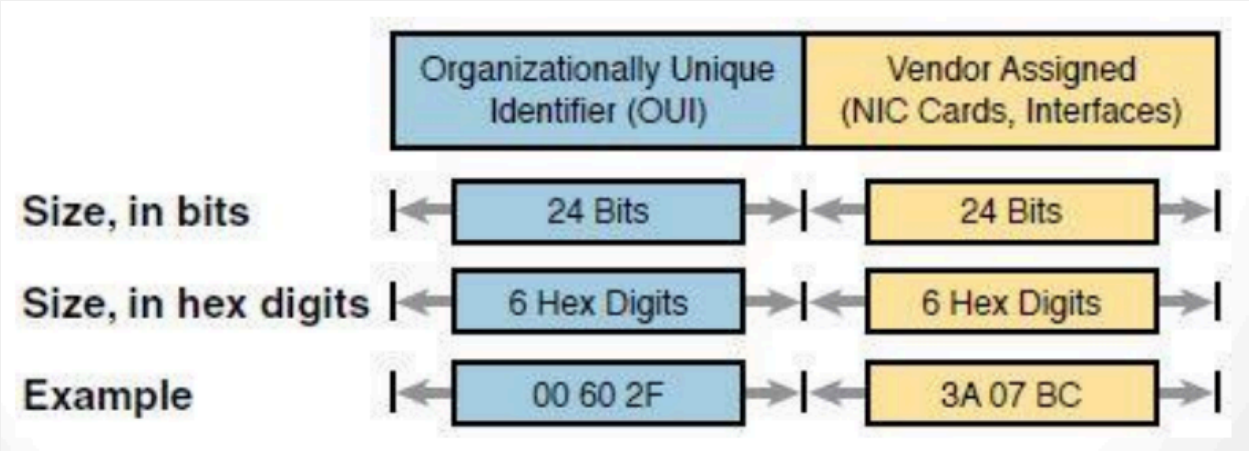
Standard	Cable Type	Max Distance
10GBASE-S	MM	400m
10GBASE-LX4	MM	300m
10GBASE-LR	SM	10km
10GBASE-E	SM	30km

Comparison: MM vs. SM vs. UTP

Criteria	UTP	MM Fiber	SM Fiber
Relative cost of cabling	Low	Medium	Medium
Relative cost of switch port	Low	Medium	High
Approximate maximum distance	100m	500m	40km
Relative susceptibility to interference	Some	None	None
Relative risk of copying from cable emissions	Some	None	None

Ethernet addressing

• Ethernet /MAC (Media Access Control)/Physical addresses are 6 bytes long, usually represented in 12 hexadecimal digits
• MAC addresses are globally unique



Frame Check Sequence (FCS)

• FCS provides a mechanism to receiving node to check the received frames are free of errors

• FCS stores the results of a math formula operated on the sending frame
• Receiving node do the same math formula on the received frame and compare results
• Receiving node discards frame if errors found
• Error **detection only, not error recovery**

Half Duplex / Full Duplex

Half Duplex logic

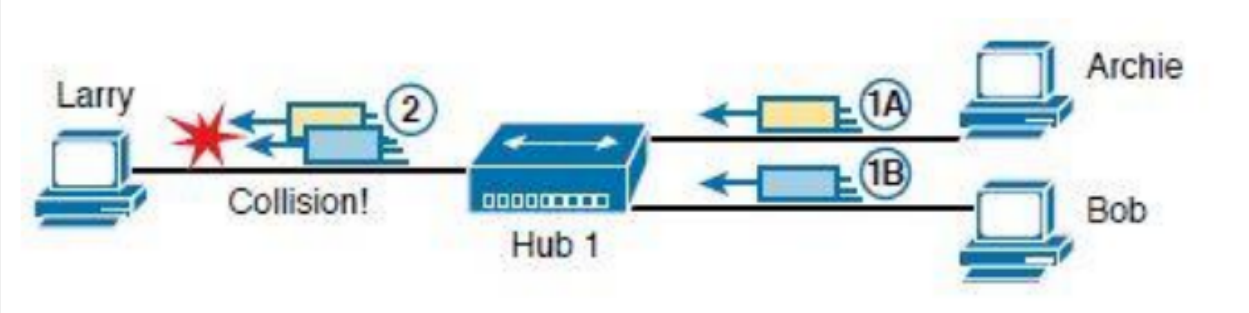
- එකපාර send & receive 2ම කරන්න බෑ.
- Hubs use කරන්නෙ Half Duplex logic.

Full Duplex logic

- එකපාර send & receive 2ම කරන්න පුලුවන්.
- Switch use කරන්නෙ Full Duplex logic.

Half Duplex with Hubs

• Hubs considered to be Layer 1 device, does not use Layer 2 services.
• Hub repeats incoming data out all ports except the incoming port.



Functions of Half Duplex Logic

• Step 1: A device with a frame to send, listens until the Ethernet is not busy
• Step 2: When the Ethernet is not busy, the sender begins sending the frame
• Step 3: The sender listens while sending to discover whether a collision occurs. If a collision is detected,

A. Device send a jamming signal that tell all nodes that a collision happened.
B. Devices independently choose random time to wait before trying again, to avoid unfortunate timing.
C. The next attempt starts again at Step 1

Accessing Network devices

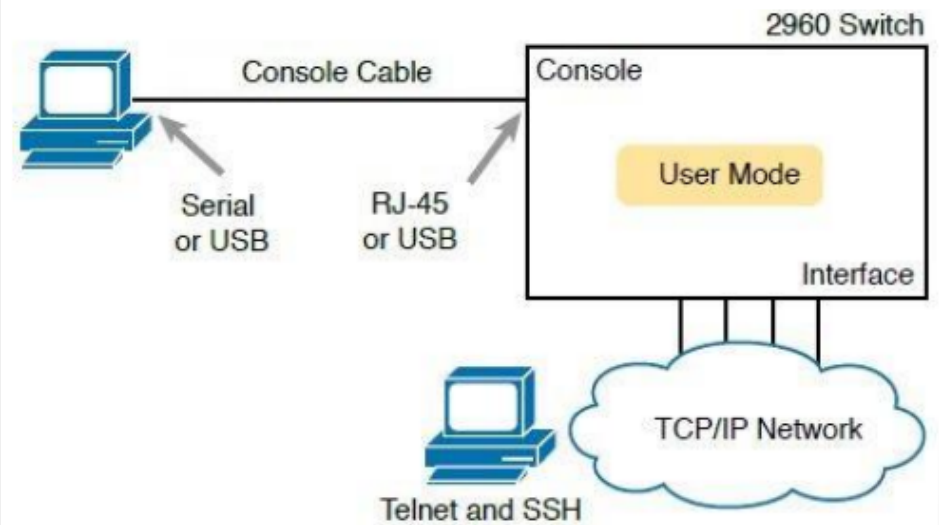
- Network එකක් access කරන්න ඕන ඒකෙ තියෙන device manage, control, monitor, configure කරන්න.

  Network එකක් **access** කරන්න පුලුවන් ක්‍රම
  - Command-line Interface (CLI) **
  - Web interfaces
  - Network management software

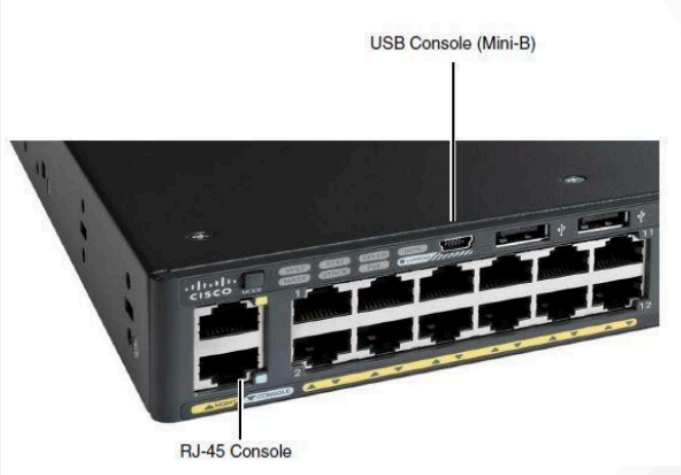
- Enterprise level network devices run වෙන්නෙ open හෝ එයාලගමෙ OS එකක් මත.
  ex: IOS for Cisco (IOS - ciscoලගෙ OS එකක්)

Accessing CLI

Network එකක තියෙන device එකක් access කරන්න තියෙන විදි
- **Console:** Through console port (most powerful & using)
- **Telnet**: Through IP network (security එක අඩුයි)
- **SSH** (Secure Shell) : Through IP network (telnet එක වගේමයි, හැබැයි ඒට වඩා secured)



Physical interface



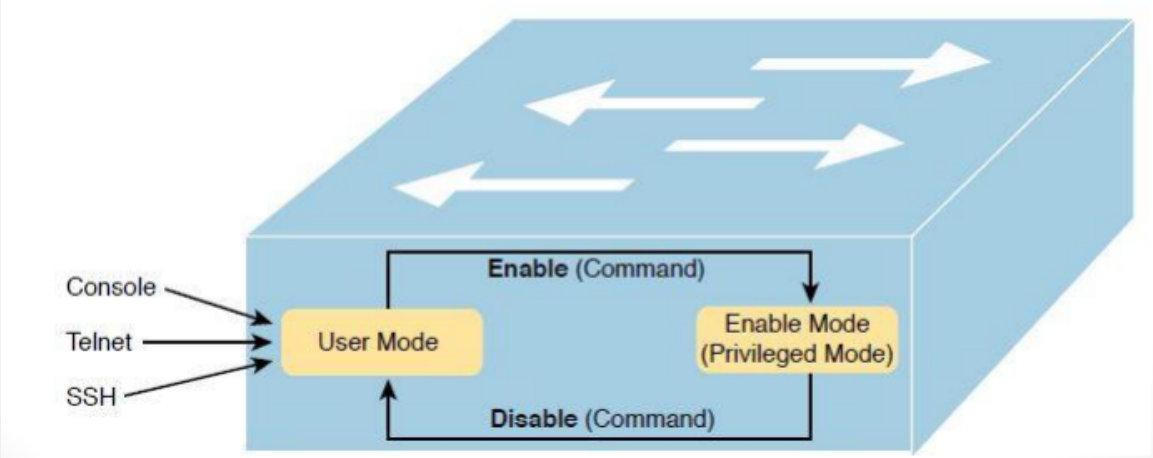
CLI Modes

- User EXEC mode >
- Privileged EXEC mode / Enable mode #

user mode එකේ limited access තියෙනෙ.

enable - user mode එකේ ඉදන් enable mode එකට යන්න
disable - enable mode එකේ ඉදන් user mode එකට යන්න

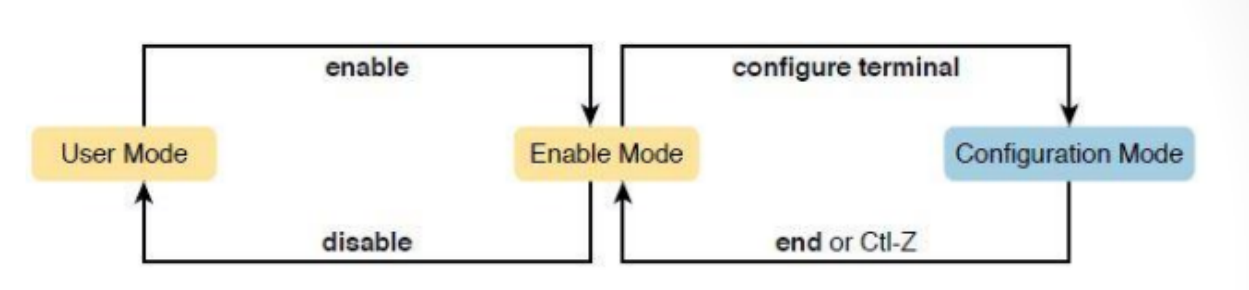
reload - connection එක restart කරනවා (user mode එකේ වැඩ නෑ, enable mode එකේදි reload කරන්න පුලුවන්)



- ඊට අමතරව තව mode තියනවා
  - Global configuration mode
  - Configuration submodes

- **Global configuration mode**

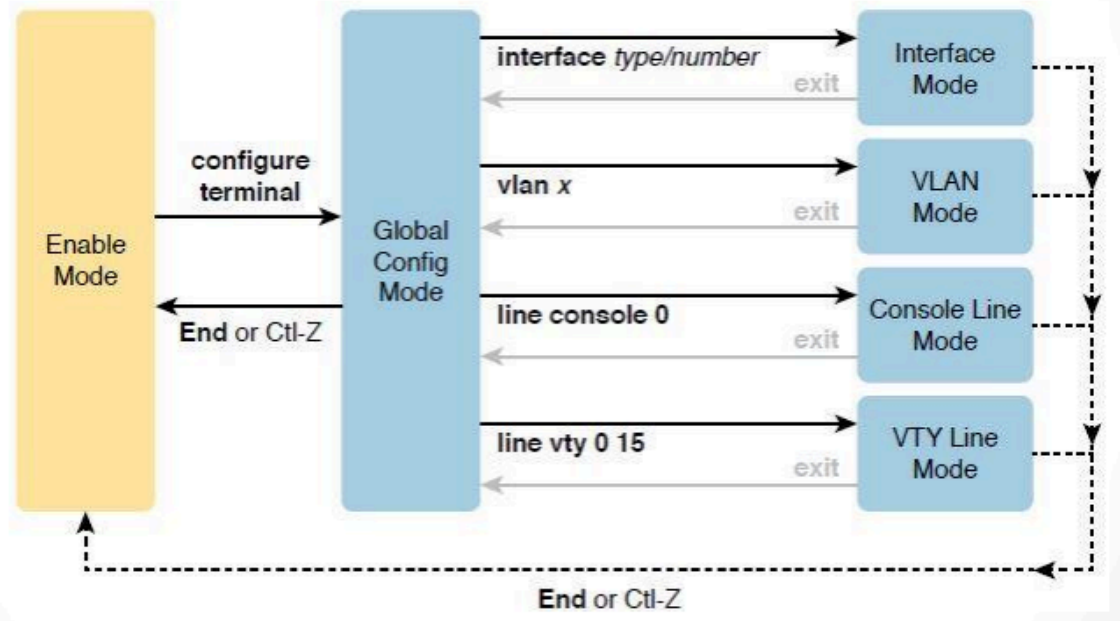
  Device එකේ configuration වනෙස් කරන්න පුලුවන් mode එක




```
Switch>enable
Switch#configure terminal ← command
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ← ඉන්නෙ Global configuration mode එකෙ
```

- **Configuration submode**

  Same kind configuration commands groups




```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#line console 0 ← command
Switch(config-line)# ← ඉන්නෙ console line Configuration sub mode එකෙ
```

Storing configuration files

RAM (random-access memory)

- running (active) configuration files save වෙන්නෙ මේකෙ.
- volatile, fast

Flash memory

- Cisco IOS images save වෙන්නෙ මේකෙ. (Cisco IOS Software එක)
- Non volatile

ROM (Read-only memory)

- bootstrap (or boothelper) store වලො තියන්නෙ මේකෙ.
- Non volatile
- Cisco IOS එක flash එකෙ ඉදන් RAM එකට load කරනෝ.

NVRAM

- startup configuration file save වෙන්නෙ මේකෙ.
- Non volatile, fast
- IOS එක start කරද්දි, switch එක reload කරද්දි, use වෙනේ.

Startup vs Running configurations

Startup-config	Running-config
Stores in NVRAM	Stores in RAM
Non volatile	volatile
initial configuration commands මේකෙ store කරල තියන්නෙ IOS එක start කරද්දි, reload කරද්දි, use වෙනේ.	currently used configuration commands මේකෙ store කරල තියන්නෙ Configuration mode එකෙ ඉදන් කරන වෙනස්කම් අනුව dynamically වෙනස් වෙනේ.

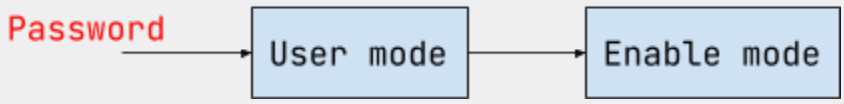
Securing Device CLI

Console access, Telnet access, SSH access, Privileged mode(Enable mode) access control කරන්න පුලුවන් CLI එකනේ.

1st Method: Use of shared passwords

- Console & Telnet usersල එකම password එකක් use කරන්නෙ. (shared password එකක්)

User mode එකට log වෙද්දිම password ඉල්ලන්න




```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#line console 0
Switch(config-line)#password 1234 ← command
Switch(config-line)#login ← shared password එක active කරනෝ
Switch(config-line)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

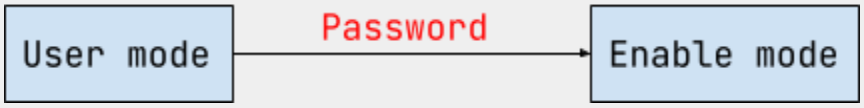
- User mode log වෙද්දි password ඉල්ලන්නෙ

```
User Access Verification

Password:
```

- අයින් කරන්න

```
Switch(config-line)#no password
```

Enable mode එකට log වෙද්දි password ඉල්ලන්න




```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable secret 1234 ← command
```

```
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

- Enable mode එකට log වේදදි password ඉල්ලන්නෙ

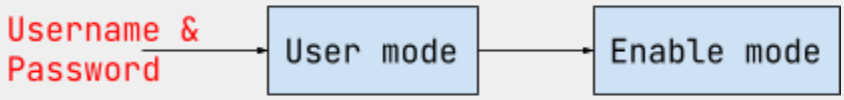
```
Switch>
Switch>enable
Password:
```

- අයින් කරන්න

```
Switch(config)#no enable secret
```

2nd Method: Use of local usernames and passwords

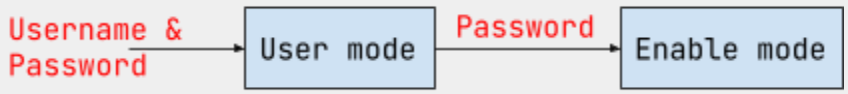
- Console, Telnet, SSH login වෙන්න username & password දෙකෙම ඉල්ලනෙ.
- username & password save වෙන්නෙ locally.




```
Switch(config)#username John secret 1234 ← config user & passwords
Switch(config)#username Tommy secret 1111 ← config user & passwords

Switch(config)#line console 0  ← go to the submode
Switch(config-line)#login local ← active passwords and users
```

```
User Access Verification

Username: John
Password:

Switch>
```

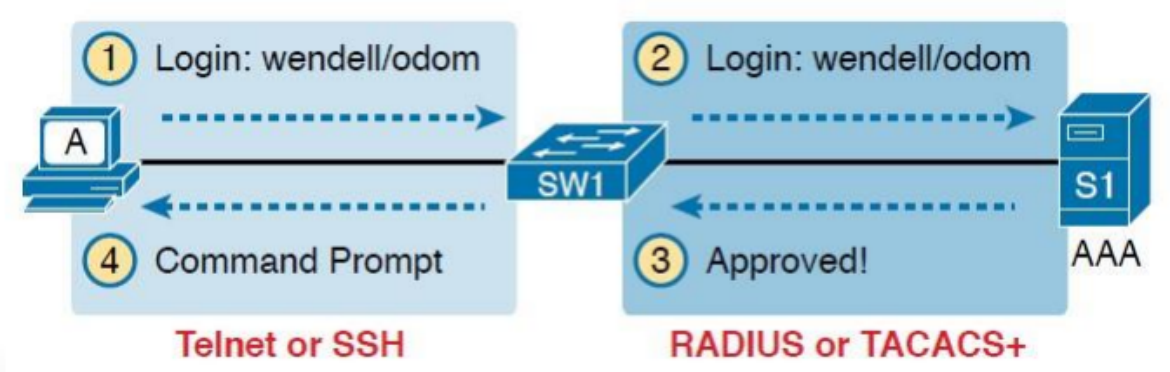
- User mode login password තිබුණ නම් ඒවා replace කරයි.
- Enable mode password replace නොකරයි.




```
User Access Verification

Username: John
Password:

Switch>enable
Password:
Switch#
```

3rd Method: Use of external authentication servers

- external authentication servers වල login data store වෙනෙ. (AAA servers - Authentication, Authorization and Accounting servers)



Useful CLI commands

- show history
  log වුණු mode එකේ ගහපු command පෙන්නනෝ
- exec timeout <mins> <secs>
  exec timeout 0 0
- no ip domain-lookup

වැරදි command execute කරන එක නවත්තනෝ (waiting time එක නැතිකරනෝ).

- no ← command එකකට කලින් දාල command එකනේ වනෙ process එක inverse කරන්න පුලුවන්.
  ex: Switch(config-line)#no password ← User mode login එකේ password අයින් කරනෝ.

Ethernet LAN Switching

Role of a Switch

1. Act as a “place” to connect devices to the LAN
2. **Forward (switch) frames to the correct device** ⇐ The primary role

(Lan එකේ devices වලට Network එකට connecting places දනෙෝ,
හරි device එකට frames forward කරනෝ)

Switches use Layer 2 logic.
Switches, OSI model එකේ 2nd layer හෝ TCP/IP model එකේ Data Link layer එකේ ක්‍රියාත්මක වන network devices වේ. එම layer එකේදි switch කරන කාර්යයන් Layer 2 logic වේ.

- MAC Address Learning
- Forwarding and Filtering
- Frame Flooding and Filtering
- Virtual LAN (VLAN) Support
- Loop Avoidance

Default Switch configurations

- All interfaces are enabled, ready to start working and switching.
- All interfaces are assigned to VLAN1
- 10/100 and 10/100/1000 interfaces use auto negotiation
- MAC learning, forwarding, flooding logics work
- STP is enabled

How do switches work?

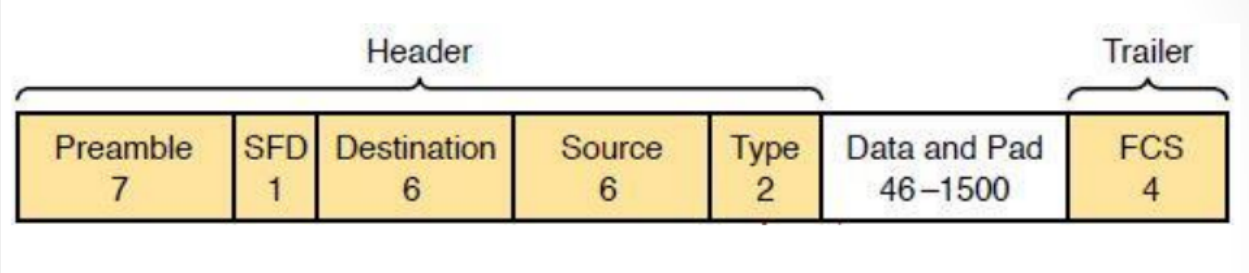
Switch එකේ main role එක කරගත්න, steps 3ක් අනුගමනය කරයි.

1. Destination MAC address එක අනුව, frame එකක් forward කරන්න/නොකරන්න ඕන port තීරණය කරනවා.
2. එක් එක් frame වල Source MAC address එක පරීක්ෂා කරලා, “learning MAC addresses” & Prepare to forward.
3. Preparing to forward only one copy of the frame to the destination by creating a loop free environment (using STP - Spanning Tree Protocol)

See ⬇ LAN Switching summary
https://docs.google.com/document/d/19bhhaxQBiD_euK2iCALqt03dQrnde77oZGhx6aIwLSo/edit#heading=h.k2slnbnxa93n

Frame structure

- Header එකයි trailer එකයි add වුනේ data link layer එකේදී.



- **Destination MAC Address**
  - receiver ගෙ MAC address එක
  - data forwarding වලදි වැදගත්

- **Source MAC Address**
  - sender ගෙ MAC address එක
  - MAC address table එක build කරද්දි වැදගත්

- 2ම 6 bytes long.

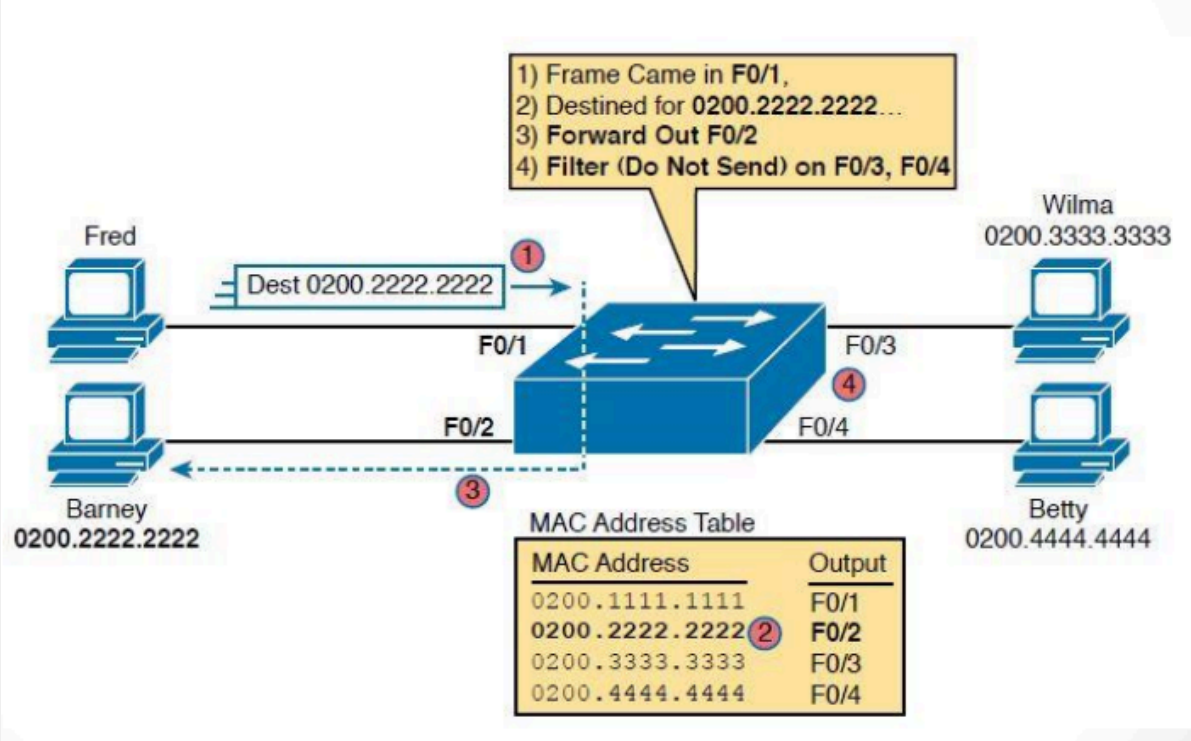
MAC Address table

- Table එක Dynamically built by switches, Maintain කරන්නේ switches. (dynamically හදාගන්නෙ device plug කරද්දිම)
- Table එකේ entry එකක තියනෙෝ, switch එකට connect කරපු device එකේ MAC address, ඒකට අදාල switch එකේ interface(port) එක.

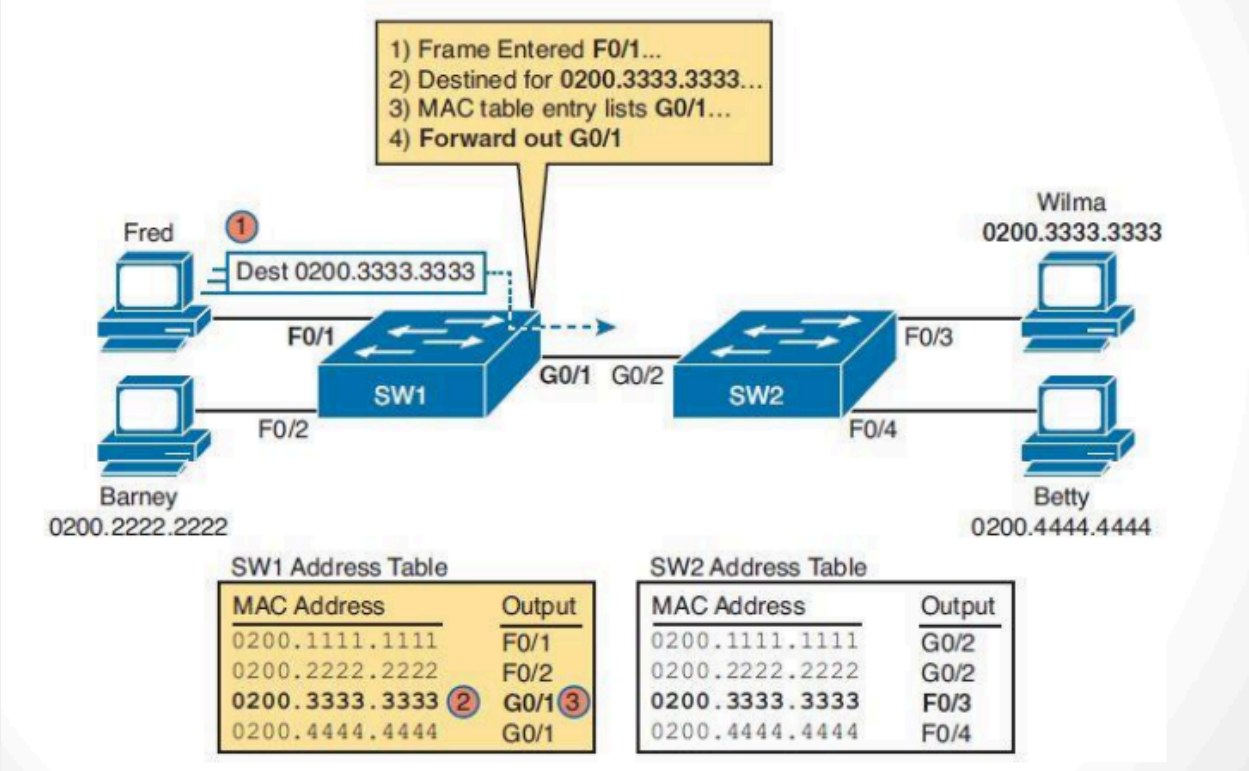
```
Switch#show Mac Address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0006.2a31.1881    DYNAMIC     Fa0/3
   1    000a.4147.a672    DYNAMIC     Fa0/2
   1    000c.8569.767e    DYNAMIC     Fa0/3
```

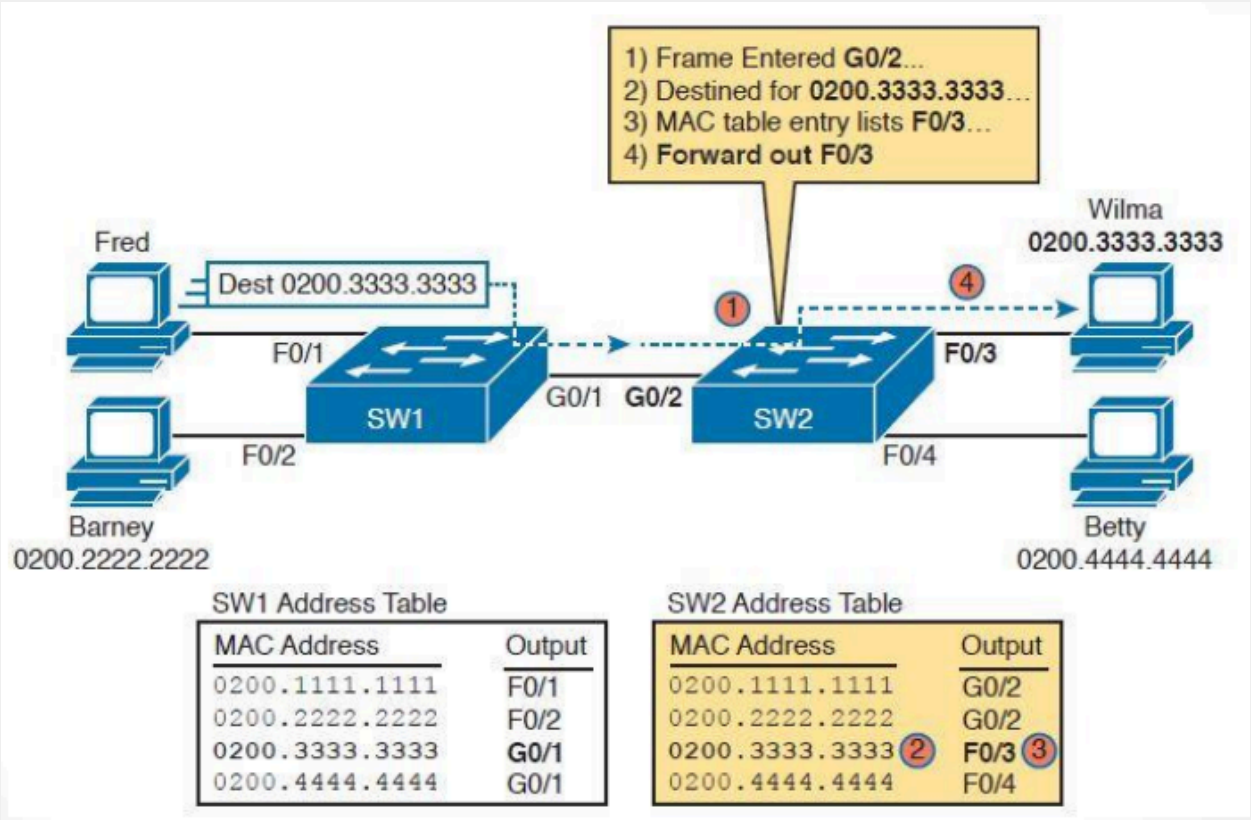
- Destination MAC address එක, MAC address table එකේ entries එක්ක compare කරලා බලනෙෝ. ඒ අනුව switch එක තීරණය කරනෙෝ මොන port එකෙන්ද frames යවන්නෙ/ යවන්නෙ නැත්තෙ කියල. (forward or filter out)
- Destination MAC address එක, MAC address table එකේ නැත්නම්, “flooding” process එක වනෙෝ.
- **Flooding** - incoming port එක හැර අනිත් port හැම එකකටම frame එකේ copies forward කිරීම.

Forwarding with One switch



Forwarding with multiple switches



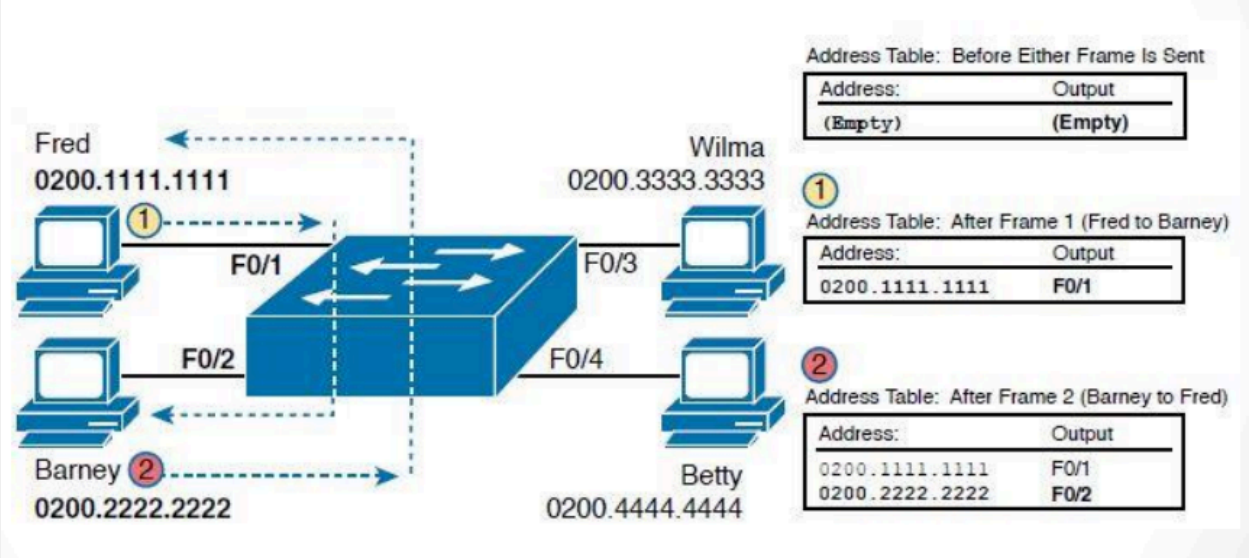


Learning MAC addresses

- Incoming frame වල **Source MAC addresses** base කරගනෙ MAC address table එකට entries දාගන්නෙ.
- Frame එකක් receive වනෙ හැම පාරම, switch එක, frame එකේ source MAC address එක බලනෙ.

- Incoming frame එකක source MAC addresses එක **table** එකෙ නැත්නම්, ඒක table එකට දාගන්නෙ. interface (port) එකත් එක්කම.

- එකම MAC address එක, port එක වනෙස් වලො තිබුනොත් (ex : device එක ගලවලා වනෙ port එකකට set කරලා),
  table එක update කරගන්නෙ අලුත් interface(port) number එක දාල.



Managing MAC Address Table

- Switch එක remove කරනෝ MAC Address Table entries,
    - Aging
    - user commands අනුව.

- Aging
    - Switch එකට අලුත් MAC address එකක් ලැබුනොත්/ දන්න එකකින් frame එකක් receive වුනොත්, inactivity timer → 0 කරනෝ.
    - pre-defined time range එකක් ඇතුලත use නොකරපු entries, remove කරනෝ.
    - Table එක full නම්, aging අනුව පරණම entries අයින් කරනෝ.

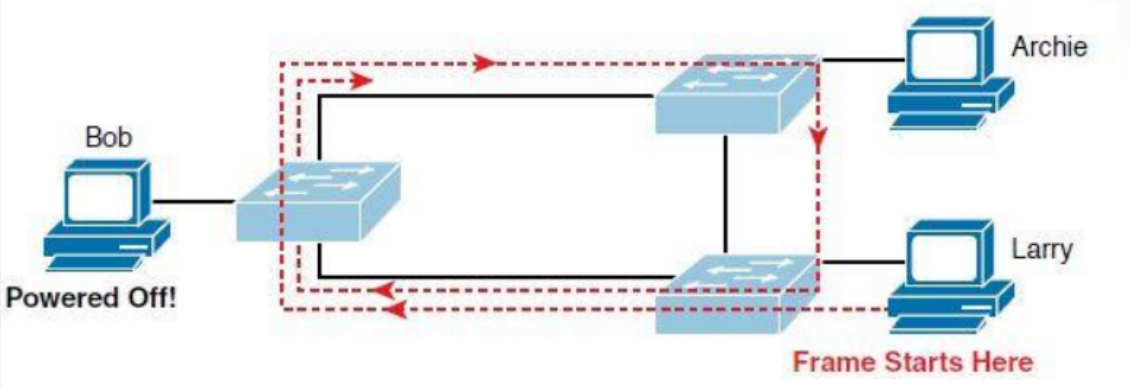
- user commands
    - **#clear mac address-table** ← හැම entry එකම remove කරනෝ
    - **#clear mac address-table dynamic** ← dynamic entry විතරක් remove කරනෝ

(dynamic - port එකට ඕනම device එකක් set කරන්න පුලුවන්.
Static - port එකට set කරන්න පුලුවන් කලින් define කරපු MAC address තියනෙ device එක විතරයි. ex: printer එකක් set කරන port එකක්)

Unicast | Broadcast | Multicast

Unicast - network එකේ එක්කනොටයි යවන්න ඕන.
Broadcast - හැමෝටම යවන්න ඕන.
Multicast - selected අයට යවන්න ඕන.

Avoiding Loops using STP



- හරි mechanism එකක් නොතිබුනොත්, network එකක තියනෙ redundant(අමතර) links , indefinite loops create වලො network එක unusable වෙන්න පුලුවන්.
- **STP - Spanning Tree Protocol**
  සමහර ports block කිරීමෙන්, Unknown unicast හෝ broadcast Frames මගින් සැදු indefinite loops ඉවත් කරයි.

LAN Switching summary

හරි device එකට frames forward කරන්න (main role of switch), switches steps 3ක් අනුගමනය කරයි.

Step 01
Switches frames forward කරන්නෙ **frames** වල **Destination MAC address** එක අනුව.

Destination MAC address එක;

a) known unicast නම්,
MAC address table එකේ තියනෙ outgoing port එකයි, frame එක එන incoming port එකයි ;

- වෙනස් නම්,
  outgoing port එකට frame එක forward කරනො.

- සමානයි නම්,
  Frame එක ignore කරනවා.(because same device)

b) Unknown unicast හෝ broadcast නම්,
   switch floods the frame.
   (flooding - incoming port එක හැර අනිත් port හැම එකකටම frame එකේ copies forward කිරීම.)

Step 02

Learn MAC address table entries

a) හැම receiving frame එකකම source MAC address එකයි port එකයි check කරනවා.

b) MAC address table එකේ නැත්නම්, ඒක add කරගන්නවා.

Step 03

Stop indefinite loops using STP (Spanning Tree Protocol)

(සමහර ports block කිරීමෙන්, Unknown unicast හෝ broadcast Frames මගින් සැදුණු indefinite loops ඉවත් කරයි.)

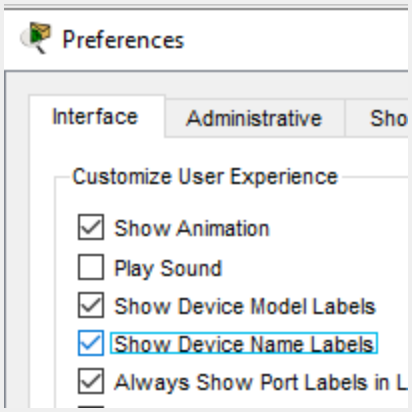
Practical

🔗Forwarding_Frames.pkt

ping command

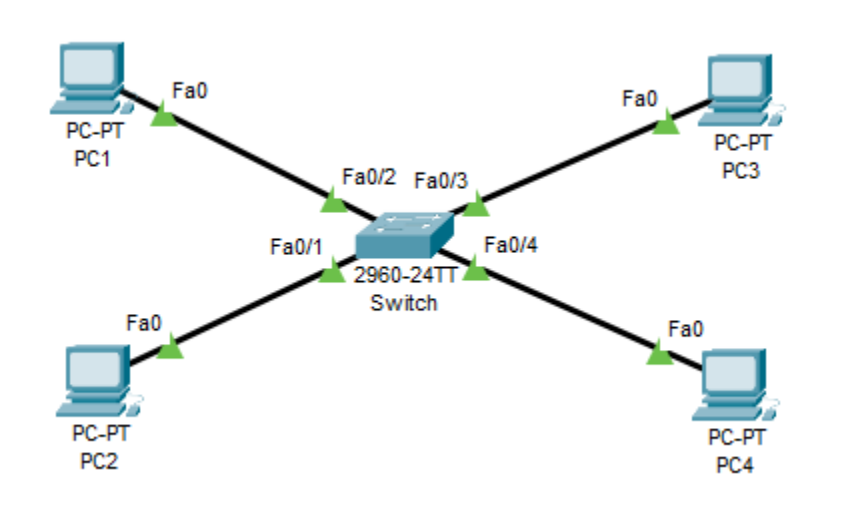
- Network එකක connectivity check කරන command එක.
- Checking msg 4 පාරක් sent කරනවා. එක device එකකින් Reply 4ක් එනවා නම් connectivity එක success නම්.
- ping 192.168.1.002 ← අදාල IP එකත් එක්ක connectivity check කරනවා
- ping 192.168.1.255 ← connect වලා තියනෙ හැම device එකක එක්ක connectivity check කරනවා

Show device labels
Option → Preferences → Interface →

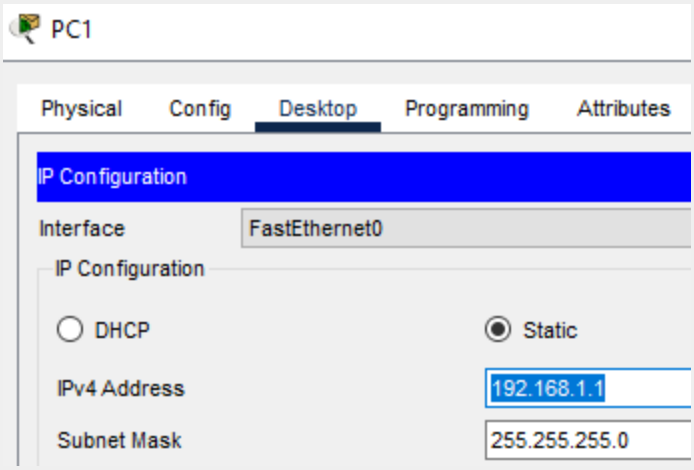


1. Forwarding Unknown Unicast Frames

a. with One switch



- Change IP address
  Click PC1 → Desktop → IP Configuration



Do the same for other PCs.

PC1 IP - 192.168.1.1
PC2 IP - 192.168.1.2
PC3 IP - 192.168.1.3
PC4 IP - 192.168.1.4

- clear mac address-table in switch (Unknown කරන්න)

```
Switch>enable
Switch#clear mac address-table
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

- Click PC1 → Desktop → Command prompt
  ping 192.168.1.2

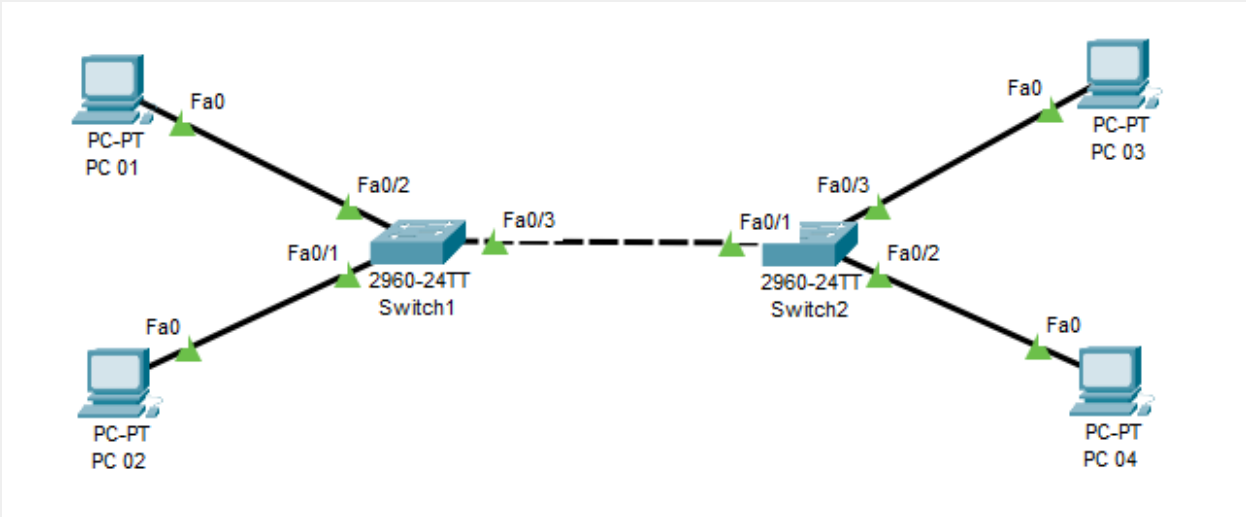
```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Switch

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0005.5e5c.ac38    DYNAMIC     Fa0/1
   1    00d0.bc68.32c3    DYNAMIC     Fa0/2
```

(PC1 → switch එකට sent msg එකේදී PC1 MAC address එක,
PC2 → switch එකට receive msg එකේදී PC2 MAC address එක,
Table එකට add කරගන්නවා [Learning MAC addresses])

b. with Multiple switches



- Change IP address
- clear mac address-table in switch 1

```
Switch>enable
Switch#clear mac address-table
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0040.0b8e.4601    DYNAMIC     Fa0/3
```

- clear mac address-table in switch 2

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

- ping PC 01 to PC 04

```
C:\>ping 192.168.1.104

Pinging 192.168.1.104 with 32 bytes of data:

Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128
Reply from 192.168.1.104: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Switch 01

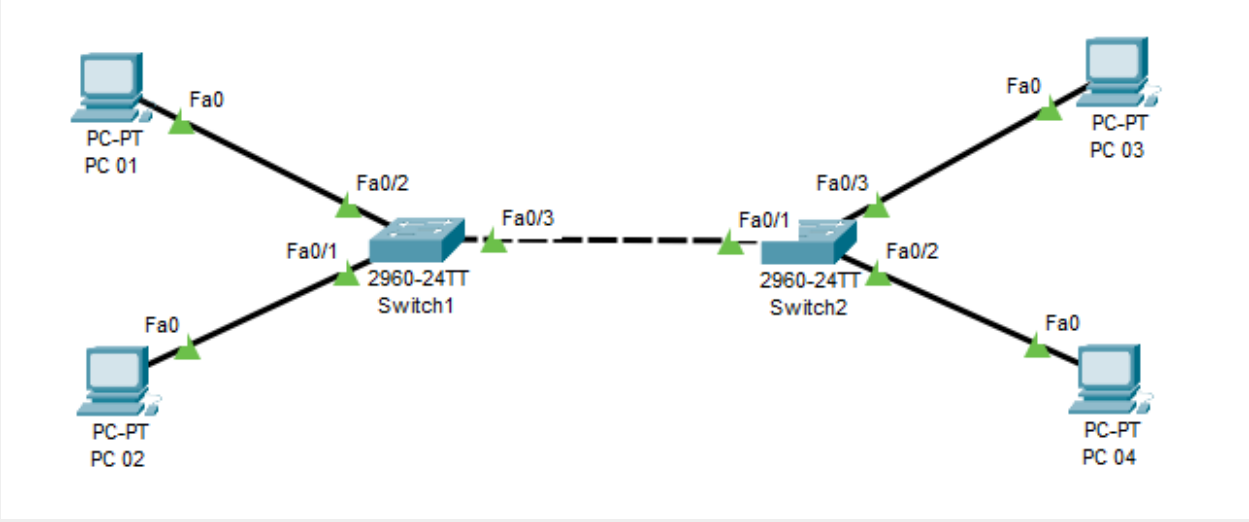
```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0006.2a31.1881    DYNAMIC     Fa0/3
   1    000a.4147.a672    DYNAMIC     Fa0/2
   1    0040.0b8e.4601    DYNAMIC     Fa0/3
```

- Switch 02

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0006.2a31.1881    DYNAMIC     Fa0/2
   1    000a.4147.a672    DYNAMIC     Fa0/1
   1    000a.4188.d503    DYNAMIC     Fa0/1
```

(switch එකට සාපේක්ශව port number දාගන්න)

2. Broadcast frames



ඕනම PC එකක console එකෙ,
ping 192.168.1.**255**

```
C:\>ping 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.13: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.13: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.13: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.13: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 4, Received = 12, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Switch එකෙන් අනිත් PC වලට copies යවන්නෙ.

Revising LAN concept

The definition of a LAN
same **broadcast** domain එකක තියෙන devices.

Segregating LAN (Lan වෙන් කිරීම)

Why segregating/separating LAN networks?

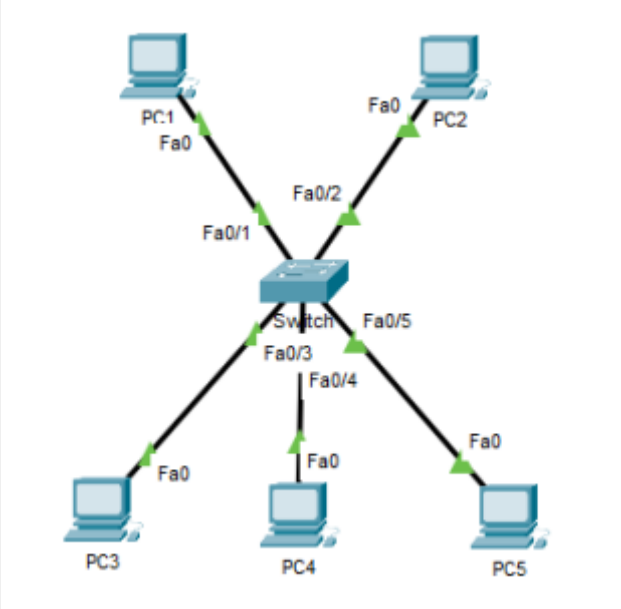
- CPU overhead එක අඩු කරගන්න. (Lan එකේ අනවශ්‍ය අයට data යන එක නවත්තන්න)
- Security risk එක අඩු කරන්න.
- එක එක host වලට වෙනස් security දෙන්න
- Users ල department වලට කඩන්න
- Troubleshoot කරන්න

Concept of VLAN

තනි device එකක් logically **broadcast** domain වලට බෙදීම.
(Virtual lan වලට)

Switch#show interfaces status ← interfaces වල status බලාගන්න

VLANs on single device



- Assign IP's for each devices
- `Switch#show vlan brief` ← device එකේ දැනට හදල තියෙන vlans බලාගන්න පුලුවන්.

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

- VLAN කඩන්නෙ නැතුව එක PC එකක ඉදල ping command එක ගහල broadcast msg එකක් (192.168.1.255) යැව්වොත්,

Sent → 4
Receive → 16 (target device 4 * 4)

- VLAN 2කට වනේ කිරීම

```
Switch(config)#vlan 2   ←අලුත් VLAN එකක් හදන්න
Switch(config-vlan)#name QA-team  ←VLAN එකට නමක් දෙන්න
```

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
2    QA-team                           active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

අලුත් VLAN එකක් හැදෙනෙ QA-team කියල. ඒකට ports configure කරල නෑ.

- VLAN 2 වලට ports assign කිරීම

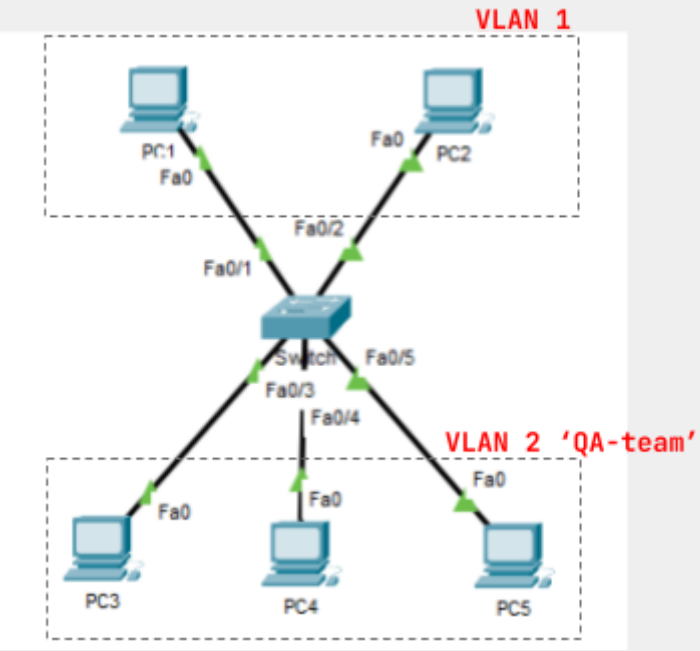
`Switch(config)#interface fa0/3` ← interface FastEthernet 0/3 වල configuration mode එකට යන්න.

`Switch(config-if)#switchport access vlan 2` ← port එක assign කරනෙ VLAN 2 වලට

// Interface range එකක් එකපාර assign කරන්න

```
Switch(config)#interface range fa0/3-5
Switch(config-if-range)#switchport access vlan 2
```

```
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/6, Fa0/7
                                                   Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                   Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                   Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                   Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                   Fa0/24, Gig0/1, Gig0/2
2    QA-team                             active    Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
```



දැන් ping command එක ගහල broadcast msg එකක් (192.168.1.255)

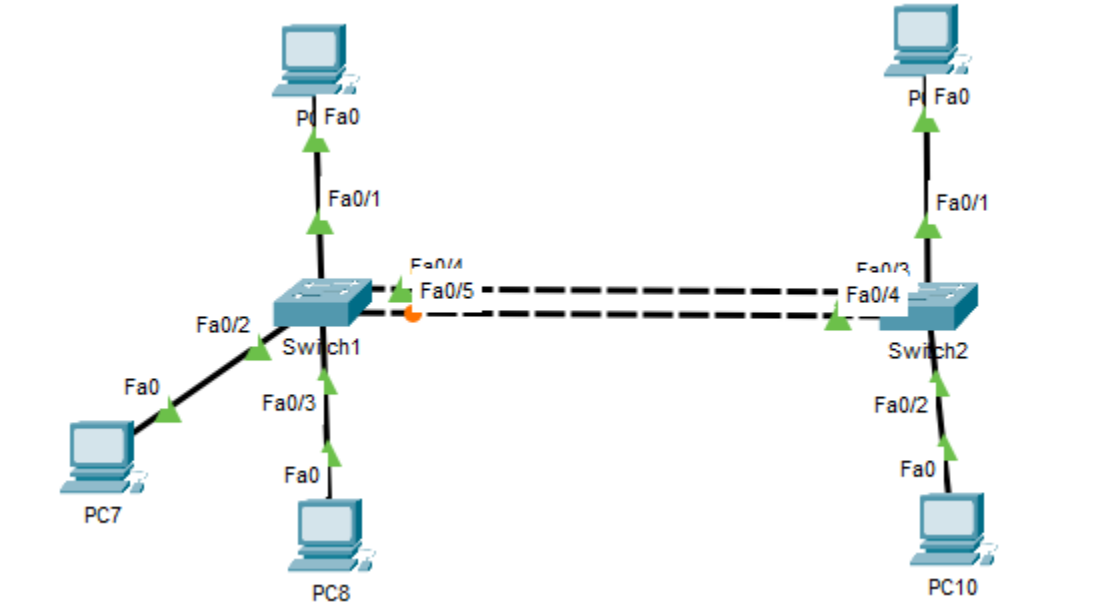
- PC 1 වල ඉඳන් යැව්වොත්,
  Sent → 4
  Receive → 4 (target device 1 * 4)

- PC 3 වල ඉඳන් යැව්වොත්,
  Sent → 4
  Receive → 8 (target device 2 * 4)

VLANs on multiple devices

🔗VLANs.pkt

1) Using two links to connect two LANs



Switch 1 & 2 (before separation)

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

- Ping broadcast msg (192.168.1.255)
  Sent → 4
  Receive → 16 (target device 4 * 4)

Switch1

- VLAN 2කට වනේ කිරීම

```
Switch(config)#vlan 2
```

- VLAN 2 වලට ports assign කිරීම

```
Switch(config)#
Switch(config)#interface fa0/2
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fa0/3
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fa0/5
Switch(config-if)#switchport access vlan 2
```

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
2    VLAN0002                         active    Fa0/2, Fa0/3, Fa0/5
1002 fddi-default                     active
1003 token-ring-default               active
```

Switch2

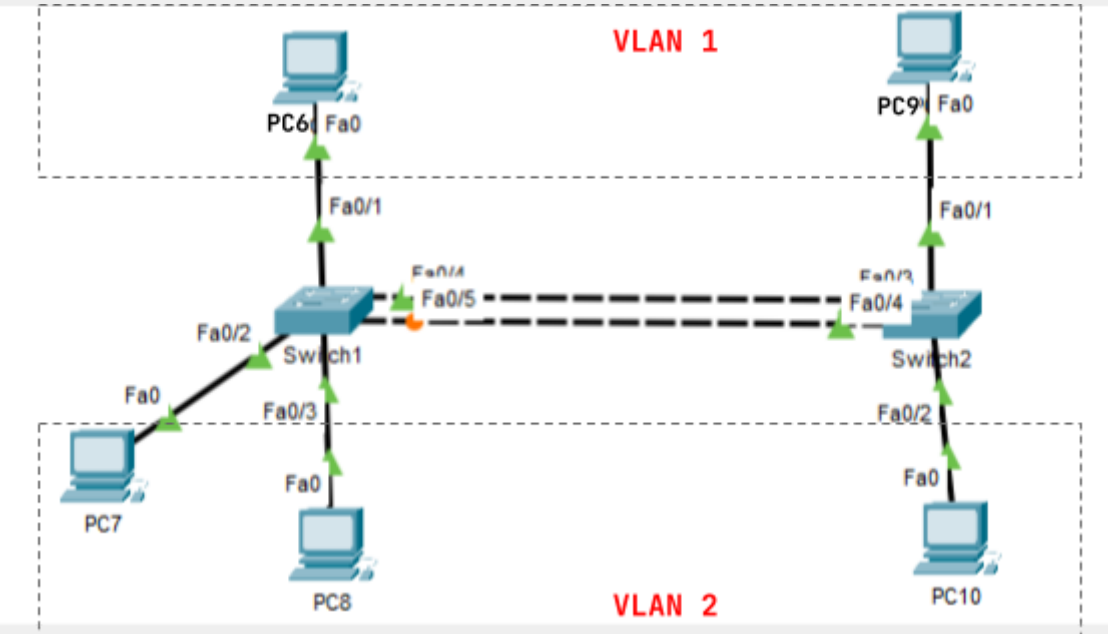
- Switch 1 වල විදියමයි.

```
Switch(config)#vlan 2
```

```
Switch(config)#interface fa0/4
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fa0/2
Switch(config-if)#switchport access vlan 2
```

```
show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
2    VLAN0002                         active    Fa0/2, Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
```

- **Switch 1 FA0/5 , Switch 2 FA0/4 ports, VLAN 2 connect** කරන්න **use** කරල තියෙන්නෙ,



Ping broadcast msg (192.168.1.255)

- **from PC7**
  Sent → 4
  Receive → 8 (target device 2 * 4)

- **from PC9**
  Sent → 4
  Receive → 4 (target device 1 * 4)

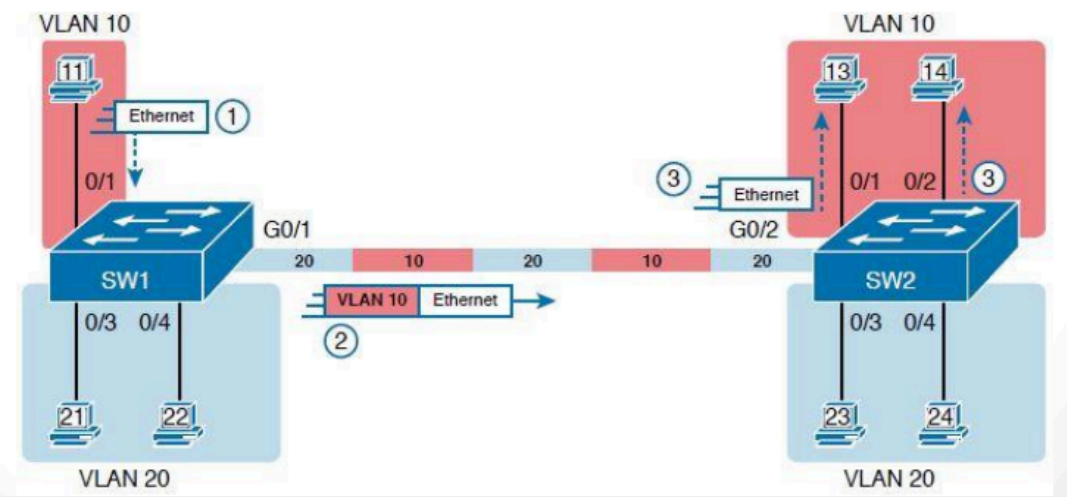
2) Using one link to connect two LANs

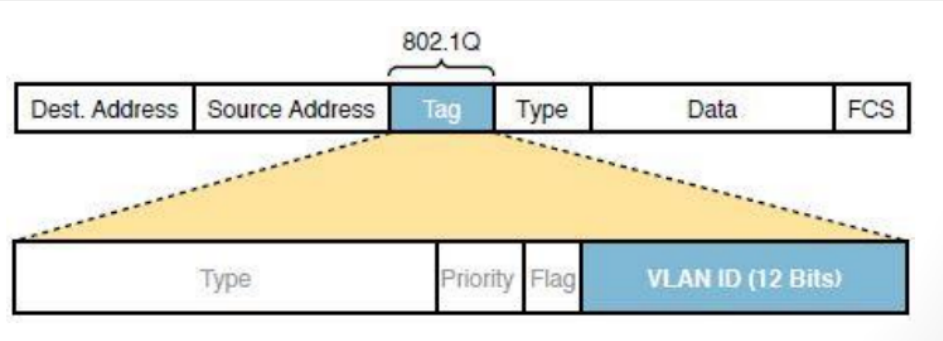
VLAN Trunking

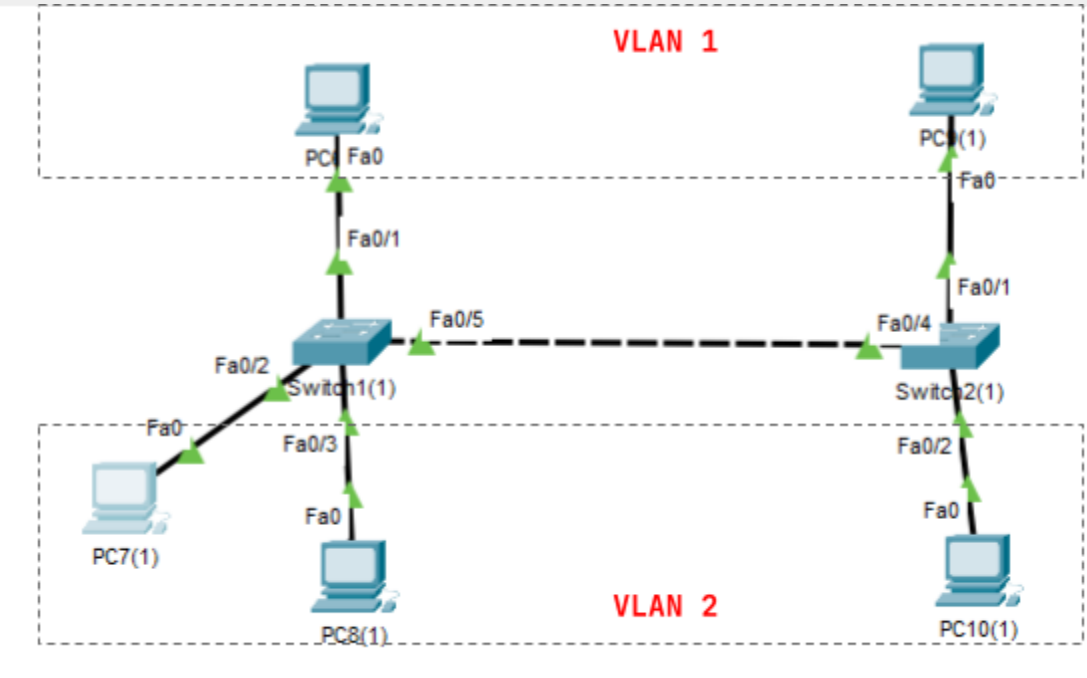
එක link එකකින් VLAN ගොඩකට connection හදාගන්නෝ.

VLAN Tagging

VLAN එකේ අදාල device එකට යවන්න, frames වල header tag කරල තියනේනෙ.







- **Switch(config-if)#switchport mode trunk**

```
Switch(config)#interface fa0/5
Switch(config-if)#switchport mode trunk
```

```
Switch#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          auto    auto  10/100BaseTX
Fa0/2                        connected    2          auto    auto  10/100BaseTX
Fa0/3                        connected    2          auto    auto  10/100BaseTX
Fa0/4                        notconnect   1          auto    auto  10/100BaseTX
Fa0/5                        connected    trunk      auto    auto  10/100BaseTX
Fa0/6                        notconnect   1          auto    auto  10/100BaseTX
Fa0/7                        notconnect   1          auto    auto  10/100BaseTX
```

Switch 2ටම කරන්න ඕන.

```
Switch(config)#interface fa0/4
Switch(config-if)#switchport mode trunk
```

```
Switch#show interface status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          auto    auto  10/100BaseTX
Fa0/2                        connected    2          auto    auto  10/100BaseTX
Fa0/3                        notconnect   1          auto    auto  10/100BaseTX
Fa0/4                        connected    trunk      auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        notconnect   1          auto    auto  10/100BaseTX
```

```
Switch#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/4       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/4       1-1005

Port        Vlans allowed and active in management domain
Fa0/4       1,2

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/4       1,2
```

#show vlan brief එකේ පෙන්නනෙ නෑ trunk ports

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
2    VLAN0002                         active    Fa0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Number Systems

Category 2යි,

1. Non-positional - number එක තියනෙ ස්ථානයේ වැදගත්කමක් නෑ
   ex: Roman, Gray Code, Tally, etc.
2. positional - number එක තියනෙ ස්ථානය වැදගත්
   ex: Binary, Octal, Decimal, Hexadecimal

Positional Number Systems

Number System	Base	Pre-defined Digits	Example
Binary	2	0, 1	101101_2
Octal	8	0, 1, 2, 3, 4, 5, 6, 7	5739_8
Decimal	10	0, 1, 2, 3, 4, 5, 6, 7, 8, 9	2467
Hexadecimal	16	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F	$1A3F_{16}$

- **Binary digit** = ‘Bit‘

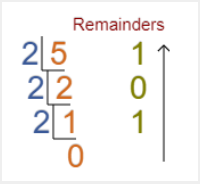
🔗BASE CONVERTERS ← with steps
🔗Base converter | number conversion

- ## Another base to Decimal

  Get the total of base powers
  ex: binary to decimal
  101_2 to decimal
  $= (1 \times 2^2) + (0 \times 2^1) + (1 \times 2^0)$
  $= 4 + 0 + 1$
  $= 5$

- ## Decimal to Another base

  Divide by the target base
  ex: 5_{10} to binary

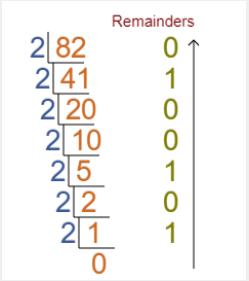
  $= 101_2$

- ## Another base to Another base

  X base → decimal → Y base

  ex: 52_{16} to binary
  1. 52_{16} convert to decimal
     $(52)_{16} = (5 \times 16^1) + (2 \times 16^0)$
     $= 80 + 2$
     $= (82)_{10}$

  2. Decimal result convert to binary

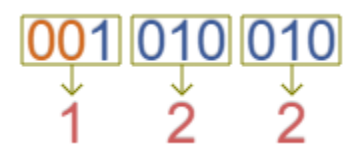
     

     $= (82)_{10} = (1010010)_2$

     So, 52_{16} binary value is → 1010010_2

- **Direct way (not valid for all bases)**
- **Binary to Octal**

  ex: 1010010_2 to octal

  $= 122_8$

- **Octal to Binary**

  ex: 122_8 to binary

  $= 1010010_2$

- **Binary to Hexadecimal**

  ex: 101001010001_2 to hexadecimal

  $= A51_{16}$

- **Hexadecimal to Binary**

  ex: $A51_{16}$ to binary

  $= 101001010001_2$

IP Addressing

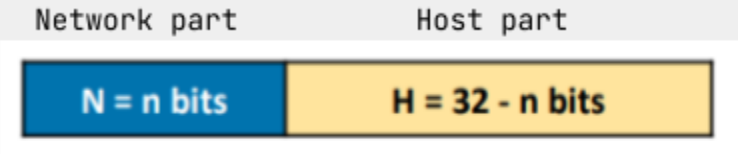
Network එකේ පිට communicate කරන්න use වෙන්නෙ.

- Two types of IP address
  - IPv4
  - IPv6

IPv4 Address structure

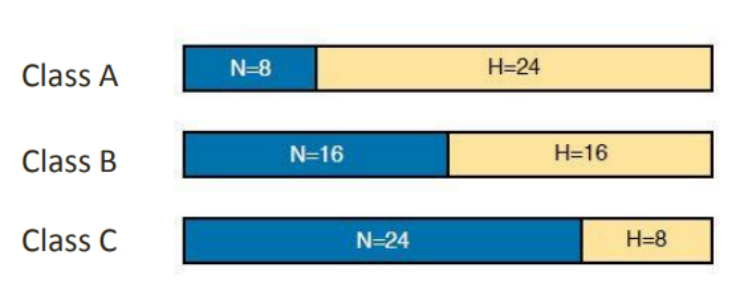
- bit 32 කින් හැදෙනෙ. (octet 4)
  xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
  (x represents either binary 0 or 1)

- parts 2යි: Network part & Host part



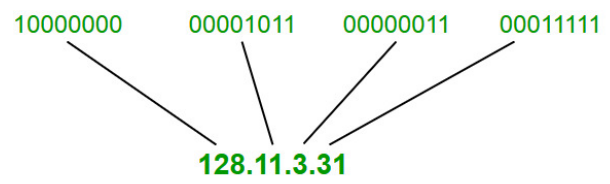
- එකම network එකක තියෙන IP address වල
  - network part එක සමානයි
  - host part එක වෙනස්

- Address classes 3යි,



Address ranges

- අදුරගන්න ලෙසි වෙන්න Dotted Decimal Number (DDN) වලින් represent කරයි.



- first octet එකේ value එකනේ class වලට වනේ කරයි.

Class	First Octet Values	Purpose
A	1 - 126	Unicast (Large-sized networks)
B	128 - 191	Unicast (medium-sized networks)
C	192 - 223	Unicast (small-sized networks)
D	224 - 239	Multicast
E	240 - 255	Reserved (Formerly experimental)

- 0 , 127 ← reserved

Address Analysis

- first octet එකේ value එකනේ class එක තීරණය කරයි.

Class	First Octet Values
A	1 - 126
B	128 - 191
C	192 - 223
D	224 - 239
E	240 - 255

- Smallest IP address in the network defines Network number (Network ID, Network address)
  reserve කරල තියනේනෙ network එක identify කරගන්න.

- broadcast address

- Highest IP address is the broadcast address

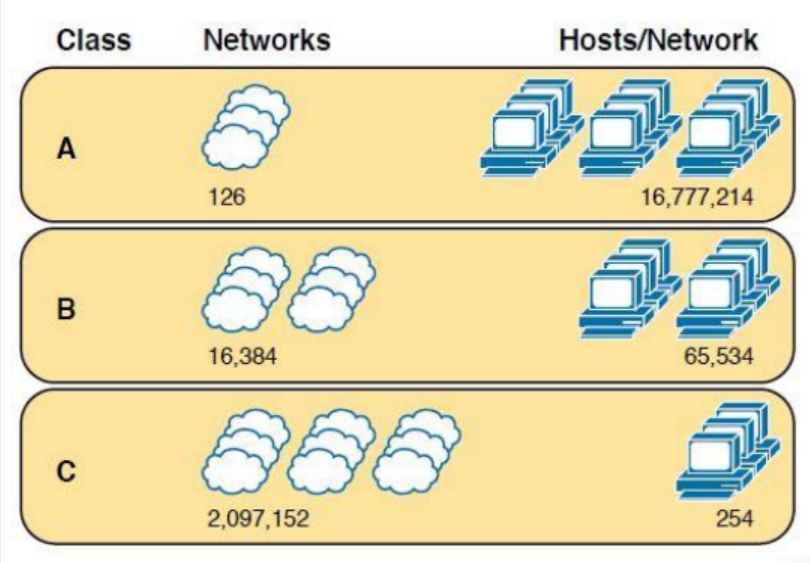
- All other IP addresses are used address hosts uniquely

- Default mask

Network part එකට උපරිම ගානයි (11111111 or 255),
Host part එකට අවම ගානයි (00000000) දැම්මම එන IP address එක.

	Class A	Class B	Class C
First octet range	1 – 126	128 - 191	192 - 223
Octets in network part	1	2	3
Bits in Network part	8	16	24
Valid network numbers	1.0.0.0 – 126.0.0.0	128.0.0.0 – 191.255.0.0	192.0.0.0 – 223.255.255.0
Total networks	$2^7 - 2 = 126$	$2^{14} = 16,384$	$2^{21} = 2,097,152$
Octets in host part	3	2	1
Bits in host part	24	16	8
Hosts per network	$2^{24} - 2 = 16,777,214$	$2^{16} - 2 = 65,534$	$2^8 - 2 = 254$
Default mask	255.0.0.0	255.255.0.0	255.255.255.0

Class comparisons



Class C

Range 192 - 223

Network part octet → 3

Lowest IP address network part value→ 192.0.0

Highest IP address network part value→ 223.255.255

192.0.0 ⟶ 11000000 00000000 00000000

192.255.255 ⟶ 11011111 11111111 11111111

Total Networks = 2^{21} = 2,097,152

Host part octet → 1
Lowest IP address Host part value→ 1
Highest IP address Host part value→ 254
Hosts per network = 254 = $2^8 - 2$

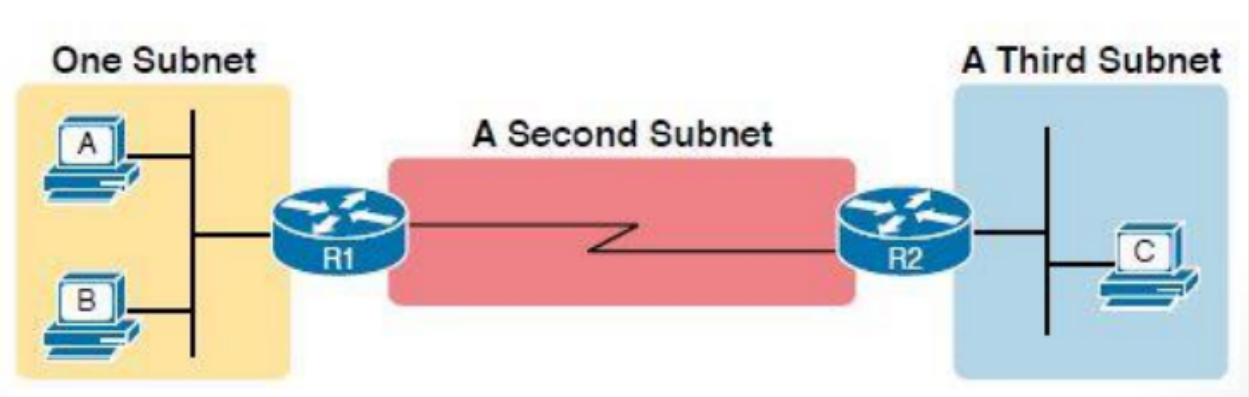
Subnetting

Needs for subnetting a network?

- Better management of enterprise internetworks
- Better management of IP addresses
- Network traffic එක අඩුකරන්න
- Network security එක වැඩිකරන්න.

Subnetting Overview

- The primary task of a router is to forward (route) packets from one subnet to another
- Addresses in the same subnet are not separated by a router
- Addresses in different subnets are separated by at least one router

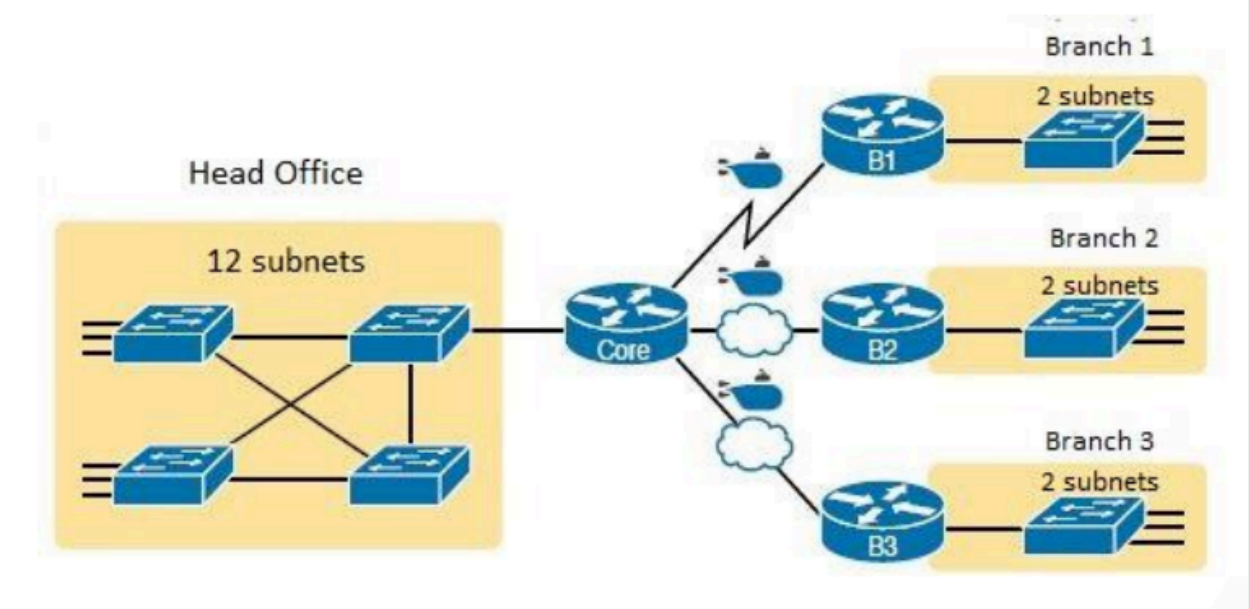


Analyzing Subnetting needs

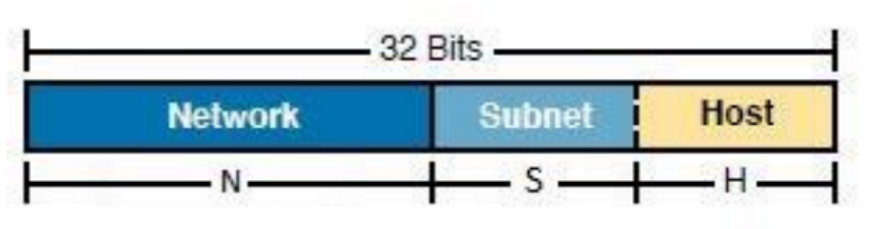
Considerations when designing a subnetted network

- Which hosts/users should be grouped into respective subnets?

- How many subnets does the enterprise need?
- How many IP addresses each subnet should provide?
- A single subnet size for all subnets or not?

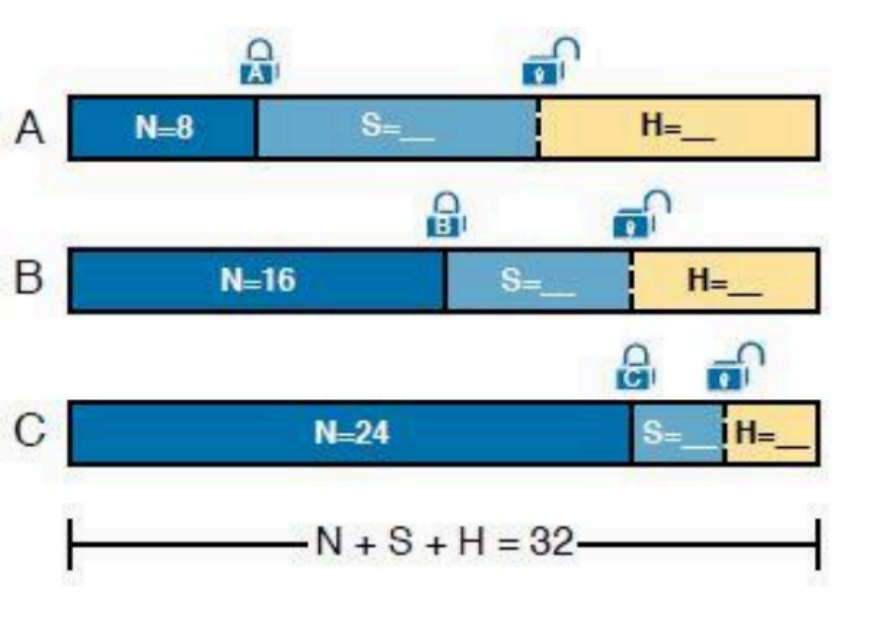


Implementing Subnets



N - network bits
S - Subnet bits
H - Host bits

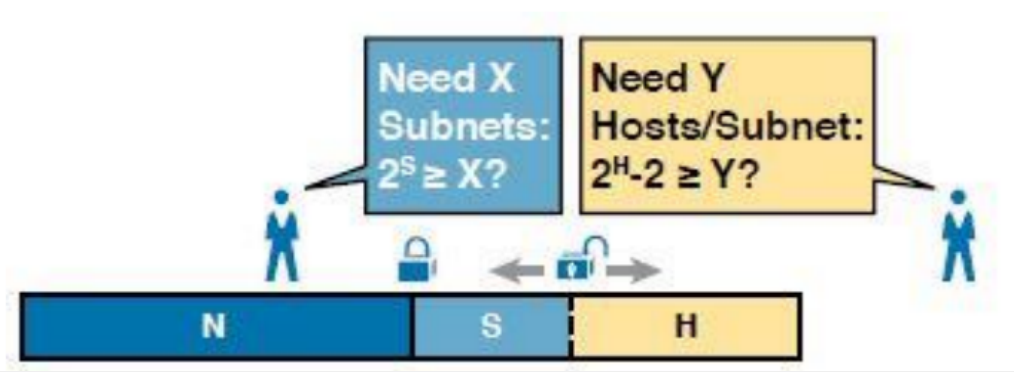
} prefix



- Host bits ගාන → H
- Subnet bits ගාන → S
- අවශ්‍ය subnet ගාන → X
- subnet එකකට අවශ්‍ය hosts ගාන → Y

  $X \leqslant 2^{s}$

  $Y \leqslant 2^{H} - 2$

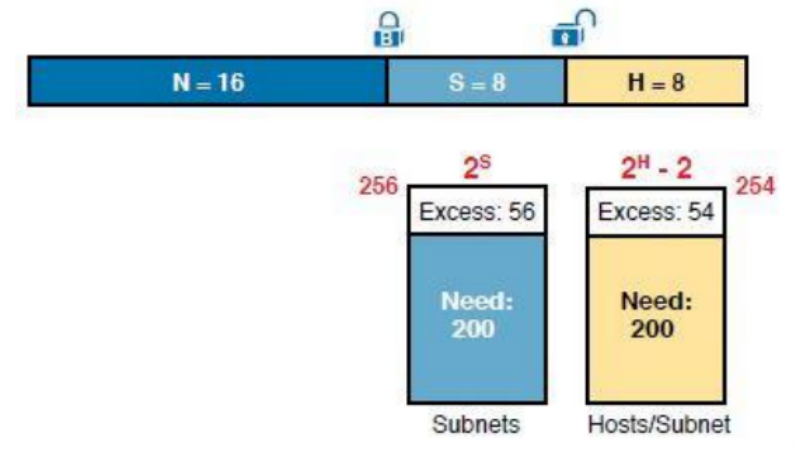


Example :

- The subnetting requirement,
  200 subnets
  200 hosts per each subnet
  Use network 172.16.0.0

  172 ← class B

Network part bits = 16
Subnet + Host bits (rest) = 32-16 = 16 bits
2^8 = 256 නිසා ආසන්නව ගැලපෙන bit ගාන 8



Subnet mask

Format 3 කට ලියන්න පුලුවන්,

- **Binary representation**
  11111111.11111111.11111111.00000000

- **Dotted Decimal Notation (DDN)**
  255.255.255.0

- **Prefix Notation** (network bits + subnet bits)
  /24

ex:

Prefix	Binary	DDN
/24	11111111.11111111.11111111.00000000	255.255.255.0
/27	11111111.11111111.11111111.11100000	255.255.255.224
/30	11111111.11111111.11111111.11111100	255.255.255.252
/16	11111111.11111111.00000000.00000000	255.255.0.0

Analysis of Subnetting

🔗 https://themiu.github.io/SubnetAnalysis/

first octet value range	class	network bits
1 - 126	A	8
128 - 191	B	16
192 - 223	C	24

```
10000000 = 128                    = 128
11000000 = 128+64                 = 192
11100000 = 128+64+32              = 224
11110000 = 128+64+32+16           = 240
11111000 = 128+64+32+16+8         = 248
11111100 = 128+64+32+16+8+4       = 252
11111110 = 128+64+32+16+8+4+2     = 254
11111111 = 128+64+32+16+8+4+2+1   = 255
01111111 = 64+32+16+8+4+2+1       = 127
00111111 = 32+16+8+4+2+1          = 63
00011111 = 16+8+4+2+1             = 31
00001111 = 8+4+2+1                = 15
00000111 = 4+2+1                  = 7
00000011 = 2+1                    = 3
00000001 = 1                      = 1
```

$$
\begin{aligned}
00000001 &= 2^0 &&= 1\\
00000010 &= 2^1 &&= 2\\
00000100 &= 2^2 &&= 4\\
00001000 &= 2^3 &&= 8\\
00010000 &= 2^4 &&= 16\\
00100000 &= 2^5 &&= 32\\
01000000 &= 2^6 &&= 64\\
10000000 &= 2^7 &&= 128
\end{aligned}
$$

🔗 https://themiu.github.io/SubnetAnalysis/

🔗 subnetting

Example:

1) IP Address: 8.1.4.5
Subnet Mask: 255.240.0.0

- Subnet Mask in Binary: 11111111.11110000.00000000.00000000
- Prefix : /12
- Address range : 1-126
- Class : A

No. of Prefix bits: 12
No. of Network bits: 8 (class A)
No. of Subnet bits: 4 (prefix bits - network bits)
No. of Host bits: 20 (32 - prefix bits)
No. of possible subnets in this network: 2^4
No. of hosts per subnet: $2^{20}-2$

DDN : 8.1.4.5
Binary : 00001000.00000001.00000100.00000101

Network part එක වනෙස් වනේන‍ෙ නෑ.
වනෙස් වනේන‍ෙ **subnet part** එකයි, **host part** එකයි විතරයි.

subnet ID - host part ඔක්කොම 0
First assignable IP - subnet ID address එකේ host part + 1
Broadcast IP - host part ඔක්කොම 1
Last assignable IP - Broadcast IP address එකේ host part - 1

Existing subnet's

	Binary	DDN
subnet ID	00001000.00000000.00000000.00000000	8.0.0.0
First assignable IP	00001000.00000000.00000000.00000001	8.0.0.1

Broadcast IP	00001000.00001111.11111111.11111111	8.15.255.255
Last assignable IP	00001000.00001111.11111111.11111110	8.15.255.254

Numerically first subnet's (subnet part එකේ 0 ඒවා)

	Binary	DDN
subnet ID	00001000.00000000.00000000.00000000	8.0.0.0
First assignable IP	00001000.00000000.00000000.00000001	8.0.0.1
Broadcast IP	00001000.00001111.11111111.11111111	8.15.255.255
Last assignable IP	00001000.00001111.11111111.11111110	8.15.255.254

Numerically next subnet's (subnet part එකට +1)

	Binary	DDN
subnet ID	00001000.00010000.00000000.00000000	8.16.0.0
First assignable IP	00001000.00010000.00000000.00000001	8.16.0.1
Broadcast IP	00001000.00011111.11111111.11111111	8.31.255.255
Last assignable IP	00001000.00011111.11111111.11111110	8.31.255.254

Numerically last subnet's (subnet part එකේ 1 ඒවා)

	Binary	DDN
subnet ID	00001000.11110000.00000000.00000000	8.240.0.0
First assignable IP	00001000.11110000.00000000.00000001	8.240.0.1
Broadcast IP	00001000.11111111.11111111.11111111	8.255.255.255
Last assignable IP	00001000.11111111.11111111.11111110	8.255.255.254

WAN Technologies

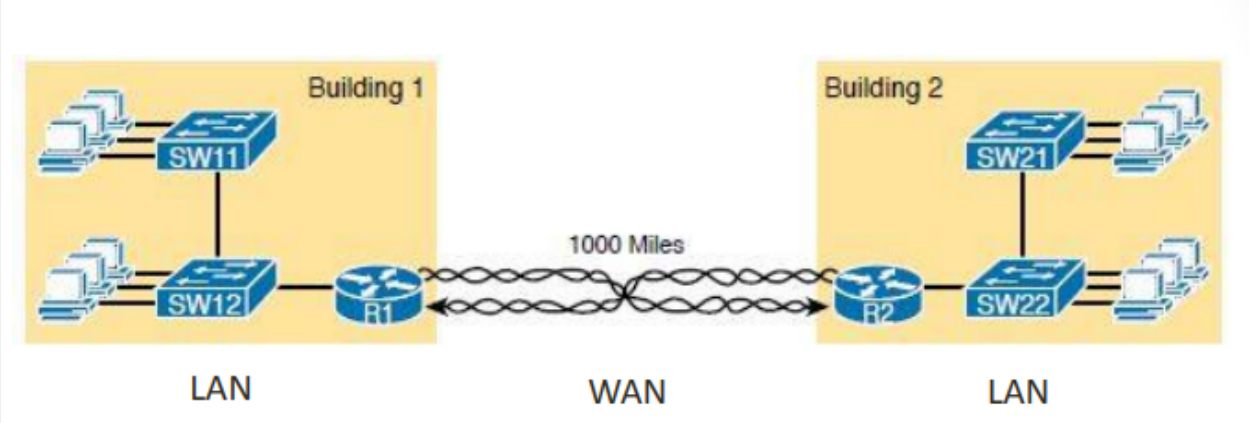
දිග දුර සන්නිවේදනයට භාවිතා කරන Physical layer (Layer1), Data-Link layer (layer2) standards & protocols වේ.

Two popular WAN technologies

1. Leased-line WANs (older)
2. Ethernet WANs (newer)

WAN connect කරන්න router ඕන.

Leased-line WANs (older)



Conceptually, WAN link is a crossover cable connecting two Routers.

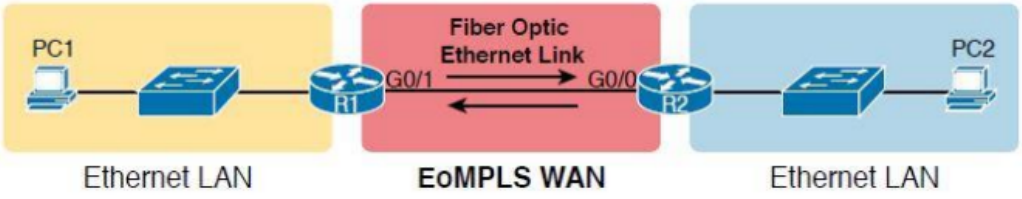
• 2 most popular data-link layer protocols for leased lines exist.
- High-Level Data Link Control (HDLC)
- Point-to-Point Protocol (PPP)

Advantages and Disadvantages of Leased lines

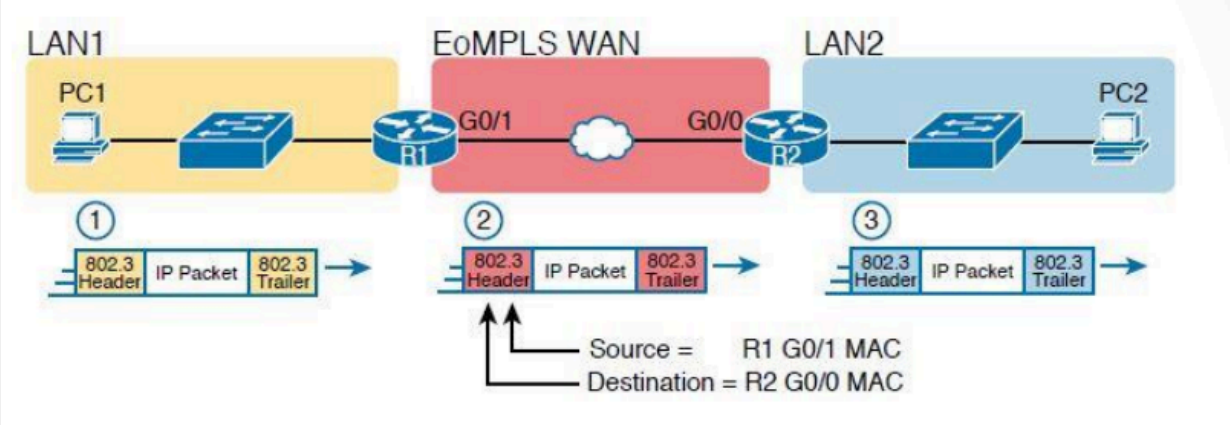
Advantages	Disadvantages
- Simple for the customer	- Higher cost
- Widely Available	- Longer lead times for installation
- High quality	- Relatively slow
- Private	

`Ethernet WAN technology (newer)`

Ethernet WAN technology



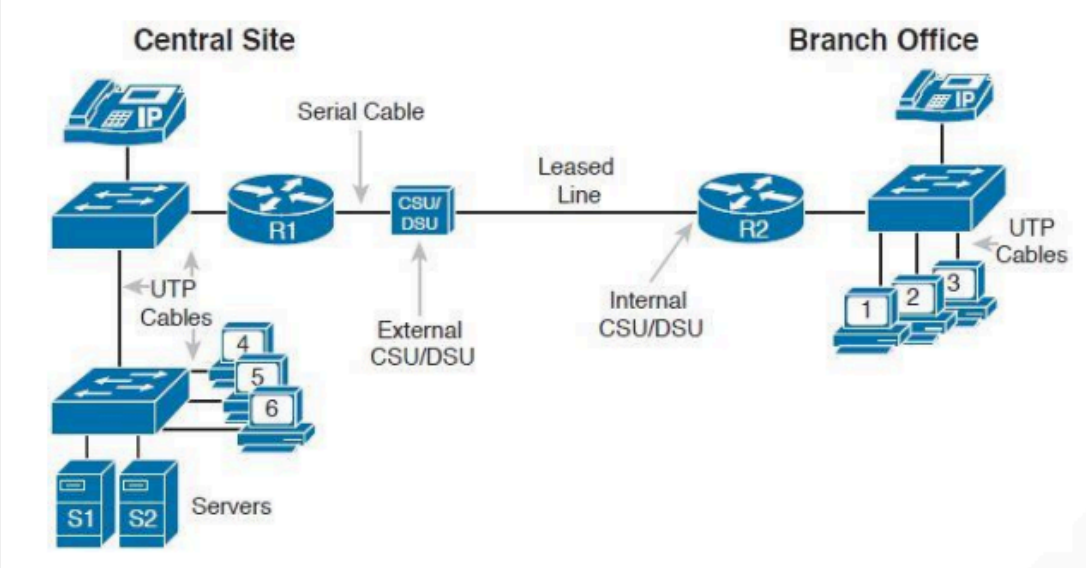
`EoMPLS - use karana protocol eka`



* Source IP, destination IP දාන්නෙ network header එකනේ.

Router

- Task → Addressing and Routing data between networks.
- networks/subnets අතර physically connect කරයි.
- network / subnet එකක gateway (entry point) එක.
- Modern router වල switching, wireless access, වගෙ functions තියනෙෝ.

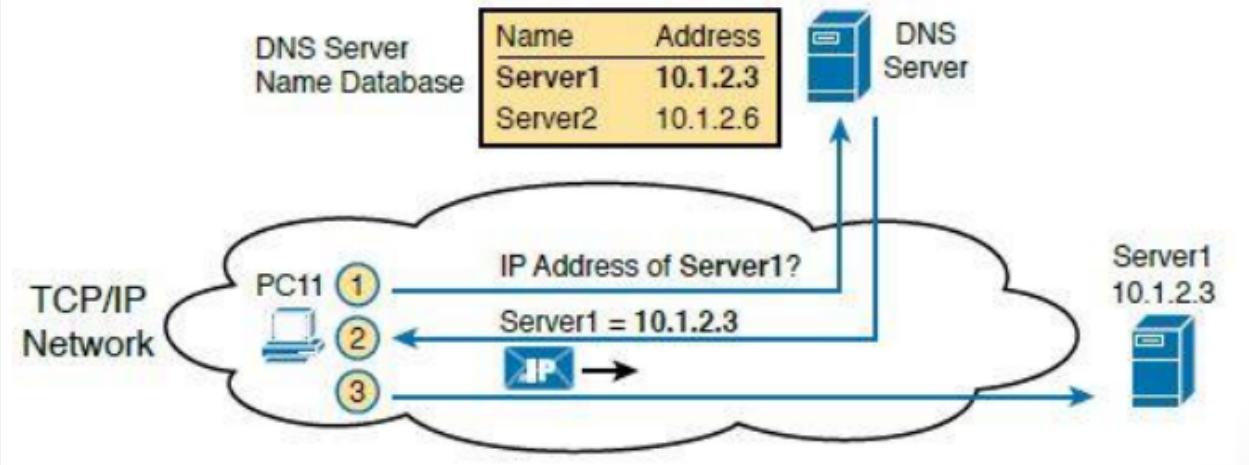


Configuring Routers

Basic configurations are similar to switch configurations

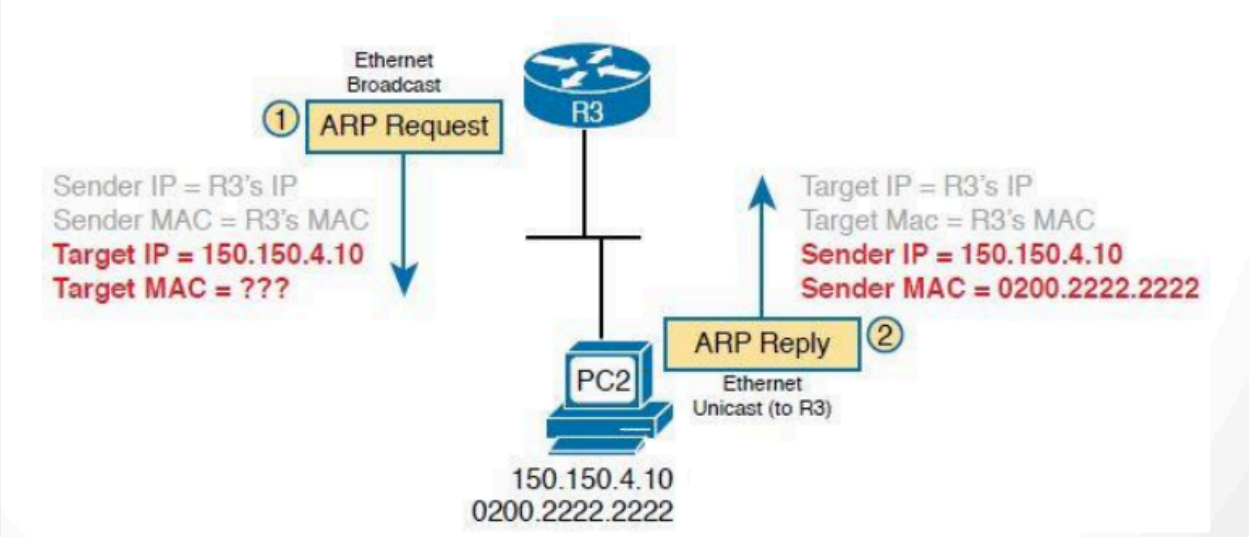
DNS (Domain Name System)

- DNS , Internet එකේ අනෙකුත් Computers/hosts/servers හඳුනා ගැනීමට hostnames නිර්වචනය කරයි
- DNS, hostnames → matching IP addresses වලට translates කරයි. ex: www.google.com ⇒ IP 64.233.177.100

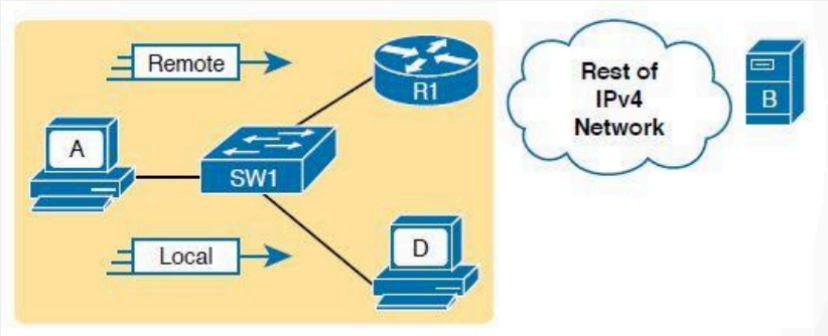


ARP (Address Resolution Protocol)

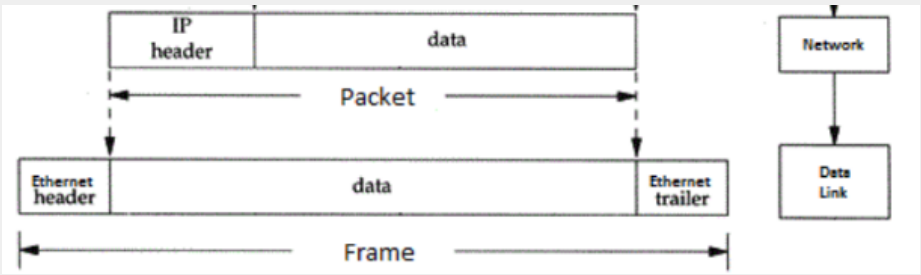
Hosts and Routers , ARP මගින් MAC address dynamically ඉගනෙ ගනී.



Host logic

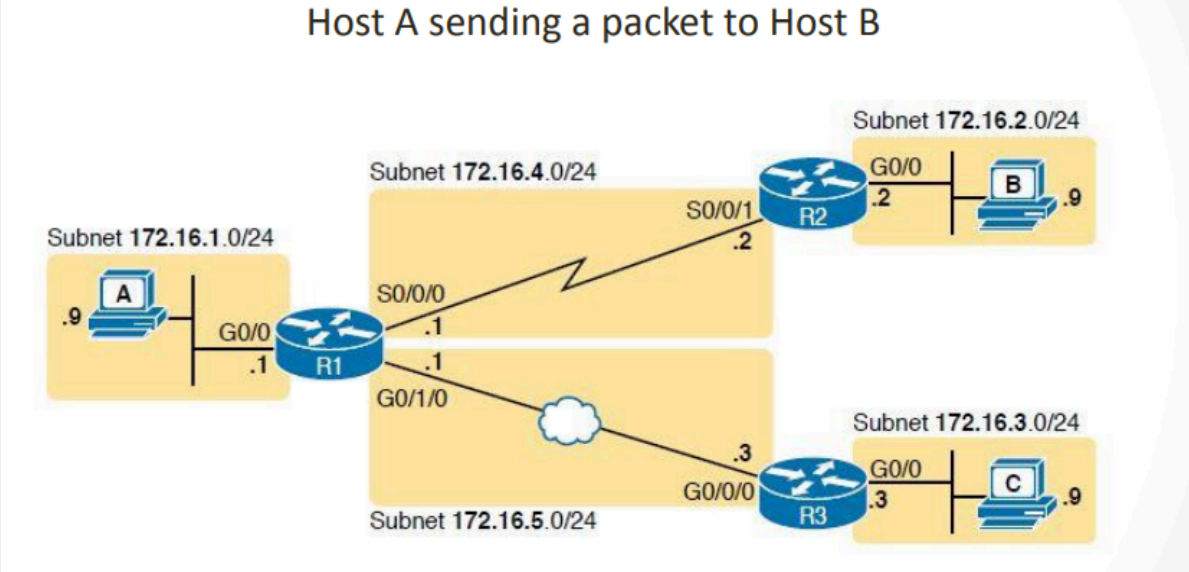


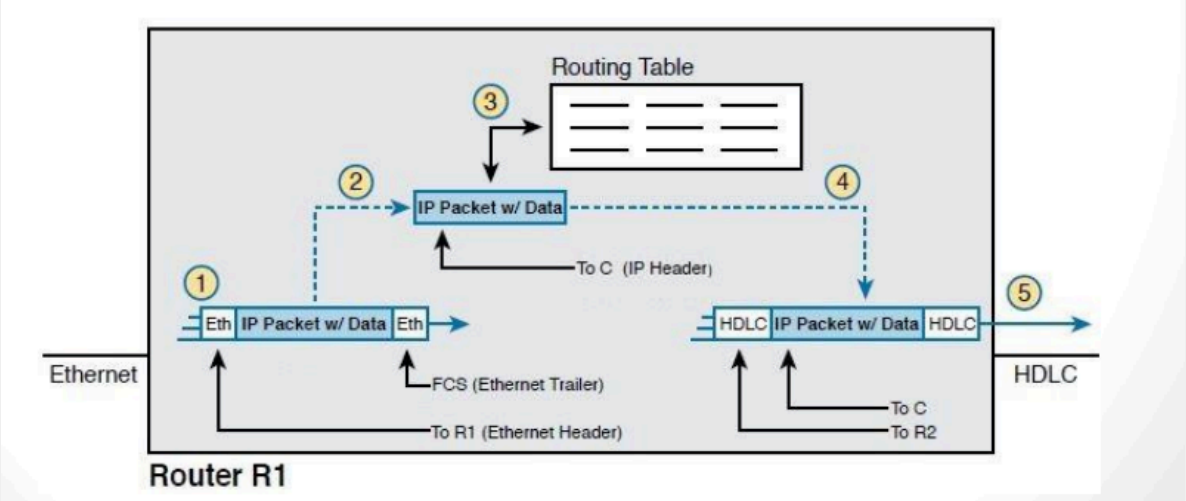
- Step 1: **destination host** ඉන්නෙ එකම **network/subnet** එකෙ නම්, **send directly.**
    - දැනටමත් දන්න ARP table එකකින් / ARP request broadcast එකකින් destination host ගෙ MAC address එක හොයාගන්නෙ.
    - Data link layer එකේ frame එක හදද්දි, packet එකත් එක්ක destination MAC address එකත් encapsulate කරනෙ.



- Step 2: **destination host** ඉන්නෙ වෙනත් **network/subnet** එකක නම්, **send to the default gateway.(router** එක**)**
    - දැනටමත් දන්න ARP table එකකින් / ARP request broadcast එකකින් default gateway (default router) එකෙ MAC address එක හොයාගන්නෙ.
    - Data link layer එකේ frame එක හදද්දි, packet එකත් එක්ක default router MAC address එකත් encapsulate කරනෙ.

Router logic





- Step 1: process කරන්න ඕන frame එකක්ද නැද්ද බලනවා.
    - frame's destination MAC address = Router interface's MAC address
    - FCS වලින් frame එකේ දෝෂ තියෙද බලනවා. තිබුනොත් frame එක නොසලකා හරිනවා.
      (Router එක frame එක recover කරන්නෙ නෑ)

- Step 2: step 1 වල conditions satisfy නම්, frame එක process කරනවා. (De encapsulate the packet)

- Step 3: routing decision

    - Packet වල destination IP address එක routing table entries එක්ක compare කරනවා.
    - අදාල interface එකට/ next hop (router) එකටද යවන්න ඕන බලනවා.

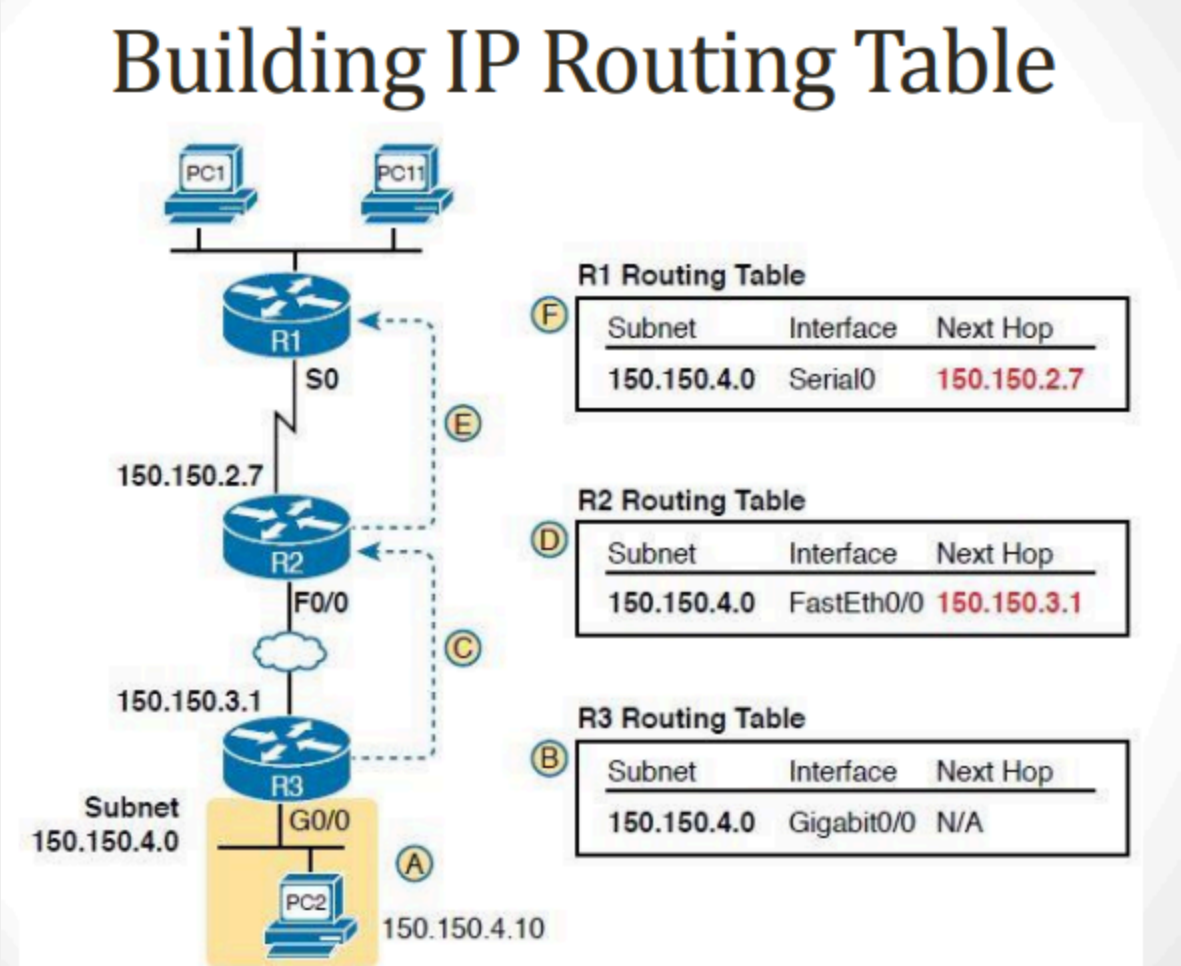
// next hop (router) එකට යවනවනම්,

- Step 4: next hop router’s interface එකේදි destination MAC address එකත් එක්ක packet එක encapsulate කරල frame එක හදනවා.
- Step 5: ගැලපෙන routing table entry එකට අනුව outgoing interface එකෙන් frame එක transmit කරනවා.

IP Routing Table

IP ප්‍රොටෝකෝල සාමූහිකව රවුටර වලට ඔවුන්ගේ routing table එක ගොඩනගා ගැනීමට උපකාර කරයි,

- සෑම රවුටරයක්ම, රවුටරයට සෘජුවම සම්බන්ධ සෑම subnet එකක් සඳහාම එහි routing table එකට route එකක් එක් කරයි.
- සෑම රවුටරයකම රවුටර ප්‍රොටෝකෝලය, එහි routing table එකේ ඇති route ගැන අසල්වැසියන්ට කියයි, අනෙක් රවුටරවලින් ඉගෙන ගත් directly connected routes සහ routes ඇතුළත් වේ.
- අසල්වැසියකුගෙන් අලුත් route එකක් ඉගෙනීමෙන් පසු, රවුටරයේ රවුටින් ප්‍රොටෝකෝලය එහි IP routing table එකට route එකක් එක් කරයි, එම route එකේ next-hop router එක සාමාන්‍යයෙන් route එක ඉගෙන ගත් අසල්වැසියා වේ.



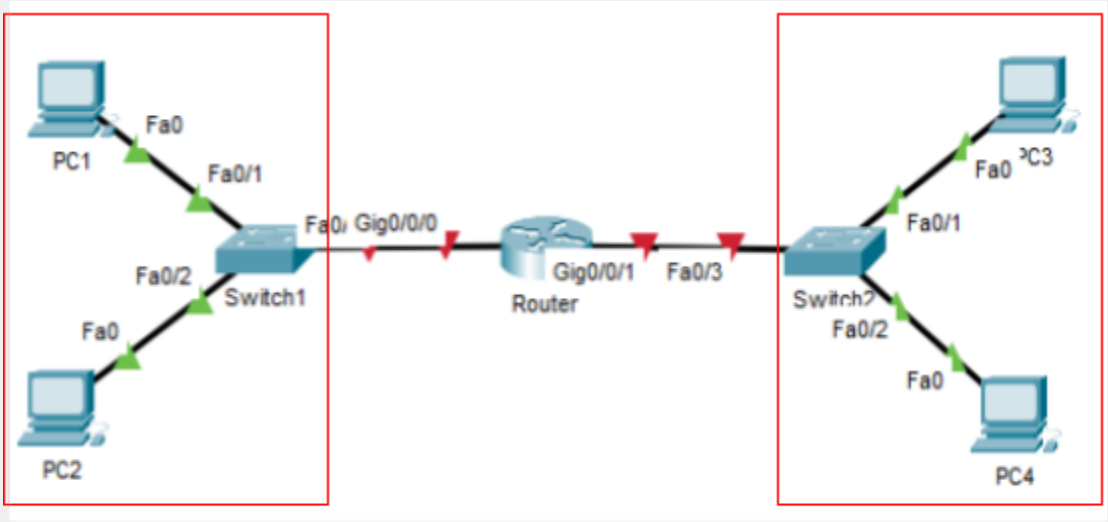
Route Types

- Connected Routes
- Static Routes
- Routing Protocols

Practical

- **With one Router**

  🔗OneRouter.pkt



- Change IP and Subnet masks
- Default gateway එකට දාන්නෙ router එකේ අදාල port එකට දෙන IP එකමයි. (IP වලට දීපු network එකෙන්ම address එකක් දෙන්න ඕන)

PC1

IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.3
DNS Server	0.0.0.0

PC2

IPv4 Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.3
DNS Server	0.0.0.0

PC3

IPv4 Address	126.1.1.1
Subnet Mask	255.0.0.0
Default Gateway	126.1.1.3
DNS Server	0.0.0.0

PC4

IPv4 Address	126.1.1.2
Subnet Mask	255.0.0.0
Default Gateway	126.1.1.3
DNS Server	0.0.0.0

- `Router#show ip interface brief` ← router එකෙ interfaces ගැන බලන්න Router by default (interface ඔක්කොම down)

```
Router>enable
Router#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0       unassigned      YES unset  administratively down down
GigabitEthernet0/0/1       unassigned      YES unset  administratively down down
GigabitEthernet0/0/2       unassigned      YES unset  administratively down down
Vlan1                      unassigned      YES unset  administratively down down
```

- Configure ports(interfaces)
  (IP address එක විදියට දාන්නෙ default gateway එකට දාන IP එක, subnet mask එක ඒ network එකට අදාල එක)

  Interface Gig0/0/0

```
Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#ip address 192.168.1.3 255.255.255.0
Router(config-if)#no shutdown
```

  Interface Gig0/0/1

```
Router(config)#interface gigabitEthernet 0/0/1
Router(config-if)#ip address 126.1.1.3 255.0.0.0
Router(config-if)#no shutdown
```

- දැන් interface වලට IP address assign වලෝ තියනේනෙ.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.1.3     YES manual up                    up
GigabitEthernet0/0/1   126.1.1.3       YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

- Router#show arp ගැහුවම router එකෙ arp table එක බලන්න පුලුවන්.

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  126.1.1.3              -   0030.A367.9A02  ARPA   GigabitEthernet0/0/1
Internet  192.168.1.3            -   0030.A367.9A01  ARPA   GigabitEthernet0/0/0
```

- PC1(192.168.1.1) ඉදන් PC3(126.1.1.1) වලට Ping එකක් ගැහුවම

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  126.1.1.1              0   0090.21C4.B289  ARPA   GigabitEthernet0/0/1
Internet  126.1.1.3              -   0030.A367.9A02  ARPA   GigabitEthernet0/0/1
Internet  192.168.1.1            0   0090.21B1.24B6  ARPA   GigabitEthernet0/0/0
Internet  192.168.1.3            -   0030.A367.9A01  ARPA   GigabitEthernet0/0/0
```

- Ping එකක් ගැහුවම, PC1 එකේ ARP table එකට entry එකක් වැටෙනවා (interface එකට අදාලව)

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.3           0030.a367.9a01        dynamic
```

- Ping හැම device එකකටම යැව්වට පස්සෙ router arp table එක

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  126.1.1.1              14   0090.21C4.B289  ARPA   GigabitEthernet0/0/1
Internet  126.1.1.2               0   0005.5E1C.CCCD  ARPA   GigabitEthernet0/0/1
Internet  126.1.1.3               -   0030.A367.9A02  ARPA   GigabitEthernet0/0/1
Internet  192.168.1.1            14   0090.21B1.24B6  ARPA   GigabitEthernet0/0/0
Internet  192.168.1.2             1   00D0.FF63.341D  ARPA   GigabitEthernet0/0/0
Internet  192.168.1.3             -   0030.A367.9A01  ARPA   GigabitEthernet0/0/0
```

- PC1 වල bordercast msg එකක් යැව්වම (ping 192.168.1.255)

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.2           00d0.ff63.341d        dynamic
  192.168.1.3           0030.a367.9a01        dynamic
```

- Router#show ip route

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     126.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       126.0.0.0/8 is directly connected, GigabitEthernet0/0/1
L       126.1.1.3/32 is directly connected, GigabitEthernet0/0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.1.3/32 is directly connected, GigabitEthernet0/0/0
```

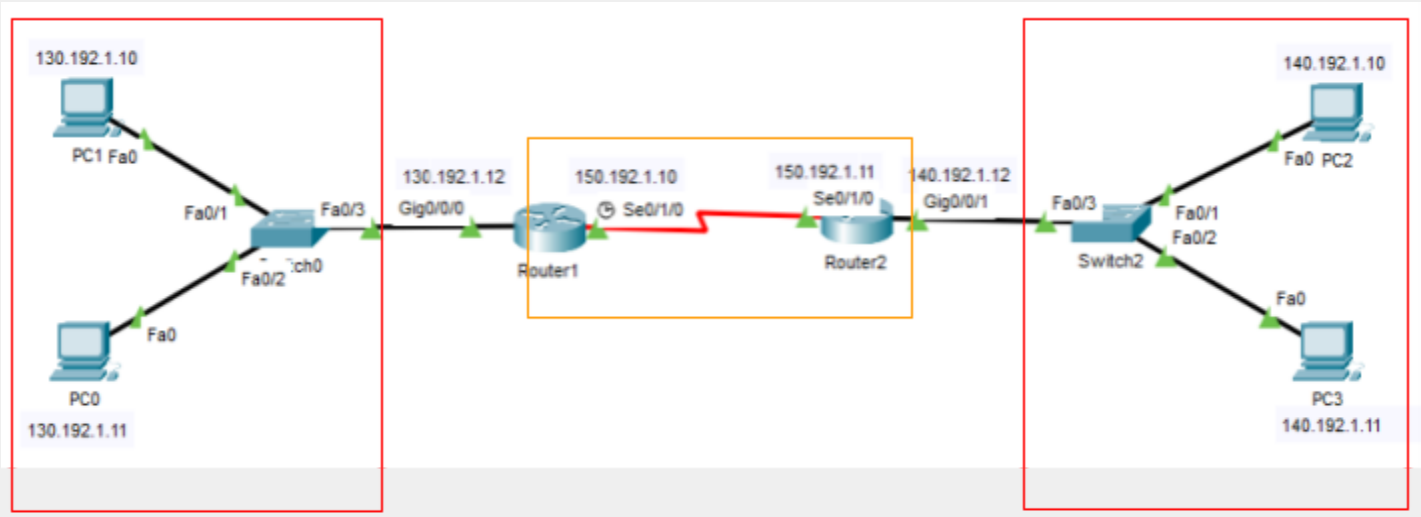
C - connected

L - local IP address එකක්

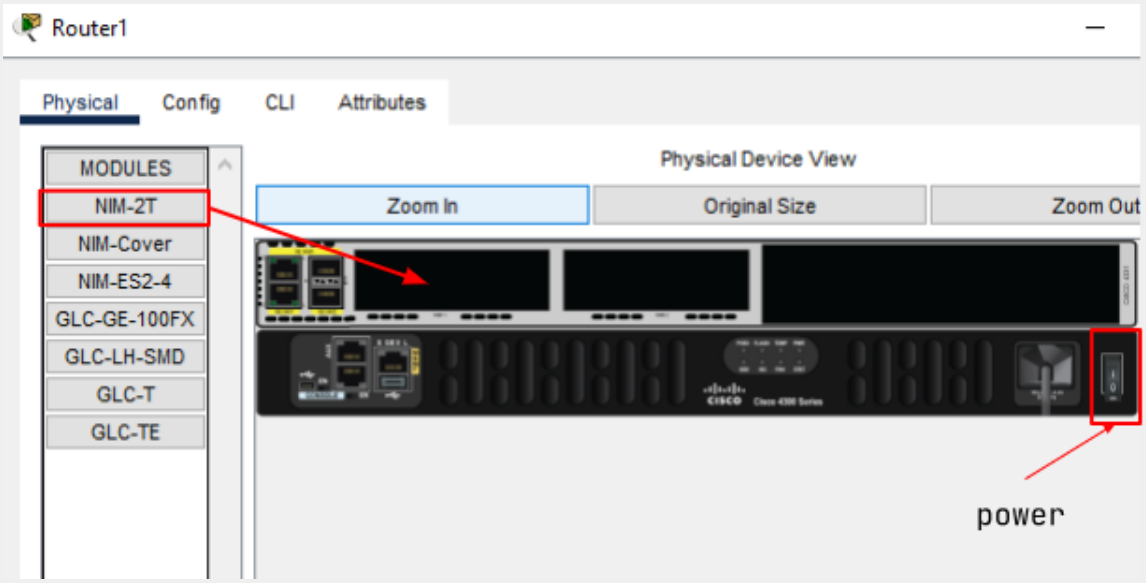
RIP - Routing Information Protocol (auto ඉගෙනගන්නවා)

- **With two Routers**

  🔗
  Cisco Packet Tracer Basic Networking - Static Routing using 2…
  🔗TwoRouters.pkt



- Configure IPs for PCs
- Network1 PCs Gateway → 130.192.1.12
  Network2 PCs Gateway → 140.192.1.12
- Set Serial cable (crossover cable එකකිනුත් පුලුවන්)
  - Router1 එකේ power off කරලා NIM-2T එකක් ඇදිල දාන්න, power on කරන්න. (Router2 එකටත් එහෙමෙමයි)3



  - Serial DCE type එකෙ cable එකකින් router 2 connect කරන්න.

- Assign IP addresses to router interfaces
    - Router1

      Router(config)#interface Serial0/1/0
      Router(config-if)#ip address 150.192.1.10 255.255.0.0
      Router(config-if)#no shutdown

    - Router2

      Router(config)#interface Serial0/1/0
      Router(config-if)#ip address 150.192.1.11 255.255.0.0
      Router(config-if)#no shutdown

- Assign IP route (make static router)

  #ip route <Destination Network> <Subnet Mask> <Next Hop>
    - Router1

      Router(config)#ip route 140.192.0.0 **255.255.0.0** 150.192.1.11

    - Router2

      Router(config)#ip route 130.192.0.0 **255.255.0.0** 150.192.1.10

- IP route එකේ බලාගන්න පුලුවන්

  (Router1)

  Router#show ip route

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     130.192.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       130.192.0.0/16 is directly connected, GigabitEthernet0/0/0
L       130.192.1.12/32 is directly connected, GigabitEthernet0/0/0
S    140.192.0.0/16 [1/0] via 150.192.1.11
     150.192.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       150.192.0.0/16 is directly connected, Serial0/1/0
L       150.192.1.10/32 is directly connected, Serial0/1/0
```

LAN Architecture

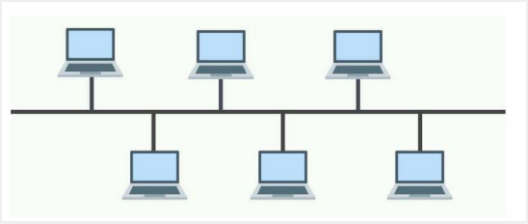
Network Topologies

- Network Topology is the arrangement / layout of nodes in a network.

- වර්ග 2යි
    - Physical Topology
    - Logical Topology

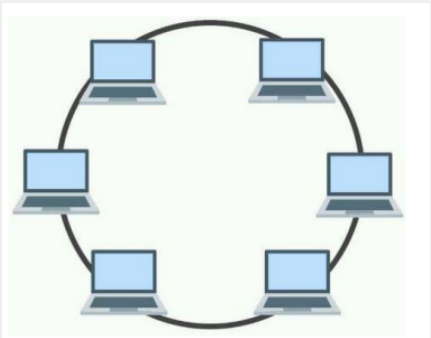
- Physical Topology එකේදි බලන්නෙ physical placement එකයි connection of nodes
- Logical Topology එකේදි බලන්නෙ data flow එක ගැන.

- **Bus Topology**



* common transmission medium fail වුනොත් network එක fail වෙනෙ.
* cable දිග limitations, traffick එක වැඩි, security එක අඩුයි

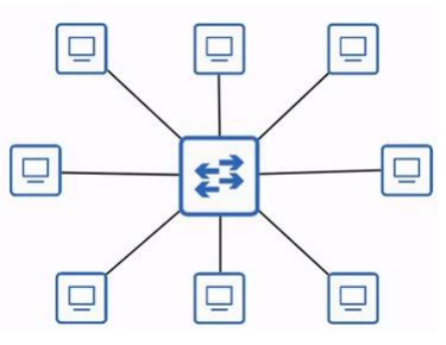
- **Ring Topology**



* එක point එකක් fail වුනොත් network එක fail වෙනෙ.
* network එකට අලුතින් device එකතු කරද්දි network එකෙ performance අඩු වෙනෙ.

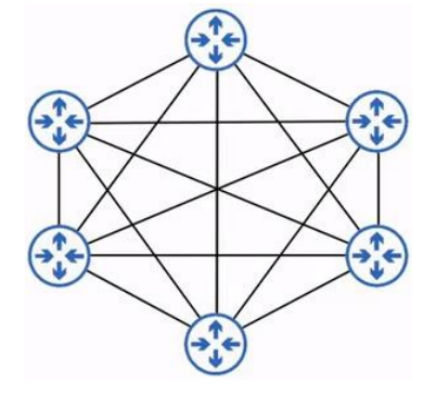
* security එක අඩුයි

- ## Star Topology



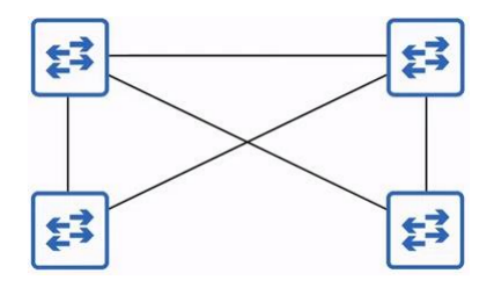
* centralized device එකකට අනිත් devices connect කරල තියනේනෙ.

- ## Mesh Topology



* හැම device එකක්ම එකිනෙකට connect වලෝ තියනේනෙ
* වැරදීම් අඩු, විශ්වාශනිය Topology එකක්

- ## Partial Mesh Topology

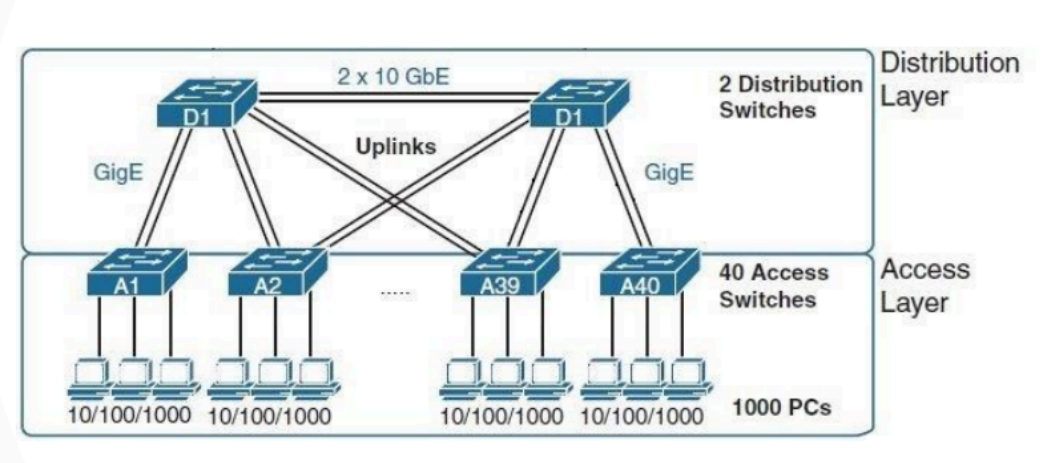


* හැම device එකක්ම සමහර device වලට connect වලෝ තියනේනෙ (හැම එකක්ම එකිනෙකට connected නෑ)
* වැරදීම් අඩු, විශ්වාශනිය Topology එකක්

Two-tier LAN Architecture

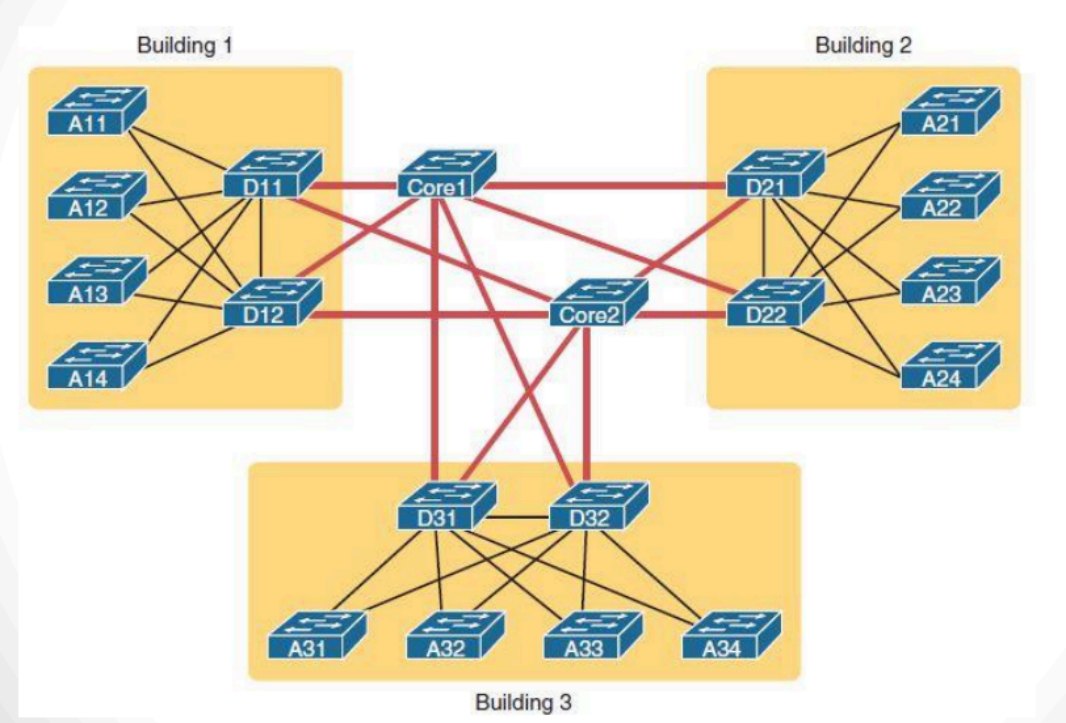
- Layers 2යි
    1. Access Layer
    2. Distribution Layer
- Access Layer
    - Device connect කරල තියන්නෙ මේ layer එකෙ
    - port security වගෙ Security services වන්නෙ මේ level එකේදි

- Distribution Layer
    - Access layers එකිනෙක connect කරන්නෙ මේ layer එකෙන්



Three-tier LAN Architecture

- Layers 3යි
    1. Access Layer
    2. Distribution Layer
    3. Core Layer
- Core Layer
    - Distribution Layers එකිනෙක connect කරයි.
    - ලොකු data traffic එක්ක තියෙන නිසා high performance devices මේ layer එකෙ තියන්නෙ
    - Core Laye එකේ මූලික කාර්ය, network එකේ විවිධ කොටස් අතර අධිවේගී, කාර්යක්ෂමව packet forwarding කිරීම.
    - ඒ නිසා security, QoS (Quality of Service) වගේ සමහර features, core layer එකේ නෑ/ අවම මට්ටමක තියන්නෙ.



======

🔗CNS Lecture Slides