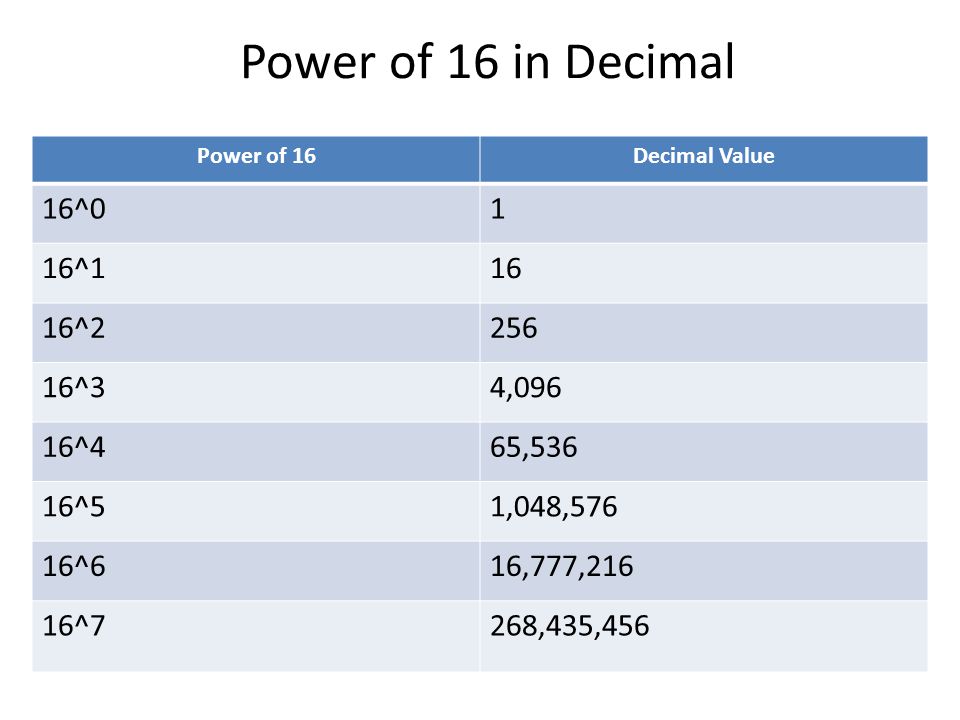
`Lecture 2 (2023-02-07)

**Power of 2: Power of 16:**

Table

Description automatically generated 

3 digits lock example:

* Range: 0+10^3-1= 000– 999
* Possibility: 10^3= 1000

Based= binary

**Bit**: **Byte**: (8 bit)

* 0/1 - Possibilities: 2^6= 256 ½ B = Nibble
* F/T - Range: 0-255 2 B = Word
* OFF/ON 4 B = Double Word
* Black/White

**Decimal** **Binary Hexadecimal**

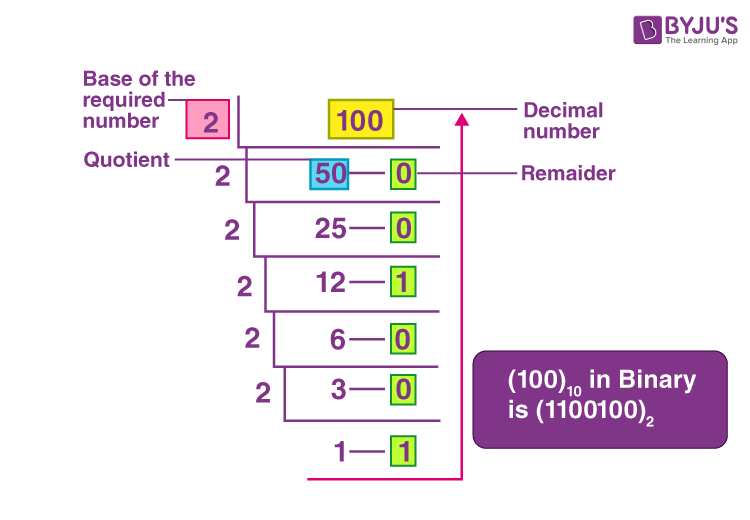
10^3 🡪 kilo 2^10 🡪 kilo Possibilities: 16

10^6 🡪 million 2^20 🡪 mega Range: 0-15

10^9 🡪 billion 2^30 🡪 giga

10^12 🡪 trillion 2^40 🡪 tera

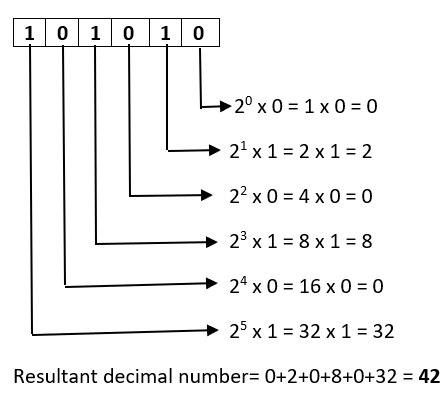
Convert Decimal to Binary



Example:

37 = 100101 63 = 111111

Convert Binary to Decimal

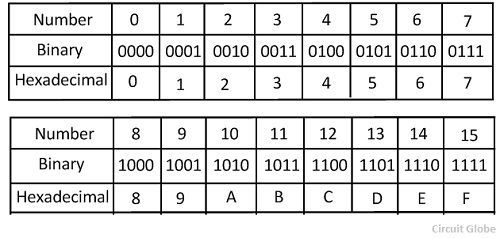


Example: 1011101 = 93

**Java Data Range**



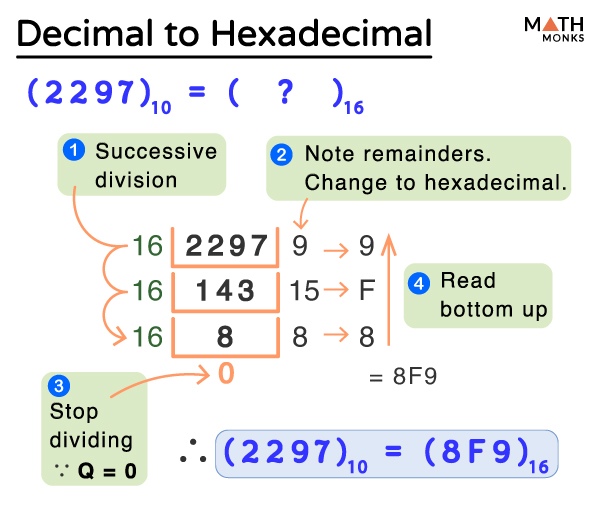
Convert Binary to Hexadecimal



Example:

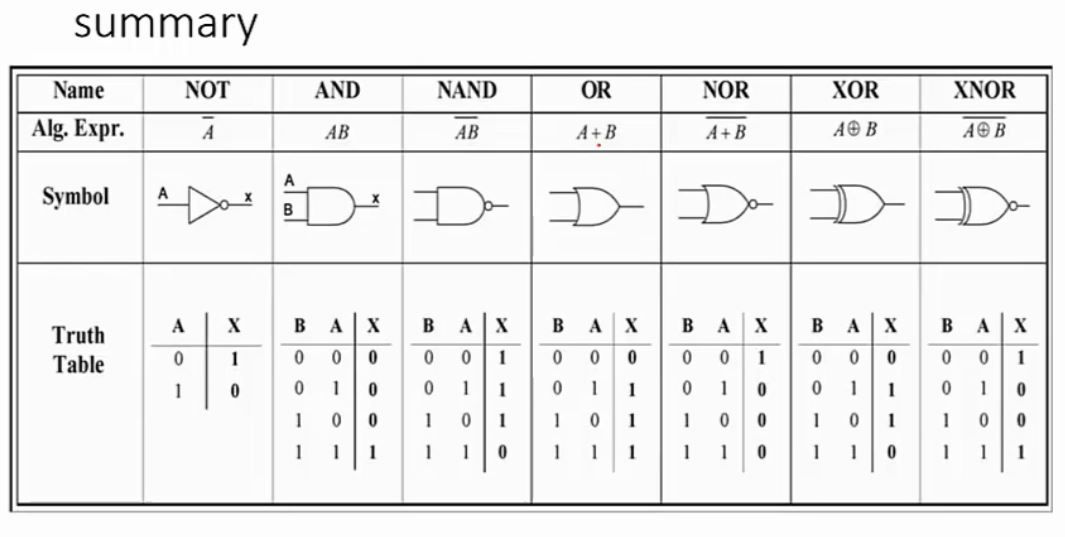
1011 0011 = B3 (00)01 1111 0110 = 1F6 F14 = 1111 0001 0100

Convert Decimal to Hexadecimal



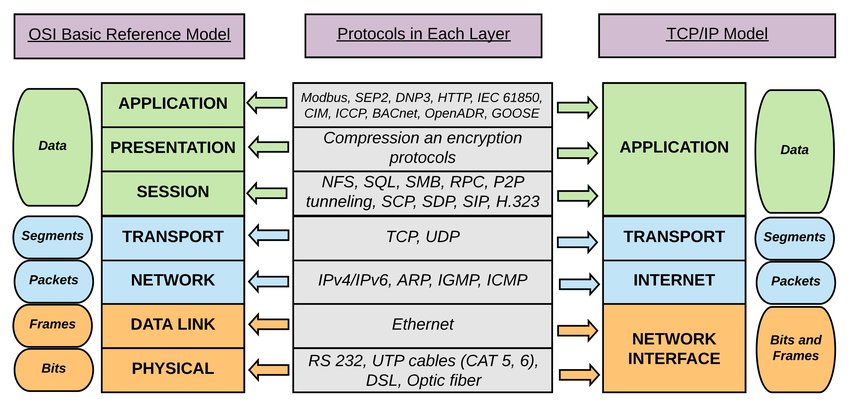
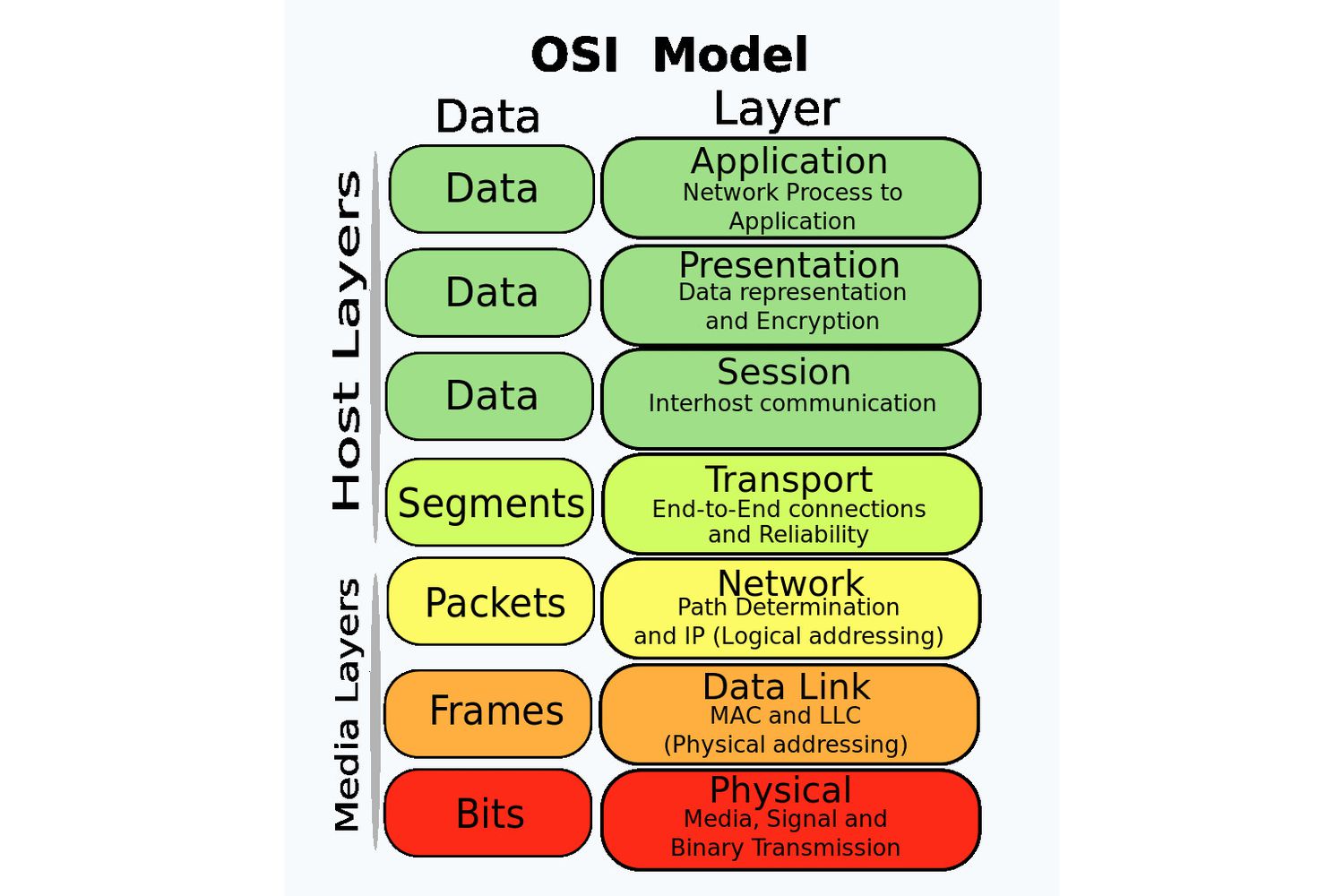
**Logical Bitwise Operations**

Truth Table



CCNA

Lecture 3 (2023-02-06)



* If a system can work up to level 3 (Network layer), we name it Medium System.
  + **Medium System** transfer data without knowing the content of the data, sometimes it knows the type of data.
* If a system can work up to level 7 (Application layer), we name it End System.

The raw data (payload) in the first three layers are not accessible.

**Layer**: a group of standards and functions that work together.

**Physical Layer:** everything in the computer network that you can touch it. It converts and transfer information/data to the signals.

Sender – Physical – Receiver

**NIC (Network Interface Cards):** a hardware component that allows a device to connect to a network and transmit/receive data. It provides a physical connection, has a unique identifier (MAC address), and can connect to one network at a time.

**Bit**: It can be 0 or 1. Everything relate to the network speed is based on bit. Everything relate to the memory is based on **byte**. Download speed is in byte, because it is something that regarding the memory of the computer.

**Bandwidth**: network speed.

Example:

A --------------------------- B --------------------------- C ---------------------------- D

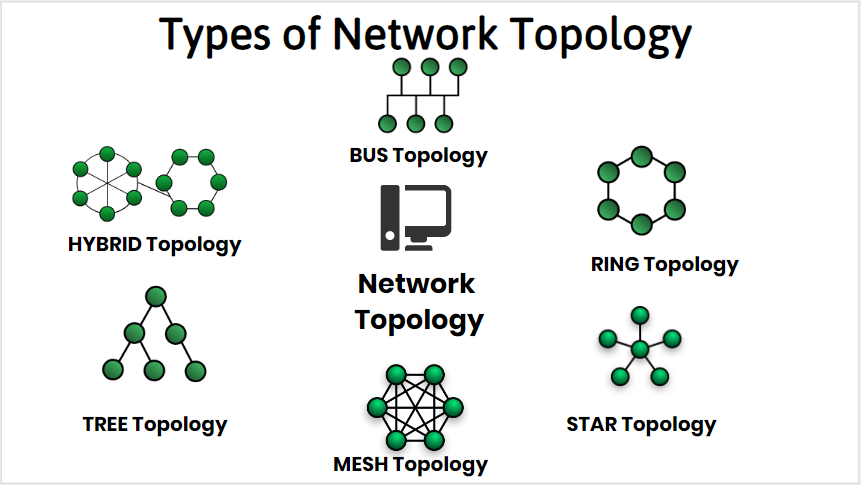
100Mb 1Mb 10Mb

Bandwidth from A to D: 1Mb

When calculating the bandwidth between two points, the minimum bandwidth is considered.

**Topology:**

* Bus
* Star
* Ring
* Mesh

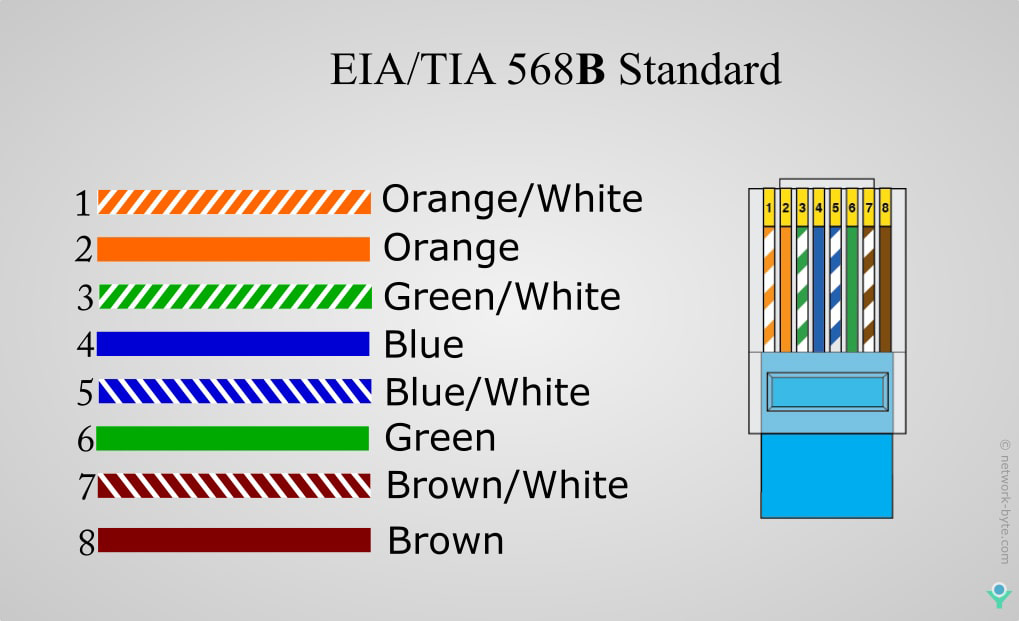


**Collision**: the result of two devices on the same network attempting to transmit data at the same time. Data is destroyed completely after collision.

**Congestion**: It happens when the amount of input is more than the output. Congestion converts to deadlock.

Star model - wire connection: **twisted pair** (UTP & STP).





1 and 2 are sender. 3 and 6 are receiver.

When connecting two computers directly together, we use same model/pattern on both sides.

In the central device, it rotates everything for us.

**UTP vs. STP:**

UTP: a cable with wires that are twisted together to reduce noise generated by an external source. There is no shield for the cable.

STP: a twisted pair cable with an additional mesh shield that guards the cable against electromagnetic interference. STP is more expensive because more material is used.



**Faceplate**: terminate the end of a network cable and provide a physical interface between the cable and the network equipment in structured cabling systems.



**Wall box:** a frame set in a wall to receive a pillow block or bearing for a shaft passing through the wall.

**Keystone:** connector used in data communications. it should be compatible to your cable type.

**Working Area:** where users complete tasks on their computers.

**Structure cabling:** a set of cabling and connectivity products that integrates the voice, data, video, and various management systems of a building.

A picture containing text, indoor

Description automatically generated

Lecture 4 (2023-02-13)



A network: Passive & Active



* NIC
* Cable



* Connection



* Outlet



* + Faceplate

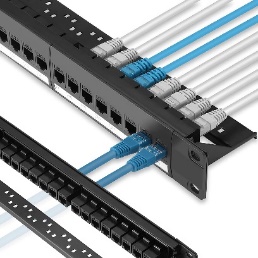


* + Wall-box
  + Key stone

One point where the network cable is terminated using a keystone jack, and another point where the network cable is connected to the patch panel in a network rack or cabinet.

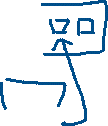
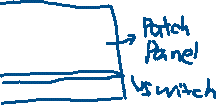


**Patch panel:** all cables from the outlet go to the back side of the patch panel. Only a connector. Passive device. No reading and writing.



**Horizontal cable:** a type of structured cabling that connects network equipment to a telecommunications room. The horizontal cable typically runs from the network outlet, where a device can be connected, to a patch panel or network switch located in the telecommunications.

**Communication closet**: a small room that encloses telecommunications network systems and devices.

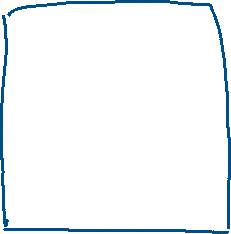
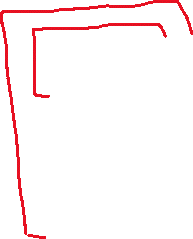
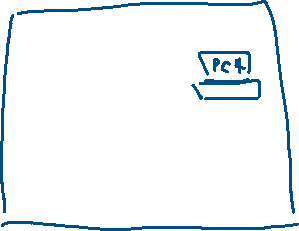
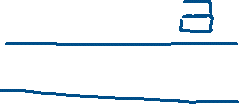


Main criteria of selecting a rack:

* Size and height (unit)
  + Unit ≈4.5 cm
* Depth

Cabling Tray:





Fiber optics: a method of transmitting information from one place to another by sending pulses of infrared light through an optical fiber.

Lecture 5 (2023-02-20)

**Scalability**: we have to be able to expand our network with minimum amount of change. Saving money.

Ex:

Switch room: has 8/16/24/32/48 ports.

Classroom: has 16 pc.

Best solution (Consider scalability): To have 24 ports in the classroom. In long term, in case we need extra pcs or ports price inflation.

Repeater and Hub only works at **physical layer**. No addressing. Bits.

**Repeater**: regenerate/amplify digital signals. Keeps data transfer.

**Hub**: central device that used in start topology. It only knows bits. The communication model in the hub is broadcast. When hub receives something from port 1 and want to transfer to port 6. It will use broadcast that send to all other ports. It causes traffic and lower speed.

**Communication Model:**

* Broadcast: one to all
* Multicast: one to some, a specific group
* Unicast: one to one

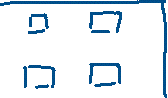
**Drop:** discarding of packets or frames by a network device. It means data is not transmitted to its intended destination and is effectively lost.

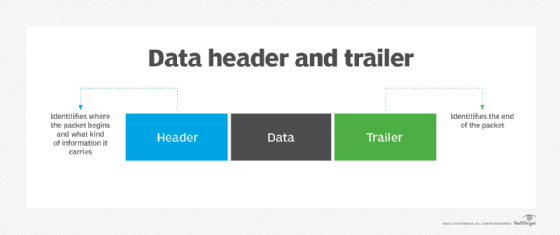
**Data link layer:** data size is different. Frame. Based on the MAC address.

**Frame**: protocol data unit at the data link layer. The result of the final layer of encapsulation before the data is transmitted over the physical layer.

**MAC Address** (Media Access Control): physical address of a network card. Unique in world domain, fixed and permanent. Size is 48 bits. Represent in 16 based hexadecimals.

A device works in layer 2 means it can detect the MAC address.





Five different types of data unit. If a device can work up to layer 3, it is something other than the payload, such as address. MAC layer is the sub link connect to the physical layer.

**PDU**: Protocol data unit. Indicate the type and size of the unit in each layer.

MAC address in layer 2:

* Source address
* Destination address

**Source address**: the address of the device sending the packet.

**Destination address**: the address of the device to receive the packet.

**MAC table:** used by network switches to store the association between MAC addresses and the port on the switch to which each address is connected. Contains port number and MAC address.

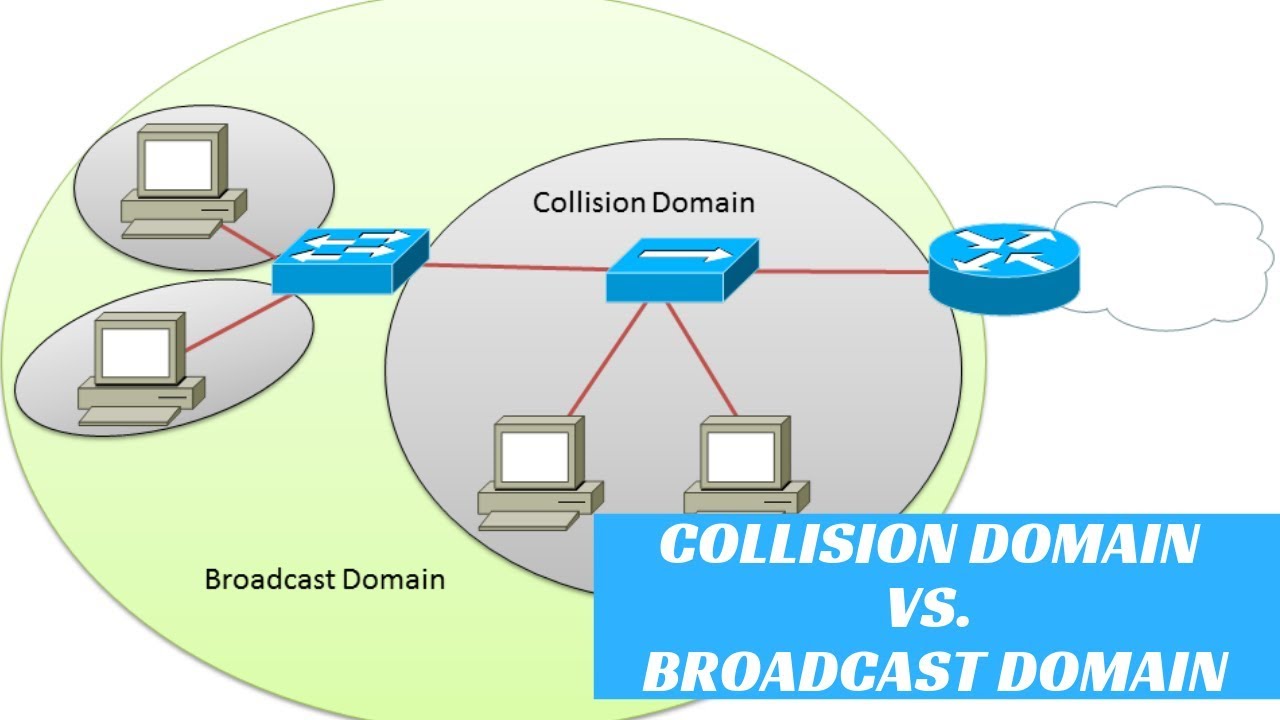
**Switch**: a device in layer 2. Use to connect computers inside a network together. It stores information about the Ethernet interfaces to which it is connected, and it learns the MAC addresses of devices connected to each interface. Switches are faster and more efficient than other devices like hubs because they forward frames only to the devices that need to receive them. Broadcast once, then unicast.

Diagram

Description automatically generated

Merge switch(unicast) and hub(broadcast).

**Broadcast Domain vs. Collision Domain**



**Broadcast Domain**: the group of network devices that can receive broadcast messages sent by any device within the domain. It is greater or equal to collision domain.

**Collision Domain**: a section of network where packet collisions can occur if two nodes attempt to communicate at the same time.

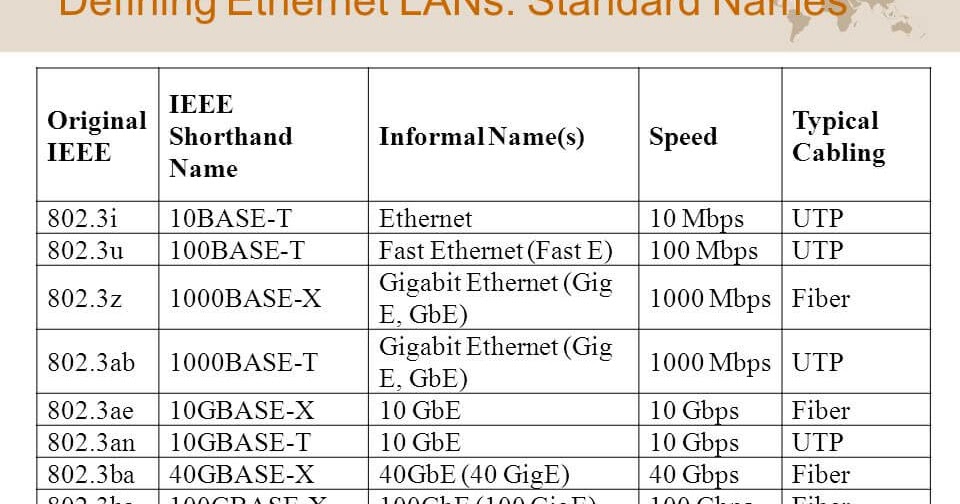
**LLC (Logical Link Control)**: a sublayer provides error control, flow control, and framing of data packets.

Protocol:

* Ethernet (layer 2, standard is 802.3)

IEEE (Institute of Electrical and Electronics Engineers): develop standards.

IEEE 802: a standard for computer network. It covers the physical and data-link layer specifications for technologies such as Ethernet and wireless.



Carrier Sense Multiple Access with Collision Detection (**CSMA/CD**): a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer.

**ACK**: message from the receiver to the sender that indicate message received successfully.

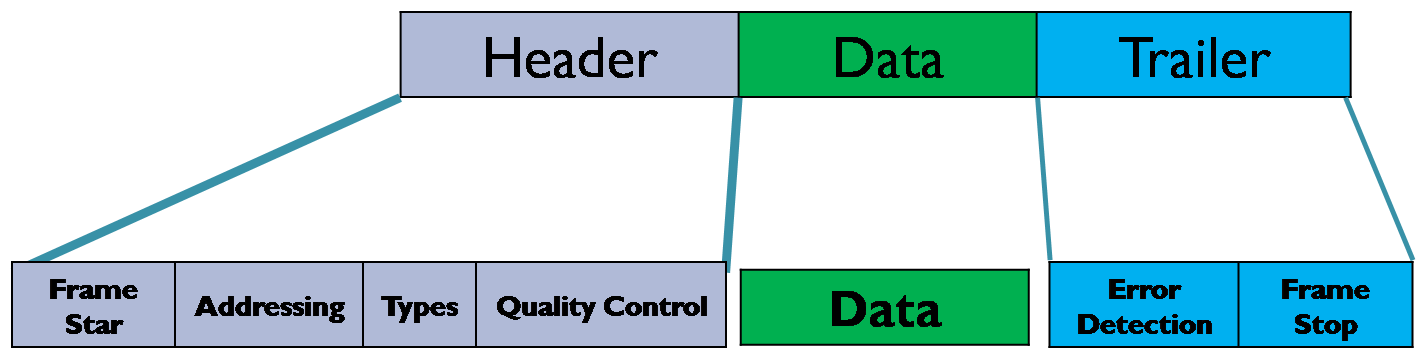
**NACK**: message from the receiver to the sender that indicate message fail to receive.

Lecture 6 (2023-02-27)

Switch in layer 2 connects different computer in same network. Ethernet Protocol is being used. PC uses a MAC address as destination address to call another PC.

**Header:** contains source & destination address based on the MAC address

**Trailer**: contains information concerning the destination of a packet being sent over a network.



**VLAN (Virtual LAN**): instead of having two individual switches, we can create VLAN. Segment a network into smaller, more manageable groups to improve performance. The maximum number of VLAN equals to the total port number. There is no connectivity between two VLANs, two different networks.

Reasons to create VLAN:

* Separate a network from the rest of networks
* Manage network

ping: command used to check the connectivity of the network.

**MAC Filter**: a security method based on access control. Assign a mac address to the port number of a switch. Lock with one port number. Block traffic coming from other machines or devices.

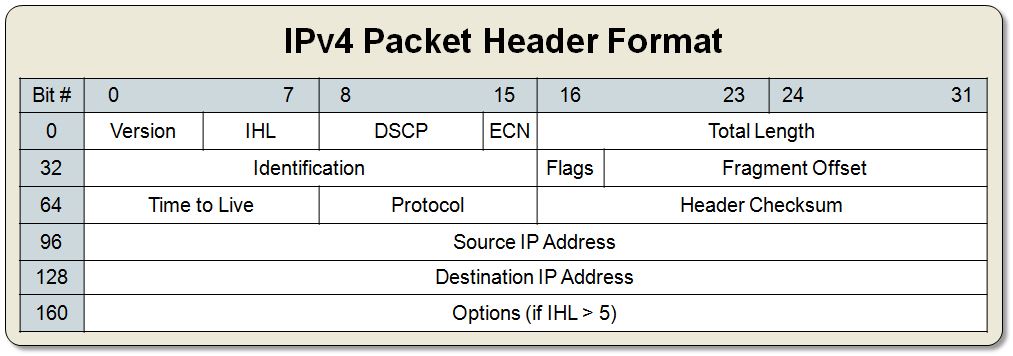
*Layer 3 – Network*

Three Main Activities:

* Segmentation
* Addressing
  + IP (version 4 & version 6)
* Routing

**Router**: device work in layer 3. Use to connect network together.

This layer adds a header containing the source and destination IP addresses to the to the data received from the Transport layer. The packet it creates will then be forwarded to the MAC or Data Link layer.



The router needs to change the size of the packet, when sending the packet.



**Fragment offset**: detects and indicates the order of the packet relate to one message.

**Identification**: shows the id number of one message.

ID: 100 ID:100

Frag:00 Frag:01

How are u?

Hello

ID: 200 ID:200

Frag:00 Frag:01

I’m here

Where are u

A layer 3 device can detect IP address.

A layer 2 device can detect MAC address.

IPv4: Maximum length is 32 bits, 4 billion MAC address.

4 different sections (octets). Each octet is 8 bits.

Table

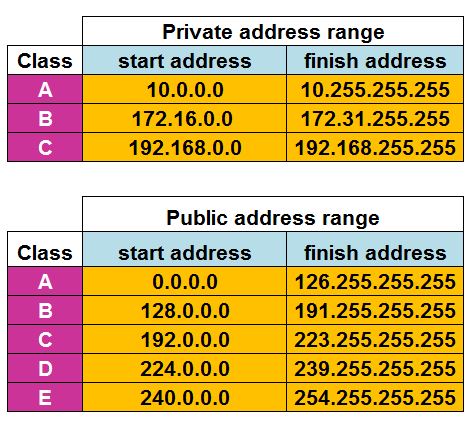
Description automatically generated

**Valid IP Address**: 200.1.20.148

**Invalid IP Address**: 100.270.10.1 Each octet maximum value: 255

**Class (decided by the number in the first octet)**

* A Range: 1-126
* B Range: 128-191
* C Range: 192-223
* D Range: 224-239 (Multicast)
* E Range: 240-255 (Reserved)

127: the localhost/loopback. It doesn’t belong to classes. 0 represent any number

**Public IP address**: an IP address is not private.

**Private IP address**: in each class, we have a range of private IP addresses. Only use inside a network. Cannot used and recognized out of the network.

ipconfig: command to display information about your network configuration.

Ex: 192.168.1.0 && 192.168.1.255

The First address is a network address.

The Last address is a broadcast address.

The first one and the last one cannot be assigned to one computer.

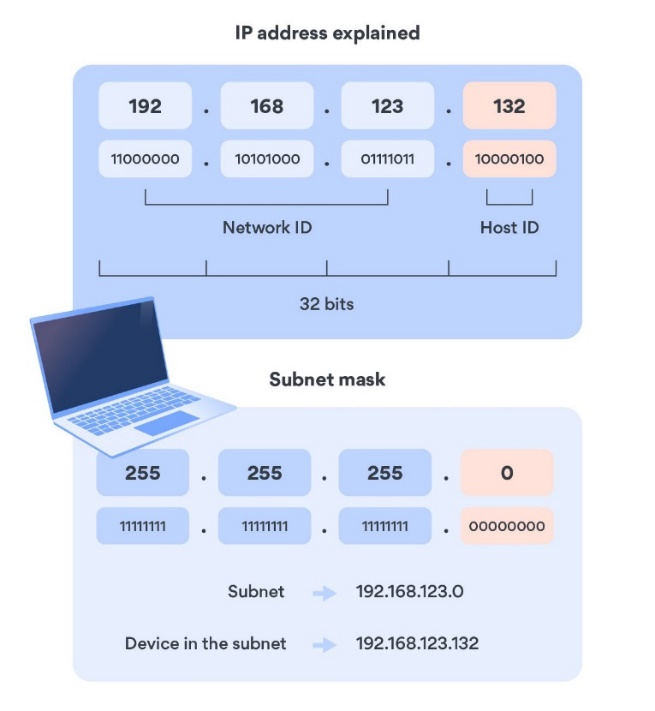
Lecture 7 (2023-03-06)

Layer 3:

* Segmentation
* Addressing
* Routing

We use a router to connect to different network together.

**Subnet mask**: 32-bit address (4 octets). It divides an IP address into network and host portions. It indicates which bits represent network & host. The combination of the IP address and subnet mask determines the range of addresses that belong to the same network. IP address needs a subnet mask.



Subnet mask models:

* Binary:
  + Format: 11111111 11111111 11111111 00000000
* Decimal
  + Format: Convert from binary. 255.255.255.0.
* Number of ones
  + /24

**Standard subnet mask:**

Class A: 255.0.0.0 /8

Class B: 255.255.0.0 /16

Class C: 255.255.255.0 /24

Ex:

192.168.1.3 /24



192.168.1.5 /24

192.168.1.3 /24



192.168.2.2 /24 The first three octets should be equal!!

172.16.21.3 /16



172.16.23.4 /16

10.1.2.3 /8



10.2.3.4 /8

Detect two computers are within the same network or not?

Check if the value in the # of octets is the same.

/24 -> 3 octets /16 -> 2 octets /8 -> 1 octet

Two nodes in the same network use switch.

Two nodes in the different network use router.

**Network address & Host address:**

Number of hosts in the network = 2 to the power of ones -2

(2 is the network address and broadcast address)

*Class A* = 2^8 -2 host address

*Class B* = 2^16 -2 host address

*Class C* = 2^24 -2 host addresses

**Difference between router and switch:**

Each computer has its own IP address. Router and switch connect them together based on the MAC table. Router is a device in layer 3 which work with IP addresses. Therefore, each port of the router needs an IP address. Switch doesn’t need IP address, because the IP address has no meaning to switch (layer 2).

**Gateway**: one side of a router that is connect to the network.

Router doesn’t pass a broadcast packet. Packet should indicate a specific IP address.

**Subnetting**: a technique used in computer networking to divide a single network into multiple smaller networks.

Example 1:

Network: 192.168.1.0 /24

* Network Address: 192.168.1.0
* Broadcast Address: 192.168.1.255

24 -> 1 8 -> 0 2^8 = 256 members

Subnetting to two smaller networks:

128 = 2^x => x = 7 (zero) 32 -7 = 25 ones

Network 1: 128 nodes /25

* Network Address: 192.168.1.0 /25
* Broadcast Address: 192.168.1.127 /25

Network 2: 128 nodes /25

* Network Address: 192.168.1.128 /25
* Broadcast Address: 192.168.1.255 /25

Example 2:

Network: 197.168.0.0 /24

* Network Address: 192.168.0.0
* Broadcast Address: 192.168.0.255

24 -> 1 8 -> 0 2^8 = 256 members

Subnetting to four smaller networks:

64 = 2^x => x = 6 (zero) 32 -6 = 26 ones

Network 1: 64 nodes /26

* Network Address: 192.168.0.0 /26
* Broadcast Address: 192.168.0.63 /26

Network 2: 64 nodes /26

* Network Address: 192.168.0.64 /26
* Broadcast Address: 192.168.0.127 /26

Network 1: 64 nodes /26

* Network Address: 192.168.0.128 /26
* Broadcast Address: 192.168.0.191 /26

Network 2: 64 nodes /26

* Network Address: 192.168.0.192 /26
* Broadcast Address: 192.168.0.255 /26

**VLSM** (Variable length of subnet mask):

192.168.3.0 /24

* Network 1: 128
* Network 2: 64
* Network 3: 32

Start with the biggest portion.

**Network 1**: 128 host

128 = 2^x => x = 7

Subnet = 25

* 192.168.3.0 /25
* 192.168.3.127 /25

--------------------------------------------------------------------

**Network 2**: 64 host

64 = 2^x => x = 6

Subnet = 26

* 192.168.3.128 /26
* 192.168.3.191 /26

----------------------------------------------------------------------

**Network 3**: 32 host

32 = 2^x => x=5

Subnet =27

* 192.168.3.192 /27
* 192.168.3.223 /27

Lecture 8 (2023-03-20)

Subnetting Example:

192.168.3.0 /24

* Network Address: 192.168.3.0
* Broadcast Address: 192.168.3.255

24 -> 1 8 -> 0 2^8 = 256 members

Subnetting to two smaller networks:

* Network 1: 64
* Network 2: 32

**Network 1**: 64 host (nodes)

64 = 2^x => x = 6 (zero) 32 -6 = 26 ones

Subnet = 26

* 192.168.3.0 /26
* 192.168.3.63 /26

**Network 2** -> 32 host (nodes)

32 = 2^x => x = 5 (zero) 32 -5 = 27 ones

Subnet = 27

* 192.168.3.64 /27
* 192.168.3.95 /27

Shortcut: For each cut, add 1 to the subnet.

192.168.1.0 /24 Subnet:24

* Network 1: 128 nodes -> Subnet:25
* Network 2: 32 nodes -> Subnet:26
* Network 3: 16 nodes -> Subnet:27

Notes: Can be use for quick validation, not in exams

**Super netting**: combine some small network to a big network.

Routing

**Routing algorithm**: a method to find the best route of sending a package to a destination.

1. **Static**: the network administrator configs the network. Human decision about the best route.
2. **Dynamic**: router makes decision automatically, no administrator need.
   * **Distance Vector** **(DV)**: decision based on distance.
   * **Link State (LS)**: consider state of the link such as bandwidth, speed, traffic.

Depends on the size of the network. Small, DV is better. Big, link state is better.

HOP: a single network segment that is traversed to reach a destination network.

Diagram

Description automatically generated

DV -> RIP I II

LS -> CSPF

Routing table: a table that is used to find the path of the route.

* Static: As an admin, we insert data into routing table.
* Dynamic: router creates the table automatically.

Send packet worldwide. Maximumly 30 HOPS.

**Time to Live (TTL)**: number that indicate maximum HOP a packet can have in the network. The initial and maximum value is 255. Decrement by 1 in each router. When it reaches 0, the router drops the packet.

**Fill a routing table**:

Router knows the IP address.

Diagram

Description automatically generated

When the initial TTL is set to 128, TTL=116, HOPS=12

When the initial TTL is set to 64, TTL=54, HOPS=10

R1

C 192.168.2.0 /24 F0/0

C 192.168.3.0 /24 F0/1

S 192.168.4.0 192.168.3.2

**Name of the port**: F0/0, F1/1



Routing table of R2:

C 192.168.3.0 /24 F0/2

C 192.168.4.0 /24 F0/0

S 192.168.2.0 192.168.3.1

Lab (2023-03-21)

Cisco command to config VLAN on switch:

Text

Description automatically generated

Table

Description automatically generated

Add an interface to vlan:

A picture containing table

Description automatically generated

enable pass (set password):

Graphical user interface, text, application, email

Description automatically generated

Show running config (has enable password):

Text

Description automatically generated

Disable password:



Enable secret (set encrypted password):

Text

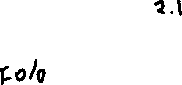
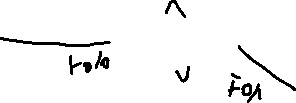
Description automatically generated

Graphical user interface, text, application

Description automatically generated

Lecture 9 2023-03-27

* Static
* Dynamic
  + DY
  + LS



C – connected S - static

*Routing table R1*

C 192.168.1.0 /24 F0/0



C 192.168.2.0/24 F0/1



S 192.168.3.0 /24 192.168.2.2



S 192.168.4.0/24 192.168.2.2



S 192.168.5.0 /24 192.168.2.2

*Routing table R2*

C 192.168.2.0/24 F0/0

C 192.168.3.0/24 F0/2

C 192.168.4.0/24 F0/1

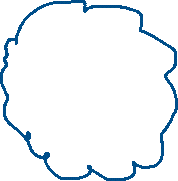
S 192.168.1.0 /24 192.168.2.1

S 192.168.5.0/24 192.168.3.2

Listener 0.0.0.0: anywhere

* Host S.A: 88.11.2.2
* Domain D.A: ~~192.168.1.12~~ 200.1.20.1
* DNS

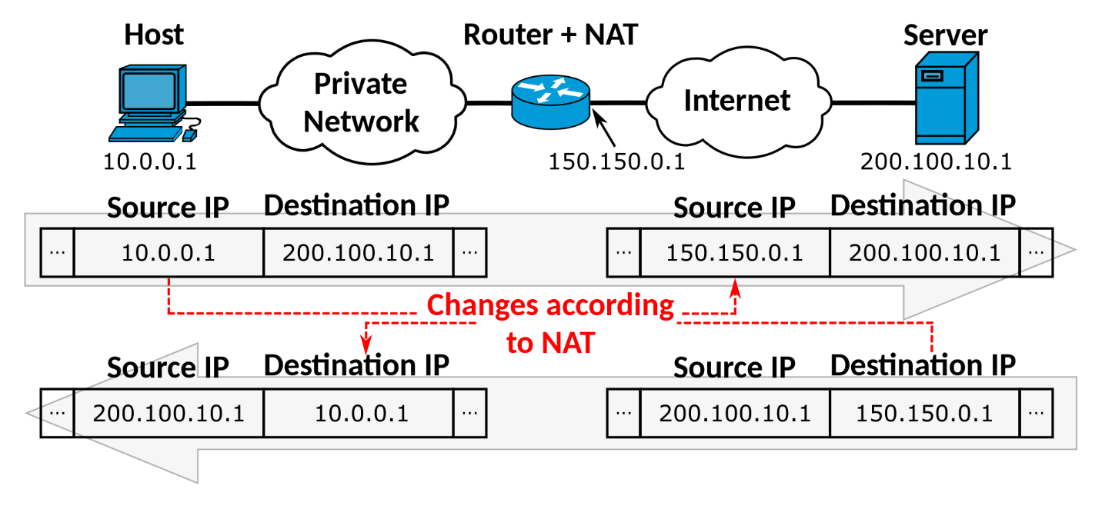
**S.A (Source Address)**: sender **D.A** (**Destination Address)**: receiver

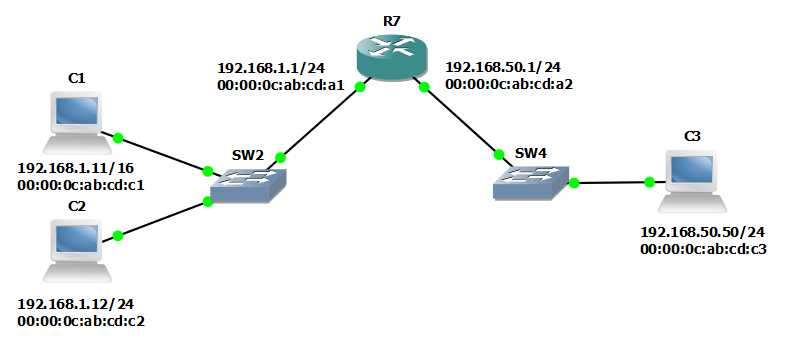


192.168.1.12 /24 S.A: 192.168.1.12 S.A: 200.1.20.1

Default Gateway: 192.168.1.1 D.A: 88.11.2.2 D.A: 88.11.2.2

**NAT** (network address translation): It's a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet. One of the main usages is to share internet.





L7

L6

L5

L4

L3 -> header

* Source Address: 192.168.1.11
* Destination Address: 192.168.1.12

L2

* Source Address: ab:cd:c1
* Destination Address: FF:FF:FF (broadcast address)
* Destination Address: ab:cd:c2

Do you know MAC of 192.168.1.12 ?

If so, tell 192.168.1.11

**Address Resolution Protocol (ARP**): communication protocol. Map an IP address to a physical (MAC) address on a local network. It enables devices to communicate with each other on a local network by associating IP addresses with corresponding MAC addresses.

arp -a: display all current arp entries.

Text

Description automatically generated with medium confidence

If we want to send something out of the network, arp needs the MAC address of the gateway.

L2 -> MAC L3-> IP

Router vs Switch L3:



Can’t tell the difference from the appearance.

Switch:

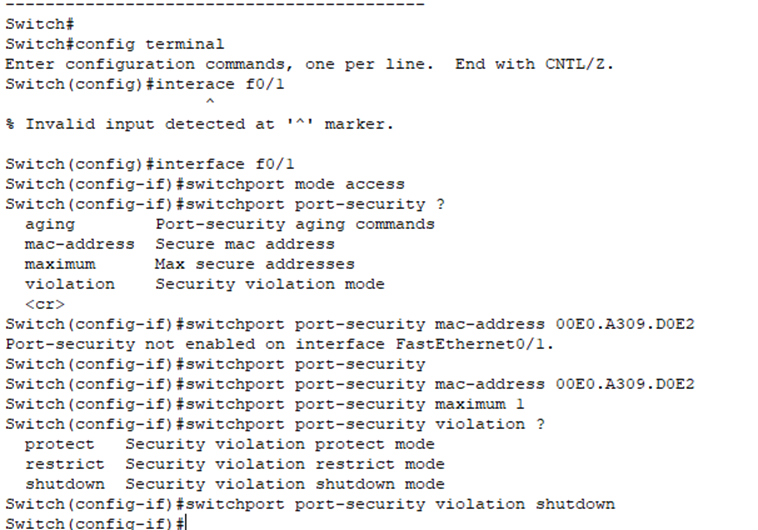
* In functionality, it can do anything that a L3 router can do.
* More number of ports

Router:

* More powerful. Desgined for heavy duty.
* Number of ports
* Variety of ports

Lab 2023-03-28

Set vlan and set port security



Graphical user interface, text, application

Description automatically generated

**Don’t know the mac address (connect to the current address that sticks to):**

Text

Description automatically generated

Show port-security interface f0/2

int f0/2

switchport mode access

switchport port-security mac-address sticky

switchport port-security violation shutdown

switchport port-security maximum 1

**Turn on ports of a router:**

Graphical user interface, text, application, email

Description automatically generated

**Show IP route (exit the current session):**

Text, letter

Description automatically generated

**Config the router**:

Text, letter

Description automatically generated

ping needs bi-directional connection.

Set the default gateway of pc, if the pc is not in the same area, but they are connected to a switch and to a router.

Connect 2 sets of 2 pcs to a switch and a router and connect the router together:

Text

Description automatically generated with medium confidence

Lecture 10 2023-04-03

C connected to the router

A whiteboard with writing on it

Description automatically generated with medium confidence

R2 Routing table

C 192.168.1.0/24 F0/0

C 192.168.4.0/24 F0/1

192.168.2.0/24 192.168.1.1

192.168.3.0 /24 192.168.4.2

192.168.5.0/24 192.168.4.2

192.168.6.0/24 192.168.1.1

*Layer 4: Transport*

* UDP
  + connection less
  + faster
  + no agreement
* TCP
  + connection oriented
  + reliable

Diagram

Description automatically generated

**Port number**: a number that indicate the type of data (TCP/UDP).

**Two types of port number:**

* Standard ports: 0-1023
  + Port 80: web service page
  + Port 443: HTTPS
  + Port 21: FTP
  + Port 22: SSH
  + Port 110: POP3 (for email)
  + Port 53: DNS (UDP port)
    - Converts domain name to IP
  + Port 49:
* Non-Standard ports: 1024-65535
  + Port 1880: Node-red.
  + Port 1883: MQTT, message queuing telemetry transport protocol

Ping doesn’t have port number. It uses ICMP.

**Header of layer 4:** additional layer that add to the payload of each layer.

*Layer 5: Session*

**Session**: controls connection. Connection between applications, not between machines. The connection should be stable or not, its duration.

*Layer 6: Presentation*

**Presentation**:

* Compression: used to maximize the use of bandwidth across a network or to optimize disk space when saving data
  + Lossy: used when a file can afford to lose some data.
  + Loss less: reduce file size by removing unnecessary metadata. Doesn’t loss data.
* Encryption: the process of scrambling data so that it's unreadable to unauthorized parties
  + Two kinds of encryption model
    - Symmetric: use one key to encrypt and decrypt. More complex, bandwidth
    - Asymmetric: two different keys
      * Public key: used to encrypt. Anybody wants to access data can have it.
      * Private key: used to decrypt. Confidential. Only owner has.
  + Key: a formula that used to encrypt/decrypt data
  + Plain text : message before encryption
  + Cipher text : message after encryption

Ex :

Encryption key : -1

DBT = CAS ≠ CAR = DBS

Which one is better? Symmetric or Asymmetric?

It depends on the usage. System, bandwidth, etc.

Length of the key is important for us to protect the data.

**Complex password:**

|  |  |
| --- | --- |
| 0-9 | 10 |
| a-z | 26 |
| A-Z | 26 |
| \*,? | 10 |

Total : 72 possibilities/digit

A complex 8 digits password: 72^8 possibilities

**Virtual Private Network (VPN**): establishes a secure connection between user and internet

* Client to Client
* Client to Site
* Site to Site

Diagram

Description automatically generated

When we use asymmetric model, we need a CA server.

Certificate authority (CA): a trusted entity that issues SSL certificates.

Certificate is not valid:

Graphical user interface, text, application, email

Description automatically generated

Public Key Infrastructure (PKI): a system of processes, technologies, and policies that allows you to encrypt and/or sign data.

Lab 2023-04-04

A picture containing text, indoor

Description automatically generated

Graphical user interface, application

Description automatically generated Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated Diagram

Description automatically generated

Lab 2023-04-11

Config default route (ip address that the port is connected to)

A picture containing text

Description automatically generated

Chart

Description automatically generated

Add RIP (two network the router connected to)

R1:

A screenshot of a computer

Description automatically generated with medium confidence

R2:

Text, letter

Description automatically generated

Diagram

Description automatically generated

Virtual Interface = number of VLANs

Config the router:

We need config virtual interface on the router because it’s connected to VLANs.

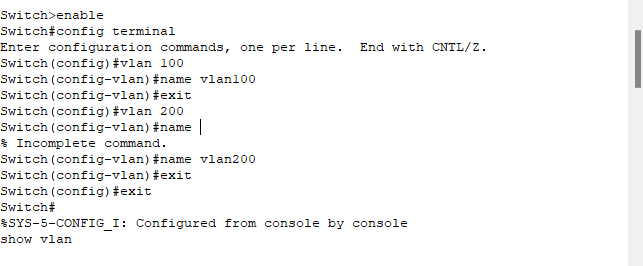
G0/0/0.100 G0/0/0.200

Config the switch: change the mode to trunk, not access mode.

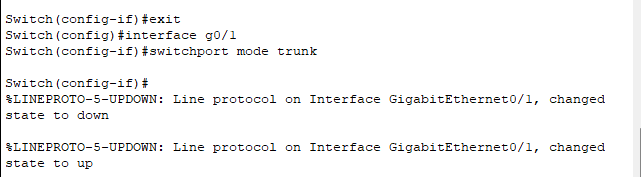
Text

Description automatically generated

Create VLAN



Change switch port mode:



Lecture 11 2023-04-24

* One way encryption: cannot decrypt
  + Hash: one way encryption, can be used for error detection to check the message
    - Ex. Cipher text, can’t convert it to plain text
* Two-way encryption: can encrypt and decrypt

Famous encryption model: AES, RSA, ECC, AEAD

*Layer 7: Application*

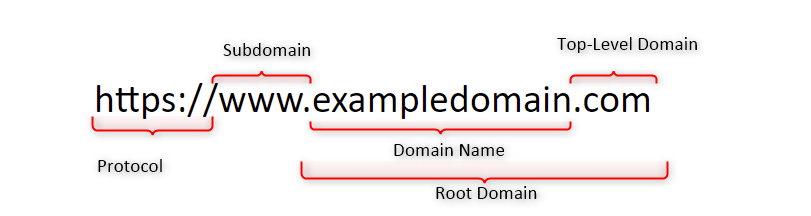
Application layer: end user.

**DNS (Domain Name System):** translate/convert IP address to name & name to IP address.

Domain: name & IP address

Host: a location to upload files

**FQDN (fully qualified domain name):** full format of a web server.



Structure:

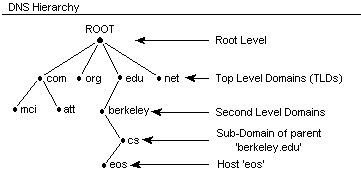
* Protocol
* Subdomain
* Domain name
* TLD (top level domain)

ping 4.2.2.4: one of the main DNS in the world, can be used to check connectivity to the internet.

scholor.google.ca

www.google.ca

DNS tree



**Dynamic Host Configuration Protocol (DHCP):** a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

**Wireless communication (W\_LAN**):

* Antenna
  + Gain: unit - dB(decibel)
  + Direction
    - Omni Directional: spread signal like a ball. Ex: WIFI router at home
    - Directional: Sense in specific angle.
      * Horizontal Angle
      * Vertical Angle
* AP
* Access Point