DevOps Training

Computer Networking

Suryaraj Timsina

Agenda

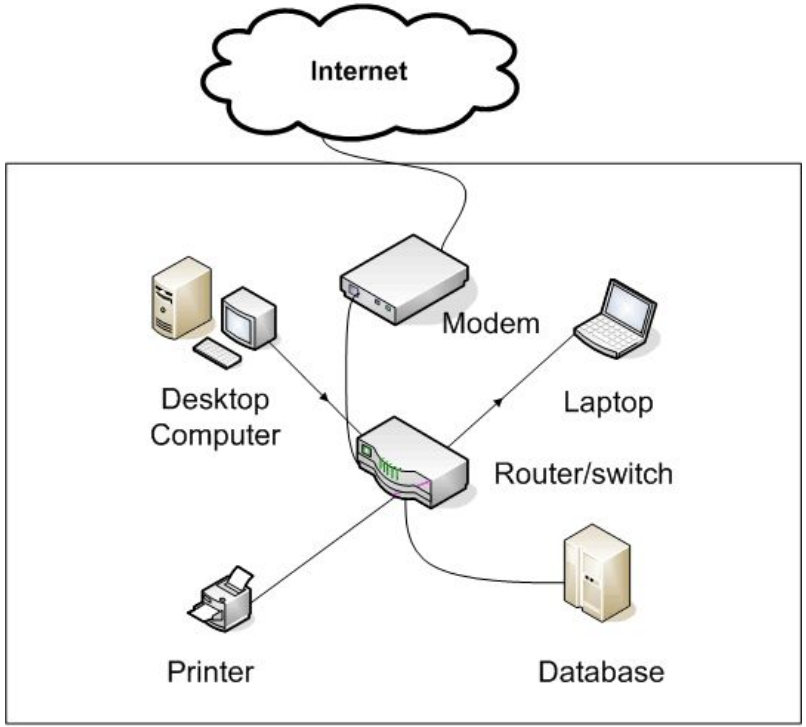
1. Introduction to Computer Network
2. Components of Network
3. Internetworking Models OSI vs TCP/IP.
4. Classification
5. Devices
6. Home Network
7. IP Addresses
8. Protocols
9. DNS and DHCP
10. Network commands

Introduction to Computer network

- A group of computer systems, network devices linked together to allow sharing of data.
- Communication between two or more network interfaces.

Components

- Internet
- Modem
- Router
- Firewall
- Switch
- Cable as links between the computers
- Computer
- Software called operating system



Internet

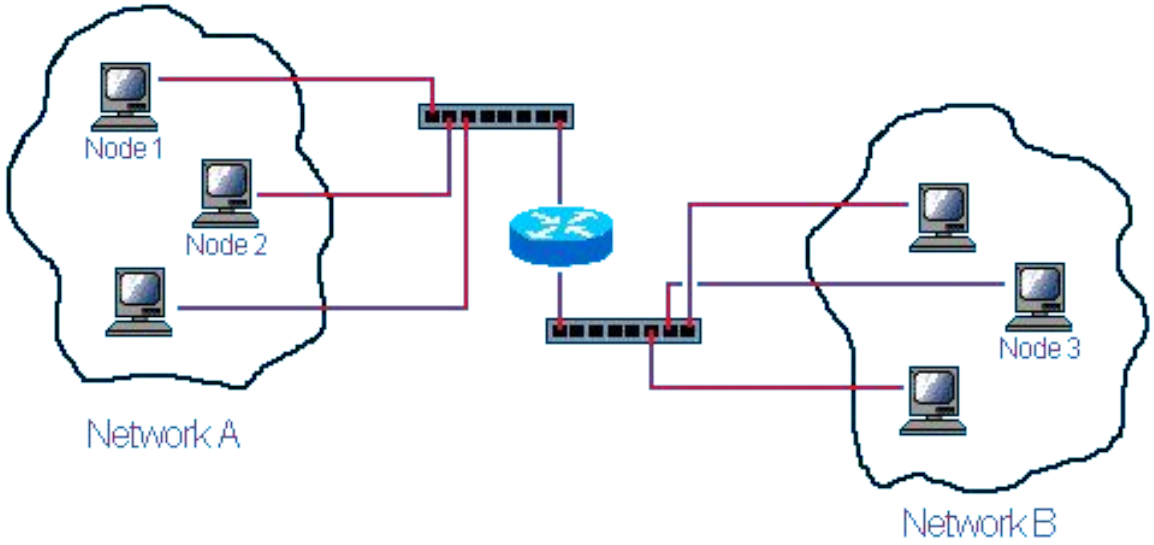
- Global system of interconnected computer networks that use the internet protocol suite(TCP/IP) to link the worldwide.
    - Also termed as internet cloud, cloud computing.

Modem

- Connects internal network to the internet.
- It turns the Ethernet signal, the protocol or the language used on your internal network into the language that can be used on the internet.

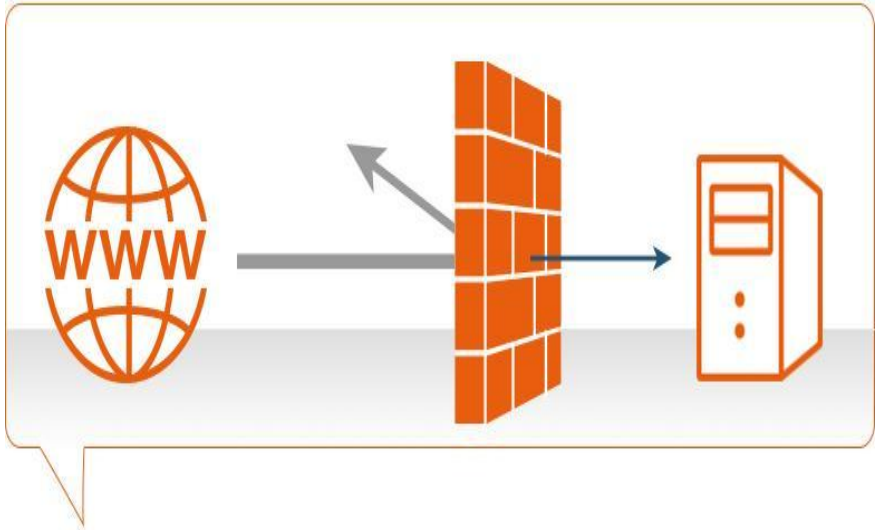
Router

It allows to separate different networks.



Firewall

- It is a device that prevent hackers from being able to get into the internal network through the internet
- Now a days
    - **Software Firewall**
        - Intrusion protection system where you have entire servers that run.
    - **Built in to Router / Modem**
        - Allows to block website.



Switch

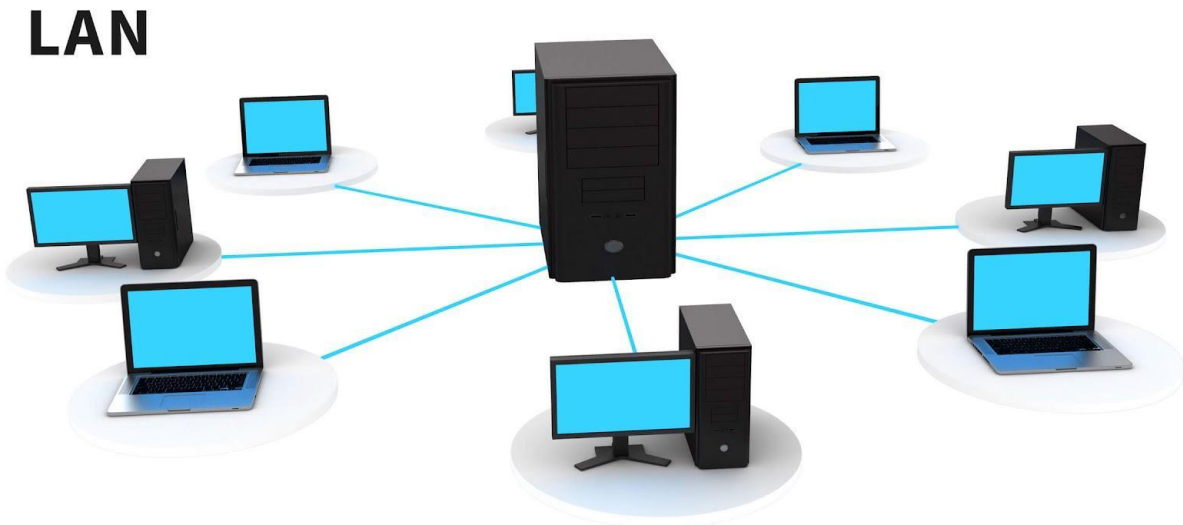
- Splitter of the internet signal.
- It allows computer to communicate with each other or to go out to the internet.
    - HUB
        - Dump, split the internet signal, network signal to everybody equally.
    - SWITCH
        - Little bit intelligence, understand how to transfer data.

Types of Computer network(Classification)

- Based on Geography.
  - LAN
  - WAN
  - MAN
  - PAN
  - CAN

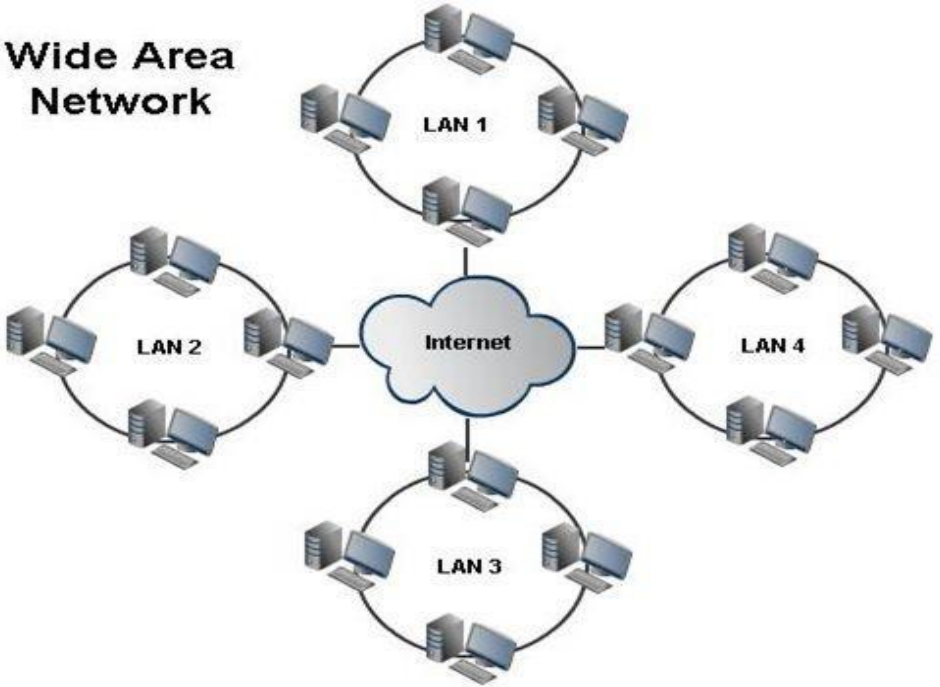
Local Area Network(LAN)

- Local within a building or within a department.
- It is typically high speed.
- Centrally located.
- E.g Ethernet, WiFi.



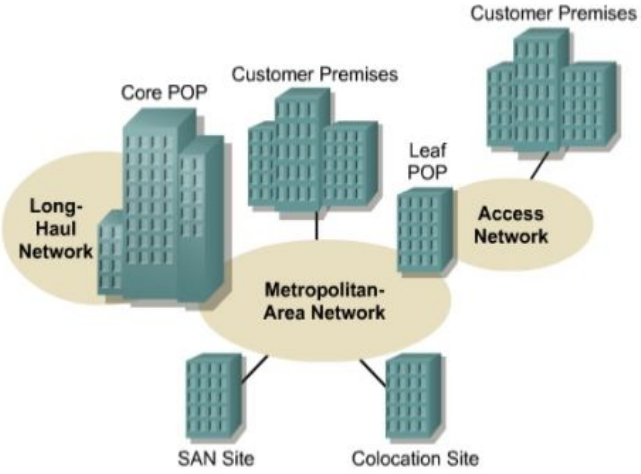
Wide Area Network (WAN)

- It interconnects geographically dispersed locations.
- Speed are typically less than LAN speeds
- Sites connect into a service provider.
- E.g: Internet.



Metropolitan Area Network

- Interconnects office locations in a Metropolitan area.
- Limited availability, not in every city.
- Very high speed connectivity between the offices.
- Redundancy, as it is connected in a ring fashion.
- E.g: Cable tv network.

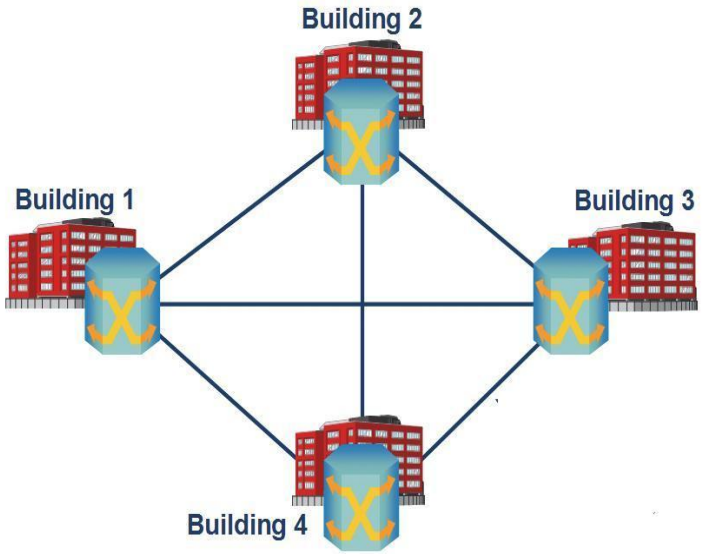


Personal Area Network

- Interconnects two devices.
- Limited distance.
- Limited throughput.
    - E.g. game remote.

Campus Area Network

- Interconnects buildings on a Campus.
- High speed.
- Interconnects nearby buildings (Fiber optic cabling).
- Easy to add redundancy(One or more links).

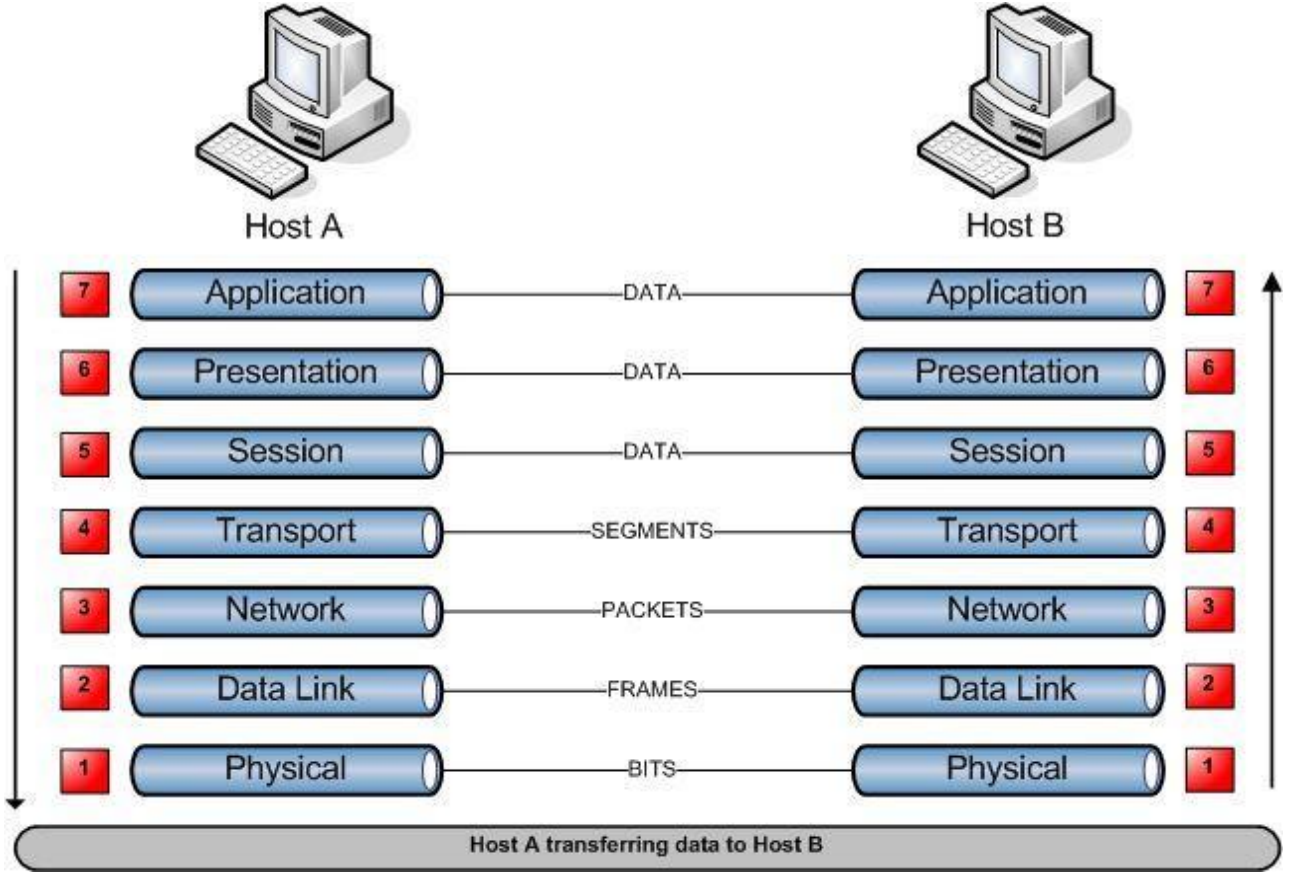


OSI Reference Model

Open

System

Interconnection



OSI Model

- People around the world uses computer network to communicate with each other.
- For worldwide data communication, systems must be developed which are compatible to communicate with each other
- There should be the standard communication method and devices
- International standard organization established a committee to develop an architecture for computer communication. This communication model is called Open system interconnection(OSI).
- It is the networking framework to implement protocols in layers with control passed from one layer to the next.
- ISO-OSI is a seven layer architecture developed in 1984

Basic Elements of OSI Model

Services

- A service is a set of actions that a layer offers to another (higher) layer.

Protocol

- A protocol is a set of rules that a layer uses to exchange information.

Interface

- A interface is a communication between layers

OSI Layer Protocol and Examples

Layer Name	Protocols and Specifications	Devices
Application, presentation, session (Layers 5–7)	Telnet, HTTP, FTP, SMTP, POP3, VoIP, SNMP	Firewall, intrusion detection systems, hosts
Transport (Layer 4)	TCP, UDP	Hosts, firewalls
Network (Layer 3)	IP	Router
Data link (Layer 2)	Ethernet (IEEE 802.3), HDLC, Frame Relay, PPP	LAN switch, wireless access point, cable modem, DSL modem
Physical (Layer 1)	RJ-45, EIA/TIA-232, V.35, Ethernet (IEEE 802.3)	LAN hub, LAN repeater, cables

Physical Layer

- Ist layer of OSI model.
- In this layer, all the physical connectivity of a network , such as connectivity of devices using wires takes place.
- It converts data into bits and forwards it to a data link layer.
- Devices used in this layer are Hub, repeaters, cables etc.
- Datagram at physical layer called bits.

Data Link Layer

- 2nd layer of OSI model.
- Provides connection between the hosts on the same network.
- Converts bits into frames and forwards it to the network layer.
- Responsible for framing, physical addressing, flow control, error control and access control.
- Devices used in this layer, Switch, bridge, and NIC.
- Protocols used,PPP, PPTP.
- Datagrams at this layer called frames.

Network Link Layer

- 3rd layer of OSI model.
- Provides connection between hosts in different network.
- Converts frames into packets and forward it to transport layer.
- Responsible for logical addressing, routing etc.
- Devices, Routers.
- Protocols used, IPv4, IPv6 and ICMP.
- Datagram at the layer called packets.

Transport Layer

- 4th layer of OSI model.
- Converts packets into segments and forward it to session layer.
- Responsible for segmentation, connection control, flow control and error control.
- Protocols works, TCP and UDP.
- Datagram at this layer called segments.

Session Layer

- 5th layer of OSI model.
- Responsible for dialog control and synchronization.
- Controls duplexing, termination and restart.
- Protocols works, PAP and RTCP.

Presentation Layer

- 6th layer of OSI model.
- Responsible for translation, encryption and compression.
- Protocols works, SSL.

Application Layer

- 7th or last layer of OSI model.
- Layer where user can directly interact with the data.
- It provides user interface and supports service such as mail access, file transfer, browsing internet, remote desktop connection etc.
- Protocols works, FTP, TELNET, DHCP, HTTP, DNS, SMTP etc.

Ref: https://www.javatpoint.com/osi-model

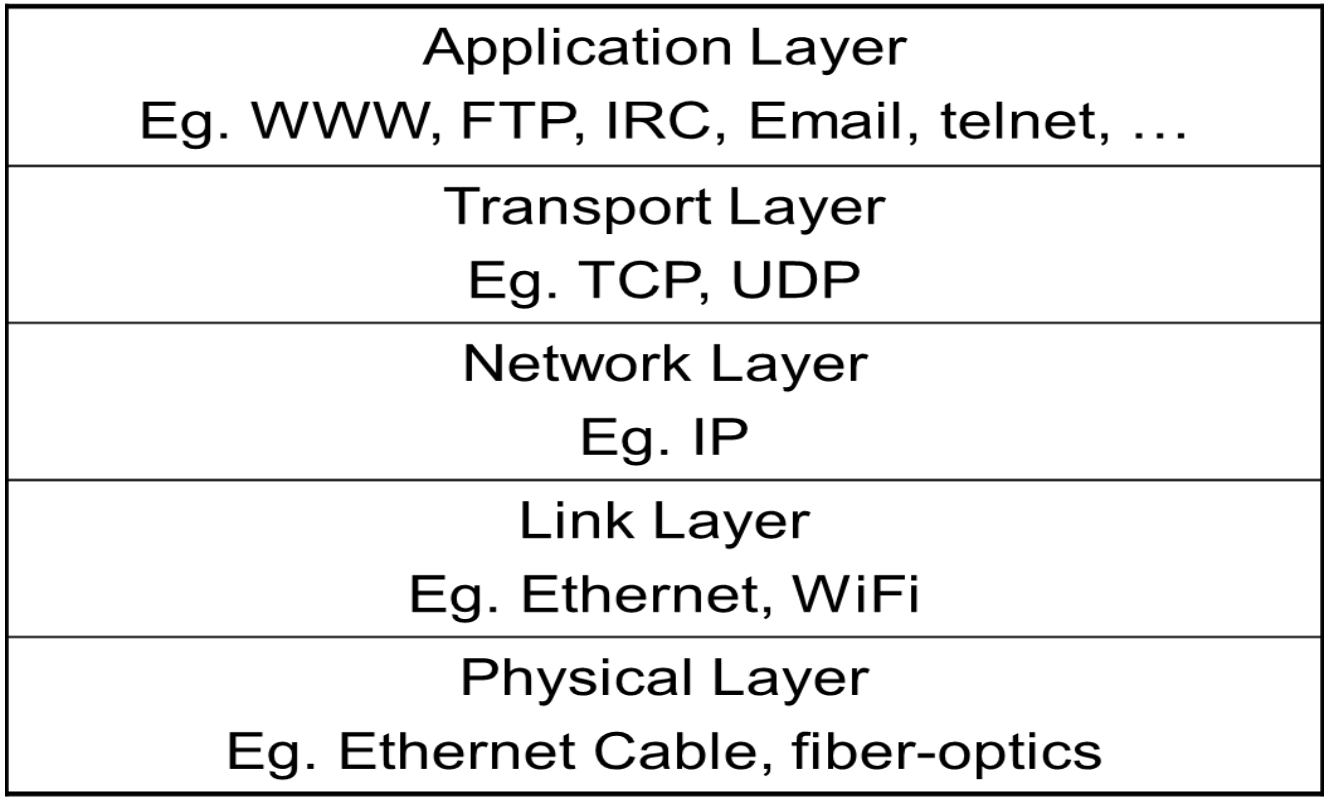
TCP/IP

- TCP/ IP is made up of TCP protocol and IP protocol.
- It is the family of protocols all tied together that make the internet works.
    - Main protocols
        - TCP
        - IP

TCP/IP

- IP
  - It is the protocol that controls routing of information to different computers, different devices in the network.
  - It deals with ip addresses, subnet mask, default gateway, DNS etc.
  - It allows two computers to find out where the other one is, therefore can start communication.
  - Importantly, it is the routable protocol.
- Routable protocol
  - It allows you to divide huge networks into smaller sub networks.
  - Being routable protocol you connect all those subnets using router.

TCP/IP


Application Layer
Eg. WWW, FTP, IRC, Email, telnet, …
Transport Layer
Eg. TCP, UDP
Network Layer
Eg. IP
Link Layer
Eg. Ethernet, WiFi
Physical Layer
Eg. Ethernet Cable, fiber-optics
Data
Segments
Packets
Frames
Bits

Protocol

- Protocol is the formal specification that defines the procedures that must be followed when transmitting or receiving data.
- Protocol defines the format, timing, sequence and error checking used on the network. E.g HTTP, FTP, SSH
- The client and server that understands this protocol knows how to communicate by following that particular protocol

TCP vs UDP

TCP

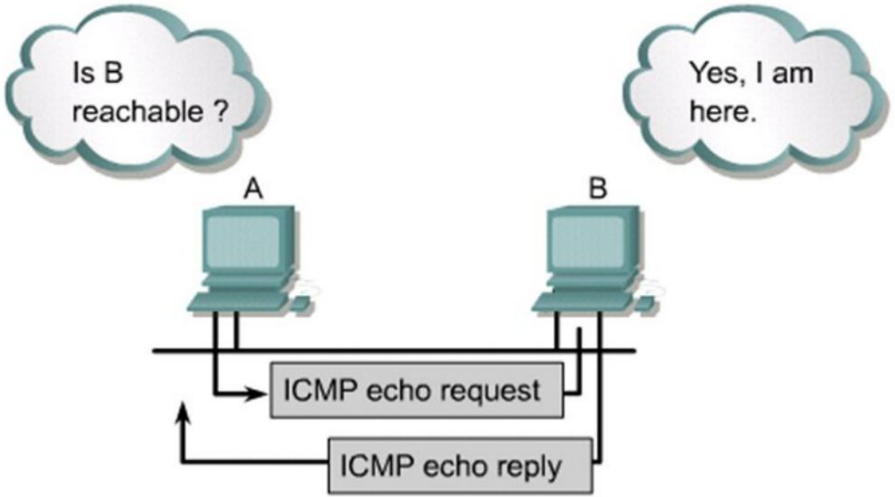
- Reliable
- Connnection oriented
- Performs 3 ways handshake
- Provision for error detection and retransmission
- Most applications use TCP for reliable and guaranteed transmission
- FTP, HTTP, HTTPS

UDP

- Unreliable protocol
- Connectionless
- Much faster than TCP
- No acknowledgement waits
- No proper sequencing of data units
- Suitable for application where speed matters more than reliability
- DNS, DHCP, TFTP, ARP

Internet Layer Protocol

- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)
- Internet Protocol(IP)



Traffic generated by the `ping` command

Internet Control Message Protocol

- It is the part of internet protocol suite and defined in RFC 792.
- It is used to report the problems with the delivery of IP datagrams within the IP network.
- It can be used to show when the particular end system is not responding, when an IP network is not reachable, when a node is overloaded, when an error occurs in IP header information.
- It can be used to check routers are correctly routing packets to specific destinations.

ICMP Applications

Ping

- It checks whether a host is alive and reachable or not.
- It is checked by sending an ICMP Echo Request packet to the host and waiting for an ICMP Echo Reply from the host.

Traceroute

- It is the utility that records the route(the specific gateway computers at each hop) through the internet between your computer and a specified destination computer.
- It also calculates and displays the amount of time each hop took.

MAC Address vs IP Address

MAC Addresses

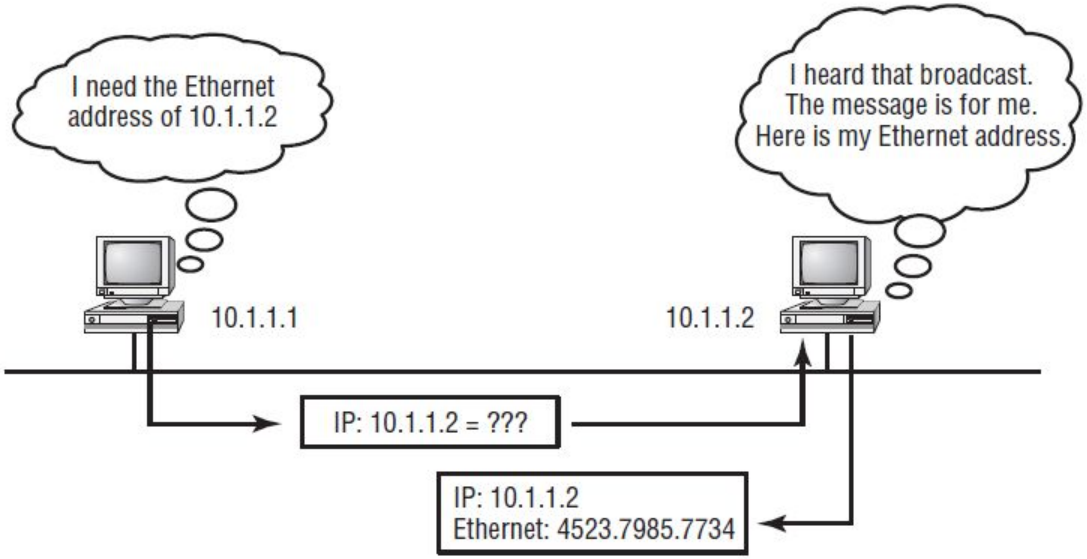
- Hard-coded in read-only memory when adapter is built.
- Like a social security number.
- Flat name space of 48 bits(e.g. 00-0e-9b-6e-49-76)
- Portable and can stay the same as host moves.
- Used to get packet between interfaces on the same network.

IP Addresses

- Configured or learned dynamically.
- Like a postal mailing address.
- Hierarchical name space of 32 bits(192.168.5.215)
- Not portable, and depends on where the host is attached .
- Used to get a packet to destination IP subnet

Address Resolution Protocol

- Hardware Address to IP address mapping



Dynamic Host Control Protocol

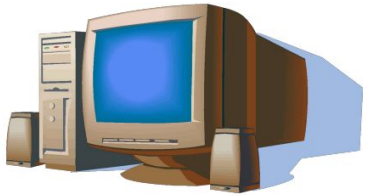
arriving client

DHCP discover (broadcast)

DHCP offer

DHCP request (broadcast)

DHCP ACK

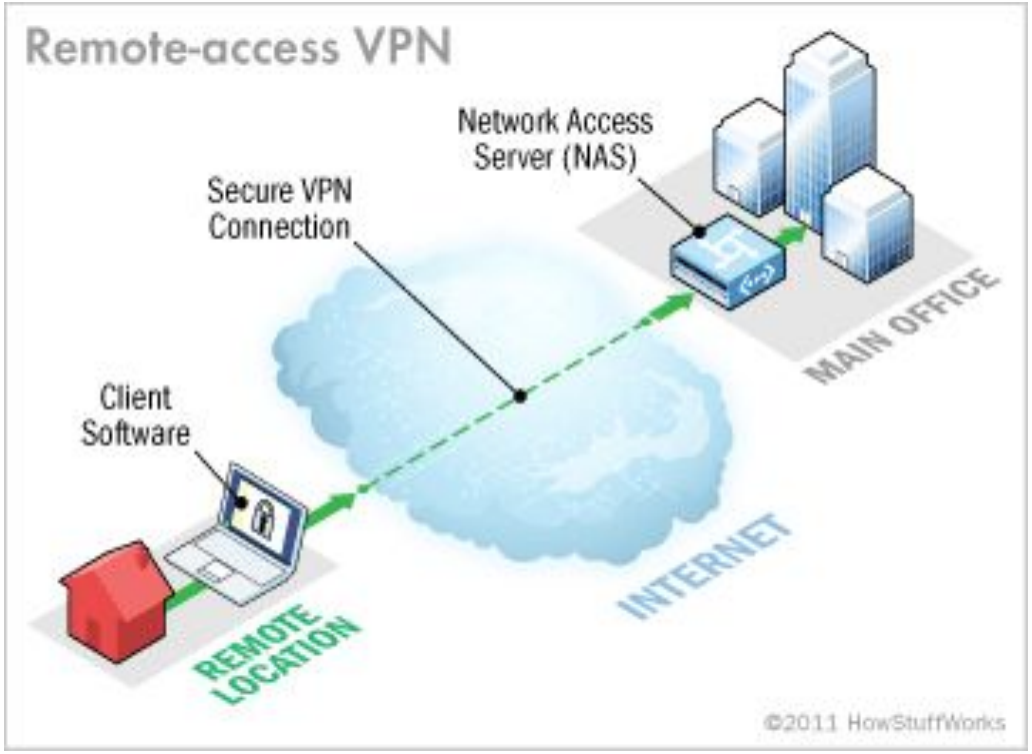


DHCP server

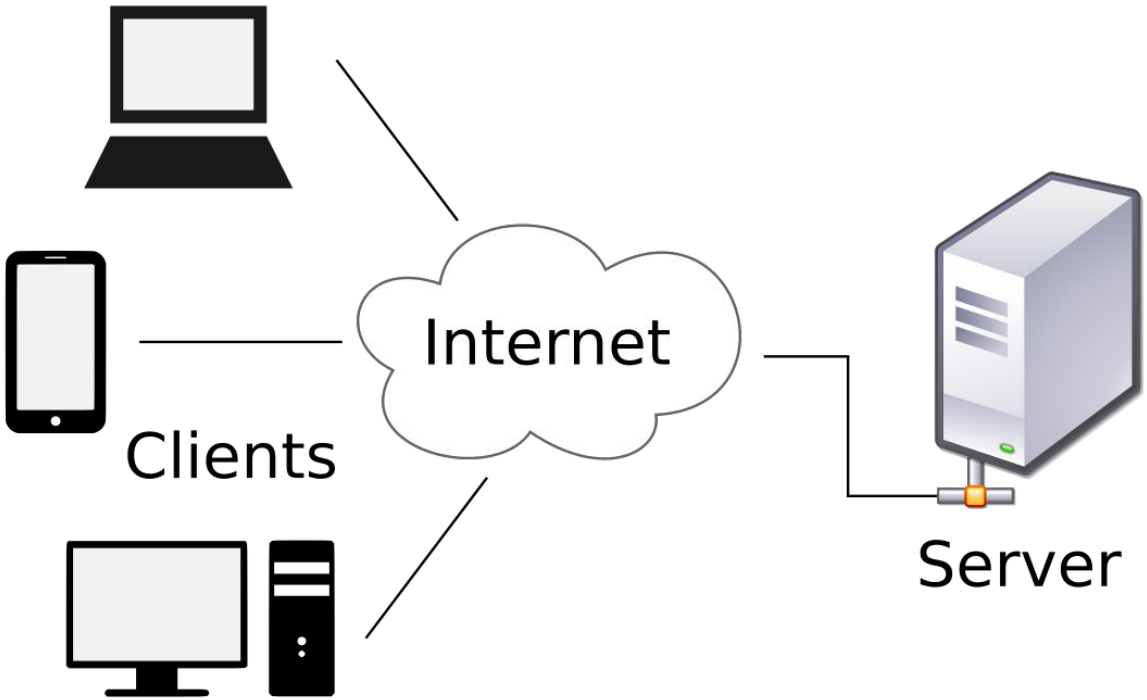
VPN

- Allows to access the internal network from outside.
- Little bit slower than the internal network.
- Works on client-server architecture.
    - Server
        - Logical server inside internal network called a VPN endpoint and it consists of credentials for people.
    - Client
        - Users install client software and enter credentials.
        - VPN endpoint authenticate and allows connection to the internal network.

VPN


Remote-access VPN
Network Access Server (NAS)
Secure VPN Connection
Client Software
MAIN OFFICE
INTERNET
REMOTE LOCATION
©2011 HowStuffWorks

Client Server Architecture

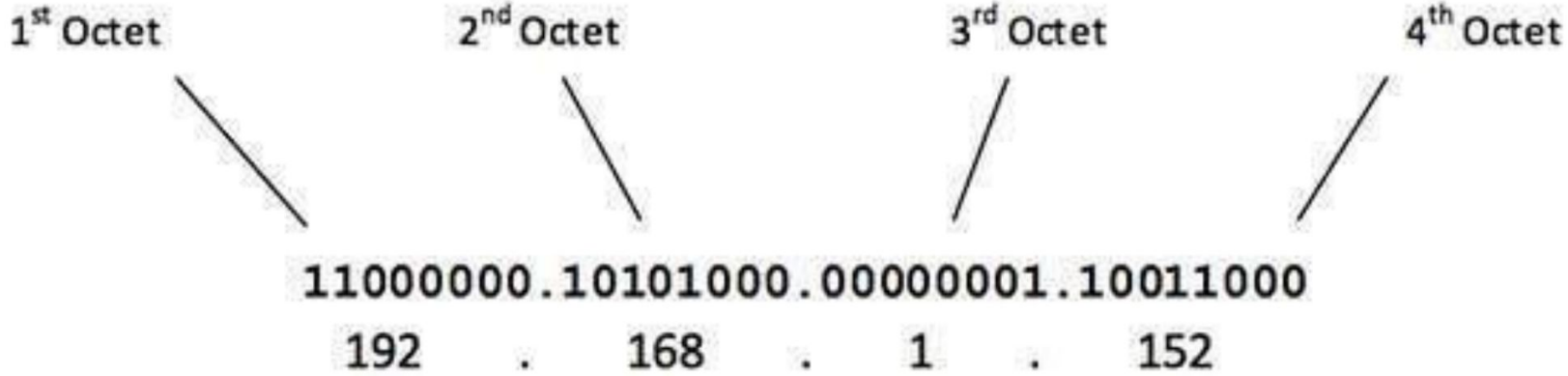


Devices, Servers & Clients

- Devices
  - Anything on the network are networking devices.
- Servers
  - Any devices that provide services and resources.
- Clients
  - Any devices that gets services, resources from servers.

IP Address

1. 32 bit logical address
2. IP address= Network Portion + Host Portion
3. Divided into 4 octets.



Classes Of Network

- Class A: 1-126(0 and 127 not used)
  - ***N.H.H.H***
- Class B: 128-191
  - ***N.N.H.H***
- Class C: 192-223
  - ***N.N.N.H***
- Class D: Multicast: 224-239
- Class E: Reserved: 240-255

Look the first octet

For class A

00000000=0

01111111=127

For class B

10000000=128

10111111=191

For class C

11000000=192

11011111=223

Class of Network

- No. of networks and no. of hosts in each class.

Class	First Octet Range	Valid Network Numbers*	Total Number for This Class of Network	Number of Hosts Per Network
A	1 to 126	1.0.0.0 to 126.0.0.0	$2^7 - 2$ (126)	$2^{24} - 2$ (16,777,214)
B	128 to 191	128.0.0.0 to 191.255.0.0	2^{14} (16,384)	$2^{16} - 2$ (65,534)
C	192 to 223	192.0.0.0 to 223.255.255.0	2^{21} (2,097,152)	$2^8 - 2$ (254)

Subnet

- Logical subdivision of an IP network.
- Dividing a network into two or more networks is subnetting.

Default Subnet Mask

Subnet Mask

- Separates network ID and host ID

Default Subnet Mask

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

Tools

Ping
Traceroute
Mtr
Nslook
Dig
Nmap
netstat