UNIT 1 NOTES

Vidyalekhan

DATE

PAGE

Basics of Networking :

Reference : Slides - Dr. Lokesh Chauhan (Network Security & Forensics)

Defn : Computer Networks connect two or more autonomous computers. The computers can be geographically located anywhere.

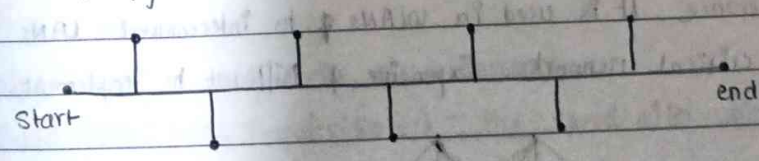
Types : LAN, MAN, WAN

Applications : 1) Resource sharing - Hardware, Software
2) Information Sharing - Easy Accessibility, Search Capability (WWW)
3) Communication - Email, Message Broadcast
4) Remote Computing - Connect to work PC from off-campus PC.
5) Distributed Processing (GRID Computing) - use of widely distributed computer resources to reach a common goal.

Defn : The Network Topology describes the way in which computers, printers & other devices are connected. A network topology describes the layout of the wire & devices as well as the paths used by data transmissions.

Types :

1) Bus Topology - all devices are connected by one single cable.

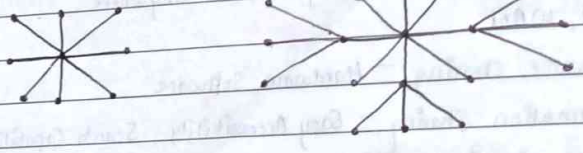


* Difference b/w media & medium?
* Types of transmissions - simplex, half duplex, duplex.

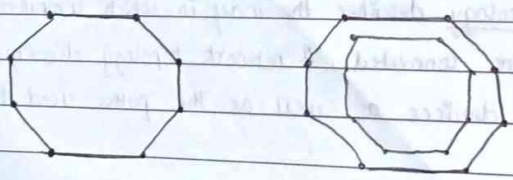
Vidyalekhan
DATE
PAGE

Star → most common in Eth. LANs

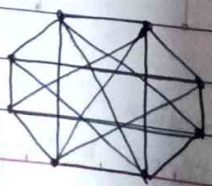
2) Star & Tree Topology – Extended star topology is called tree topology. When used with network devices that filter frames or packets like bridges, switches & routers, this topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.



3) Ring Topology – A frame travels around the ring stopping at every node. If a node wants to transmit data, it adds the data as well as the destination address to the frame.
Single Ring (Unidirectional), Dual Ring (Bidirectional)



4) Mesh Topology – Connects all devices to each other for redundancy & fault tolerance. It is used in WLANs & to interconnect LANs and for mission critical networks. Expensive & Difficult to implement.



Defn :

TCP/IP Stac

Client-Serve

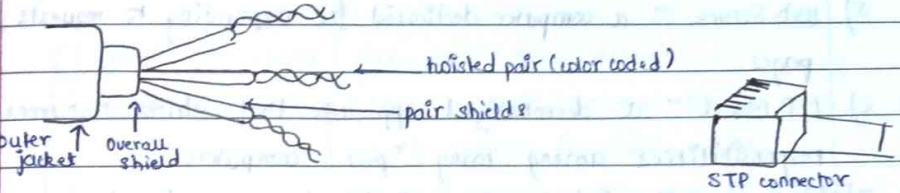
Terminolo

1)

2)

STP
Spanning Tree Protocol – Network layer.
Reduce ~~reduces~~ redundancy in LANs.
Prevent looping within a network topology.

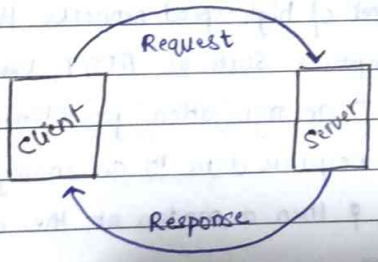
Defn: Networking Media can be defined simply as the means by which signals (data) are sent from one computer to another (either by cable or wireless means).



TCP/IP Stack:

Application Layer	→ FTP, SMTP, Telnet, DNS
Transport Layer	→ TCP, UDP
Network layer	→ IP, ICMP, ARP
Data Link layer	} ~~Network Interface layer~~
Physical layer	

Client-Server Model:



Type of Network Architecture

Terminology:

1) Node (host) – any device on a network
2) Bandwidth (Data Transfer Rate) – the speed with which data is moved from one place to another in a network.

3) Protocol - a set of rules that defines how data is formatted & processed on a network.
4) File Server - a computer dedicated to storing & managing files for network users.
5) Web Server - a computer dedicated for responding to requests for web pages.
6) P2P Model - a decentralized approach that shares resources & responsibilities among many "peer" computers.
7) Ethernet - the industry standard bus technology for local area networks.
8) Gateway - one particular setup to handle all communication going between that LAN and other networks.
9) Internet - a wide area network that spans the planet
10) Wireless Network - a network in which devices communicate with other nodes using a wireless access point.
11) Bluetooth - a technology used for wireless connections over short distances
12) Internet Backbone - a set of high-speed networks that carry internet traffic provided by companies such as AT&T, Verizon, GTE, IBM etc.
13) Internet Service Provider - an organization providing access to the internet.
14) Phone Modem - converts computer data to an analog signal for transfer over a telephone line, & then a modem at the destination converts it back again into data.
15) Digital Subscriber Line (DSL) - uses regular copper phone lines to transfer data to & from the phone company's central office.
16) Cable Modem - uses same line as cable TV signals to transfer data
17) Broadband - a connection in which transfer speeds are faster than 768 kilobits per second (DSL, cable modem). Download & Upload speeds may not be the same.

Vidyalekhan

DATE
PAGE

Defn: An ISO (International Standards Organization) standard that covers all aspects of network communication is the OSI (Open Systems Interconnection) model first introduced in the late 1970s.

OSI Stack:

Gateway	Application Layer	allow access to n/w resources
	Presentation Layer	translate, encrypt, compress data
	Session Layer	establish, manage, terminate sessions
	Transport Layer	process to process message delivery & error
Router	Network layer	move packets from source to destination
Bridge	Data link layer	hop to hop delivery of data frames
Repeater	Physical layer	transmit bits (0,1) over a medium

→ **Addressing in Networks**

Specific	Port	Logical	Physical
User-friendly address (email, URL)	Transport layer identifier (port/service)	identifies n/w device or host (IP)	unique ID for network interface (MAC)

Types of N/W Devices:

1) Repeater - allows us to extend the physical length of a network.
2) Bridges - divide a large network into smaller segments
3) Routers - relay packets among multiple interconnected networks.

Vidyalekhan
DATE
PAGE

ITU-T X.80
RFC 2828
X.800 - Aut
Access Control,
Non-repud

Defn: Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations of imminent threats of violation of CSP, AUP or standard security practices.

Defn: Intrusion Prevention is the process of performing intrusion detection & attempting to stop detected possible incidents.

Defn: The goal of a Network Operations Centre (NOC) and a Security Operations Centre (SOC) is to ensure that the hardened corporate network meets business needs.

Defn: Security Information & Event Management (SIEM) provides real-time analysis of security alerts generated by applications & network hardware.

Types of Servers

DNS	TLD	Proxy	Mail	Application
translating domain names to correct IP address	maintains info for all domain names	intermediary b/w client & server	receives & holds incoming & outgoing emails	hosts applications or software

Defn: Attacks:

1) Active - Interruption, Modification, Fabrication (Impersonation)
2) Passive - Interception.

Defn:

Defn:

Defn:

IP Address

MAC Addres

ARP:

ARP Table

Defn:

ITU-T X.800
RFC 2828
X.800 - Auth. Access control, CIA, Non-repudiation

Vidyalekhan
DATE
PAGE

...ity Service is something that enhances the security of the data processing systems and information transfers of an organization

Defn: A Security Mechanism is designed to detect, prevent or recover from a security attack. (specific & pervasive)

Defn: An attack vector is a method of gaining unauthorized access to a network or computer system (threat vector)

Defn: An attack surface is the total number of attack vectors an attacker can use to manipulate a network or computer system or extract data.

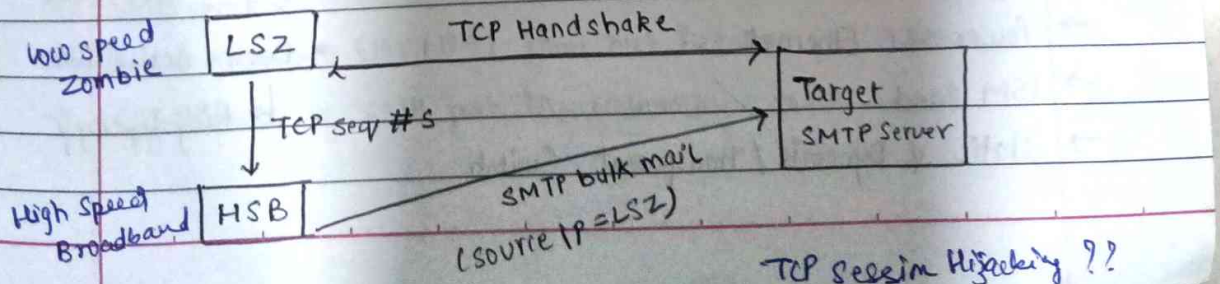
IP Address: 32-bit addresses used to get datagram to destination IP subnet

MAC Address: 48-bit addresses used to get datagram from one interface to another

ARP: Maps IP address to MAC address.

ARP Table: <IP; MAC; Time To Leave (TTL)>

Defn: ARP Poisioning is a type of cyberattack carried out over a LAN that involves sending malicious ARP packets to a default gateway on a LAN in order to change its pairings in the table.



TCP Session Hijacking ??

06/01/25

→ RIP & OSP protocols
→ Concepts in Digital Evidence:
  ↳ Real (Hardware)
  ↳ Best (CCCTV)
  ↳ Direct (Logs)
  ↳ Circumstantial (search history)
  ↳ Hearsay (testimony)
  ↳ Business Records (Agreements – bitcoins, games)
→ 5 Rules of Digital Evidence – admissible, authentic, complek, reliable, believable.

7/01/25 Basics of Networking

→ Transmission Media Impairment – Attenuation, Distortion, Noise (→ frequency, bandwidth, data rate)
→ Transmission Media classification – Guided, Unguided
→ Physical Media Types – twisted pair, coaxial, fiber optics.
→ Physical Media Comparison.

$$FSPL = \left(\frac{4\pi df}{c}\right)^2$$

c : speed of light

↳ free space loss

→ Cable Configuration – A simple X-over, CAT 5 X-over, Straight thru cable, X-over cable.
→ Power over Ethernet
→ ISM Band
→ Static & Dynamic / Transparent Switch

* Dark & Active fibre
  ↳ Ring Topology

→ CSMA/CD Media Access Control - Collision Detection (CD)

→ CSMA/CA v/s CSMA/CD
↳ wireless medium ↳ wired media

→ Significance of guided & unguided media in CSMA/CA & CSMA/CD.

→ N/w devices - hub, switch, bridge, router, repeater, modem

→ At the level of LAN, there is only the physical address i.e MAC.

→ Difference b/w switch and bridge

→ Number conversions.

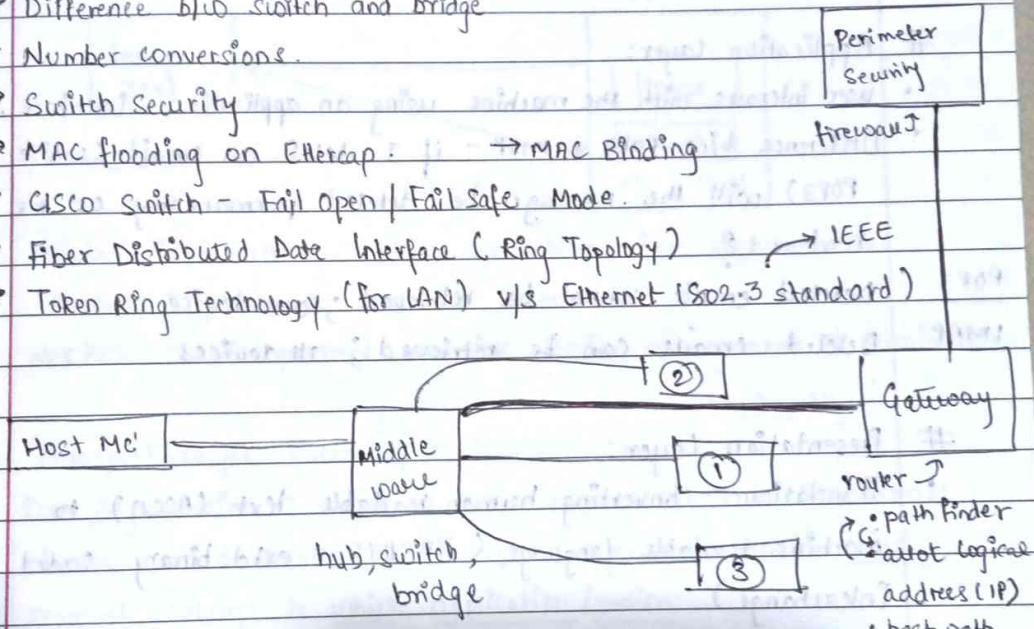
→ Switch Security

→ MAC flooding on Ettercap. → MAC Binding

→ CISCO Switch - Fail open / Fail safe Mode.

→ Fiber Distributed Data Interface (Ring Topology) → IEEE

→ Token Ring Technology (for LAN) v/s Ethernet (802.3 standard)



→ SMB port ?

→ Block SMB port (135/137) from host firewall

→ Significance of SMB port in wannacry attack.

↓ sender ↑ receiver

17/01/25 OSI Model (blueprint for communication on a network)

→ TCP/IP (1972) came before OSI
→ TCP/IP (1983) formalized
→ OSI (1984) was introduced.

} OSI is conceptual because it subsumes TCP/IP

→ Encapsulation - process of adding header or trailer at each layer (n → n+1) each layer of the OSI model is a package of protocol.

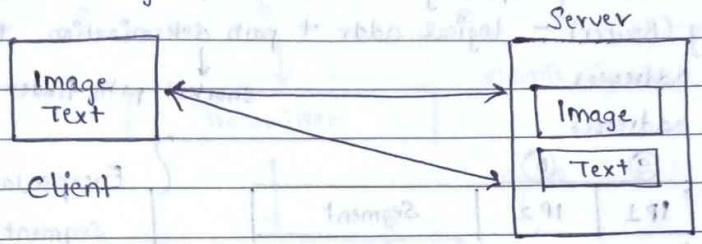
Application Layer:
- User interacts with the machine using an application interface.
- Difference b/w POP3 & IMAP - if I delete an email (while using POP3) will the message be deleted permanently or be retrieved?

POP3 Deleted emails cannot be retrieved; one device
IMAP Deleted emails can be retrieved; all devices

Presentation Layer:
- Translation - converting human readable text (ASCII) to machine readable language (EBCDIE - extd binary coded decimal interchange).
- Data compression - to improve bandwidth.
  a) lossy - removing insignificant / redundant bits from data.
  b) lossless - removing bits from metadata, not original data.
- Encryption - ensuring security of data / communication.
  a) SSL - can be compromised.
  b) TLS ✓

Session Layer :

- Setup sessions (client - server communication)
- Session Establishment - using API (netBIOS)
  - a) Authentication - username, pwd
  - b) Authorization - user, admin, superuser.
- Session Management -



- Session Termination - close connection, free up resources. (example - printer as a shared resource).

* NetBIOS - LAN protocol used for session management & termination.

→ reliability

Transport layer (Heart of OSI) :

- Data Segmentation - converting large volumes of data into small chunks (called segments). Transport layer must know which segment belongs to which application / session
  - ↳ segment no.
  - ↳ port number.
- Maintains reliability (integrity) of communication, how? - segmentation, error control, flow control.
- Flow control - controls amt. of data being transmitted (bandwidth)

* Windowing Technique (window size)

* Forward ACK no. - tells which window was rcd. & which was lost.
  - ↳ what I am expecting now

Are segment no. & sequence no. the same thing?

- Error Control – identify & rectify corrupted segments using checksum algorithm.

TCP – connection-oriented ; SYN / SYN-ACK / ACK (reliability)

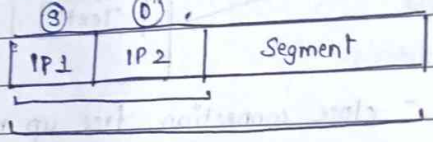
UDP – connection-less ; only SYN & no Ack (time-critical)

Network layer:

- Logical Addressing – finding destination for pkts (IP addr)
- Routing (Router) – logical addr + path determination + delivery
  - shortest path finder

IPv4: 2^{32} addresses

IPv6: 2^{128} addresses



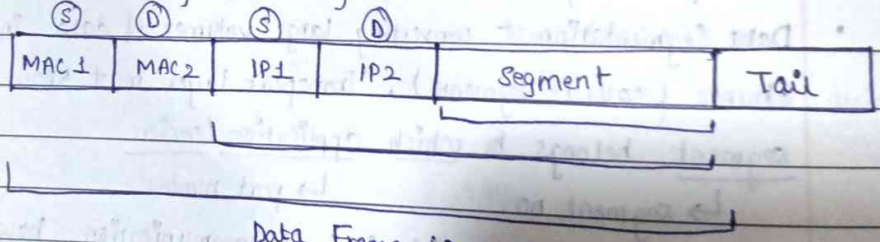
Data Packet

Encapsulation:
Segment (n)
pkt (n+1) → IP1 / IP2

router → switch IP → MAC (LAN)

Data link layer:

- Physical Addressing – adding source & dest. MAC addresses

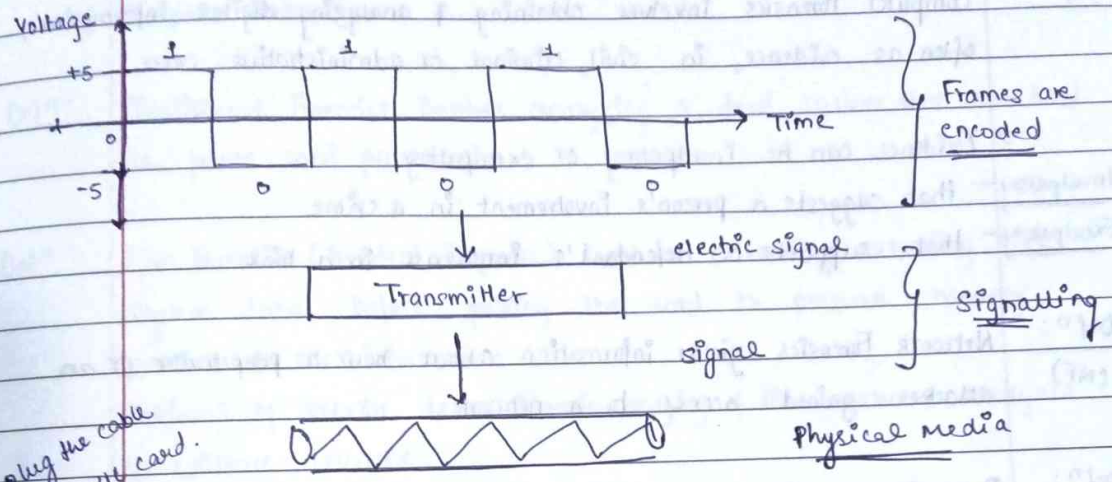


Data Frame (802.3)

* Tail – CRC algorithm, error detection
- ~~Framing & phy address~~
- How data is placed and received from the media such as MAC (CSMA/CD).
- trsfr data from one cmp to another using local media.

Physical layer :

- Converts binary segment into signal & transmit over media.



* PDU (Protocol Data Unit) - $n \rightarrow n+1$.
* Difference b/w PDU & Encapsulation ?

L FORENSICS,
NIVERSITY
T, INDIA.

Vidyalekhan

DATE
PAGE

UNIT 5 NOTES

Reference: Slides - Dr. Lokesh Chauhan (Network Security & Forensics)

Defn: Computer Forensics involves obtaining & analyzing digital information, often as evidence, in civil, criminal or administrative cases.

→ Evidence can be Inculpatory or exculpatory

Inculpatory - that suggests a person's involvement in a crime

Exculpatory - that supports a defendant's innocence in a trial

Defn: (NF) Network Forensics yields information about how a perpetrator or an attacker gained access to a network.

Defn: Data Recovery is recovering information that was deleted by mistake or lost during a power surge or server crash.

Defn: Locard's Principle states that "every contact leaves a trace".

Defn: Digital Evidence is any information, stored or transmitted in digital form, that a party to a court case may use at a trial.
(Admissibility + Authenticity)

NF challenges: Access to IP address, Data Integrity, High Speed Data Transmission, Data Extraction locations, Data privacy, Data Storage.

Defn:

Defn:

→ Where evidence resides ?

1) Computer Systems - file system, slack space, unallocated space
2) Computer Networks

Defn: Traditional Forensics involves analyzing a dead system that has had its power cord pulled.

Defn: Live Forensics (Incident Response) involves advocating extracting live system data before pulling the cord to preserve memory, process & n/w information.
Retrieval of volatile data, Forensic Imaging of live system, analysis of evidence collected

1) Binwalk
2) Bulk extractor
3) HashDeep
4) Magic Rescue
5) Guymager
6) Pdfid
7) Pdf-parser
8) Peepdf
9) Autopsy
10) Img-cat

Vidyalekhan
DATE
PAGE

TA-1

CIA Triad:
1) Access control - DAC, MAC, RBAC
2) CIA principles
3) Insecuring, Internal Security, Seperation of Duties, PoLP

DHCP, VLAN, CAM.
1) ARP spoofing, ARP poisoning
2) MAC flooding, CAM overflow
3) DHCP starvation attack
4) VLANs.

DNS.
1) Ports, Port range, Port Scanning
2) RNS, TLDNS, ANS.

Introduction to Perimeter Devices
1) IDS, NIDS
2) IPS, NIPS
3) Firewall - pkt filtering, Stateful Inspection, app-level, Next-gen
4) NOC, SOC
5) SIEM

Introduction to Threats & Vulnerabilities
1) Attack Vector, Attack Surface
2) VA, PT, log analysis, TI
3) PT - black, white, gray

Vidyalekhan
DATE
PAGE

Network Basics.

1) Types of transmission - simplex, half duplex, duplex
2) Transmission Media - wired, wireless
3) Transmission Impairment - attenuation, distortion, noise
4) Cables & Cable connections
5) Topology - P2P, Bus, Ring, Star, Tree, Mesh, Hybrid
6) Ethernet, LocalTalk
7) Token Ring Technology
8) FDDI Technology (Dual Ring Topology)
9) CSMA/CA v/s CSMA/CD
10) LAN Types & LAN Data Transmission Methods
11) NIC, Repeater, Hub, Switch, Bridge
12) Router - Static, dynamic, distance vector, link state
13) Gateway, CSU/DSU
14) Wireless Access Points, MODEM
15) OSI Model, TCP/IP Model
16) TCP v/s UDP
17) N/w Vulnerability Assessment
18) Web Proxy

Network Forensics.

1) Footprint, Challenges, Examples
2) OSCAR

ORENSICS,
ERSITY
NDIA.

Vidyalekhan
DATE
PAGE

TA-1

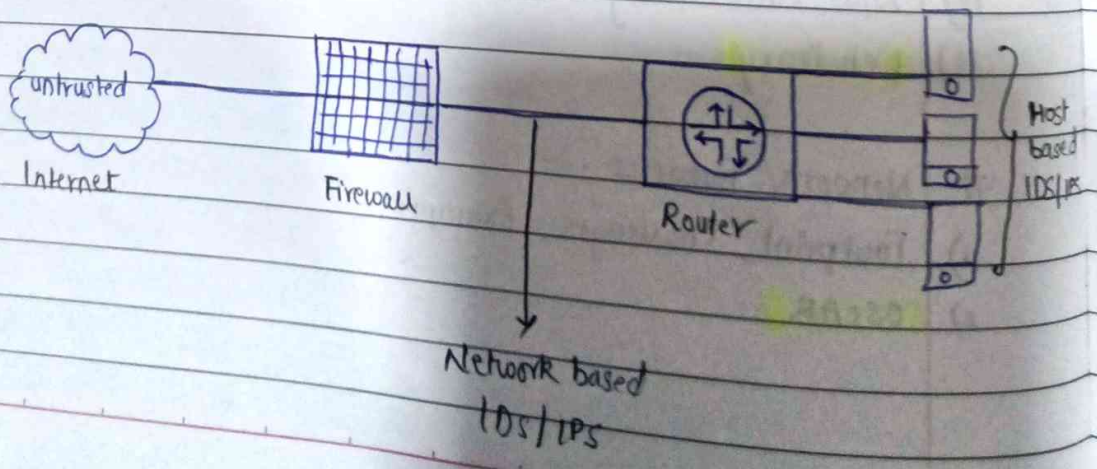
PPT ①: Why Investigate NIDS / NIPS ?

Difference b/w IDS & IPS:

	Category	IDS	IPS
1)	Definition	IDS's are threat detection & monitoring tools	IPSs are threat prevention & control systems
2)	Autonomy	These do not take action on their own	These have a pre-defined ruleset to take an action.
3)	Human-interference	They require a human to look at the result	They require that the database gets updated with new threats.

* Both read n/w packets & compare the data to the database of known threats.

Examples: Solarwind, Open DLP, Kismet, Security Onion



Methods of IDS:

1) Signature based detection - compares signatures against observed events to identify possible incidents. This is the simplest detection method because it compares only the current unit of activity (such as a packet or log entry) to a list of signatures using string comparison operations.

2) Anomaly based detection - compares definitions of what is considered normal behaviour with observed events to identify significant deviations. This method is effective to identify previously unknown threats.

3) Stateful Protocol Analysis - compared predetermined profiles ~~for~~ of generally accepted definitions ~~of~~ ~~pr~~ for benign protocol activity for each protocol state against observed events to identify deviations.

* A proxy server is a server or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources.

Application layer	} Application gateways
Presentation layer	
Session layer	
Transport layer	→ Circuit gateway
Network layer	→ Packet filtering
Data link layer	→ MAC layer firewalls
Physical layer	

PPT ②: Web Proxy

Defn: A proxy server is a web server that acts as an intermediary between your client application (browser) & the web server. It makes requests to the real server on behalf of the client or sometimes fulfills the claim itself. (VPN – Virtual Private Network)

Types of

- filter requests
- improve performance

* Web server → web client : Reverse Proxy

s: control internet access, privacy benefits, access to blocked sites, improved securing.

Types: Transparent Proxy – does not modify device's request to the website.
Anonymous Proxy – privacy (IP) of client device.
Distorting Proxy – masks client's IP & presents fake IP to server
High Anonymity Proxy – hide IP + cannot be identified as a proxy

Need:

1) Caching – locally storing web objects for a limited amount of time & serving them in response to client web requests to improve performance (Caching Proxy)
2) Content Filter – Dynamically reconstructing & filtering content of web requests & responses based on keywords, antivirus scan, etc.
3) URI Filter – filtering web requests from clients in real time according to blacklist, whitelist, keywords etc.

4) Distributed Caching - caching web pages in a distributed hierarchy consisting of multiple caching web proxies in order to provide locally customized web content, serve ads, improve performance.

5) TLS/SSL proxy - intercepts web traffic at the session layer to inspect the content of TLS/SSL encrypted web traffic.

Types of Evidence: HTTP/HTTPS history, web access logs, blocked web traffic attempts, summarized user activity reports, web proxy config files, cache in RAM, cache on disk, authentication info.

* Cached content is volatile (prone to changes). Volatility varies based on storage space, level of web activity, config options.

Q: Do clients know if a web proxy is enabled?

Q: Do clients enable a proxy or server?

PPT ③ : Protocol Analysis

Defⁿ: A network consists of two or more computers that are connected to share resources, exchange files or allow electronic communication. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, IR beam.

Defⁿ: A network protocol is an established set of rules that determine how data is transmitted b/w diff devices. They take large scale processes & break them into small, specific tasks/functions.

IEEE: Institute of Electrical & Electronics Engineers
IETF: Internet Engineering Task Force
ISO: International Organization for Standardization
ITU: International Telecommunications Union
W3C: World Wide Web Consortium

Why? Automation, Routing, IP, Encryption, Transportation, Nw mgmt

* Protocol analyzers decode the stream of bits flowing across a network & show you those bits in the structured format of a protocol.

OSI model was introduced by ISO in 1984.

Vidyalekhan
DATE
PAGE

Tools:

1) Fault mgmt - HP OpenView, Aprisma Spectrum
2) Performance Mgmt - CompuWare, NetIQ Chariot
3) Protocol analyzers - N/w Associates Sniffer, Microsoft NetMon
4) App specific - CompuWare, NetIQ chariot

Defn: A Vulnerability is a weakness or flaw in software, hardware or organizational processes which when compromised by a threat can result in a security breach.

Types: Malware, Social eng, outdated software, misconfig firewalls

Defn: Network Vulnerability Assessment reviews & analyzes an organization's network infrastructure to find cybersecurity vulnerabilities & network security loopholes.

Tools: N/w based scanning, host based scanning, wireless n/w scan, application scan, database scan.

Process: Initial Preperation (Scope, goals, AC, baselines) → VA Testing (scans, tools) → Prioritization (false pos, impact analysis) → VA Report (proof of concept + plan)

PPT ④ & ⑤ : OSI_TCP_IP_Model_FD & OSI

Defn : The Open Systems Interconnection Reference Model is a description for layered communications & computer network protocol & transmission design.

- ISO began to develop OSI framework architecture in 1978
- Concept was provided by Charles Bachman, Honeywell
- Various aspects of OSI evolved from ARPANET

Keywords: conceptual model, standardization, protocols, blue print, ISO 7498.

Data Units: Application, Presentation, Session – Data
Transport – Segments
Network – Packets
Data Link – Frames
Physical – Bits

sender ↓ Data to the n/w
receiver ↑ Data from the n/w

Application layer :

- Used by network applications to handle the exchange of information & provide user interaction.
- Example – web browser, skype, outlook etc.
- HTTP (80), HTTPS (443), FTP (20/21), NFS (111), DHCP (67), SMTP (25), TELNET (23), POP3 (110/995), IMAP (143 | 993), IRC (194), NNTP (119).

Presentation Layer :

1) Translation - converting characters / numbers to machine readable lang.
American Standard Code for Information ~~Exc~~ Interchange (ASCII)
TO
Extended Binary Code Decimal Interchange code (EBCDIC)

2) Compression - technique for bit reduction to improve bandwidth.
Lossy - redundant / ~~signif~~ insignificant bits are removed.
Lossless - bits are removed from metadata & not original data.

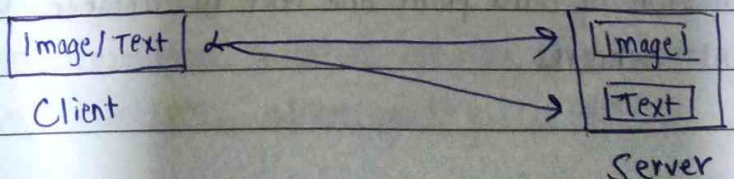
3) Encryption - n/w protocol for securing communication b/w web client & web server.
SSL - Secure Socket Layer (compromised)
TLS - Transport Layer Security.

Session Layer :

- Responsible for establishment of connection, maintainance of sessions, authentication & security.

1) Session Establishment - using APIs like NetBIOS (lan protocol used for session mgmt & termination)
   (a) Authorization - user, super user, admin
   (b) Authentication - username, pwd

2) Session Management -



Server stores image & text contents seperately - which data pkt belongs to text & image & put it together on client side.

3) Session Termination - close connection, free up resources.

* Synchronization - allows a process to add checkpoints which are considered as sync. points to the data. These help identify error so that data is re-sync. & ends are not cut properly & data loss is avoided.

* Dialog controller - the session layer allows two systems to start communication with each other in half-duplex or full-duplex.

Transport layer. ⟶ heart of OSI (why? → reliability) how? (x3)

1) Data Segmentation - dividing large amt of data into small chunks. which segment belongs to which application?
   Seg no. Service point addr / port no.

2) Flow control - controls amt of data being transmitted (bandwidth)
   (a) Windowing Technique (window size)
   (b) Forward ACK no - which wdow was rec. which was lost.

3) Error control - identify & rectify corrupted segments using checksum algorithm.

TCP: connection oriented ; SYN / SYN-ACK / ACK ; reliability (www, email)
UDP: connection less ; only SYN no ACK ; time criticality (video, games)

Network layer.
Transmission of data from one host to another located in different networks.

IPv4
IPv6

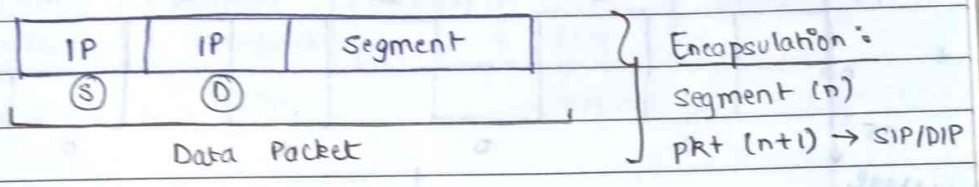
1) Path Determination – selection of shortest path to transmit packet from all routes available.

2) Logical Addressing – finding destination for packets by looking at IP addresses in the header.

IPv4: 2^{32} addresses

IPv6: 2^{128} addresses.

3) Routing – logical addr + path determination + delivery.



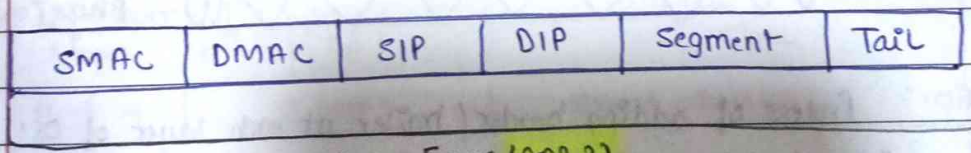
Data Link Layer.

Responsible for node to node delivery of the message.

Frame size is mentioned in NIC (Network Interface Card)

ARP – find MAC given IP.

1) Physical Addressing / Framing – adding SMAC & DMAC → Frame.



Data Frame (802.3)

2) Error Control

* Tail – CRC algorithm, error detection

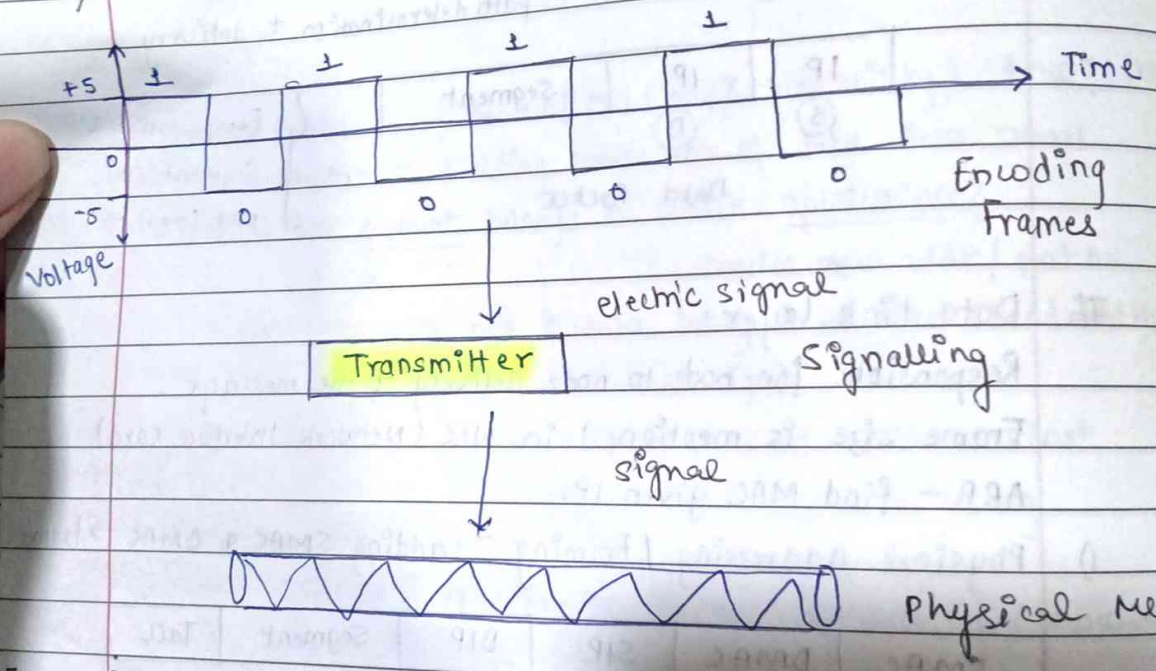
CSMA/CA: collision avoidance ; before sending ; random wait ; wireless

CSMA/CD: collision detection ; after sending ; wired

Physical layer.

Converts binary segment into signal & transmits over media.

1) Bit Synchronization – clock ; sending & receiving bits
2) Bit Rate control – no. of bits sent per second
3) Physical Topologies – way in which devices are arranged
4) Transmission mode – simplex, half duplex, full duplex.



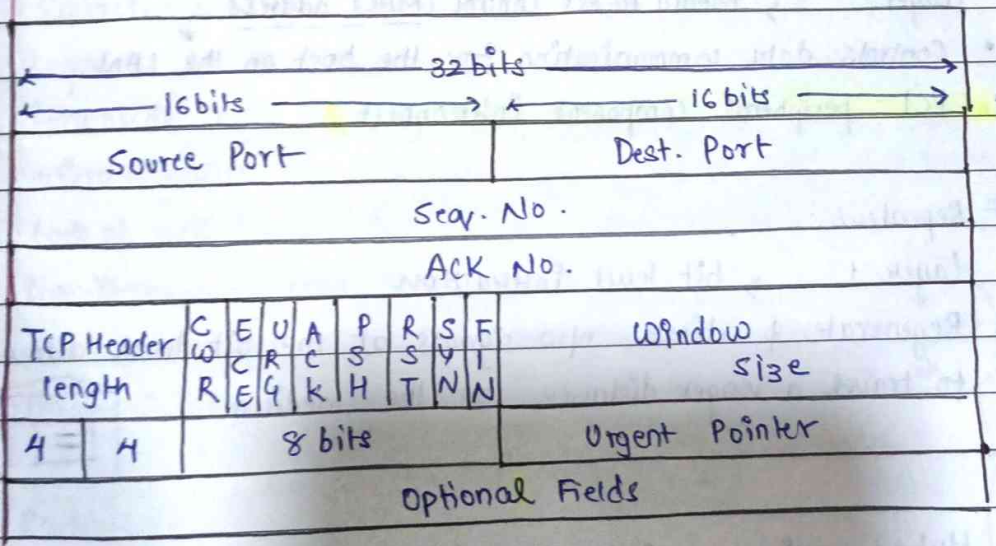
Encapsulation: Process of adding header / trailer at each layer of OSI

PDU: consists of layer n control info & layer n+1 encapsulated data for each layer.

Q: Theoretical difference b/w OSI & TCP/IP

OSI v/s TCP/IP

OSI	TCP/IP	Protocols				
Application	Application	HTTP	FTP	Telnet	SMTP	DNS
Presentation						
Session						
Transport	Transport	TCP		UDP		
Network	Network	IP				
Data link	Network Interface	Ethernet	Token Ring	Others		
Physical						



TCP Header

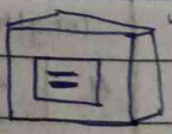
PPT ⑥ & ⑦ : Network_Devices_Final & network_devices

Defn: Network Devices are equipment that directly connect to a network segment.

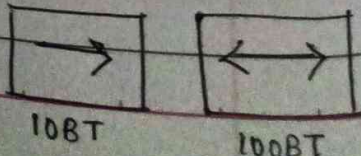
hosts → (a) End-user devices - provide services directly to user
(b) Network devices - connect EUD for communication.

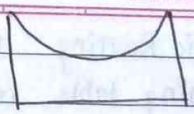
Network Interface Card (NIC): (n/w adapter)
- host devices are physically connected to the n/w media using NIC.
- A NIC is a PCB (printed circuit board) that fits into an expansion slot of a bus on a computer motherboard or peripheral device.
- Layer 2 → Media Access Control (MAC) address
- Controls data communication for the host on the LAN.
- PCI - peripheral component interconnect.

Repeaters:
- Layer 1 → bit level interaction
- Regenerate & retime n/w signals at the bit level allowing them to travel a longer distance on the medium.



Hubs: multiport switch.
- layer 1 → transmission of signal
- receives on one port & transmits on all others (4-20)
- Ethernet 10Base-T or 100Base-T
- Passive Hub ; Active Hub (Hub + Repeater)





Bridges:

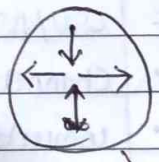
- Layer 2 ⟶ filtering / flooding frames based on MAC.
- Designed to create more usable bandwidth
- Create 2 or more LAN segments, each of which has a seperate collision domain.
- MAC address Tables.

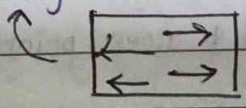
1) Transparent Bridge - devices are unaware of its existence.
2) Source Route Bridge - entire path that the pkt is to take through the n/w is embedded within pkt (Token Ring)
3) Translational Bridge - convert one data format to another (TR→ETH)

Switch: multiport bridges.

- port mirroring
- Layer 2 ⟶ MAC Table
- Layer 3 ⟶ Enterprise Switches
- forwards data to port that connects destination device
- micro segmentation - one host per segment; full bandwidth
- lack of collisions; full-duplex communication.

1) Cut Through - send as soon as recd.
2) Store & Forward - error checking then send
3) Fragment Free - error check enough then send





Router:

- Layer 3 ⟶ connects n/w segments
- creates larger n/w by joining two n/w segments
- logical addressing + path determination + delivery.

1) Static Routing - routes & route information are entered into the routing table manually.

2) Dynamic Routing - uses special routing protocols to enable routers to pass on information about themselves to other routers so that other routers can build routing tables.

(a) Distance Vector Routing Protocol - each router sends updates about all known routes to the routers directly connected to it. triggered update & convergence. (split horizon & poison reverse)

(b) Link State Routing Protocol - Link State Advertisements (LSAs) are broadcasted to every router to help create a network map.

Gateways:

- Any device that translates one data format to another.
- A default gateway refers to a router to which all n/w transmissions not destined for the local n/w are sent.

Example: Router, Bridge, Software Application.

CSU/DSU:

- Channel Service Unit; Digital Service Unit; Data Service Unit
- converts digital signal format used on LANs to one used on WANs
- sits b/w LAN & access point.

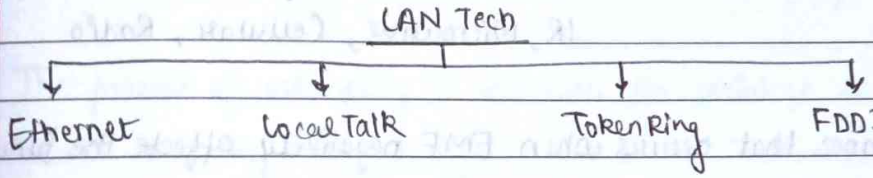
Wireless Access Points:

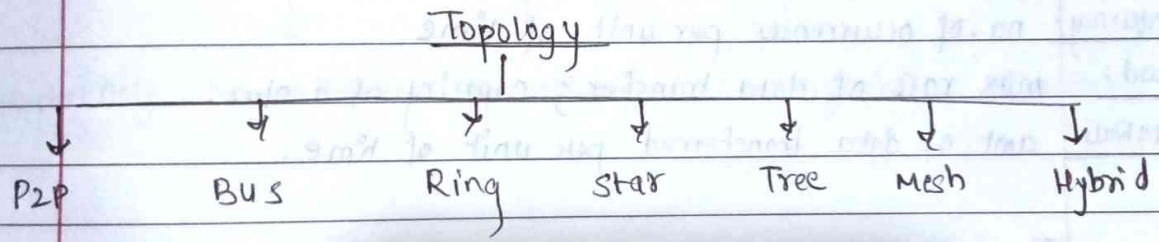
- Seperate n/w devices with antenna, transmitter, adapter
- used to create wireless LAN
- switch + DHCP server + router + firewall.

Modem:

- modulator / demodulator
- converts the digital signals generated by a computer into analog signals that can travel over conventional phone lines.

→ Types of storage used on switch, router, firewalls.
DRAM, CAM, NVRAM, ROM, HDD





Straight Through – diff devices Crossover – same device

$$FSPL = \left(\frac{4\pi d}{\lambda}\right)^2 \text{ or } \left(\frac{4\pi df}{c}\right)^2$$

PPT (8) : Network_Basics

Standalone: Input → Processing → Output

Medium: Wired / Wireless / Optical Fibre

Transmission Types - simplex, half duplex, full duplex

Transmission Media - Coaxial, STP, UTP
Optical Fibre single/multi mode
IR, Microwave, Cellular, Radio

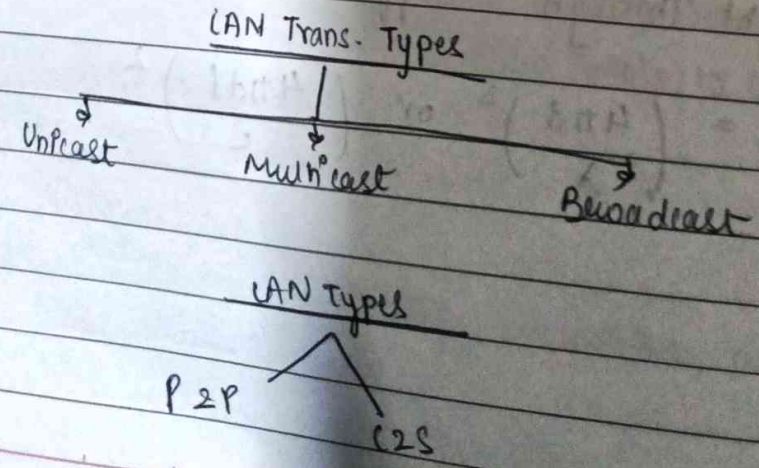
EMI: disturbance that occurs when EMF negatively affects the functioning of an electrical device.

Frequency: no. of occurrences per unit of time

Bwd: max rate of data transfer; capacity of a nlw.

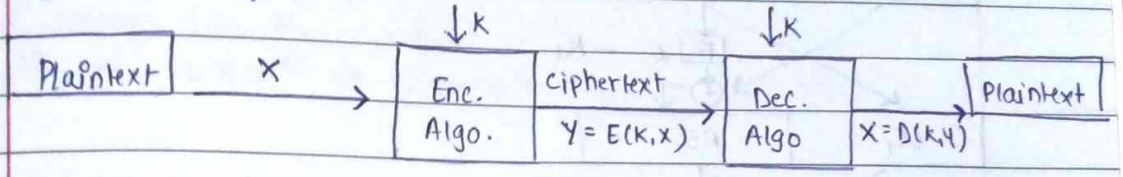
DataRate: amt. of data transferred per unit of time.

Transmission Impairment - Attenuation, Distortion, Noise



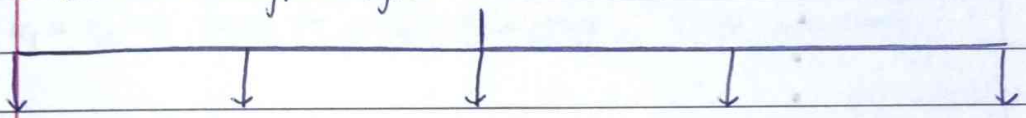
Reference: Chp (2) - Cryptography

- Symmetric Encryption Model -

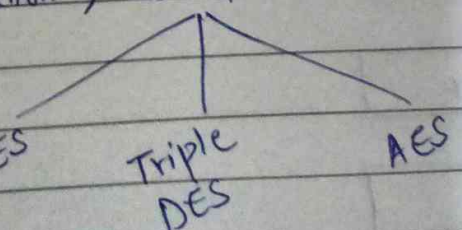


1) Opponent should not be able to decipher key given plaintext - ciphertext.
2) Sender & receiver must have received the keys securely.

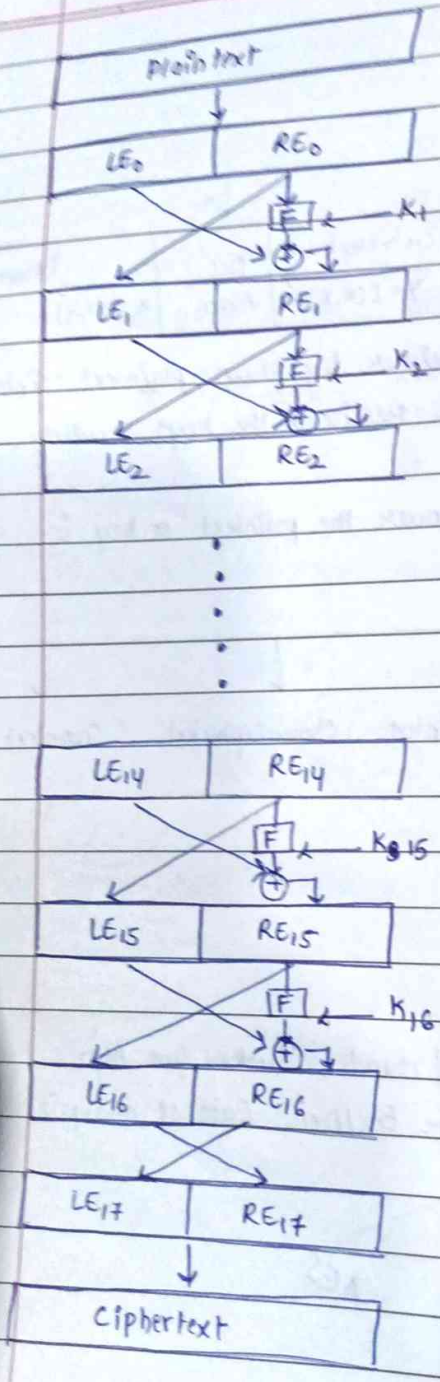
Defn: The process of attempting to discover the plaintext or key is known as cryptanalysis.



Fiestel Structures:
→ Horst Fiestel, IBM
→ Used in symmetric block ciphers.
Block size, Key size, No. of rounds, Subkey Gen. Algo, Round function, Fast Software Enc/Dec, Ease of analysis



In decryption, sequence of keys is reversed.



1) DES :

64-bit plaintext block(s) ; 56-bit key

16 rounds of processing

16 subkeys ($K_1, K_2, \cdots, K_{16}$)

$2^{56} \rightarrow 7.2 \times 10^{16} \rightarrow$ 10 hours to crack (July 1998)

2) Triple DES :

~~$C = E(K_3, D(K_2, E(K_1, P)))$~~

$C = E(K_3, D(K_2, E(K_1, P)))$

$P = D(K_1, E(K_2, D(K_3, C)))$

3 distinct keys $\rightarrow 3 \times 56 \rightarrow$ 168 bit key length

$K_1 = K_3 \rightarrow 2 \times 56 \rightarrow$ 112 bit key length (FIPS approved).

3) AES :

128-bit plaintext block(s)

Key lengths $\rightarrow$ 128 bit, 192 bit, 256 bit

Plaintext $\rightarrow$ add round key $\rightarrow$ shift rows $\rightarrow$ mix columns $\rightarrow \cdots$