CNS

Page No.
Date

U-3

Network layer

- 3rd layer of OSI model.
- transmission of data from one host to another → located in diff network
- Packet routing → select of shortest route to transmit packet. (from no. of routes available)
- segment → network layer → Packet

~~functions are~~

1) Routing -

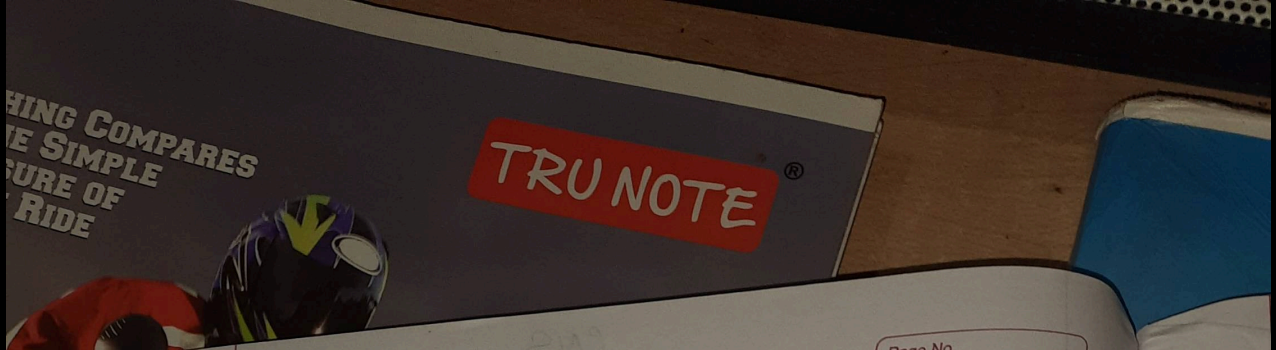
- Combo of LANs, WANs & routers with interconnected forms physical network
- There are multiple routes from source to destination
- Network layer responsible → best one among all possible routes.
- selection of route → performance criteria.
  ↳ choose shortest route throught network.

2) Packetizing - (Service by NL)

- encapsulating payload in network layer packet at source.
  decapsulating → payload in network layer → destination → packetizing
- Source host → receives payload → adds header → source & destination addr

3) Forwarding - (Service by NL)

- Router → receive packet → one of it's attached networks.
  forward packet → another attached network.
- Forwarding → way of packet delivered → next node.
  host / router → routing table.



Page No.
Date

4) Path determination → (Service by NL).

Route → packets from source to determination.
• Routing algo.

5) Switching - (Service by NL)

move packets from router's input to appropriate routes

6) Call setup - (Service by NL).

router call setup along path before data flows.
• packet → group of bits → include data bits plus source & destination address.

* Function of NL -

1) logical addressing -

device → communicate over network → logical address (layer three address).

Eg → Internet Protocol → network layer protocol → every machine → ip address.

2) Routing -

moving data across a series of interconnected networks.

3) Datagram encapsulation → encapsulates msg → received higher layer → datagram → network layer

4) Fragmentation & reassembly - network layer → send msg → data link layer for transmission.

5) Error handling & diagnostics - special protocol → allow device to logically connected → route traffic.

Basics

Connection Creation

Queuing

Msg & Packets

Routing

Address sequenci

Propaga Delay

Transm Capac

Seque Order

Use Band

Page No.
Date

Basics

Basics	Circuit	Msg	Packet.
Connection Creation	• Source → Destⁱⁿ • dedicated path	• links → one by one b/w nodes on way	• links → one by one b/w nodes on way.
Queuing	• No Queue	• Queue → formed	• Queue → formed.
Msg & Packets	• one big entire data stream → msg	• one big entire data stream → msg	• big msg divided → small packets
Routing	• Source → Destⁱⁿ ↓ Single path	• Msg → independant route ↓ distⁱⁿ	• Packets → independant route ↓ distⁱⁿ.
Address & sequencing	• msg → no address needed	• msg → addressed as independent routes	• packets → addressed sequencing → independant path.
Propagation Delay	• NO	• Yes	• Yes.
Transmission Capacity	• Low	• Maximum	• Maximum.
Sequence Order	• Msg → sequence arrives	Sequence Msg✓	• Packets → no sequence
Use Bandwidth	• Wastage	• Max extent used	• Max used.

* Network Addressing.

- major responsibility → Network Layer
- address → logical i.e. software based address.
- host → end system
- IP address → 32 bit long
  - dot decimal notation.
  - each bit → decimal form → separated by period.

* classful addressing

32bit → five sub-classes.

	B1	B2	B3	B4
Class A	NETID	HOST ID		
Class B	NETID		HOST ID	
Class C	NETID			HOSTID
Class D	MULTICAST ADD.			
Class E	RESERVED			

	A	B	C	D	E
NetworkID	8 bits	16 bits	24 bits		
Host ID	24 bits	16 bits	8 bits.		
	↓ large organisation with large no. of hosts or routers	↓ midsize organizations 10 of thousands attached hosts or routers.		↓ multicast services allow host to send to group of hosts simultaneously	

	IPv4	IPv6.
	32-bit length	48 bit length.
Address config	Manual & DHCP address	Auto & renumbering add.
	end to end connectivity ↳ unachievable	end to end connectivity ↳ acheivable.
	4.29×10^9 address space.	3.4×10^{38} addspace
	Security feature → dependant on applcn	IPSEC → inbuilt security feature
	Add represent → decimal	• Hexadecimal
	Fragmentation → Sends & forwarding routers	• Frag → sender
	Packet flow identification → ✓	✗
	checksumfied → ✓	✗
	Has msg Transmission Scheme	Has multicast & any cast msg transmission scheme
	encryption & Authenicity → ✗	✓
	Header → 20-60 bytes	40 bytes.

Page No.
Date

ARP

Address Resolution Protocol

find → IP address of remote machine

MAC add → requested
IP add → known

Value 1 → requests
Value 2 → responses

RARP

Reverse Address Resolution Protocol

IP add of our own.

MAC add → known
IP add → request

Value 3 → request
4 → response

ICMP → Internet Control Message Protocol

supporting protocol → Internet protocol suite.

- used by network devices (routers)
- send error msg.
- operational info → indicating success of failure.
- reporting errors & management queries.

	Static Routing	Dynamic Routing
Routing Pattern	User defined routes → routing table	routes updated → changes in network
Routing algorithm	No complex algo	Dynamic routing employs complex algo.
Security	Higher	less.
Automation	Manual	Automatic
Applicability	small network	large networks
Protocols	No specific	BGP, RIP & EIGRP
Add'n resources	No add'n resource.	Memory bandwidth etc.

Distance Vector

- Bandwidth ↓ → small packet & no flooding
- Bellman Ford algo
- local knowledge
- Traffic → less
- converges → slow
- count to infinity problem
- simple configure
- Updates → broadcast

Link State

- ↑ bandwidth.
- Dijkastra algo.
- Global knowledge.
- more Traffic.
- fast
- No cont to infinity prob.
- difficult configure
- on multicast.

Page No.
Date

BGP

- Border Gateway Protocol
- Best path algo
- large size ~~algo~~ organisn
- external gateway protocol

- Intelligent protocol
- classes → areas & table

- metric → Hop counts
- hybrid type
- no restriction → hop count

RIP.

- Routing Info Protocol
- Bellman Ford algo.
- small size organ
- industry standard dynamic protocol

- not intelligent
- array, sub ~~classes~~ autonomous system & backbone area

- Bandwidth.
- Vector State type
- max 15 hops

U-4 Transport Layer.

- logical communication b/w appln process running on diff hosts.
- peer to peer communication.
- 4th layer of OSI model.
- reliable data delivery.
- packets delivered → error free
  → in sequence
  → with no losses or duplications.

* Transport layer fun^{n} -

- message → packets
- error recovery → if lower layer isn't error free.
- flow control
- multiplexing & demultiplexing sessions.
- setting up & release connection across network.

Flow Cntl	Error Control.
• trans^{n} data from sender to receiver.	• trans^{n} of error free data from sender to receiver.
• prevents loss of data & avoid overrunning of receive buffer	• used to detect & correct the error occured in code.
• Stop & wait Protocol & sliding window Protocol	• Stop & wait ARQ & slidind window ARQ.

Page No.
Date

* Socket -

one endpoint of two-way communication - running on network.

- establish named contact points
- bidirectional FIFO communication facility over network.
- each socket → specific address.
  - IP add
  - Port no.
- employed in client server applications.
- attach to network port address then wait for client to contact.

*

TCP	UDP
transmission control protocol	user datagram protocol.
Secure	Unsecure
connect-oriented	connectionless
slow	Fast
Guaranteed Transmission	No Guarantee
Flow control	No Flow control
20 Byte Header	8 byte Header
Adv Error Checking	Basic error check
Packet Reorder Mechanism	No Reorder.
Used by Critical Apps	Used by Real time apps
Acknowledgement Mechanism.	No Acknowledgement
Threeway handshake	No Handshake
DNS, HTTPS, FTP, SMTP, etc	DNS, DHCP, TFTP, SNMP

TCP handshake → client & server to exchange synchronization & acknowledge ma

Page No.
Date

* Silly Window Syndrome -

↳ problem → poor implementation of TCP.

- degrades performance
- data transfer → inefficient.

- when large data is passed from sender

↓

but receiver reads data one byte at a time

ie. Receiver → TCP buffer full

Receiver → acknowledgement of 1-byte segment.

window set to → 0.

→ 1) sender ~~sending~~ windows transmit one byte of data repetedly.

2) Receiver windows accept one byte of data repetedly.

- Nagle algo
- clark's soln.

* Sliding window (windowing)

- controlling sending of data packets b/w two network devices dependable & sequential delivery of data packets

- each data pack & byte include unique consequtive sequence number used by receiving computers to place data in correct order.

- sequence no's to avoid duplicate data & to request missing data.

Page No.
Date

* QOS - Quality of Services

- traffic control mechanism
- packet delay & losses of various kinds

Need → 1) Audio & Video conferency → bonded delay & loss rate
2) Streaming → bonded packet loss rate
3) time critical appln → bonded delay
4) Valuable appln → better services

Principle 1 -
packet marking allows a router to distinguish among packets belonging to diff classes of traffic

Modified Princ 1 -
Packet classification allows a router to distinguish among packets belonging to diff class of traffic

Principle 2 -
Degree of isolation is desirable among traffic flows, so one flow is not adversely affected by another misbehaving flow.

Principle 3 - For isolating flows, desired to use resources like BW & Buffers as efficiently as possible.

	Leaky Bucket	Token Bucket
Token dependency	independent	dependent.
Bucket ~~Transmission~~ Filled bucket	Bucket full → data/packet discarded.	Bucket full → token discarded not packets.
Packet transmission	packets → constant rate.	packets ⇒ faster rate
Condition for Packet Transmission	Packets → continously transmitted	packets → enough token at any transfer.
Token saving	Doesn't save	saves token
Restrictive Algo.	Restrictive	less restrictive

L25 - Applic^n Layer.

- top of layers of OSI model
- produce data → transfered over his network

✱ Functions -

Network Virtual Terminal
FTAM - File transfer access & management.
Mail Services
Directory Services

✱ Design Issues -

- Appl^n layer protocols & can be addressed by pattern from several diff^n languages.
  pattern
- Pattern Language for Appl^n level communication Protocol
- Service Design Patterns
- Patterns of enterprise Appl^n Architecture
- Pattern - Oriented Software Architecture.

Page No.
Date

Internet

- global ~~system~~ network of connecting millions of computer
- TCP/IP.
- each comp is independent
- First version → ARPANET

Nature → Hardware

comprises → network of computers, copper wires, fire-optic cables & wireless networks

WWW.

- System of internet servers that support specially formatted docums.
- HTTP.
- Hyperlinks.

NSFnet.

Software.

Files folders & documents stored in various comp

NOTHING COMPARES TO THE SIMPLE PLEASURE OF A BIKE RI

Page No.
Date

HTTP

Hypertext Transfer Protocol

don't encrypt text.

no SSL → Transport layer

sender & receive can understand code.

no TLS or SSL

port no 80 → default

- handshake schema
  sender ↔ receiver
  & data transfer

port no 80

URL → http://

Unsecure

No validation req.

simple address bar.

can be hacked

HTTPS

Secure.

encrypt code → no one can access

SSL ✓ → encrypt code

decipher code & get msg

TLS or SSL ✓

default ✗ port no.

- secure connection.
  data transfer
  sigh certificate
  sender & receiver cipher code

port no 443.

https://-

safe transfer protocol

validation → domain verification

green coloured add bar
↳ secure

can't be hacked

* Web Caching -

activity of storing data for resuse, such as a copy of webpage served by web server.

Adv -
- Reduces Bandwidth Consumption. ↓traffic
- Reduces access latency
- Reduces workload of remote web services
- Remote serve → crash or network partioning
  client → cached copy at proxy.

Disadv -

Cache → lack of proper proxy updating
single proxy cache → bottleneck. → single point of failure
Reduce hit on original remove service.

* Domain Name Service -

↳ host name to IP translation services

DNS Server →

DNS loopup saves website in priority order.

- Authorative name server provides ip address to DNS.

Domain → Generic → .com .org .net
Country → .in .us .uk
Inverse: ip → domain name mapping

SMTP

Simple Mail Transfer Protocol

- TCP/IP
- control/manages transn of email msgs on Internet
- single body of ASCII text meaning msg
  ↓
  NVT- 7bit ASII format
- can't send picture as attachment or send formatted text in email msg

MIME

Multipurpose Internet mail extension

- email appl'n program
  ↳ email format
  ↳ handle ob SMTP can't do
- supplementary email to support non-ASCII data
- can send multiple attachment with single email msg
  ↳ msg, binary files, audio, video, pictures, & non-ASCII

Page No.
Date

* DHCP – Dynamic Host Configuration Protoc.

client/server protocol
↳ automatically provide an IP host with its IP address using DHCP server.

Components of DHCP → DHCP server
DHCP client
IP address pool
Subnet
Lease
DHCP relay

Benefits →
- Centeralized administration of IP config.
- Dynamic host config.
- Seamless IP host config
- Flexibility & Scalability.

* TELNET → TErminal NETwork.

enables one computer to connect to another local computer

2 login → • Local login • Remote login

Mode of oper" → • Default mode Character mode • Line mode

Syntax → telnet hostname port.

FTP

File transfer protocol.

TCP port no → 20 & 21

transfer files from remote comp to established one/vice

2 way communication
upload & download of file

FTP is slower.

Used to access & transfer files.

access → command line or GUI

Few people

HTTP

Hyper Text Transfer Protocol

80 & 8080.

transfer web pages from one to other

1 way communication
↳ pictures, texts transferred from server to client

Faster.

used to view websites

Browser.

Most widely used.

---

* SNMP → Simple Network Management Protocol.
- framework used to manage devices in internet.
- provides set of operations for monitoring & managing internet
- concept of manager & agent.

manager → any machine that can send query requests to SNMP agents with correct credentials

agent → info in database → no of packets received & forwarded

V-6 Security.

- Network Security -

measures taken by enterprise or organisation to secure its network & data using both hardware & software.

- Network Security (working) [3 levels]
  → physical → technical → administrative

- need for info security -

→ protecting functionality of organization
→ enabling safe operation of applications.
→ protecting data that organisation collect & use.
→ safeguarding technology assests in organisation.
→ cyber security is rising
→ Damage → significant.
→ Cybersecurity → builds trust
→ our identities. protect our data.
→ every organization has vulnerabilities

- principles

→ confidentiality
→ Authentication
→ Integrity
→ Non Repudiation.
→ Access Control.
→ Availability.

$R = A + T + V$

Risk = Asset + Threats + Vulnerability

Date

Threat

- Is a person or thing likely to cause danger or damage.
- Danger posed by someone else
- Can be identified, but can't be controlled
- eg → computer virus
  data breaches
  dishonest employee

Vulnerability

- being open to attack or damage.
- Flaw or weakness in system
- can be identified & corrected.
- eg- cyberattacks, virus downloaded by employee

* Types of Attacks

Passive Attacks

- nature of eavesdropping on, or monitoring of, transmissions.
- difficult to detect
- doesn't affect system
- prevention rather than detection
- types → Release of msg contents & traffic analysis

Active Attacks

- involve modification of data stream or creation of false stream
- easy
- affects system.
- difficult to prevent
- types → masquerade, replay, modification of msg & denial of service

Page No.
Date

OSI security Architecure –

- systematic way of defining security req. & charaterizing
- International standard
- defined by ITU-T (the Internation Telecommunication Union Telecomm Standardization Sector).

- Need → • access security needs.
  • need of systematic ways.
  • difficult → decentralized data processing environment.
- Benefits → useful to managers → organization task of providing security.
  → developed security feature for their product & sevice relate to this structured defination.

Symmetric Encryption	Asymmetric Encryption.
• Smaller cipher text compared to orignal.	• Large cipher text compare to orignal.
• Transmit big data	• small data.
• low usage of resources	• high usage
• 128 or 256-bit key size.	• 2048 bit or higher.
• Less secure → single key	• safer → 2 keys. encryption & decrypt.
• old technique	• modern encryption technique
confidentiality • single key → might be compromised	• 2key → share key not required.
• fast technique	• slow technique
Algo → • RC4, AES, DES, 3DES & QUAD	• RSA, Diffie-Hellman ECC algo.

Page No.
Date

SSL → Secure Socket Layer.

→ Internet protocol for secure exchange of info between web browser & a web server.

→ Uses TCP → provide reliable end to end secure service

→ security service b/w TCP & appln that use TCP.

Features -

- SSL server authentication → user to confirm server identity
- " client " → server to confirm user identity.
- encrypted SSL session → info b/w browser & server is encrypted.
- SSL → supports multiple cryptographic algorithms.

SSL
- 1) confidentially → handshake protocol → SSL payload (encryption)
- 2) Msg integrity → Handshake protocol → Msg Authentication code

	AES	DES.
Block size	128 bits	64 bits.
key length	128, 192, 256-bits	56-bits (effective length)
encryption primitives	substitution, shift, bit mixing (xing)	substitution + Permutation.
crypto primitives	confusion, diffusion	confusion, diffusion.
Design Rationale	closed	Open

Bus

- nodes → connected
- main cable → back bone
- Adv -
  - easy to setup, handle, implement
  - small networks
  - cost - less
- Disadv -
  - Cable length → limited → devices to connect
  - limited no. of nodes.
  - efficiency ↓ → ↑ no. of devices
  - Network with low traffic.

Star

- each computer is connected to central hub.
- Adv -
  - Centralized nature
  - achieves isolation of devices in network
  - adding/removing node is easy.
- Disadv -
  - oper" dependson central hub.
  - Central hub failure whole network down
  - setup → high
  - more nodes can be added.

Mesh

- every node point to point connectivity.
- connective direct high vol. traffic.
- Adv - Data → 1 node to many nodes
- entire network doesn't fail due to one.
- easy to identify faults.
- Disad -
  - many connection ↓ no major process.
  - lot of cabling.
  - cost high
  - Administration is difficult.

Ring

- connected in circular fashion.
- data travels in 1 direction /central
- * Adv - No service server.
- * ~~Traffic~~ - Unidirection
- * High speed
- node's → network performance.
- Ring → better.

Disadv -
- single node failure → whole network fails
- movement/changes → affect entire performance.
- Data sent → one node to another has to pass through all intermediate nodes.
- Slow compared to star.
- Speed ↓ ↑ no. of loads

Tree

- elements are arranged as branches of tree.

* Adv -
- where star/bus can't be implemented
- multiple dept of university or operation.
- centralization archived.
- each star segment → dedicated link from central bus.

* Disadv -
- network depends → Bus
- maintenancy → not easy
- cost → high
- config → difficult

Hybrid

- different links & node to transfer data.
- 2 or more topology is Hybrid

* Adv -
- combine
- benefit → 2-3 topology
- modified → per requirement
- Reliable.
- easily scalable.
- easy integration of new components

* Disadv -
- expensive
- complex
- change hardware
- larger in scale → lots of cable.