2 primary function
1) — determine best path
2) — forward packets

Routing: when router receives an IP packet on one interface, it determines which interface (next hop) to use to forward the packet to the destination.

1 no)
a) use its IP routing table to determine path.

b) Best path (longest match)

Dest IP address: 192.168.2.82

Binary: 11000000.10101000.00000010.01010010

Prefix: 192.168.2.80

Binary: 11000000.10101000.00000010.01000000

c) How Router building routing table?

→ 1) Directly connected networks

2) Remote Networks → not directly connected with router
   - static
   - dynamic

Default routing ..../0
no bits to match the dest. IP address for this route entry to be used

→ using protocol : static and dynamic

Static
- ip address of remote net.
- sub. mask " "
- next hop router's ip add

manually configure the routing table on each router

manually enters the routes and associated next hop info.

complexity: increases with net. size.

when topology changes, administraton intervention needed.

less scalable

small network

no. additional resource needed

explicitly defined by administraton

Dynamic

automate the process of building and maintaing routing table by allowing routers to exchange routing info.

complexity doesn't depend on size.

automatically adapts to change.

more scalable

large network

use cpu, memory and link b/w

auto. determine best path.

Routing Table Entries: (7)

1) Route source
2) destination network
3) administrative distance
4) metric
5) next hop
6) route timestamp
7) exit interface

Default routing? specify a next hop en route to use routing table doesn't contain a specific route that matches dest. IP add.

— dynamic / static

IPv4 route entry: 0.0.0.0/0

IPv6 : ::/0

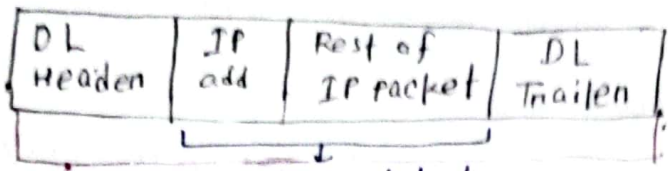
Some formats of DL frame
- PPP
- HDLC
- Layer 2

encapsulate packets in the appropriate DL frame type for outgoing interface

Packet Forwarding Decision Process:

Router do this

1)



1) Process switching
2) Fast "
3) Cisco Express forward

2) Router examines IP address of packet header then consults its IP routing table.

3) finds longest matching prefix

4) encapsulates packet, forwards it to next hop / next connected device (remote network, LAN)

5) If no route entry matches, packet drops.

* What is IP routing table? → a data structure used by routers to determine the next hop router for forwarding packets to their destinations.
  - contains a list of routes to known networks

* Source of route → identified by code.
* Some codes:
  - L → identifies router interface address
  - C → directly connected network
  - S → static route
  - O → dynamically learned net (ospf routing protocol)
  - * → default route

* 3 routing principles:

1) routers make own decision based on its own routing table's info.

2) one router's routing table info may not match info of other one.

3) routing info about a path → not provide return routing info

→ know how to forward packets to dest

→ may not know how to route packets back to source

* ICMP — Internet Control Message Protocol.
  - ICMPv4
  - ICMPv6
  — provides feedback about IP packet processing issues.

* Host reachability test: → ICMP Echo Message do this

- local host sends request to host
- if host available, the dest. host responds with a echo reply.

Lecture - 10

* TCP server processes are assigned port numbers. A server can't have 2 services assigned to the same port number within the same transport layer services

* TCP connection Establishment

1) client requests a client-to-server communication session with the server.
2) server acknowledges and request
3) client acknowledges

* TCP connection termination:

1) when the client has no more data to send in the stream, it sends a segment with FIN (finish) flag set.
2) the server sends an ACK to acknowledge the receipt of FIN and terminate session from client to server.
3) the server sends a FIN
4) the client responds with ACK

1) Urgent pointer field
2) acknowledgement flag
3) Push func 4) Reset connection
5) synchronize sequence

→ 6 ctrl bit flags:
1) URG 4) RST
2) ACK 5) SYN
3) PSH 6) FIN – termination

* TCP [3-way] handshake:
— establish reliable connection between client and server.

3 steps: 1) client sends (SYN) to server to initiate the connection
2) server receives SYN and sends SYN-ACK
3) client sends ACK to complete the handshake

TCP → Transmission control Protocol

TCP provides —

1) Reliability

- assigns sequence number to packets
- receiver reassemble data in correct order
- Retransmit segments that are not acknowledged by receiver
  ↳ · manage segment loss
  - ensure data integrity
- ↳ Soln: Selective acknowledgement (SACK)

2) Flow Control

- Regulate data flow rate between source and destination.
  ↳ dest. device receive and process data reliably.
- window size and acknowledgements use

data amount that the dest. can handle and acknowledgement provide feedback to sender about successful data receipt.

3) Handling Network congestion

- utilizes timers, algorithms and congestion handling mechanisms
  ↳ ctrl and mitigate congestion
  prevent packet loss
  ensure efficient data transmission

→ User datagram protocol

UDP provides -

(1) low overhead data transport

- small datagram header
- absence of network mgmt. traffic
- not track sequence no. of packets
  ↳ no mechanism to reorder datagrams into their transmission order
  ↳ reassembles the received data in the order it was received and forwards it to application

(2) not establish a connection

not provide
- reliability guarantee
- data ordering
- flow ctrl mechanisms

used where low overhead and speed are prioritized over reliability

reliability << low overhead and speed

→ real time streaming
✓ video conferencing
✓ DNS queries
✓ broadcasting

mechanisms of UDP:

server side:
- assign servers registered port no. (1)
- when UDP datagram received, (2) this port pairs → consistent throughout transaction
- forwarded to dest. based on port no.

client side:
- dynamically selects port no. (1) → assign port no. (2) to server process as dest. port

Quality of service

QoS Models

— implement and manage different levels of ~~the~~ service for network traffic

- choice of model depends on
  - specific requirements
  - network characteristics

Best Effort (1)

- basic design of internet
- all network packets are treated equally
  - → no guaranteed delivery
  - → no preferential treatment

Pros: scalability
simplicity

Cons: lacks reliability

Differentiated Services (DiffServ) (3)

- classify network traffic into diff. class
- apply QoS on a hop-by-hop basis
- each net. device identifies the packet class and services it

Pros: scalable, flexible
- diff. levels of service to diff. class

Cons: not guarantee end-to-end service quality

Integrated Service (IntServ) (2)

- high level of QoS
- designed for real-time apps.

Pros:
- manages network resources to deliver guaranteed QoS to individual flows.
- establish/maintain QoS
  - ↳ uses resource reservation and admission ctrl mechanisms

Cons: not scalable for large implementation
- resource intensive

FIFO – equal priority to all
WFQ – fair b/w allocated to all
CBWFQ – " " "
based on class

Queuing algo: Voice → Priority
– FIFO
– WFQ (Class Based Weighted Fair)
– CBWFQ
– LLQ ↓ Low Latency

Network Transmission Quality factors:

1) Prioritizing Traffic:
if traffic volume > network capacity
store packet in memory (delay)
until resource available to transmit them

≠ queue – grow → packets drop
→ soln: QoS technique
– classify data into multiple queues.

2) Bandwidth: amt of data that can be transmitted in a given time

3) Congestion: when the network experiences more traffic than it can handle, leading to delays

congestion points: – aggregation
– speed mismatch
– LAN to WAN connection
solve: QoS

4) Latency/ Delay: is the time it takes for a packet to travel from source to dest.

→ fixed delay
1 – processing time
2 – queuing
4 – propagation time
5 – de-jitter
6 – code
2 – serialization

variable delay
traffic load

Voice
- delay sensitive
- drop "
- higher priority

Video
- loss sensitive
- higher data volume per pkt

Data
less sensivite to delay and drops delay untill b/w provided

5) **Jitter:** variation in packet delay
   - impact quality of time sensitive apps

6) **Packet Loss:** occurs when packets drop
   - affect reliability of data transmission
   ↳ solve: QoS — minimal loss.