Internet: network of networks that are provided by ISP

ISP: Internet service provider (stc, mobaily, etc)

protocols control sending, receiving of data

OR

Protocol is a set of rules that controls the connection and the communication

Internet services

1-Infrastructure that provides services to applications like (Web, streaming video, games)

2-Provides **programming interface** to distributed applications:

- “hooks” allowing sending/receiving apps to “connect” to use Internet transport service
- provides service options, analogous to postal service

Network edge

hosts: clients and servers

Access networks, physical media

Is the connection between the network edge and the network core

Wired or wireless communication links

Network core

interconnected routers

network of networks

Access networks

DSL or digital subscriber line

use existing telephone line to provide Internet connection

- data over DSL phone line goes to Internet
- voice over DSL phone line goes to telephone net
  - 24-52 Mbps dedicated downstream transmission rate
  - 3.5-16 Mbps dedicated upstream transmission rate

Wireless access networks

Shared wireless access network connects end system to router

WLANs or Wireless local area networks

typically, within or around building (~100 ft)
802.11b/g/n (WiFi): 11, 54, 450 Mbps transmission rate

Wide-area cellular access networks

provided by mobile, cellular network operator (10's km)
10's Mbps 4G, 5G, etc.

Data center networks

high-bandwidth links (10s to 100s Gbps) connect hundreds to thousands of servers together, and to Internet

Host: sends packets of data

host sending function:

- takes application message
- breaks into smaller chunks, known as packets, of length L bits
- transmits packet into access network at transmission rate R. link transmission rate, aka link capacity, aka link bandwidth

$$\text{packet transmission delay} = \text{time needed to transmit } L\text{-bit packet into link} = \frac{L \text{ (bits)}}{R \text{ (bits/sec)}}$$

Network core

mesh of interconnected routers

packet-switching: hosts break application-layer messages into packets

Forwarding

local action moves arriving packets from router's input link to appropriate router output link

Routing

global action determines source destination paths taken by packets

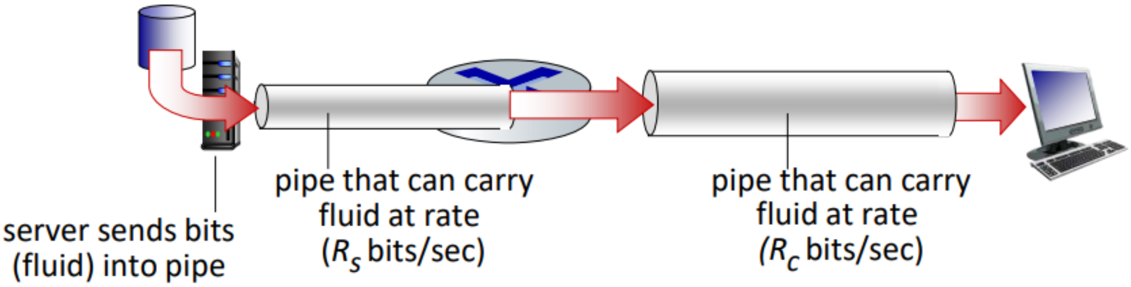
packet transmission delay: takes L/R seconds to transmit (push out) L-bit packet into link at R bps

store and forward: entire packet must arrive at router before it can be transmitted on next link

Queueing occurs when work arrives faster than it can be serviced

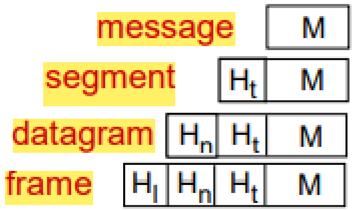
1. **packets will queue**, waiting to be transmitted on output link
2. **packets can be dropped** (**lost**) if memory (buffer) in router fills up

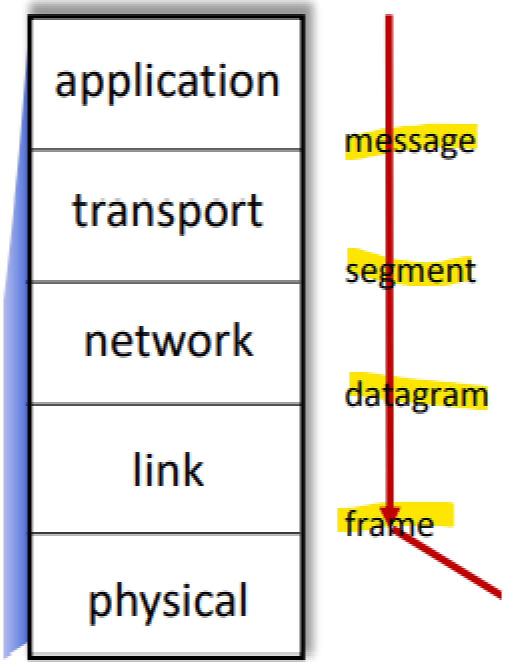
throughput is the rate (bits/time unit) at which bits are being sent from sender to receiver


server sends bits (fluid) into pipe
pipe that can carry fluid at rate (R_s bits/sec)
pipe that can carry fluid at rate (R_c bits/sec)

layers each layer implements a service

1. **application**: supporting network applications • HTTP, IMAP, SMTP, DNS
2. **transport**: process-process data transfer • TCP, UDP
3. **network**: routing of datagrams from source to destination • IP, routing protocols
4. **link**: data transfer between neighboring network elements • Ethernet, 802.11 (WiFi), PPP
5. **physical**: bits "on the wire"





دور شرح

Client-server architecture

Server

- always-on host
- Static IP address
- often in data centers

Clients

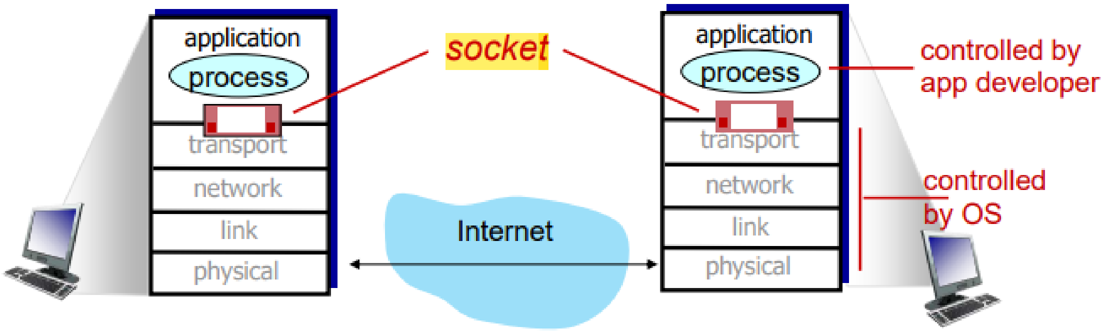
- contact, communicate with server
- may be intermittently connected
- may have dynamic IP addresses
- do not communicate directly with each other
- examples: HTTP, IMAP, FTP

Peer-peer architecture

- no always-on server
- arbitrary end systems directly communicate
- peers request service from other peers, provide service in return to other peers
- self-scalability – new peers bring new service capacity, as well as new service demands
- peers are intermittently connected and change IP addresses
- complex management
- example: P2P file sharing

Sockets

process sends/receives messages to/from its socket
socket analogous to door
two sockets involved: one on each side



Application-layer protocols

- **types of messages exchanged:** request, response
- **message syntax:** what fields in messages & how fields are delineated
- **message semantics:** meaning of information in fields
- **rules:** for when and how processes send & respond to messages
- **open protocols:** defined in RFCs, everyone has access to protocol definition (HTTP, SMTP)
- **proprietary protocols:** Skype, Zoom

Transport services

1. **Data integrity:** some apps require 100% reliable data transfer // file transfer, web transactions
2. **Timing:** some apps require low delay to be "effective" // Internet telephony, games
3. **Throughput:** some apps require minimum amount of throughput to be "effective" // multimedia
4. **Security:** encryption, data integrity

TCP or Transmission Control Protocol	UDP or User Datagram Protocol
Reliable	Unreliable
Flow control	No flow control
Congestion control	No congestion control
Connection-oriented	Connection-less

Reliable: between sending and receiving process

Flow control: sender won't overwhelm receiver

Congestion control: throttle sender when network overloaded

Connection-oriented: setup required between client and server processes

Web and HTTP

Web page: consists of objects, each of which can be stored on different Web servers
// object can be HTML file, JPEG image, Java applet, audio file, etc.

HTTP or HyperText Transfer Protocol: is a Web's application-layer protocol

Server and Client using HTTP

Client	Server
browser that requests, receives, and "displays" Web objects	Web server sends objects in response to requests

Note// HTTP uses TCP at port 80
HTTP is stateless
HTTP messages: request, response

HTTP request message

Is written by ASCII (human-readable format)

1. **POST method:** user input sent from client to server
2. **GET method:** used to read or retrieve a resource
3. **HEAD method:** requests headers (only) that would be returned if specified URL were requested with an HTTP GET method.
4. **PUT method:** completely replaces file that exists at specified URL with content

HTTP response status codes

200 OK

request succeeded

301 Moved Permanently

requested object moved

400 Bad Request

request messages not understood by server

404 Not Found

requested document not found on this server

505 HTTP Version Not Supported

HTTP cookies is a small piece of data that a server sends to a user's web browser.

What cookies can be used for:

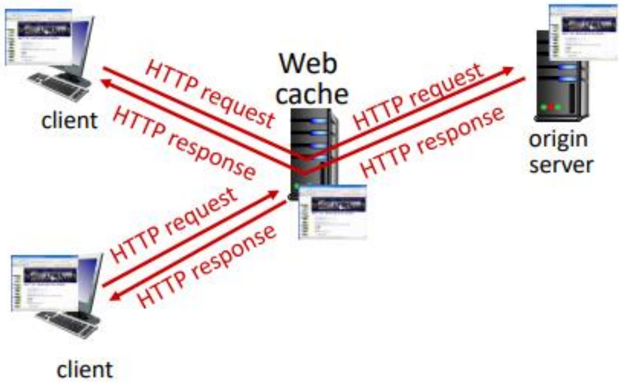
1. authorization
2. shopping carts
3. recommendations
4. user session state (Web e-mail)

Web caches

satisfy client requests without involving origin server

▪ browser sends all HTTP requests to cache

- if object in cache: cache returns object to client
- else cache requests object from origin server, caches received object, then returns object to client



E-mail

Three major components:

1. user agents
2. mail servers
3. simple mail transfer protocol: SMTP

User Agent

composing, editing, reading mail messages (Outlook, gmail)

Note// outgoing and incoming messages stored on server

Mail servers

1. **mailbox** contains incoming messages for user
2. **message queue** of outgoing (to be sent) mail messages

SMTP protocol

between mail servers to send and receive email messages

SMTP RFC (5321)

uses TCP at port 25 to reliably transfer email message from client to server

Direct transfer

send an email without relying on an SMTP server using Direct Send

Three phases of transfer

1. SMTP handshaking (greeting)
2. SMTP transfer of messages
3. SMTP closure

HTTP	**SMTP**
Client pull	Client push
ASCII	ASCII
each object encapsulated in its own response message	multiple objects sent in multipart message
	uses persistent connections
	requires message (header & body) to be in 7-bit ASCII
	server uses CRLF.CRLF to determine end of message

SMTP: delivery/storage of e-mail messages to receiver's server

IMAP: Internet Mail Access Protocol [RFC 3501]: messages stored on server, IMAP provides retrieval, deletion, folders of stored messages on server

HTTP: gmail, Hotmail, Yahoo!Mail, etc. provides web-based interface on top of STMP (to send), IMAP (or POP) to retrieve e-mail messages

Domain Name System (DNS)

translates domain names (mansourhaneen.com) to IP (10.5.6.177) addresses
Note// implemented as application-layer protocol

DNS services

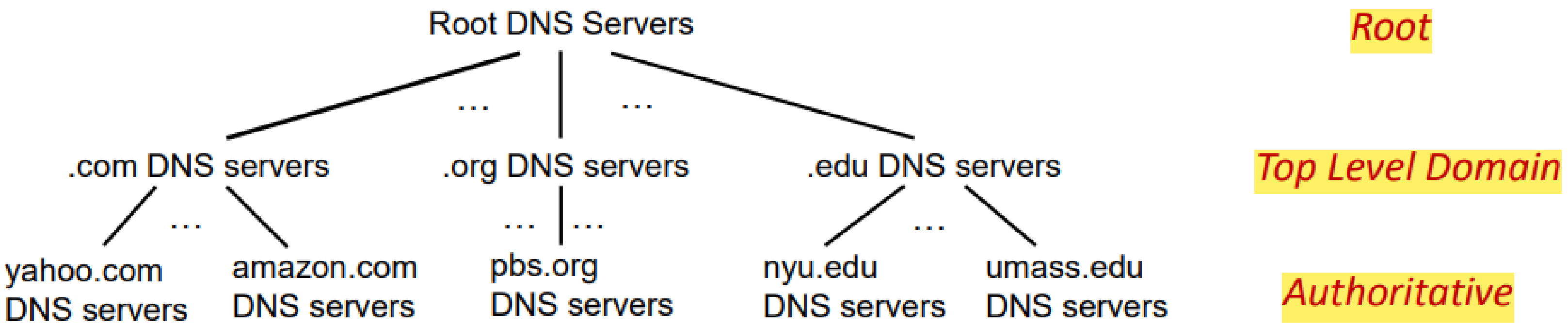
1. **Hostname-to-IP-address translation**
2. **Host aliasing**
3. **Mail server aliasing**
4. **Load distribution**
   Replicated Web servers: many IP addresses correspond to one name
   (mansourhaneen.com) to (10.5.6.177 and 10.100.155.4)

Why not centralize DNS?

1. single point of failure
2. traffic volume
3. distant centralized database
4. maintenance

hierarchical database

1. Root
2. Top Level Domain
3. Authoritative



DNS protocol messages

DNS query and reply messages, both have same format

Transport Layer

provide logical communication between application processes running on different hosts.

transport protocols actions in end systems

sender: breaks application messages into segments, passes to network layer

receiver: reassembles segments into messages, passes to application layer

transport protocols

TCP and UDP

Network layer: logical communication between hosts

Transport layer: logical communication between processes

Multiplexing: Handle data from multiple sockets and add transport Header

Demultiplexing: use Header info to deliver received segments to correct socket

UDP checksum

Used to detect errors in transmitted segment

Pipelining

is the method of sending multiple data units without waiting for an acknowledgment for the first frame.

1. **Go-Back-N**

   Note// Receiver window size is 1.

   if a sent packet is dropped, all the packets in the window are retransmitted until the last packet.

   1- **Sender**

   - cumulative ACK: ACK(n): ACKs all packets up to, including seq # n
     on receiving ACK(n): move window forward to begin at n+1
   - timer for oldest in-flight packet
   - timeout(n): retransmit packet n and all higher seq # packets in window

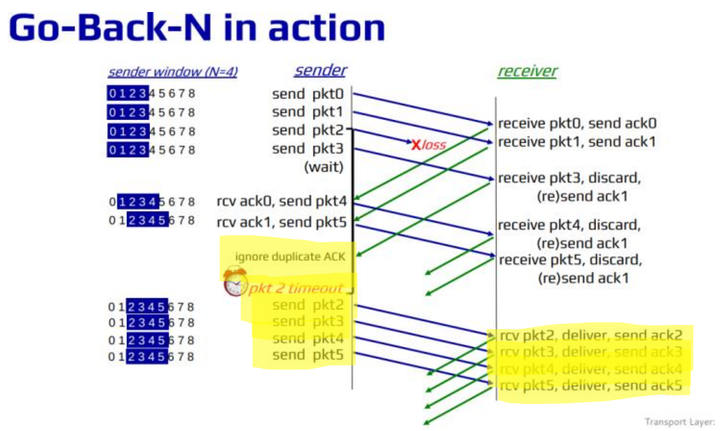
   2- **Receiver**

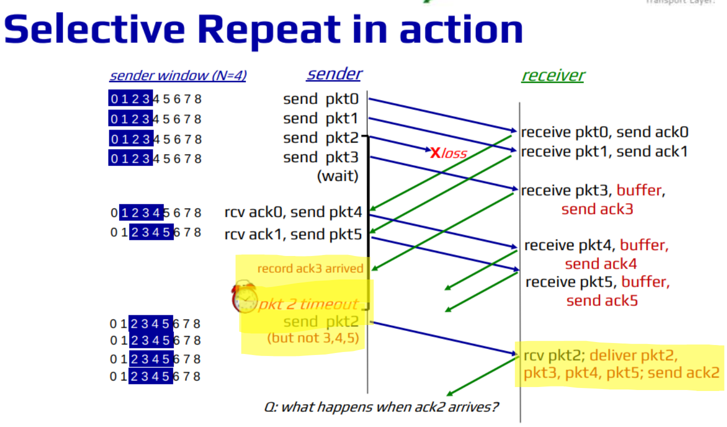
   ACK-only: always send ACK for correctly-received packet so far.

2. **Selective repeat**

   Note// Receiver window size is n.

   if a sent packet is dropped, then only the dropped packet will be retransmitted.





أفهم من المقطع افضل لك و اذا سألك عن شي تقدر تسوي له مثال من كيسك وتشرحه احسن من ذا الغثا اللي في السلايدات

https://youtu.be/TSI84aVI7bI

TCP

- point-to-point
- reliable
- full duplex data
- cumulative ACKs
- pipelining
- connection-oriented
- flow controlled

TCP fast retransmit

if sender receives 3 additional ACKs for same data (“triple duplicate ACKs”), resend unACKed segment with smallest seq #
likely that unACKed segment lost, so don’t wait for timeout

TCP flow control

receiver controls sender, so sender won’t overflow receiver’s buffer by transmitting too much, too fast.

TCP connection management (handshake)

1- agree to establish connection.
2- agree on connection parameters.

Congestion

occurs if too many sources sending too much data too fast for network to handle.

Chapter 4

Network-layer Data plane

Network-layer services and protocols

transport segment from sending to receiving host.
sender: encapsulates segments into datagrams, passes to link layer.

receiver: delivers segments to transport layer protocol.

routers examine header fields in all IP datagrams passing through it and moves datagrams from input ports to output ports to transfer datagrams along end-end path.

Data plane

local, per-router function
determines how datagram arriving on router input port is forwarded to router output port.
(Forwarding)

Control plane

network-wide logic
determines how datagram is routed among routers along end-end path from source host to destination host. **(Routing)**

- **traditional routing algorithms**: implemented in routers.
- **software-defined networking (SDN)**: implemented in (remote) servers.

Dynamic Host Configuration Protocol (DHCP)

A Dynamic method to assign IP Addresses to hosts.

Not only IP Addresses:

- Subnet Masks
- Gateways IP address
- DNS server IP address

How DHCP works?

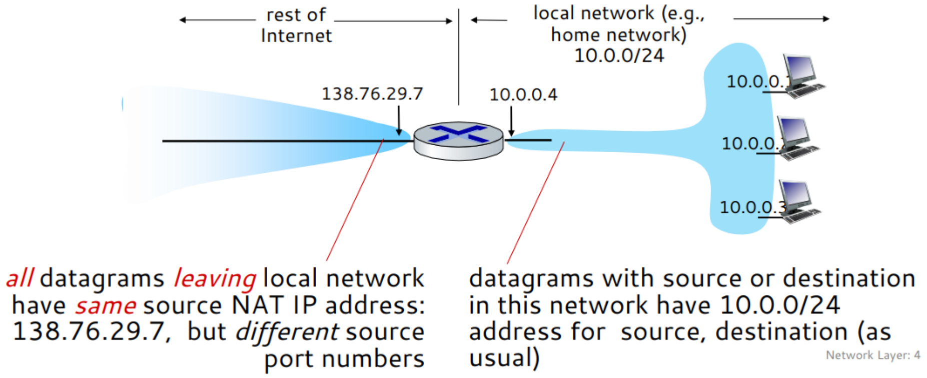
1- host broadcasts **DHCP discover** msg [optional]
2- DHCP server responds with **DHCP offer** msg [optional]
3- host requests IP address: **DHCP request** msg.
4- DHCP server sends address: **DHCP ack** msg.

Internet Corporation for Assigned Names and Numbers (ICANN)

- allocates IP addresses, through 5 regional registries (RRs)
- manages DNS root zone, including delegation of individual TLD (.com, .edu , …) management

Network Address Translation (NAT)

a way to map multiple local private IP addresses to one public IP address before transferring the information.



all datagrams *leaving* local network have *same* source NAT IP address: 138.76.29.7, but *different* source port numbers

datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

advantages:

1- just one IP address needed from provider ISP for all devices.
2- can change addresses of host in local network without notifying outside world.
3- can change ISP without changing addresses of devices in local network.
4- security: devices inside local net not directly addressable, visible by outside world.

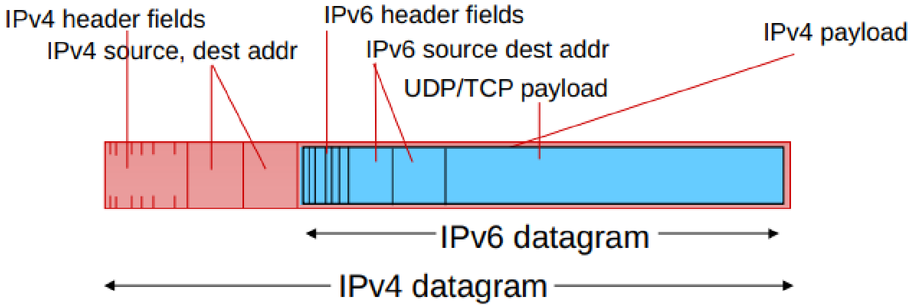
IPv6

- **initial motivation**: 32-bit IPv4 address space would be completely allocated.
- **additional motivation:**
  - speed processing/forwarding: 40-byte fixed length header.
  - enable different network-layer treatment of "flows".

Note// IPv6 consists of 128 bit divided into 8 octets

Transition from IPv4 to IPv6

Tunneling provides a way to use an existing IPv4 routing infrastructure to carry IPv6 traffic.



Chapter 5

Network-layer Control plane

Routing protocols

determine “good” paths from sending hosts to receiving host, through network of routers.

path: sequence of routers packets traverse from given initial source host to final destination host

“good”: least “cost”, “fastest”, “least congested”

Routing algorithm classification

1- **global**: all routers have complete topology, link cost info.
2- **decentralized**: routers initially only know link costs to attached neighbors.
3- **static**: routes change slowly over time.
4- **dynamic**: routes change more quickly.

Dijkstra’s link-state routing algorithm

centralized: network topology, link costs known to all nodes

- accomplished via “**link state broadcast**”.
- all nodes have same info.

intra-AS

routing among within same AS (“network”)

- all routers in AS must run same intra-domain protocol.
- routers in different AS can run different intra-domain routing protocols.

most common intra-AS routing protocols:

1- RIP
2- OSPF
3- IS-IS
4- EIGRP

gateway router

at “edge” of its own AS, has link(s) to router(s) in other AS’s.

gateways perform inter-domain routing (as well as intra-domain routing)

inter-AS

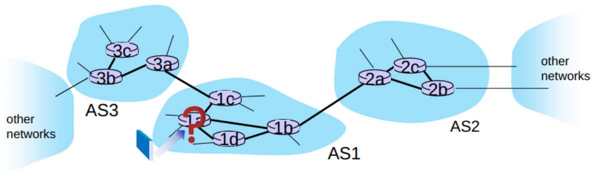
routing among AS’s

inter-AS routing protocols:

Border Gateway Protocol (BGP)

§ suppose router in AS1 receives datagram destined outside of AS1:
- ? router should forward packet to gateway router in AS1, but which one?

AS1 inter-domain routing must:
1. learn which destinations reachable through AS2, which through AS3
2. propagate this reachability info to all routers in AS1



OSPF (Open Shortest Path First)

"open": publicly available

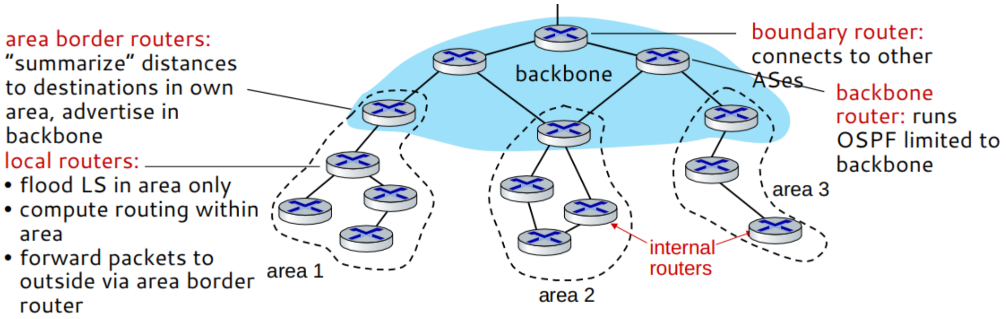
- each router floods OSPF link-state advertisements (directly over IP rather than using TCP/UDP) to all other routers in entire AS.
- Metric = Cost (lesser = Better)
- each router has full topology, uses Dijkstra's algorithm to compute forwarding table.

security: all OSPF messages authenticated (to prevent malicious intrusion)

Hierarchical OSPF

two-level hierarchy: local area, backbone.

- link-state advertisements flooded only in area, or backbone.
- each node has detailed area topology; only knows direction to reach other destinations.


area border routers: "summarize" distances to destinations in own area, advertise in backbone
local routers:
• flood LS in area only
• compute routing within area
• forward packets to outside via area border router
backbone
boundary router: connects to other ASes
backbone router: runs OSPF limited to backbone
area 1
area 2
area 3
internal routers

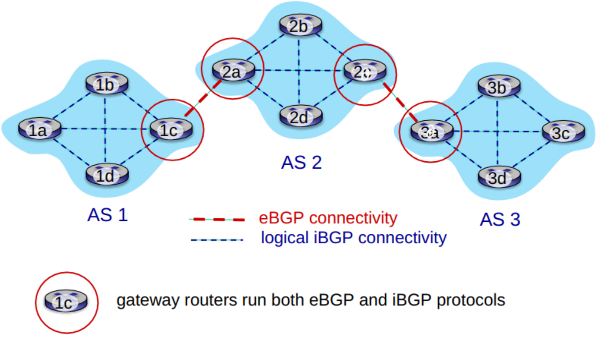
BGP (Border Gateway Protocol)

the de facto inter-domain routing protocol

"Glue that holds the Internet together"

allows subnet to advertise its existence, and the destinations it can reach, to rest of Internet: "I am here, here is who I can reach, and how"

1- **eBGP**: obtain subnet reachability information from neighboring ASes
2- **iBGP**: propagate reachability information to all AS-internal routers.


1a
1b
1c
1d
AS 1
2a
2b
2c
2d
AS 2
3a
3b
3c
3d
AS 3
eBGP connectivity
logical iBGP connectivity
1c
gateway routers run both eBGP and iBGP protocols

Software defined networking (SDN)

In SDN the control plane logic resides completely in the controller and the controller has a complete control over programing the forwarding decisions of the networking devices.

Internet Control Message Protocol (ICMP)

used by hosts and routers to communicate network-level information.

error reporting: unreachable host, network, port, protocol

echo request/reply (used by ping)

ICMP message: type, code + first 8 bytes of IP datagram causing error

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Chapter 6

Link Layer and LANs

Link Layer

has the responsibility of transferring the datagram from one node to a physically adjacent node over a link.

links

- wired
- wireless
- LANs

layer-2 packet: frame, encapsulates datagram

Link Layer Services

1- **framing, link access:** encapsulate datagram into frame, adding header, trailer.
2- reliable delivery between adjacent nodes
3- **flow control:** pacing between adjacent sending and receiving nodes.
4- **error detection:** errors caused by signal noise.
5- **error correction:** receiver identifies and corrects bit error(s) without retransmission.
6- half-duplex and full-duplex.

Note// MAC addresses in frame headers identify source, destination.

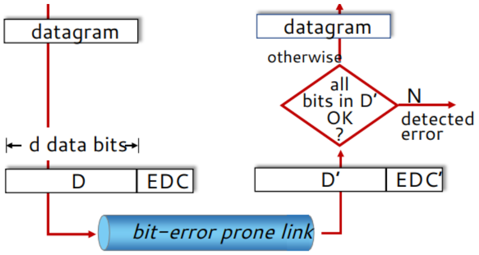
Where is the link layer implemented?

link layer implemented in **network interface card (NIC)** or on a chip in each-and-every host.

Error Detection

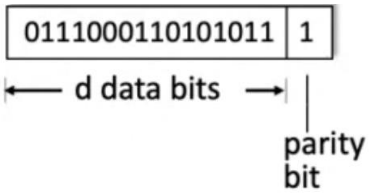
Error detection not 100% reliable!

Error Detection and Correction bits (EDC)

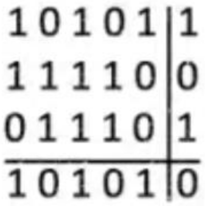


Parity checking

single bit parity: detect single bit error.



two-dimensional bit parity: detect and correct single bit errors.



```
10101|1
11110|0
01110|1
10101|0
```

Cyclic Redundancy Check (CRC)

more powerful error-detection coding that uses binary division.

Multiple access links protocols

1- point-to-point

2- broadcast

Multiple Access protocols

Used to control nodes transmission to avoid collision/interference.

Multiple Access Control (MAC) protocols

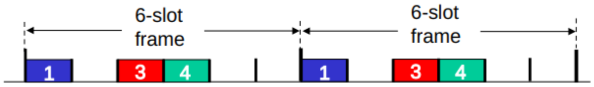
I. channel partitioning

divide channel into smaller "pieces"

1- TDMA: time division multiple access

access to channel in "rounds"

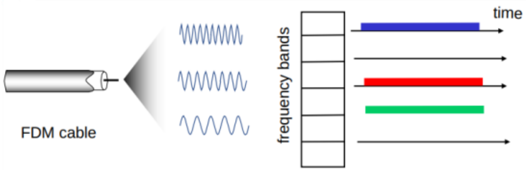
each station gets fixed length slot in each round



2- FDMA: frequency division multiple access

channel spectrum divided into frequency bands

each station assigned fixed frequency band



II. random access

channel not divided, allow collisions, "recover" from collisions

1- CSMA: Carrier Sense Multiple Access

listen before transmitting.

- if channel sensed idle: transmit entire frame.
- if channel sensed busy: don't transmit.

2- CSMA/CD: CSMA with Collision Detection

collisions detected within short time.

stop colliding transmissions, reducing channel wastage.

Note// collision detection easy in wired, difficult with wireless.

III. "Taking turns"

nodes take turns, but nodes with more to send can take longer turns.

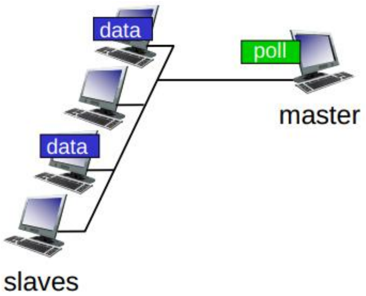
1- Polling

master node "invites" other nodes to transmit in turn.

typically used with "dumb" devices

concerns:

- polling overhead
- latency
- single point of failure (the **master** node)

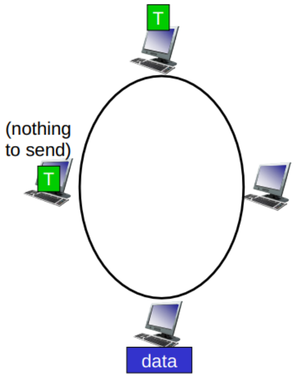


2- token passing

control token passed from one node to next sequentially.

concerns:

- token overhead
- latency
- single point of failure (**token**)



Media Access Control Address (MAC Address)

is a unique identifier assigned to a NIC for use as a network address.

48-bit MAC address burned in NIC ROM, also sometimes software settable

3A-34-52-C4-69-B8

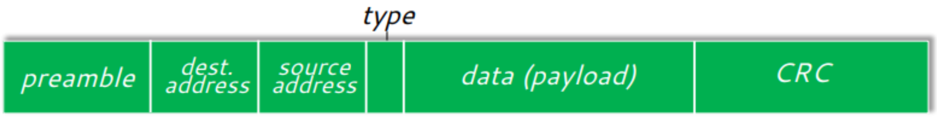
ARP: address resolution protocol

ARP table: each IP node (host, router) on LAN has table that maps IP address with its MAC address + TTL

Time To Live (TTL) time after which address mapping will be forgotten (typically 20 min)

Ethernet frame structure

sending interface encapsulates IP datagram in Ethernet frame.



preamble: used to synchronize receiver, sender clock rates 7 bytes of 10101010 followed by one byte of 10101011.

addresses: 6 byte source, destination MAC addresses

type: indicates higher layer protocol

CRC: cyclic redundancy check at receiver

Ethernet switch

Switch is a link-layer device takes an active role.

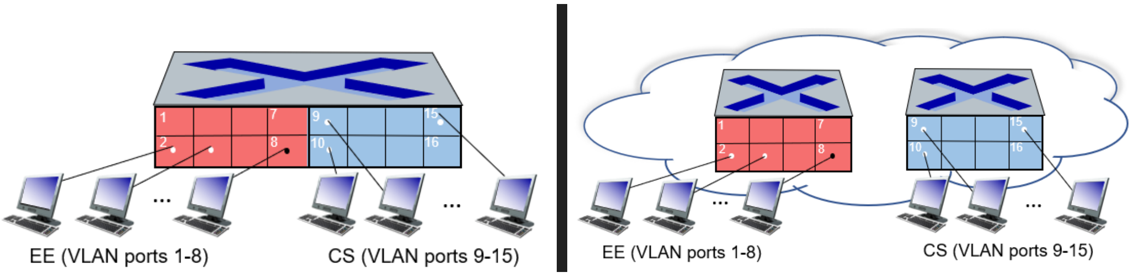
- **transparent**: hosts unaware of presence of switches.
- **plug-and-play**: switches do not need to be configured.
- **self-learning:** switch learns which hosts can be reached through which interfaces

Switches	Routers
store-and-forward	store-and-forward
link-layer devices	network-layer devices
forwarding tables	forwarding tables
learn forwarding table using flooding, learning, MAC addresses	compute tables using routing algorithms, IP addresses

Virtual Local Area Networks (VLAN)

switch(es) supporting VLAN capabilities can be configured to define multiple virtual LANS over single physical LAN infrastructure.

port-based VLAN: switch ports grouped so that single physical switch operates as multiple virtual switches


1
2
7
8
9
10
15
16
...
...
EE (VLAN ports 1-8)
CS (VLAN ports 9-15)
1
2
7
8
9
10
15
16
...
...
EE (VLAN ports 1-8)
CS (VLAN ports 9-15)