DES232
Lecture 7-9 (Error & flow control - IP Address)

Error & Flow Control

- usually together because the data-link protocol used for error control also used for flow control.

Definition

error control - method using to handle errors in frames
- those use "retransmission" in case error occurs in the frame
  ↳ called ARQ : Automatic repeat request
- retransmission is needed when
  frame is erroneous or lost

flow control - set of procedures used to restrict the amount of data that TX can send before waiting for an acknowledgement from RX
- to avoid overwhelming the RX with flow of data from TX

Control Protocols

error control
1) Stop-and-wait ARQ
2) Sliding windows ARQ → 2.1) Go-back-N ARQ
   2.2) Selective-Reject ARQ

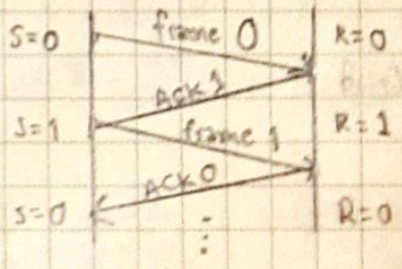
flow control
1) Stop-and-wait
2) Sliding windows

- Stop & wait → send one frame at a time / wait for acknowledgement
- sliding window → send many frames at a time / w/o waiting for acknowledgement

Stop-and-wait ARQ

- half-duplex link
- simple protocol
  - TX keeps the copy of last frame
  - after receiving, RX send back ACK
  - after receiving ACK, TX send next frame
  - ACK "1" if dataframe is "0"
    ACK "0" if data frame is "1"

Normal operations



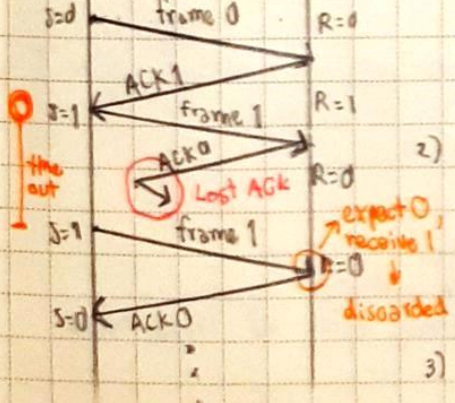
Abnormal Operation

1) Lost/Damage Frame
   - RX discards them silently, if damage
   - no ACK coming back after a while
   → Frame is lost → resend

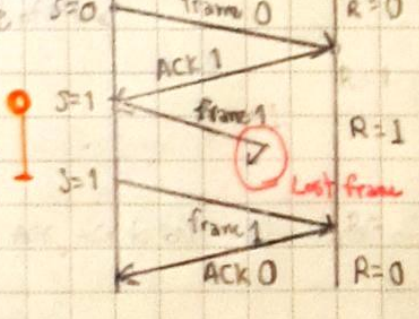
2) Lost/Damage ACK
   - TX Discards ACK
   - TX keeps time after the
   - TX sends frames again.

3) TX receives late ACK
   - timer already expired. - frame - resent, RX has duplicate → discard
   - late ACK receives, send next frame.

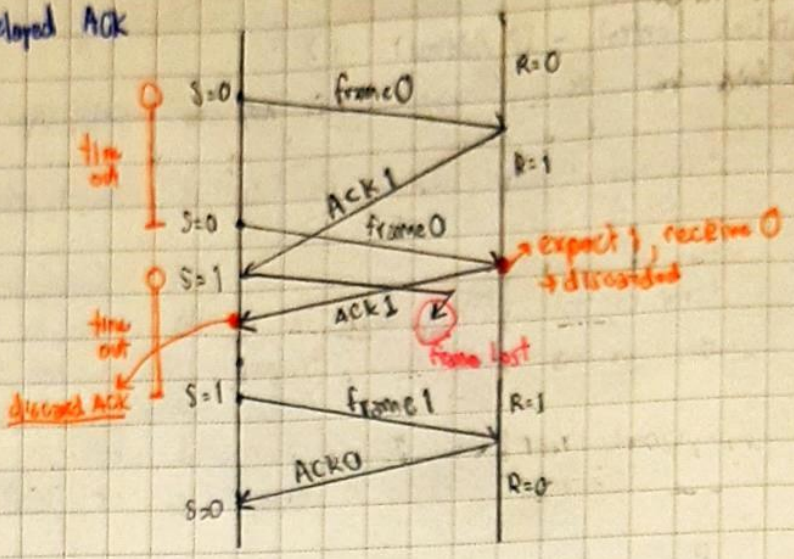
Lost/Damage ACK



Lost/Damage Frame



Late / Delayed ACK



piggybacking : combine data & ACK in 1 frame, useful for bidirectional communications
faster & saves bandwidth

drawbacks of stop&wait ARQ
- line is not fully utilized, only 1 frame is sent per time
- ACK must be waited for, no frames send during this time.
* Inefficiency get worse when
  - TX speed is high - Propagation distance is high
  * both leaves TX waiting idle for longer time)

Efficiency : utilization of link : $U = T_f / T_{total}$
$= T_f / (T_f + 2T_{prop})$

f => transmit frame
prop => propagation

or just $U = \frac{1}{1+2a}$; $a = \frac{T_{prop}}{T_f}$

a : keeping of the link in bits

* Stop-and-wait ARQ inefficient when $a > 1$, efficient when $a \ll 1$
$U \to 0\%$ ⇐ ⇒ $U \to 100\%$

■ Sliding Window Protocol
- assuming it's full duplex line
- RX & TX have buffers each of size W frames
- m-bits sequence ; frames & ACK are $0, 1, 2, \ldots, 2^m - 1$

* allowed TX to send upto W frames w/o waiting for ACK
RX received upto W consecutive frames
* ACK J ⇒ sent by RX ⇒ means RX received frames upto J-1, ready to receive J
* window size W can be less or equal to $2^m - 1$

■ Go-back-N ARQ : pipelining / frame is sequentially numbered
↳ improves efficiency of the line by sending upto W frames before waiting about ACK

* Go-back-N ARQ :

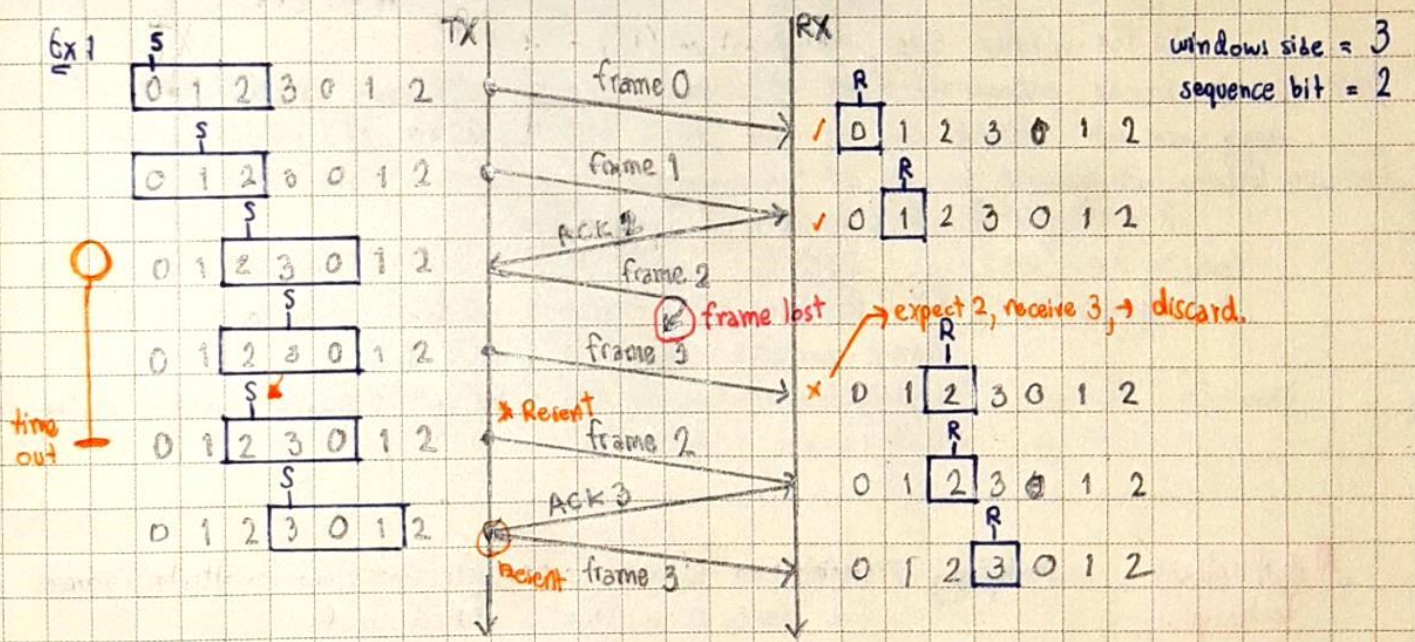
→ TX : hold the outstanding frames until they are individually ACK
- window size W cannot exceed $2^m - 1$, W is fixed
- ACK received properly, window slide pass that frame, purged of memory

→ RX : size of window always 1, on next expected frame.
- others frame arrive, immediately discarded
- correct frame arrive, window slided

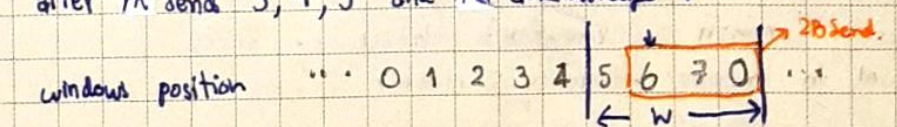
→ TX tracks; recently sent (S), first frame in window (S_F) & last frame (S_L)
$W = S_L - S_F + 1$

→ TX sets a timer for each frame sent

→ RX has no timer, send ACK if properly received frame from TX
* if RX received out of sequence / damaged frame, silently discard
cause TX timer expired, TX go back and send all frames start from non-ACK frame.



Ex 2 3-bits sequence number, window size = 4
after TX send 3, 4, 5 and RX acknowledge 4

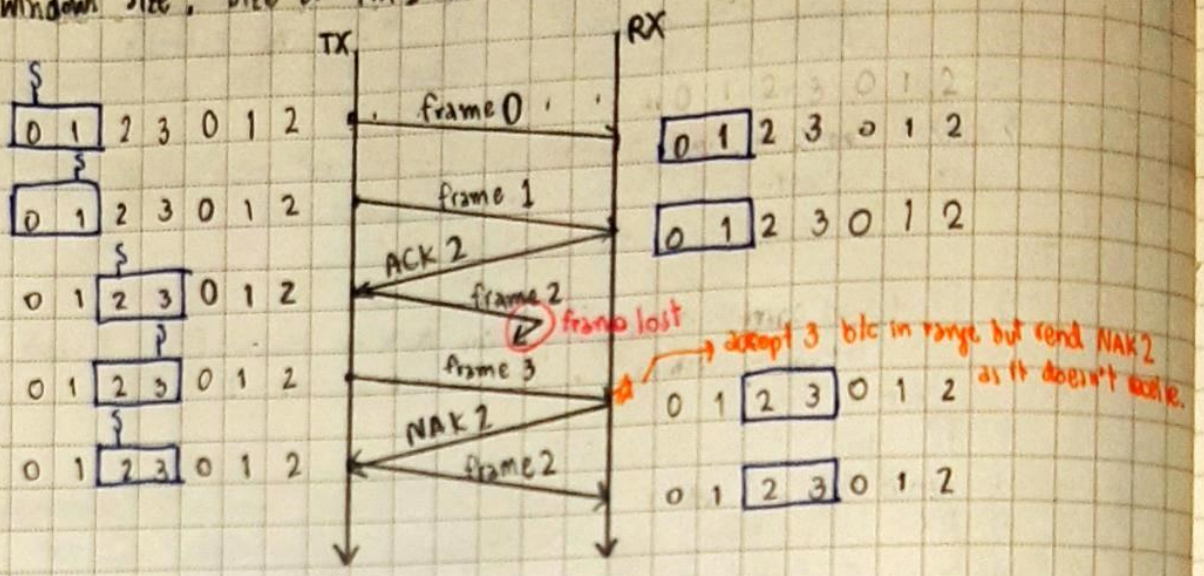


* Selective Repeat ARQ
→ go-back-N ARQ is very inefficient for noisy link,
bandwidth inefficient & slow down of transmission

→ selective ARQ, only damage frame is resent, more bandwidth efficient, more complex at RX
define NAK (negative ack) to report the number of sequence of a damaged frame before timer expires.

→ • Selective Repeat ARQ

• TX window size : size of RX & TX windows is at most one half of 2^m #



→ efficiency of sliding window protocol

W for window size, Utilization (U) = $\begin{cases} 1 ; & W \geq 2a+1 \\ \frac{W}{2a+1} ; & W < 2a+1 \end{cases}$, 100% utilization

a = length of link in bits (T_{prop} / T_f)

→ piggy backing : TX maintains own transmit window
frame contains data field + ACK field
sequence number for the data field and sequence number for the ACK field

---

■ Multiplexing Techniques

Multiplexing : combination of information streams from multiple sources for transmission over a shared medium

Demultiplexing : separation of a combination back into separate information streams

pretty common on long-haul, high capacity links
used to improve efficiency & number of user using network simultaneously

Bandwidth utilization is the wise use of available bandwidth to achieve specific goal
efficiency achieved by multiplexing ; sharing bandwidth b/w multiple users.

■ FDM : frequency-division multiplexing

↳ analog multiplexing technique that combines analog signals.

↳ # total BW in medium is divided into series of non-overlapping frequency band to carries separate signal

- baseband / low pass signal is a signal that include f that are very near zero (sound waveform)
→ modulate to higher f to be transmitted, shift the signal up to much higher frequency
→ using bandpass filter to filter out / demultiplexing the signal & demodulate it to get baseband

* guard band
- prevent interference b/w data sources
- channel too close, lead to inter-channel crosstalk
- must be separated by strip of unused bandwidth → guard bands

FDM → set of radio/TV can transmit EM signal simultaneously,
multiple carrier on over single copper wire
→ demultiplexer applies a set of filters that each extracts a small range of f near carrier frequency

Analog carrier system : use an FDM - hierachy

Group :	→ Supergroup :	→ Mastergroup	etc
12 VC (4 kHz each)	FDM of 5 groups	FDM of 10 supergroup!	
[60 kHz, 108 kHz]	60 VC, [420, 612 kHz]	600 VCs	

ex A system used 2 bands, first band of 824-849 MHz for sending, second of 869-894 MHz for receiving. Each user has a BW of 30 kHz in each direction. How many people can use their device in the system simutaneously; 42 channel reserved for control purposed.

Each band → 849 - 824 = 25 MHz
Each channel → 30 kHz = 0.03 MHz
} $25 / 0.03 = [833.33]$ channel
$= 833$ channel

deduct 1 channel for reality: 832 channel available - 42 control channel
↳ 790 channel are available! ez

■ WDM : Wavelength Division Multiplexing
↳ used in fiber-optics; multiplex a number of optical carrier signals onto a single fiber by using different wavelengths of laser light
↳ enable bidirectional communication over one fiber, multiplication of capacity

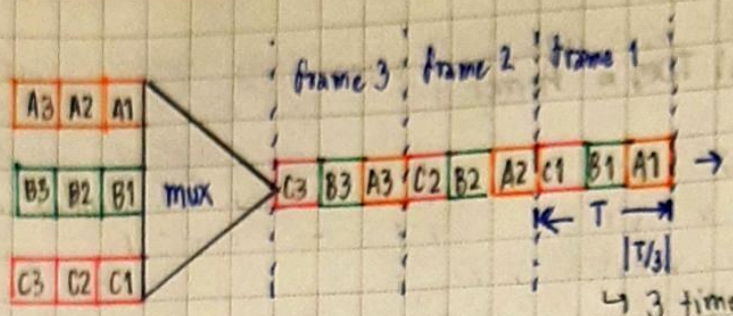
aka. FDM with multiple beams at different frequencies on same cable.
* analog multiplexing techniques combine optical signals

→ Ingress → multiple optical are combine into single optical signal (differing → combine)
Egress → separate multiple to differing wavelength (refraction)

■ TDM : Synchronous Time Division Multiplexing
↳ method of transmitting & receiving signal over a common path by means of synchronized switches at each end of the transmittion line, each signal appears on the line only a fraction of time
↳ * digital multiplexing techniques for several low-rate digital channel to one high-rate.

* FDM same time diff frequency, TDM, same frequency diff time.

TDM:



each time slots ⇒ T/N s (time/frame, number of input)

↳ 3 timeslot / frame

* Sync TDM, data rate of link is n times faster, unit duration is n times shorter

↳ from this figures: bit rate for each input connection is 1kbps
1 bit at a time is multiplex (unit is 1 bit)

then, duration of each input slot ⇒ bit rate of each input is 1000 bps
bit duration = 1/1000 s = 1 ms
∴ duration of each input timeslot = 1 ms.

duration of output slot ⇒ 1/3 of input time slot
⇒ 1/3 ms

duration of 3 frames ⇒ duration of slot × number of frames
⇒ 1/3 × 3 = 1 ms

* duration of frame is the same as duration of input unit

* frame rate = input rate = data stream rate × number of stream

TDM Link Control: ⇒ no header & trailers, flow control & error control can be provided on a per-channel basis by using a data link control

ex HDLC is a group of communication protocols of the data link layer for transmitting data between network points or nodes. data organized into frames, frame sent to a network, verify on its arrival.

For flow control: - data rate is fixed (of multiplexed lines)
- mux & demux designed to operate at the same rate
- one channel Rx cannot receive data, other must carry on,
- leaving empty slots

error control: - Errors detected & handled on individual channel

■ Framing
- There's no flag/Sync character to bracket TDM, some means needs to assure synchronization
- manage framing/ one control bit is added to each TDM frame
- an identifiable bit pattern is used on control channel to differentiate control data
- To synchronize, a receiver compares the incoming bits of one frame to the pattern
↳ search until match

■ Bit Stuffing * if each source has separated clock, variation in clock = loss of synchronization
↳ have outgoing data rate > sum of incoming rates / stuff dummy bit until clock is matched
↳ stuffed at fixed location in frame, remove at demux

Statistical TDM

→ drawback of Sync TDM → many time slots in frame are wasted
→ Statistical TDM = Asynchronous TDM

→ dynamically allocates timeslot on demand to separate input channel
→ multiplexer scan input line, collect data until frame is full
→ may have problem during peak

Different of Async & Sync TDM

Criteria	Sync TDM	Async TDM
• Working	divide into units input occupy one output time slot	allocated to timeslot dynamically, based on arrival of data
• No. of Slot	slot in each frame are equal to no. of input	slot in each frame are less than the no. of input
• Buffers	Buffering is not done, frame is sent after a particular interval of time whether send or not	Buffering is done and only those input are given slots in output frame buffer contain data to sent
• Addressing	carry data only, no addressing needed	contains both data & address of the destination
• Synchronization	used at beginning of each frame	No synchronization bit are used.
• Capacity	Max BW Utilization if all inputs have data to send	capacity of link is normally less than the sum of capacity of each channel
• Data Separation	demux on RX → decompose each frame → discard framing bits → extract data unit in turn	demux on RX → decompose each frame → checking local address of each data unit

IP Addressing

→ IP Addressing is Logical Addressing
→ works on Network Layer (Layer 3)

→ IPV4 - 32-bit
→ IPV6 - 128-bit

IPv4 32-bits → 4 octets, dotted decimal
ex 172.174.32.15

IPv6 128-bits → 8 blocks of 4-bit hexadecimal, Colon-Hex
ex FEDC:BA98:7654:3210:0123:4567:89AB:CDEF

IP Address Classes

IP address scheme is divided into 5 classes

			Range
LAN&WAN	Class A	→ 0	0.0.0.0 - 127.255.255.255
	Class B	→ 1 0	128.0.0.0 - 191.255.255.255
	Class C	→ 1 1 0	192.0.0.0 - 223.255.255.255
Multicasting	Class D	→ 1 1 1 0	224.0.0.0 - 239.255.255.255
R&D	Class E	→ 1 1 1 1	240.0.0.0 - 255.255.255.255

priority bit : used to identify class, located the leftmost in the first octet of IPv4

Thus, it can be written when divided into network bit (N) and Host bit (H)

Class A → N.H.H.H Class B → N.N.H.H Class C → N.N.N.H

Calculation of No. of Network / Host on Network

No. of network ⇒ $(2^{n-p}) - 2$; n ⇒ number of network bit
p ⇒ priority bit

Host / Network → $2^h - 2$; h ⇒ number of host bit

★ valid IP address lie between network address and broadcast address
network address → first IP address on the network
broadcast address → last IP address on the network

Private IP Address

- reserved for LAN & private use
- not connect to the internet

Class A: 10.0.0.0 to 10.255.255.255
Class B: 172.16.0.0 to 172.31.255.255
Class C: 192.168.0.0 to 192.168.255.255

Subnet Mask

- differentiates network & host portion
- represented in form of 1's in network portion, 0's in host portion

Subnetting

- breaking large network in small networks known as subnets.
- ★ borrow host bit to create network / subnet
- also called FLSM (fixed length subnet mask)

Can be done in 3 ways

① divide host into small group
Ex group A: 192.168.1.1 to 192.168.1.20
group B: 192.168.1.21 to 192.168.1.40
⋮

- disadvantage: difficult to distinguish IP address for each group b/c of same network mask.

② allocate different network to each department
Ex group A: 192.168.1.1 to 192.168.1.20
B: 192.168.2.1 to 192.168.2.20
⋮

- disadvantage: loss of Bandwidth broadcast for 254 instead of 20
waste of IP address
no security

③ subnetting to change host bit to network bit.

ex Class C: 192.168.1.0 // network address
want for 5 subnetworks ?

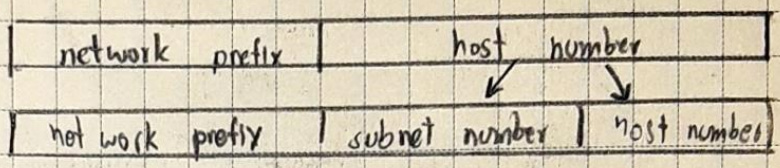
- No. of subnet $2^n - 2 \geq$ Req. of subnet

$2^3 - 2 \geq 5 \rightarrow$ 6 Subnets → 3 bits of subnet

No. of host $2^h - 2 = 2^5 - 2 = 32 - 2 = 30$ Host/Subnet

* every subnet need network ID & broadcast ID in there *

■ Basic Idea of subnetting



result is a 3-layer hierachy

- subnets can be freely assigned within the organization
- Internally, subnets are treated as Separated networks
- subnet structure is not visible outside the organization

advantage ; reduce router complexity ; the complexity of routing table at external routers is reduced.

ex Major network info ;

Host IP Address : 172 . 16 . 18 . 33
Network Mask : 255 . 255 . 0 . 0
Subnet mask : 255 . 255 . 255 . 0

find the following information

▶ Major network information
- Major network address: 172 . 16 . 0 . 0
- Major network broadcast address : 172 . 16 . 255 . 255
- Range of host if not subnetted: 172 . 16 . 0 . 1 - 172 . 16 . 255 . 254

▶ Subnet Information
- Subnet Address 172 . 16 . 18 . 0
- Range of host address (first host & last host) 172 . 16 . 18 . 1 - 172 . 168 . 18 . 254
- Broadcast address: 172 . 16 . 18 . 255

▶ Other subnet information
- Total of non-reserved subnet $2^8 - 2 = 254$ subnet
- Number of host per subnet $2^8 - 2 = 254$ host/subnet.

DES232
Lecture 10-12 (Routing Algorithm, topology, email)

Routing (Lecture 10)

→ key function: to determine the best path (there's multiple path on network
→ depend on objective of network (minimize hops, minimize end-to-end delay, maximize BW)

Criteria of good routing algorithm

→ 1) Correctness : correct & accurate delivery
→ 2) Robustness : adaptive to change & varies load
→ 3) Cleverness : detour congestion ability, & connectivity of network
→ 4) Efficiency : rapid route finding, minize control message

Classification

1) Static vs Dynamic
Static → manually compute route, simple, not scalable
Dynamic → automatic route computation, dynamic adaptation

2) Centralized vs Distributed
Centralized → center compute all route & load to router
Distributed → router exchange topology info, perform own route computation, inconsistent & loop

In datagram, routing is based on packet by packet
VC, routing is executing during setup.

Routing table

→ store routing info, looked up by packet
2 types: 1) virtual circuit packet switching
2) Datagram Packet Switching network

→ virtual circuit packet switching routing table

Incoming		Outgoing	
Node	VCI	Node	VCI
prevNode	linkName	nextNode	linkName
:	:	:	:

* if a link breaks, all tables in network must be updated to secure liability of network

* Reason to use local VCI rather global VCI
- search is easier b/c local uniqueness
- more avail local VCI, more connection

→ datagram packet switching network routing

Destination	Next hops
destNode	nextNode
:	:

* assume to find next hops to that destination at shortest path

Hierarchical Routing

→ size of routing table will be very large if network is too large

→ solution

→ host close to each other are assigned w/ network address same prefix

→ In remote routing table, all hosts are treated as one address, one entry to table.

ex IP hierarchical addressing → Host ID = subNetwork ID + Host ID
IP address = Network ID + Host ID

Routing Algorithm

types of algorithms

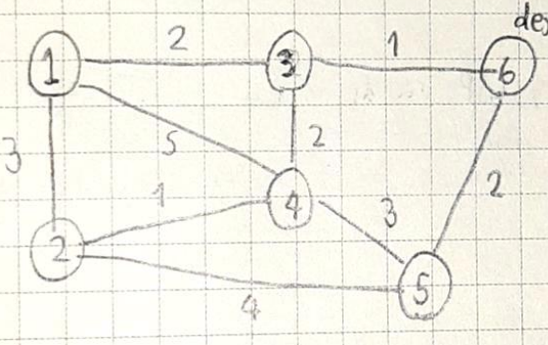
↳ Distance Vector Routing → Link State Routing

* Routing information excharge is the most important and should be efficient & not consume much BW

→ Distance Vector Routing (w/ Bellman-ford!)

Principle: if N is in the shortest path from A to B
then A to N and N to B is also the shortest path

ex compute shortest path from any node to Node 6



(x,y) = node x cost y

Iteration	N1	N2	N3	N4	N5
Init	(-1,∞)	(-1,∞)	(-1,∞)	(-1,∞)	(-1,∞)
1	(-1,∞)	(-1,∞)	(6,1)	(-1,∞)	(6,2)
2	(3,3)	(5,6)	(6,1)	(3,3)	(6,2)
3	(3,3)	(4,4)	(6,1)	(3,3)	(6,2)
4	(3,3)	(4,4)	(6,1)	(3,3)	(6,2)

→ distributed implementation
Bellman-ford can be executed at any node from any to any, thus totally distributed.
A neighbors exchange DV periodically
→ whenever a node receives a distance vector from its neighbor, check if there's new shortest path or not, if yes, modify DV.

Recomputation if links break. some eventually converge / set broken with (-1,∞) then recompute w/ bellman-ford.

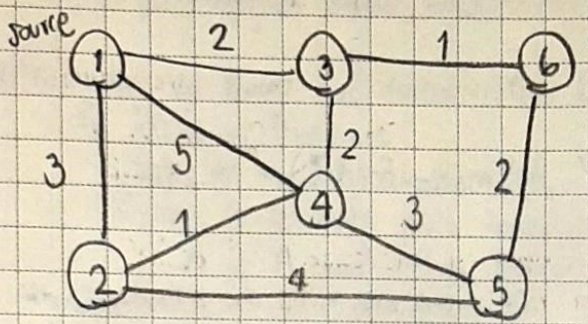
→ some leads to counting to infinity problems
"good news travel fast, bad news travel slow"
→ solution to counting to infinity
"Split horizon with poisoned reverse"
→ Minimize cost to a destination is set to infinity if neighbor is the next node along shortest path

→ link state routing (w/ DIJKSTRA's ALGORITHM)

→ suppose that topology of network is known

→ how to get network topology?
  → every node has link state packet (LSP) records neighbors & cost to neighbors.
  → every node flood LSPs if there's a change of link state
  → any node can construct network topology after receives all LSPs

ex calculate from node 1 to any node



Iteration	N2	N3	N4	N5	N6	select
init	3	2	5	∞	∞	{1}
1	3	2	4	∞	3	{1,3}
2	3	2	4	7	3	{1,2,3}
3	3	2	4	5	3	{1,2,3,6}
4	3	2	4	5	3	{1,2,3,4,6}
5	3	2	4	5	3	{1,2,3,4,5,6}

Comparison of DVR and LSR

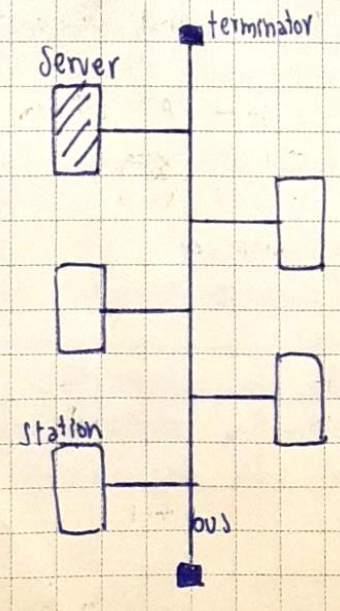
→ DVR records cost to all node, LSP records cost to its neighbors
→ DVR converges slow, may loop for a while, reacts to failure slowly
→ LSP reacts to failure fast, but too much flood if topology changes quickly and consume BW

Network Topology (lecture 11)

LAN TOPOLOGY

physical → describe geometric arrangement
logical → describe possible connections b/w endpoints that communicate

→ ① Bus topology

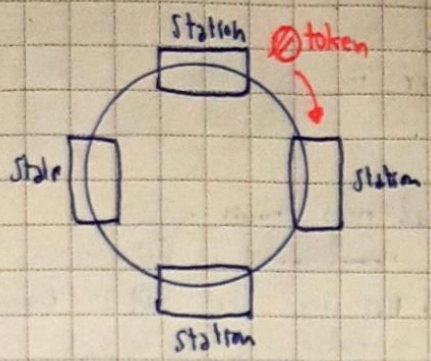


→ node directly connected to half-duplex common link called bus
→ every station will receive all network traffic and it has equal transmission priority
→ all nodes are interconnected, peer to peer, using single open-ended cable with both ends terminate w/ resistor to prevent bounce.

✳ Advantages
- easy to implement & extend, suited for temp. network, cheapest, failure of one don't affect another

✳ Disadvantages
- difficult to admin & troubleshoot, limit length & station, link break can disable entire network, long run gives maintenance cost high, performance degrade if added station more.

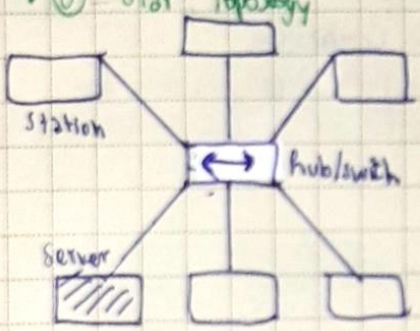
② Ring Topology



- each node exactly connect w/ 2 others node forms continuous pathway like a ring
- data travels from node to node w/ each node handling the packet
- simple peer-to-peer LAN topology
- data transmit unidirectional around the ring & help by TOKEN with the sending & receiving data
  - 3-bytes frame contains control info, who holds the token can send data, prevent data from colliding.

- advantage: organized, better than bus, no network control server, equal access to resource, more component has no effect on performance of network
- disadvantage: all data must pass btw source and dest on each station along the way, one pcs down network down too, highly dependent on wire which connect components

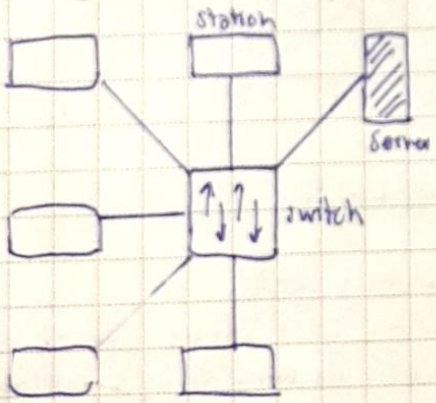
③ Star Topology



- every stations connect w/ central hub
- have connections to network device that radiates from common point
- access the media independently
- common topology

- advantage: better performance, easy to add new node, centralized management, failure of one don't affect network
- disadvantage: if hub down, network down, increase cost of network, performance number depends on control device

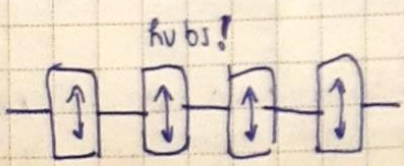
④ Switched Topology



- both logical & physical topology
- use switch instead, support small (16-24) LAN
- support point-to-point circuit, no sharing circuit
- switch reads dest addr and only send to the corresponding, hub broadcast to all
- learn MAC address and stored it lookup table internally
- feature multiple connection
- each port & device that connect has its own dedicate BW

- advantage: improve LAN performance
  - increase aggregated BW on network, reduce number of device that shared BW, less collision
- disadvantage: more expensive, issue is difficult to traced, broadcast maybe troublesome.

⑤ Daisy Chain



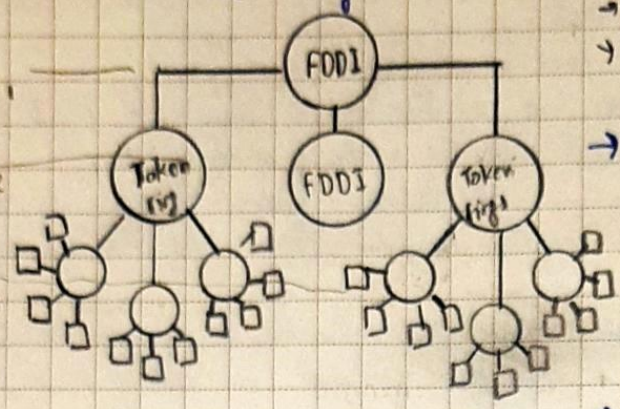
- generally connect hubs on the network, easy to built, first-gen inter connection method for emerging LAN

- advantage: increase number of connection and devices
- disadvantage: too many compete for BW, create collusion thus incapacitate.

→ ⑥ Hierarchy

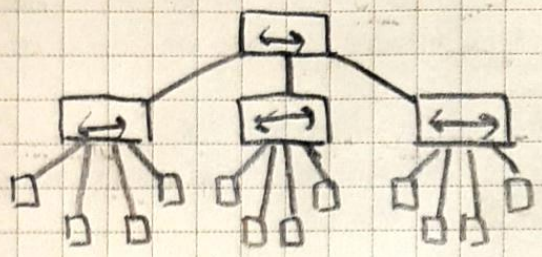
→ more than 1 layer of hubs
→ each layers serves different network function
→ bottom tier for user & server connection
→ higher tier for aggregation of user level tier
→ best for N-to-1 site w/ scalability concern

→ hierarchical rings



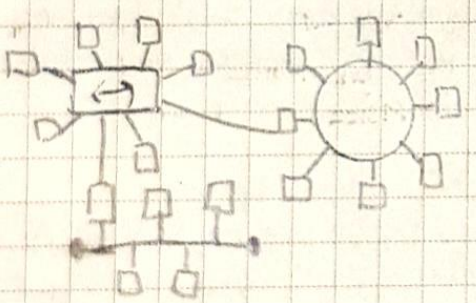
→ hierarchical rings
→ rings interconnected in hierarchical fashion
→ second-tier ring either FDDI (fiber distributed data interface) or token ring can be used to connect all user rings and access to WAN

→ hierarchical star



→ hierarchical star / Tree topology
→ implemented as single collision domain or multiple collision domain using switch / router / bridges
→ collision domain = network segment connected by medium/repeater where simultaneous data transmission collide w/ one another

→ hierarchical combination

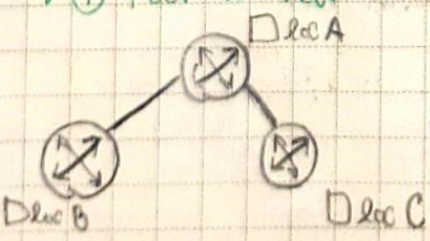


→ hierarchical combination
→ combine multiple topologies into one
→ not force-fit all requirement into one solution

■ WAN Topology

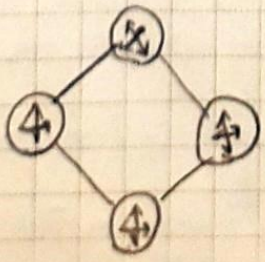
→ describe transmission they interconnected

→ ① Peer-to-Peer



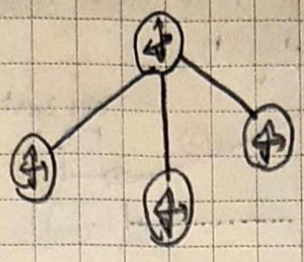
→ simple of connecting smaller sites
→ develop by using leased private line or another facility
→ least cost solution for WAN w/ small internetwork location
✱ disadvantages
→ not scale well → any break could split WAN

→ ② Ring topology



→ can use dynamic routing protocol
→ construct with point-to-point transmission facility
→ from P2P by add one transmission facility, an extra port on 2 routers
✱ advantages provides alternative routes, less expensive other than P2P
✱ disadvantages geographic dispersion, cost may depends
rings are not scalable

→ ③ Star Network Topology

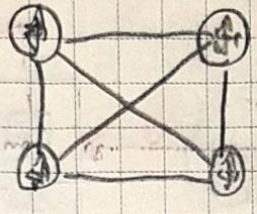


→ homing all location to common location
→ can constructed using almost any dedicated transmission facility includes frame relay and point-to-point private line

※ advantages
→ more scalable → improve network performance

※ disadvantages
→ single-point of failure → no route redundancy

→ ④ Full-Mesh topology

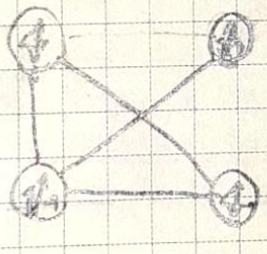


→ ultimate reliability & fault tolerance
→ aka. complete graph (node connect to all others)
→ static routing is impractical / use dynamic
→ use for network with requirement of high availability

※ advantages
→ minimize hops → can be built with virtually any transmission tech

※ disadvantages
→ expensive to build

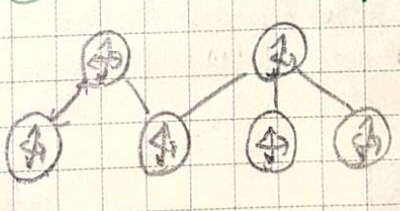
→ ⑤ Partial-Mesh topology



→ can take) variety of different configuration
→ much more tightly coupled but not fully connected, almost connected by all nodes)

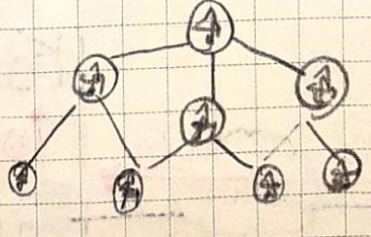
※ advantage
→ minimize hops for bulk WAN users
→ more affordable and scalable than mesh (not connecting w/ low traffic segment

→ ⑥ Two-tiered topology



→ mod. version of basic star
rather use one, used two or more concatenator router instead
→ construct w/ dedicated facility offers improved fault tolerance w/o compromise scalability

→ ⑦ Three-tiered topology



→ WAN w/ large number of sites, or built with small router that can support few serial conn.
→ more scalability

※ advantages → greater falut tolerance and scaability

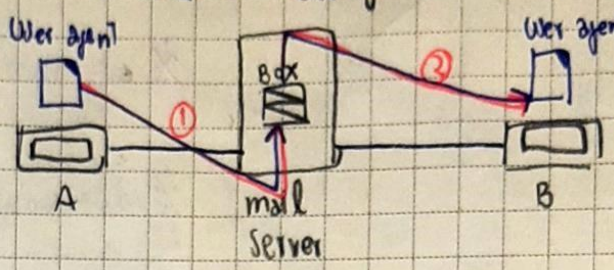
※ disadvantages → expensive to build, operate, maintain

→ ⑧ Hybrid. → useful in larger & complex network, → develop w/ multitiered WAN w/ full-mesh of backbone

Email (Lecture 12)

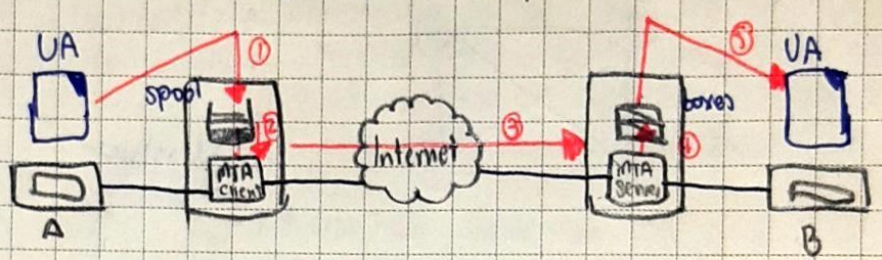
4 Scenarios (less to most complexity)

→ Scenario 1 → Sender on the same mail server w/ receiver
* need 2 user agents.



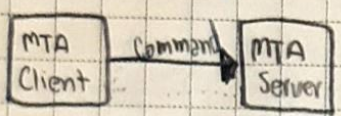
UA = user agent
MTA = message transfer agent
MAA = message access agent

→ Scenario 2 → sender & receiver on different mail server
* need 2 UAs & 1 pair of MTA (client and server)

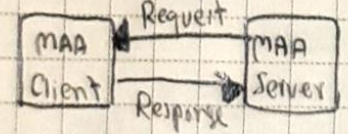


Generally,

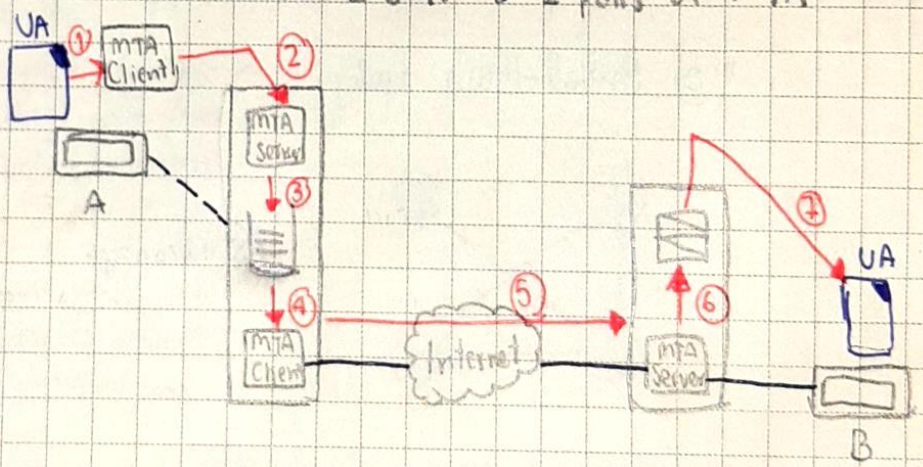
* Push Message



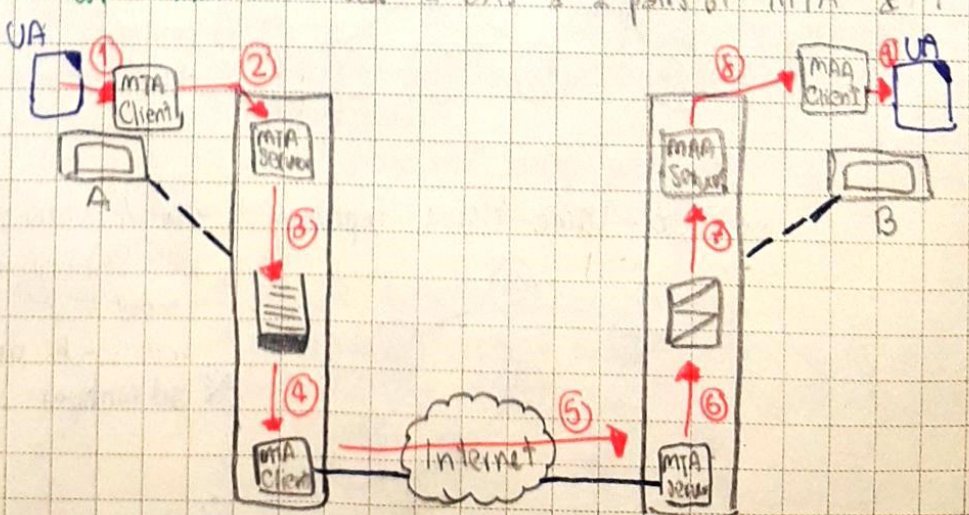
* Pull Message



→ Scenario 3 → Sender connect to mail server via LAN or WAN
* need 2 UAs & 2 pairs of MTA



→ Scenario 4 → sender & receiver connect by LAN or WAN
* Most Common * need 2 UAs & 2 pairs of MTA & 1 pair of MAA



UA : USER AGENT

provides services to the user to make the process of sending and receiving a message easier.

Structure of email

→ Envelope	→	front of envelope From / To
→ Message	→	Header → date / subject etc.
	→	Body → message / text.

local @ domain name

↑ mail box address

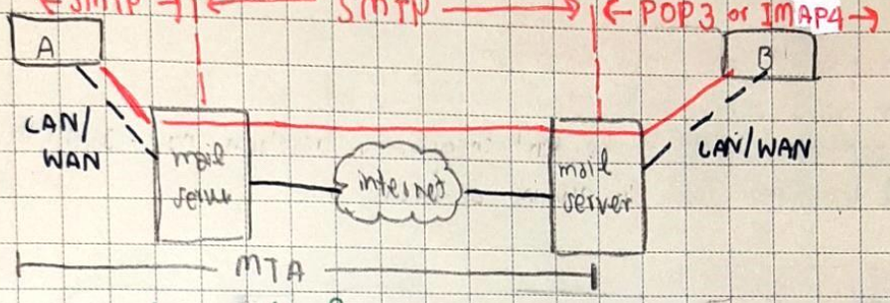
↑ mail server domain name

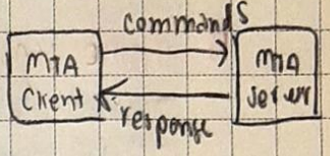
MTA : Message transfer agent

actual message transfer is done by MTA, used protocol SMTP (simple mail transfer protocol)

→ to send, use client MTA, to receive, use server MTA

→ Protocol Range





→ command example & response example

Command	
HELO	sender host's name
MAIL FROM	Sender of message
RCPT TO	intended recipient
DATA	body of the mail

Response	
220	Service ready
250	Request command completed
354	Start mail input
221	Closing transmission channel
554	Transaction failed

→ establishment

response	server → client	220
command	client → server	HELO
response	server → client	250

→ termination

S → C	QUIT
C → S	221

→ transfer

S → C	MAIL FROM
C → S	250
S → C	RCPT TO
C → S	250
S → C	DATA
C → S	354
S → C	-header part- and blank line
S → C	-body part- and single dot
C → S	250

MAA: Message access agent

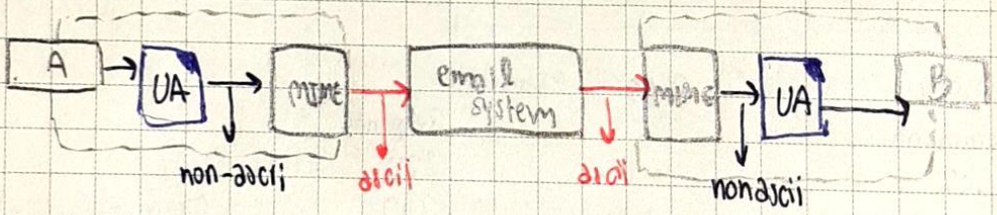
→ SMTP is push protocol in first stage and second stage.
→ need protocal to pull message in third stage of transmission [POP3 or IMAP4]
→ use MAA, to direct bulk data from server to client

→ POP3 Protocol call

C→S	username
S→C	OK
C→S	password
S→C	OK
C→S	list
S→C	email number & size
C→S	retreive 1
S→C	email 1
	⋮
C→S	retriere n
S→C	email n

MIME : Multipurpose Internet mail extension

→ current mail can send only simple structure, NVT 7-bits ascii format.
→ MIME allowed non-ascii data to be sent through by transform non-ascii to NVT ascii at sender site and transform back to original at receiving site



→ in header send info ex version, type/subtype, encoding type, content-id, content-description
→ Ex of type/subtype

Text → Plain
→ HTML

Multipart → Mixed (body contain ordered part of other type)
Parallel (—n— unordered ——— n ———)
Digest (similar to mixed : default is message/RFC 822)
Alternative (parts are different version of the same message)

Message → RFC 822
Partial
External Body

Image → GIF
→ JPEG

Video → MPEG

Audio → Basic

→ encoding type

7-bits → NVT ASCII and short line

8-bits → Non-ascii and short line

Binary → Non-ascii & unlimited line)

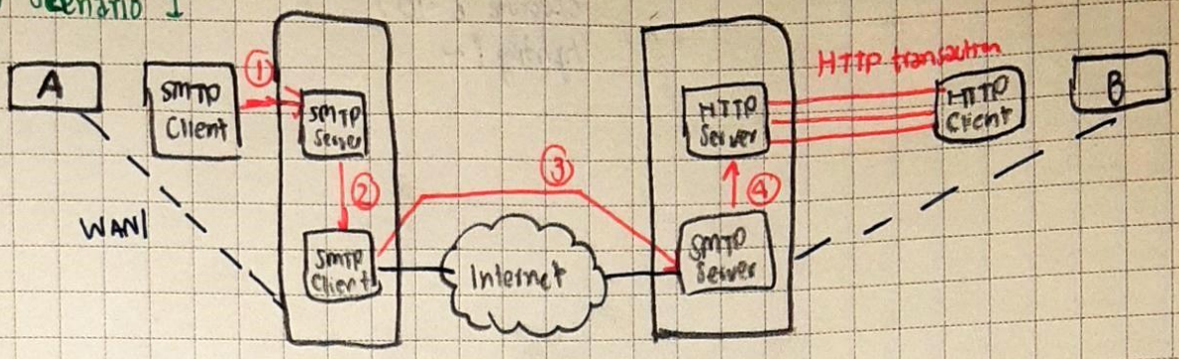
Quoted-printable → non-ascii encoded as equal sign with ascii code of that.
ex [9D] ⇒ [=|9|D]

Base-64 → 6-bit block of data to 8-bit ascii character
↳ A-Z, a-z, 0-9, +, / : 0-63

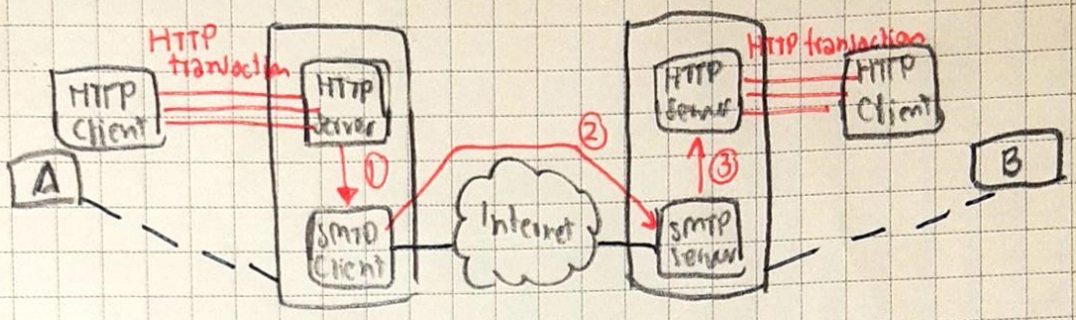
Web-based email common on website.

→ 2 cases

→ Scenario 1



→ Scenario 2.



Email Security

→ email exchanges can be secured by 2 application layer securities for email system

→ Protocol → PGP: Pretty Good Privacy
→ popular program to encrypt and decrypt email over the internet
→ authenticate message w/ digital signature and encrypt stored files

→ Secure MIME
• internet standard of digitally signing MIME based on email data and public key encryption