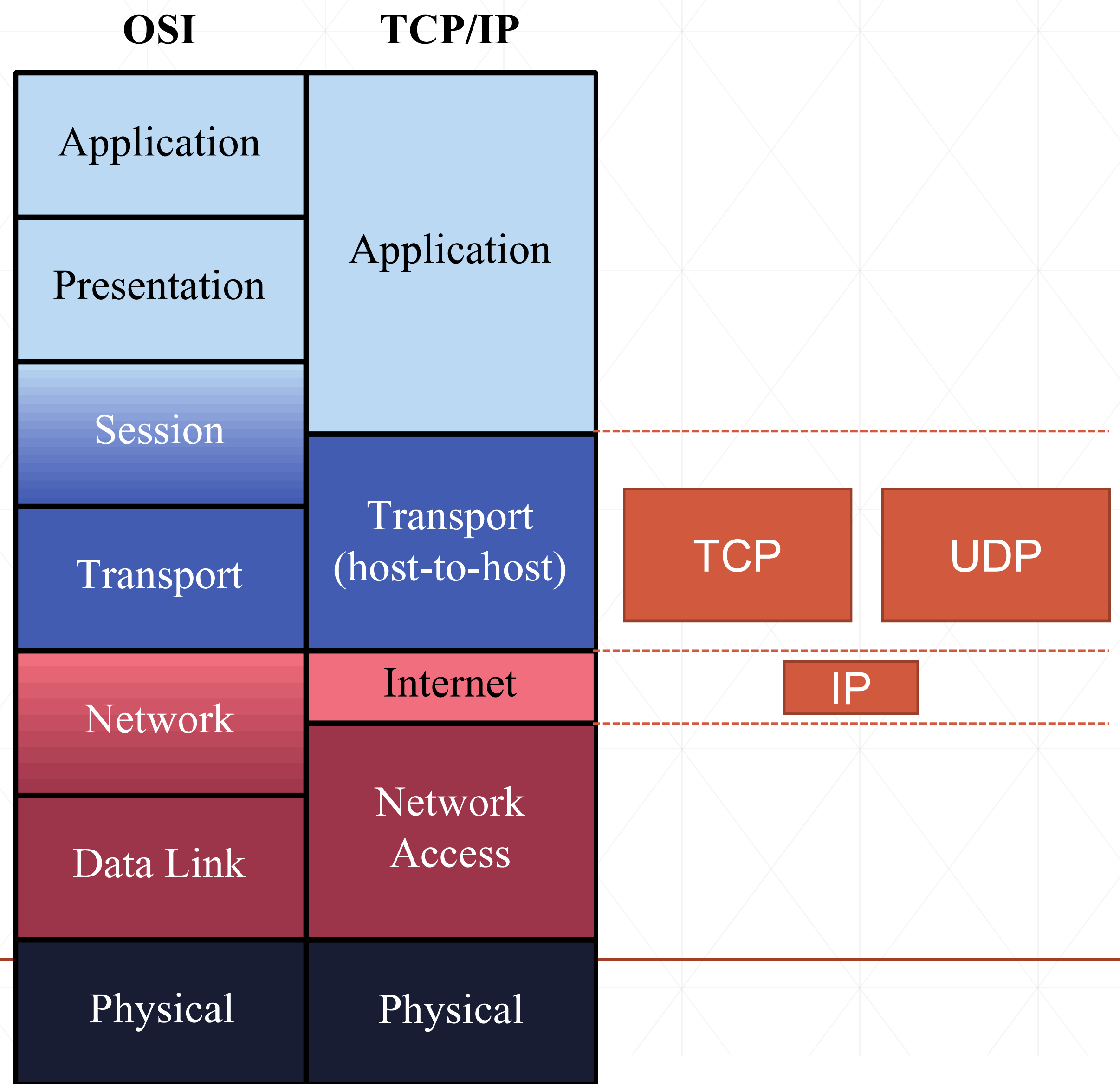
Fundamental concepts in communication :

TCP/IP Protocol Suit

TCP/IP and OSI



TCP End to End Protocol Layer

- Transport Control Protocol
  - Connection-oriented
    - Provides establishment, maintenance and termination of logical connection between end users/host
      - Establishment is initiated by originating end user by sending SYN segment and accepted/acknowledged by receiving end user (Three-way handshake)
      - Termination is made through FIN-ACK segment exchange between user
    - Imposes a reliable connection between users in packet switching network
      - Flow control to maintain the rate of the segment
        - The user of the receiving entity should be able to keep up with the flow of data
        - Include sequence number, acknowledgement number, and window in each segment
      - Congestion control
        - Deals with varying delay within network
  - End user/host identification
    - Port, and protocol

TCP End to End Protocol Layer

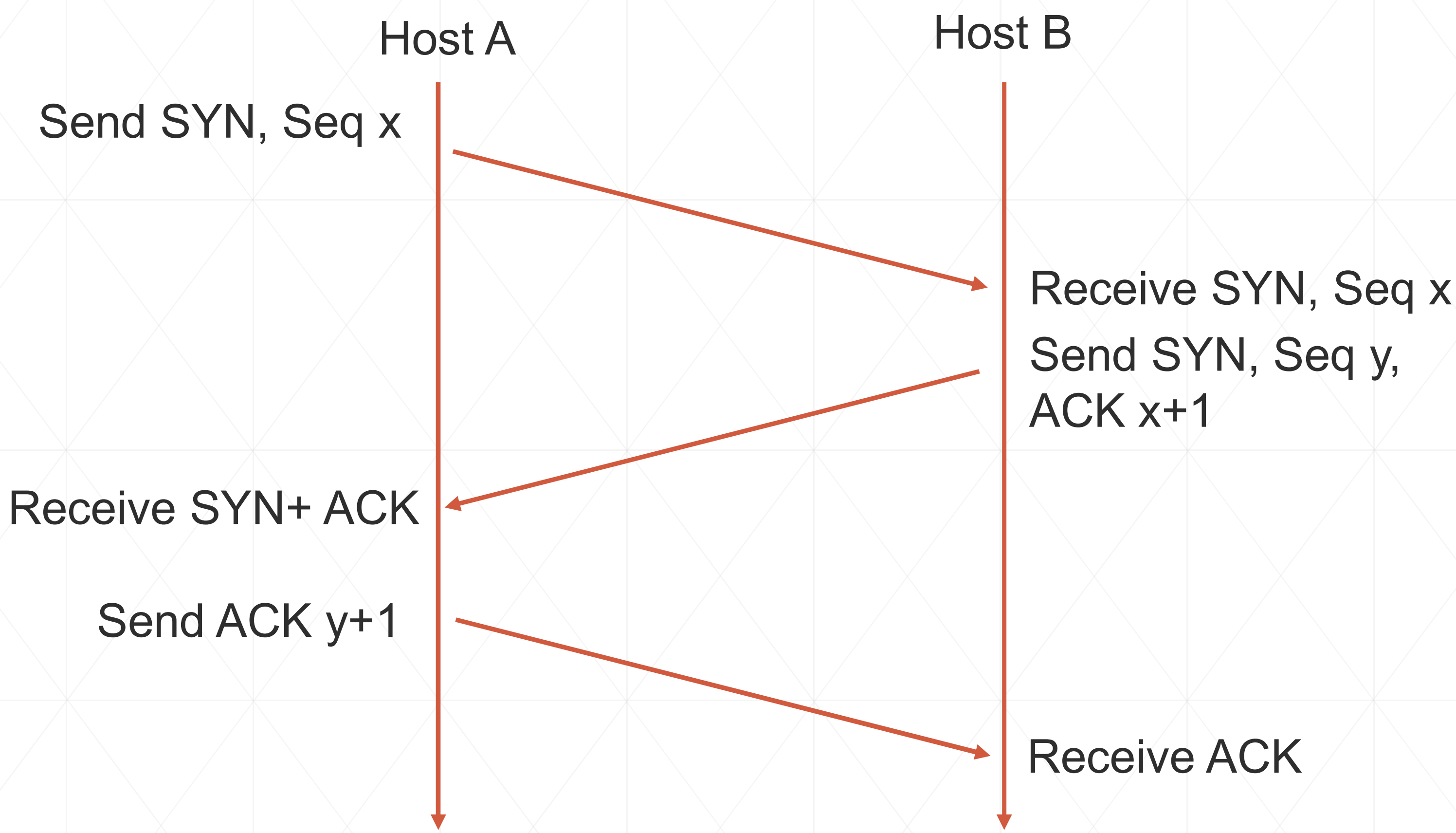
TCP Header

Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Source port																Destination port															
32	Sequence number																															
64	Acknowledgment number (if ACK set)																															
96	Data offset				Reserved				CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
128	Checksum																Urgent pointer (if URG set)															
160 ...	Options (if Data Offset > 5) ...																								padding							

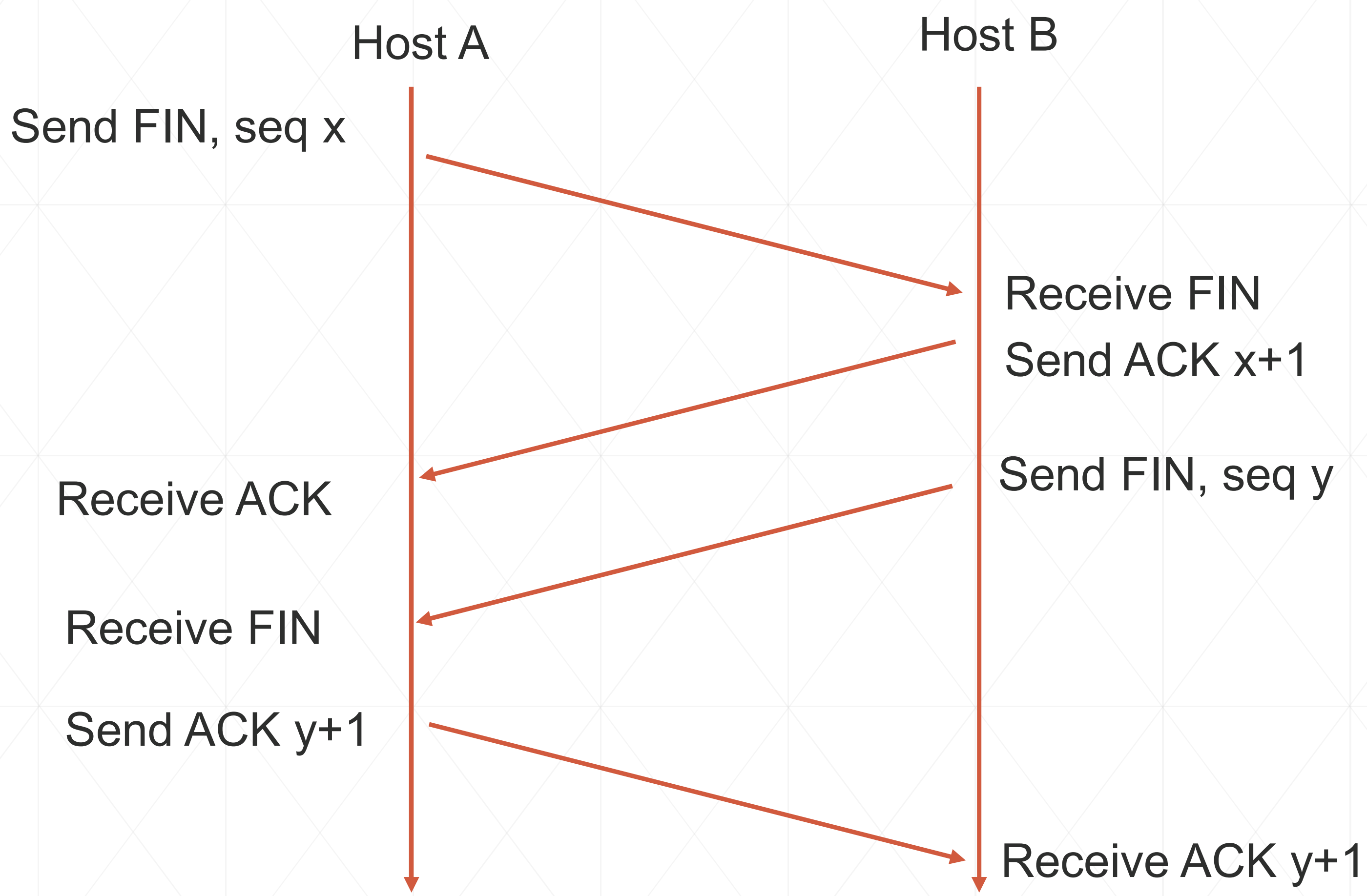
Source : https://caleudum.wordpress.com/2011/05/08/tcp-header-format/

Further explanations on the format can be found at "Data and Computer Communications, eight edition" William Stallings

TCP Connection Establishment



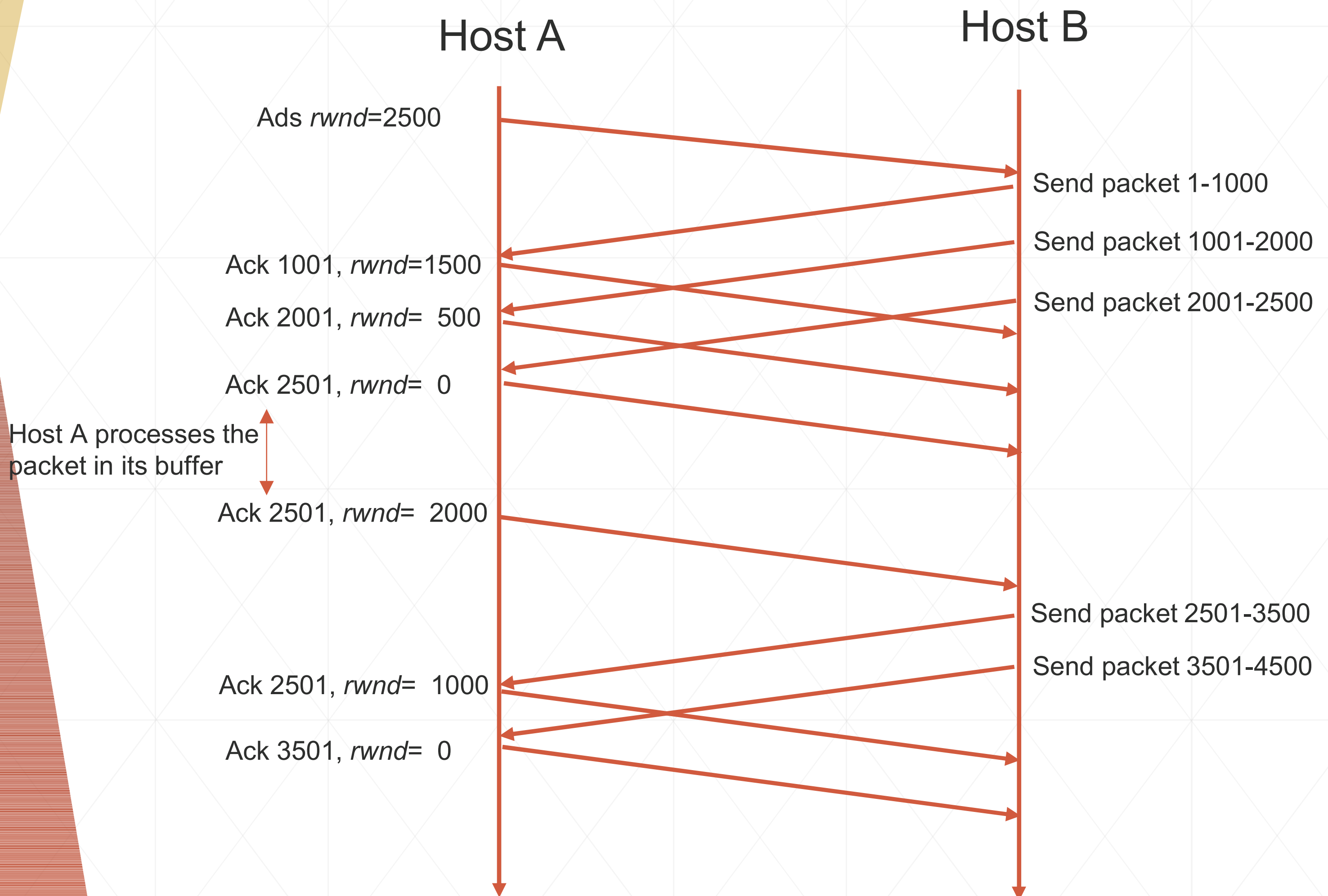
TCP Connection Termination



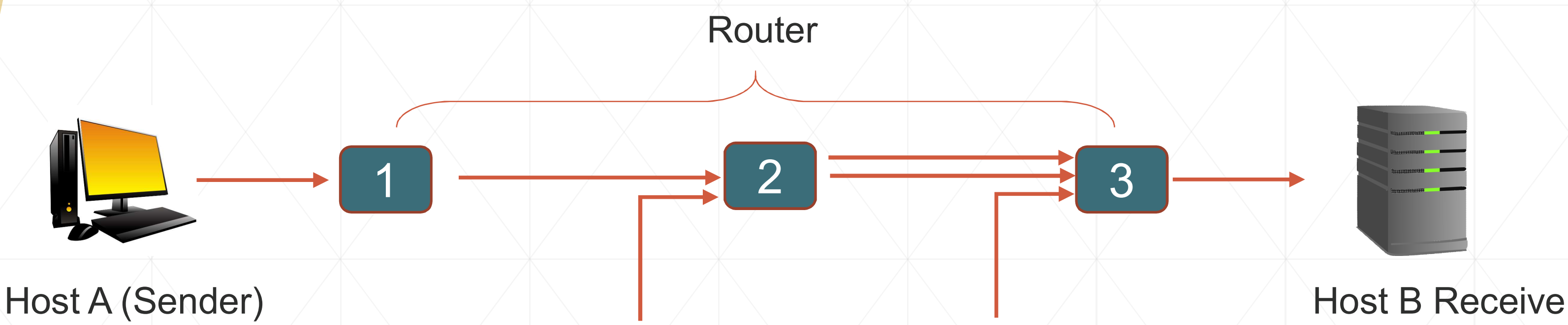
TCP Flow Control

- Flow control is implemented to prevent the sender flooding the receiver with packet
  - Receiver's buffer capacity and speed may not be the same as sender
  - It uses selective ARQ with positive acknowledge
  - Using sliding window with bytes basis as the unit
  - Receiver advertises the maximum receiving window, *rwnd*, to sender
    - The size of the windows changes dynamically, depending on the capability of receiver
- Sender can only send the remaining packet min(*cwnd,rwnd*), where *cwnd* is sender congestion window
- Example : (see following slide)
  - Suppose host B has 4500 bytes data to send, its *cwnd* is 4000 bytes.
  - Host B also knows that host A can only accept 2500 bytes from previous *rwnd* advertisement

TCP Flow Control : illustration

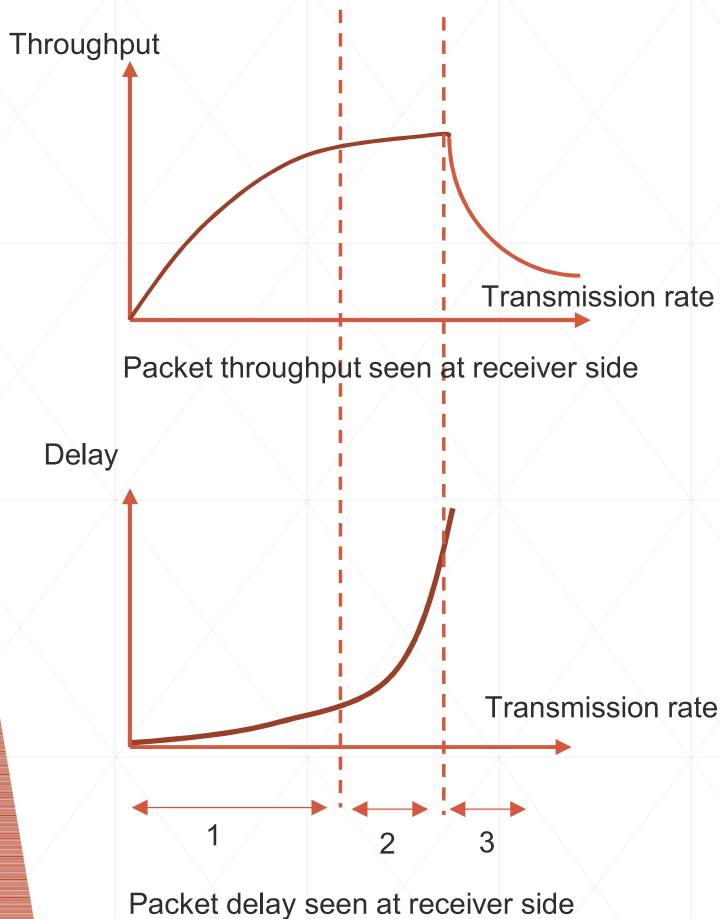


TCP Congestion Control



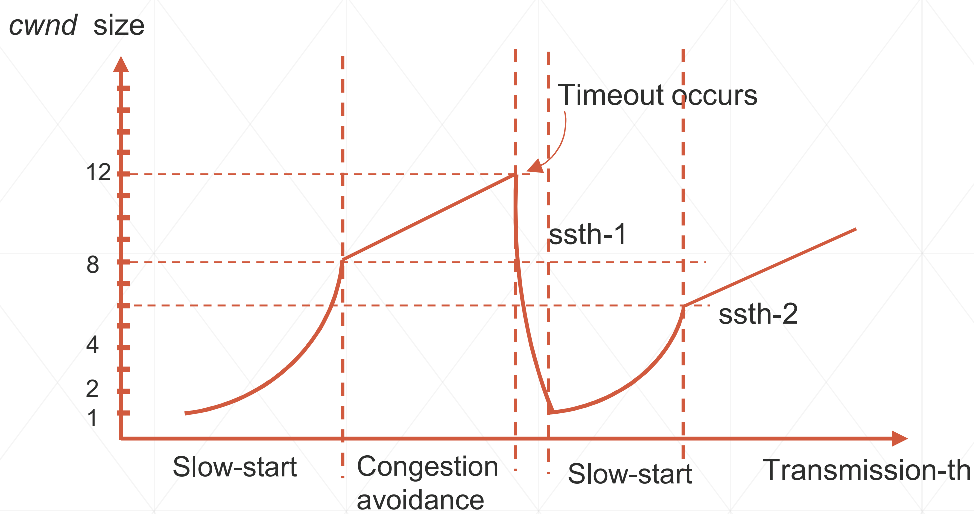
- To deal with varying delay due to network load
  - Flow control is implemented between host A and B.
    - No explicit flow control among router or between router and host
    - Host may not know explicitly the condition at router 1,2, and 3
      - In the picture above, link between router 2 and 3 may present bottleneck
  - Solution : Host A probe the network by observing the delay of the packet it transmit
    - Increased delay may indicate the network getting congested
      - Dynamically adjust the rate by adjusting the *cwnd.*

TCP Congestion Control



- (1) : Light traffic
  - The transmission rate < network bandwidth
  - Low delay
  - Can increase transmission rate without incurring excessive delay
- (2) : Knee (Congestion onset)
  - Transmission rate approaches network bandwidth
  - The increase of throughput starts to saturate.
  - Delay starts increasing rapidly
- (3) : Congestion
  - Throughput decrease rapidly as the transmission rate is increased
  - Large delay, packet loss

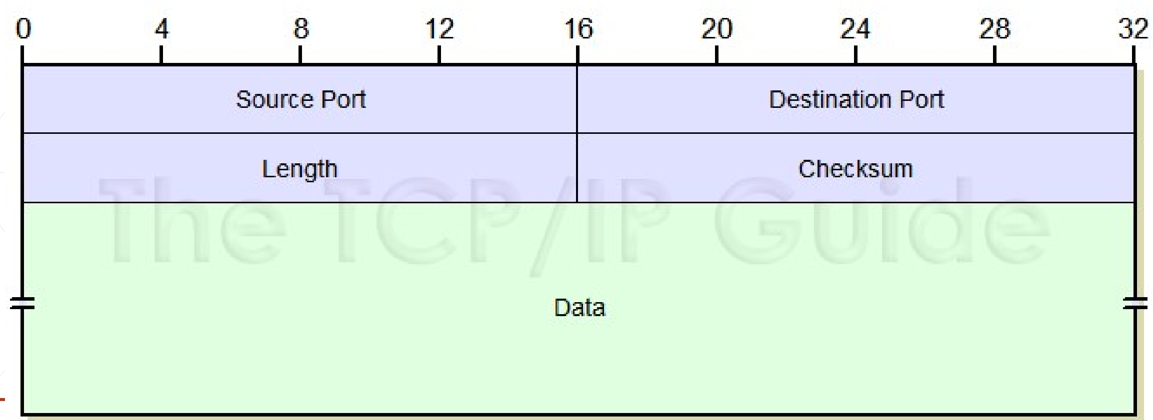
TCP Congestion Control: Adjusting cwnd



- Slow-start
  - Start sending segment with the lowest cwnd
  - Increase the cwnd exponentially as ACKs are received for corresponding transmitted segment.
  - The exponential increase would stop at threshold ssth-1
- Congestion avoidance
  - The cwnd is increased linearly as long as ACK packet is received after cwnd reach ssth-1
  - If timeout occurs, decrease cwnd to 1 and set a new threshold ssth-2 equals to half to ssth-1

TCP End to End Protocol Layer

- User Datagram Protocol
  - Simple
  - Connection-less : No logical connection setup performed
  - Unreliable
    - No segment acknowledgement is applied
  - Delivery and duplicate protection are not guaranteed
  - Fast and less overhead
  - UDP Segment header format

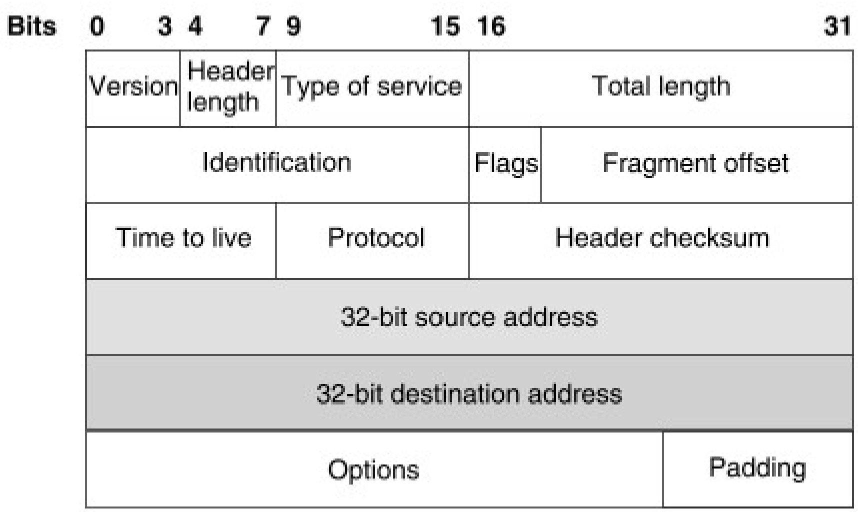


Internet Layer

- Addressing scheme
  - Need addresses that are *globally unique*
  - Accommodating diverse networks
- Routing algorithm
  - Needs to find the path in which the packet traverses
- Two version of internet layer
  - IPv4 and IPv6

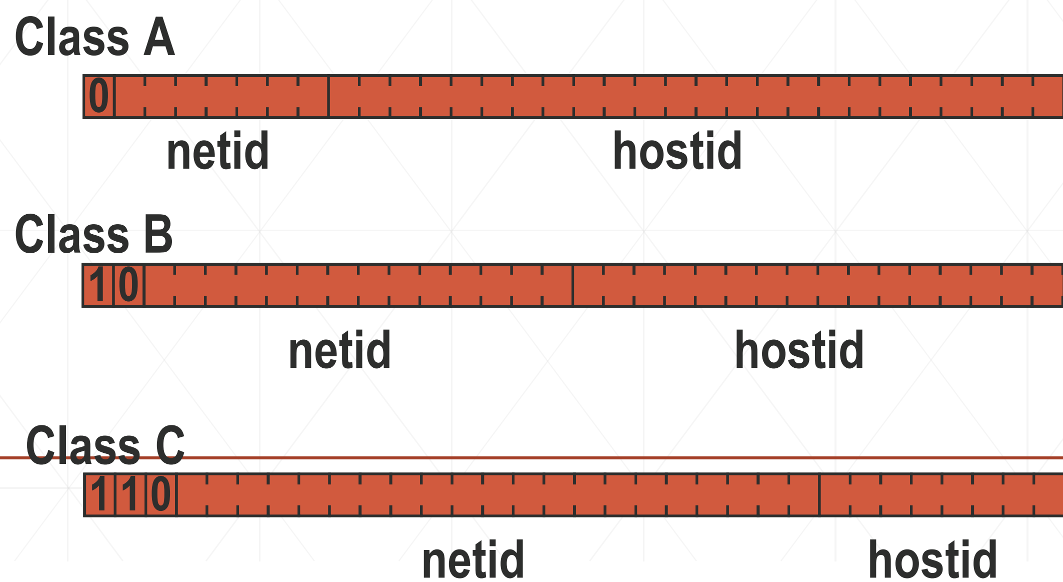
Internet Layer : IP Datagram Header Format

- Header Format (IPv4)
  - Size minimum 20 bytes
  - Addressing scheme uses 32 bits, generally consist of network identifier and host identifier
  - Managed using subnets and subnet mask



Internet Layer : IP Addresses

- In IPv4, the size of the address is 32 bits
  - Four groups of 8 bits. Theoretically can accommodate up to 2^{32} addresses
  - Use decimal equivalent to represent the address
- Initially, IP addresses were grouped in several classes, in order to alleviate the complexity of routing
  - An address consists of network ID and host ID part
  - Different class allocates different number of networks IDs and host IDs
    - Class A, Class B, Class C (These first-three are commonly used), Class D (Multicast) and Class E



Internet Layer : IP Addresses

- Problem with class system
  - Unavailability of address blocks of reasonable size
  - Explosive growth of routing tables
- Classless Inter-Domain Routing
  - Eliminates the classed IP address scheme
    - Address class is no longer uniquely identifiable from the address
    - Primary beneficiaries of CIDR addressing are medium-sized organizations
      - Too big for Class C (~250 hosts), too small for Class B (~65,000 hosts)
    - Host number can be arbitrary length
  - In routing table, the router stores the information of the length of bits for network ID (netID) part of an IP address (also called netmask)
    - Example : 73.5.0.0/17
      - Called a /17 network. So, the netmask has 17 bits length, which is in IP-style presentation would be: 11111111.11111111.10000000.00000000(255.255.128.0)
      - The remaining 15 bits identify the host
      - So, the network can have 215 = 32,768 computers

Internet Layer : IP Addresses

- Determine the network ID of following IP address
  - 172.16.17.30/20
  - 172.16.28.15/20

To obtain network ID, do AND logic operation IP address and netmask

```
172.16.17.30        10101100.00010000.00010001.00011110
255.255.240.0       11111111.11111111.11110000.00000000
Network         =   10101100.00010000.00010000.00000000   (AND operation)
                =    172.16.16.0

172.16.28.15        10101100.00010000.00011100.00001111
255.255.240.0       11111111.11111111.11110000.00000000
Network         =   10101100.00010000.00010000.00000000  (AND operation)
                =   172.16.16.0
```

They belong to the same network

Internet Layer : IP Addresses

- Special set of IP address
  - Local IP address
    - Used for private or local network, not routable from “outside”

Start Address	End Address
10.0.0.1	10.255.255.254
172.16.0.1	172.31.255.254
192.168.0.1	192.168.255.254

  - Broadcast IP address
    - Destined to every station in the network:
      example: 255.255.255.255
    - The scope may be localized/directed
      example: consider a local network with network ID: 192.168.1.0/24; then the broadcast address for this network would be the host ID part is set (in binary) all ones

Internet Layer : IP Addresses

- Subnetting
  - Allow us to create multiple logical networks that exist within a single address pool
    - Using subnet mask
  - Example:
    - Assume we would like 6 different network, with only 20 host each.
      - Request for six of 24 bit netmask, each of those can accommodate 256 addresses (unrealistic)
      - Get one address of 24 bit netmask, then split 256 host into 6 subnetworks
        - Since address split is done internally, internal router will perform routing task
        - Example : 202.168.5.0/24
          - Extended netmask into 27 bits internally 202.168.5.0/27

204.17.5.0	11001100.00010001.00000101.00000000
255.255.255.224	11111111.11111111.11111111.11100000

Internet Layer : IP Addresses

- Then we will have and extra 3 bits for network ID (actually, we are given 8 address space)
  - Possible assignment:
    - Sub network Address : 204.17.5.0 , host address range 1 to 30
    - Sub network Address : 204.17.5.32, host address range 33 to 62
    - Sub network Address : 204.17.5.64, host address range 65 to 94
    - Sub network Address : 204.17.5.96, host address range 97 to 126
    - Sub network Address : 204.17.5.128, host address range 129 to158
- However, in some cases, it is still not efficient

Internet Layer : IP Address Assignment

- Static
  - Assigned and configured at startup, usually permanently dedicated to a device
- Dynamic
  - IP Addresses are "leased" from a pool
  - Use Dynamic Host Configuration Protocol (DHCP)
    - New Host broadcasts a *Discover* message via UDP to Port 67
      - Destination address: 255.255.255.255
      - Source address: 0.0.0.0
    - DHCP server responds with an *Offer* message
      - Transaction ID of *Discover*
      - Proposed IP address
      - Network mask
      - IP address lease time
    - New Host responds with an *DHCP Request*
      - Mirrors information in *Offer*
      - Goes to selected DHCP server in the case of multiple servers
    - Server responds with a *DHCP ACK*
      - Confirms parameters
      - Initiates lease

Internet Layer : IP Addresses

- IPv4 is now replaced with IPv6
  - Address allocation in IPv4 exhausted
  - Enhancement IPv6 over IPv4
    - Expanded address space : using 128 bit address. This allows the use of 6×10^{23} addresses in 1 meter square of earth surface
    - Improved option mechanism
    - Address auto-configuration
    - Increased addressing flexibility : any-cast addressing and multi-cast routing
    - Support for resource allocation
  - IPv6 basic header has fixed size of 40 bytes plus optional extension header