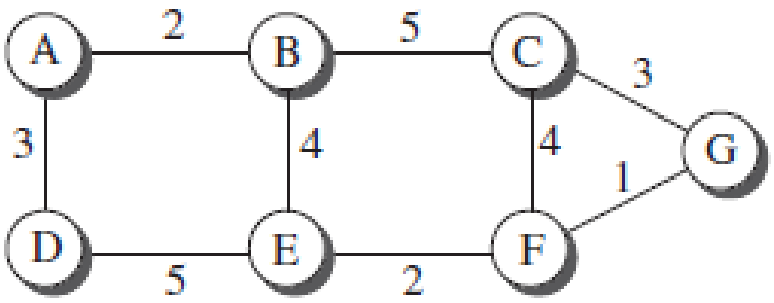
Q 1) Explain formation of least cost tree for the given graph using Dijkstra's algorithm

ANS:



a. The weighted graph

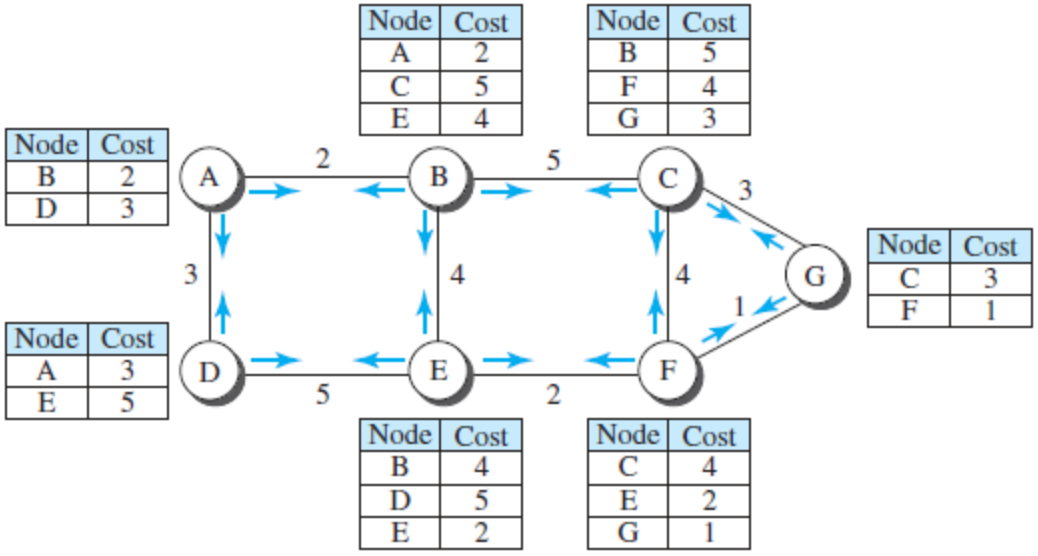
	A	B	C	D	E	F	G
A	0	2	∞	3	∞	∞	∞
B	2	0	5	∞	4	∞	∞
C	∞	5	0	∞	∞	4	3
D	3	∞	∞	0	5	∞	∞
E	∞	4	∞	5	0	2	∞
F	∞	∞	4	∞	2	0	1
G	∞	∞	3	∞	∞	1	0

b. Link state database

Link-State Database (LSDB)

To create a least-cost tree with this method, each node needs to have a complete *map of* the network, which means it needs to know the state of each link. The collection of states for all links is called the ***link-state database (LSDB).*** Each node can create this LSDB that contains information about the whole internet. This can be done by a process called **flooding. Each node can** send some greeting messages to all its immediate neighbors (those nodes to which it is connected directly) to collect two pieces of information for each neighboring node: the identity of the node and the cost of the link. The combination of these two pieces of information is called the *LS packet (LSP);*

When a node receives an LSP from one of its interfaces, it compares the LSP with the copy it may already have. If the newly arrived LSP is older than the one it has (found by checking the sequence number), it discards the LSP. If it is newer or the first one received, the node discards the old LSP (if there is one) and keeps the received one. It



Formation of Least-Cost Trees

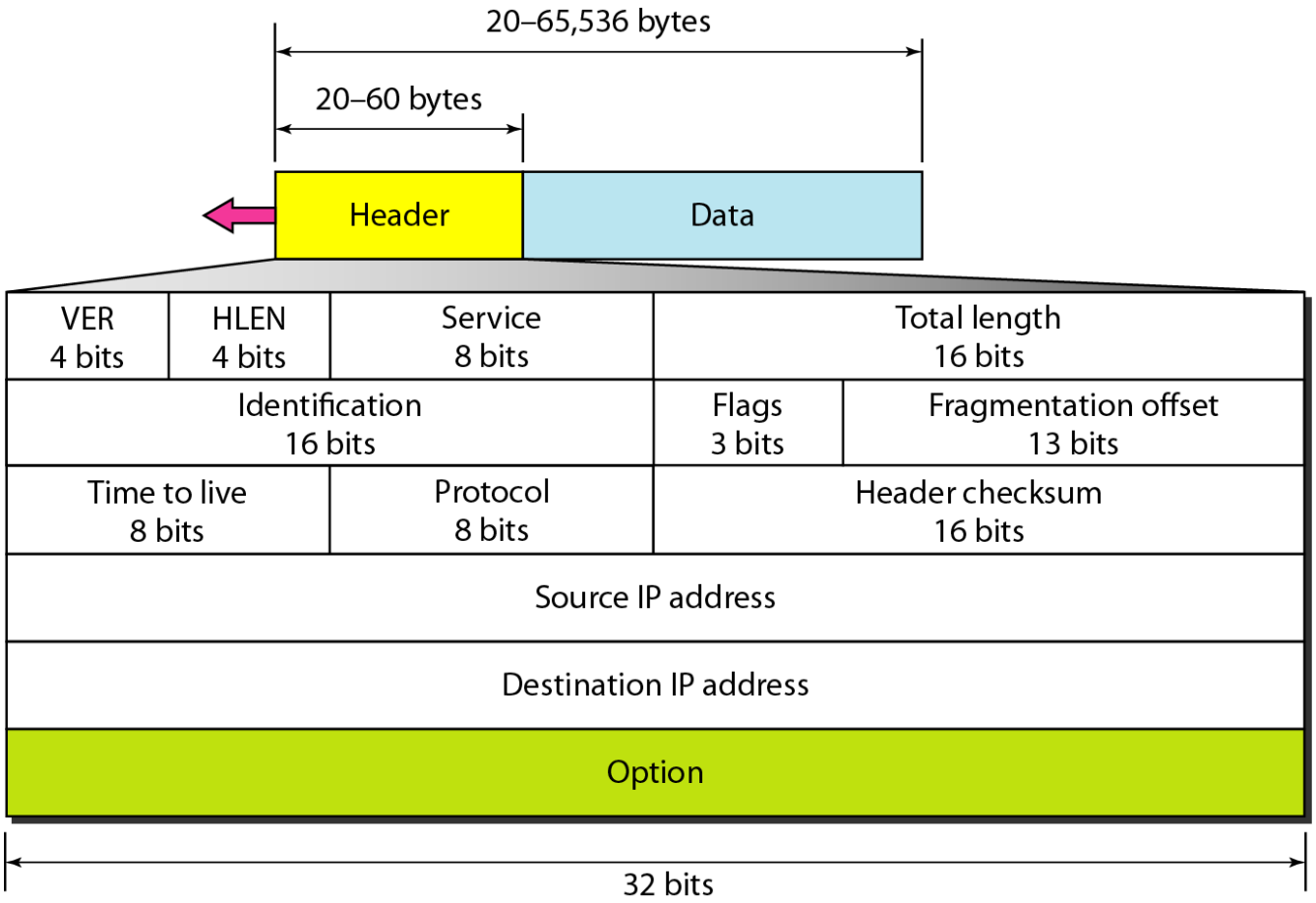
To create a least-cost tree for itself, using the shared LSDB, each node needs to run the **Dijkstra Algorithm. This iterative algorithm uses the following steps:**

1. The node chooses itself as the root of the tree, creating a tree with a single node, and sets the total cost of each node based on the information in the LSDB.

2. The node selects one node, among all nodes not in the tree, which is closest to the root, and adds this to the tree. After this node is added to the tree, the cost of all other nodes not in the tree needs to be updated because the paths may have been changed.

3. The node repeats step 2 until all nodes are added to the tree.

Q2 a) Explain IPv4 datagram format with neat figure.



Version (VER). This 4-bit field defines the version of the IPv4 protocol.
Currently the version is 4.

Header length (HLEN). This 4-bit field defines the total length of the Datagram header

in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes). i.e. minimum 20 bytes and maximum 60 bytes.

Services. This field, previously called service type, is now called differentiated services.
The total length field defines the total length of the datagram including the header.

Identification,Flags, Fragmentation offset.- used in fragmentation

Time to live: A datagram has a limited lifetime in its travel through an internet. This field was originally designed to hold a timestamp (It records the time of datagram processing by the router, expressed in milliseconds) and it is decremented by each visited router. The datagram was discarded when the value became zero

This value is approximately two or more times the maximum number of routes between two hosts.

Protocol. This is an 8-bit field. The higher-level protocol such as TCP, UDP, ICMP, and IGMP uses the services of the IPv4 layer. This field specifies the final destination protocol to which the IPv4 datagram is delivered

Checksum: When a data packet travels on the network then it can be corrupted in way, hence a value called checksum is added to the Header and it is transmitted along with message.

At the destination side, the checksum is re-calculated and crosschecked with the existing checksum value in header to see if the data packet is OK or not. If it matches then datagram is accepted and if not then it is discarded

Calculation of checksum:

- Divide the IP header is 16 bit words and sum each of them up

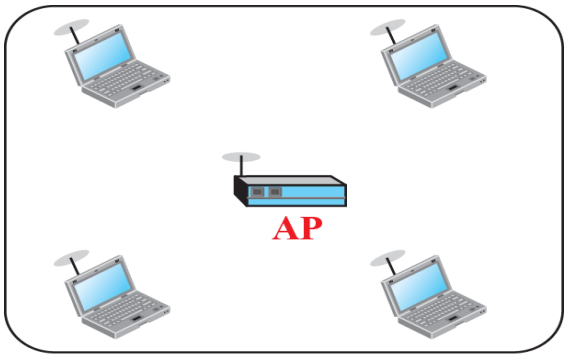
- Do one's compliment of the sum then the value generated is called as the checksum and inserted in checksum field.

Source address. This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

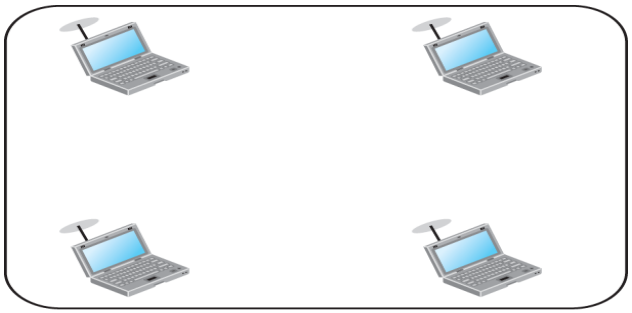
Destination address. This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

Q2 b) Explain about basic service set and extended service set with neat figures.

Basic service sets (BSSs)



Infrastructure BSS


Ad hoc BSS

Infrastructure BSS

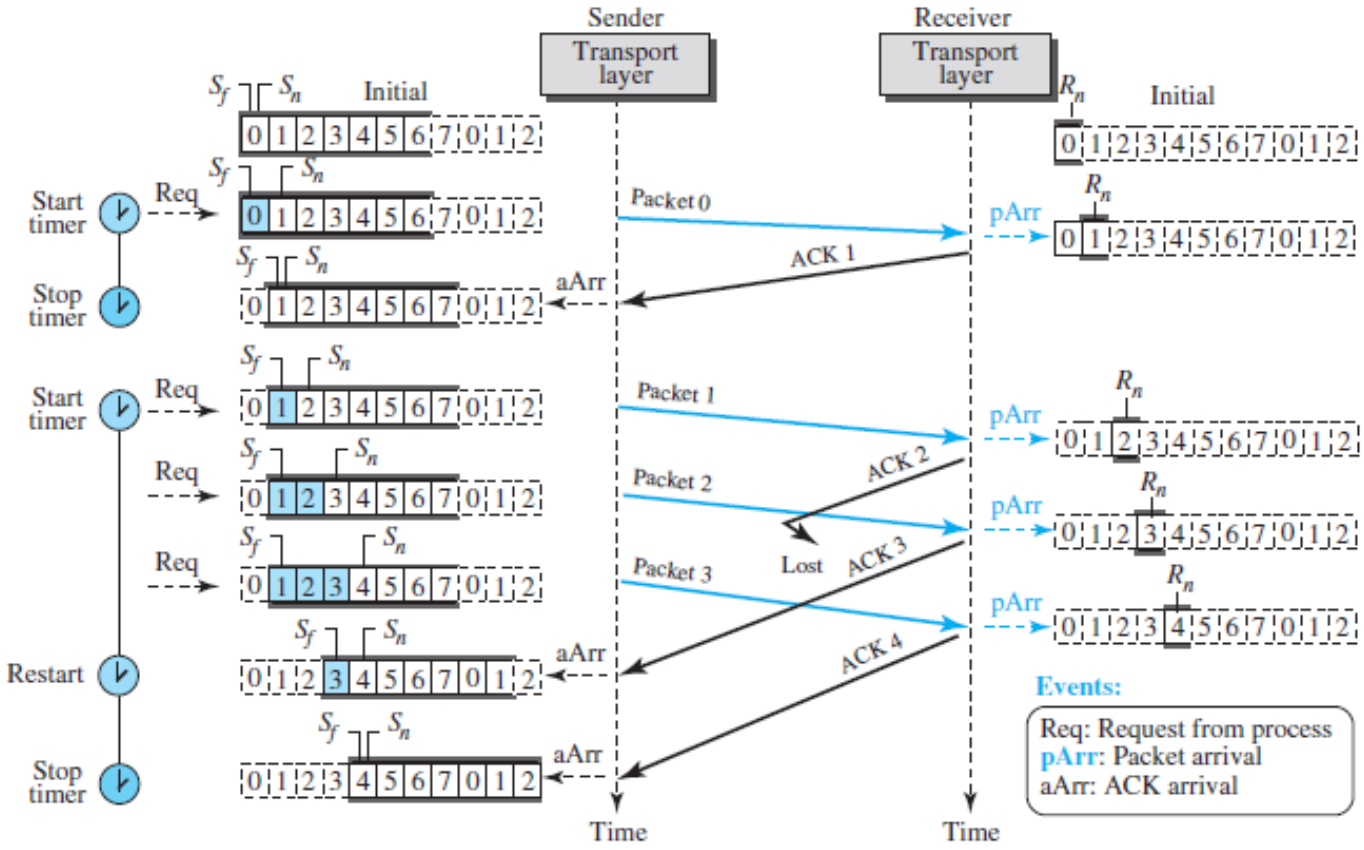
- A BSS with an AP is sometimes referred to as an infrastructure BSS.
- Nodes communicates and form network using Access Point (AP)

Ad hoc architecture

- In this architecture, nodes communicates without using AP;
- It is a stand-alone network and cannot send data to other BSSs.
- Nodes can be stationary or mobile.

Q 3 a) Explain Go back N protocol with neat diagrams of send and receive window.

Ans : The key to Go-back-*N is that we can* send several packets before receiving acknowledgments, but the receiver can only buffer one packet. We keep a copy of the sent packets until the acknowledgments arrive.


Sender
Transport layer
Receiver
Transport layer
Initial
Start timer
Req
Stop timer
Packet 0
ACK 1
pArr
aArr
Packet 1
ACK 2
Packet 2
Lost
ACK 3
Packet 3
ACK 4
Restart
Events:
Req: Request from process
pArr: Packet arrival
aArr: ACK arrival
Time
Time

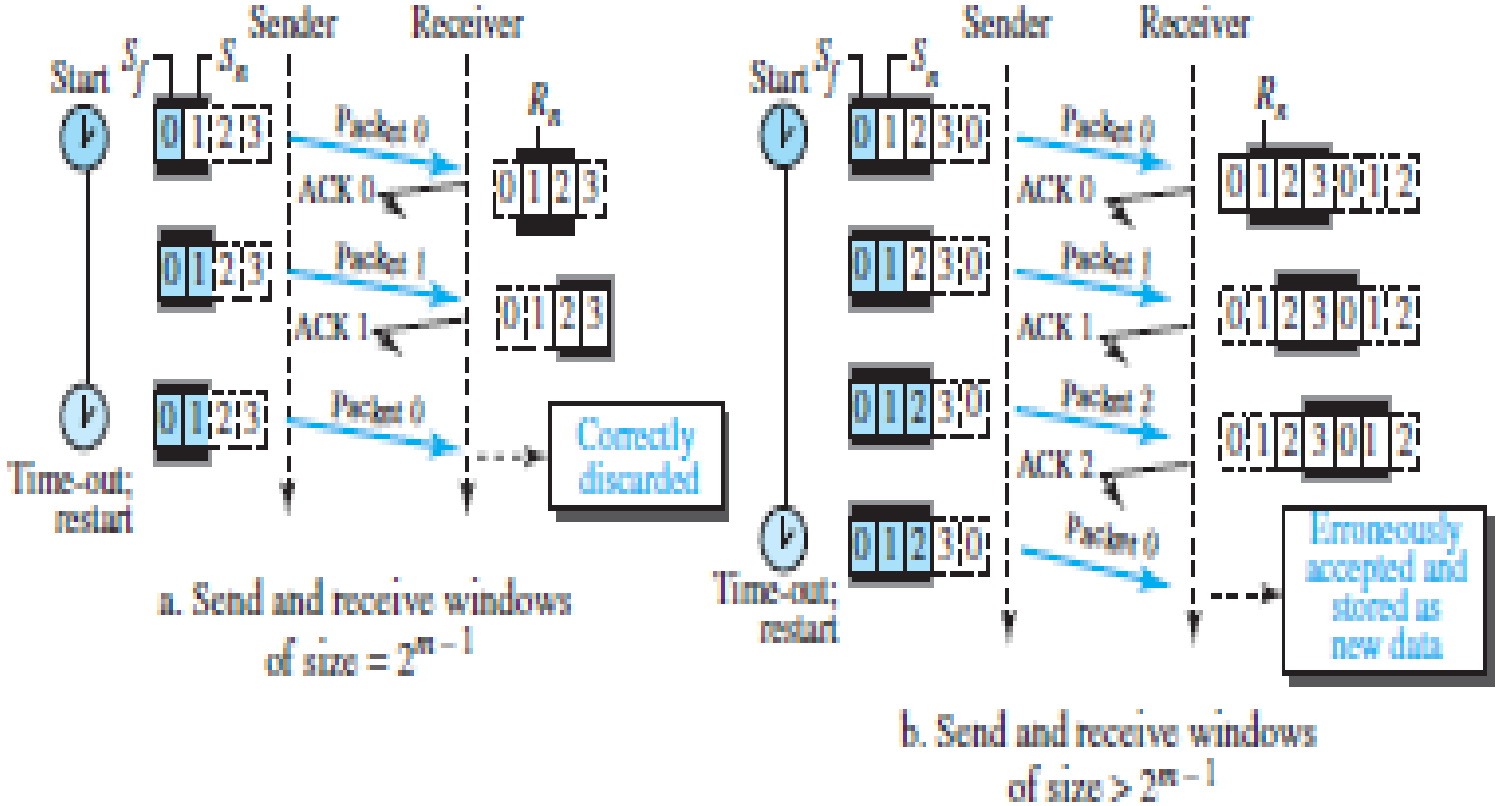
Send Window

The send window is an imaginary box covering the sequence numbers of the data packets that can be in transit or can be sent. In each window position, some of these sequence numbers define the packets that have been sent; others define those that can be sent. The maximum size of the window is $2^m - 1$.

Receive Window

The receive window makes sure that the correct data packets are received and that the correct acknowledgments are sent. In Go-Back-*N*, *the size of the receive window is* always 1. The receiver is always looking for the arrival of a specific packet. Any packet arriving out of order is discarded and needs to be resent

Q3) b Explain why the size of send window and receive window of selective repeat protocol should be less then 2^m/2.



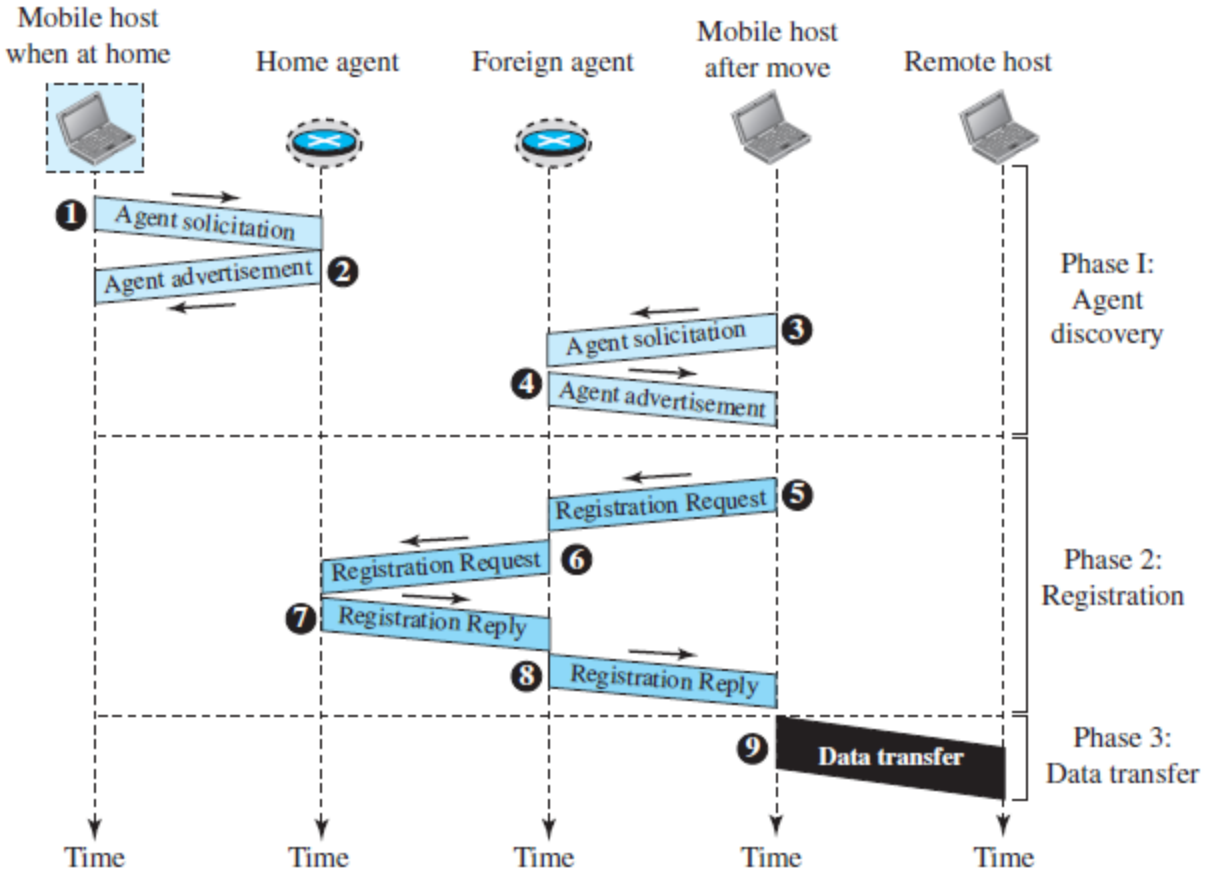
Consider two cases as shown in the figure

Case 1)
let the window size = 2m/2 =2. with a window size of 3.
Let all the packets are send but all acknowledgments are lost, now as the new timer starts the protocol will start resending from the packet 0. But, the window of the receiver is now expecting packet 2, not packet 0, so this duplicate packet is correctly discarded (as the sequence number is not matching).

Case 2)
When the size of the window is 3 and all acknowledgments are lost, the sender sends a duplicate of packet 0. However, this time, the window of the receiver expects to receive packet 0 of next new cycle (0 is part of the window) and protocol resends the packet 0 of previous cycle, so the receiver will accepts the packet 0 of previous cycle as first packet of next cycle, which is clearly an error.

Q 4) Explain three phases of Remote host and Mobile host communication.

Ans: Three phases



The first phase, agent discovery, involves the mobile host, the foreign agent, and the home agent. The second phase, registration, also involves the mobile host and the two agents. Finally, in the third phase, the remote host is also involved. We discuss each phase separately.

Agent Discovery

The first phase in mobile communication, *agent discovery, consists of two subphases*. A mobile host must discover (learn the address of) a home agent before it leaves its home network. A mobile host must also discover a foreign agent after it has moved to a foreign network. This discovery consists of learning the care-of address as well as the foreign agent's address. The discovery involves two types of messages: advertisement and solicitation.

Agent Advertisement

When a router advertises its presence on a network using an ICMP router advertisement,
it can append an *agent advertisement to the packet if it acts as an agent*

Agent Solicitation

When a mobile host has moved to a new network and has not received agent advertisements, it can initiate an *agent solicitation*. *It can use the ICMP solicitation message to* inform an agent that it needs assistance.

Registration

The second phase in mobile communication is *registration*. *After a mobile host has* moved to a foreign network and discovered the foreign agent, it must register. There are four aspects of registration:

1. The mobile host must register itself with the foreign agent.

2. The mobile host must register itself with its home agent. This is normally done by the foreign agent on behalf of the mobile host.

3. The mobile host must renew registration if it has expired.

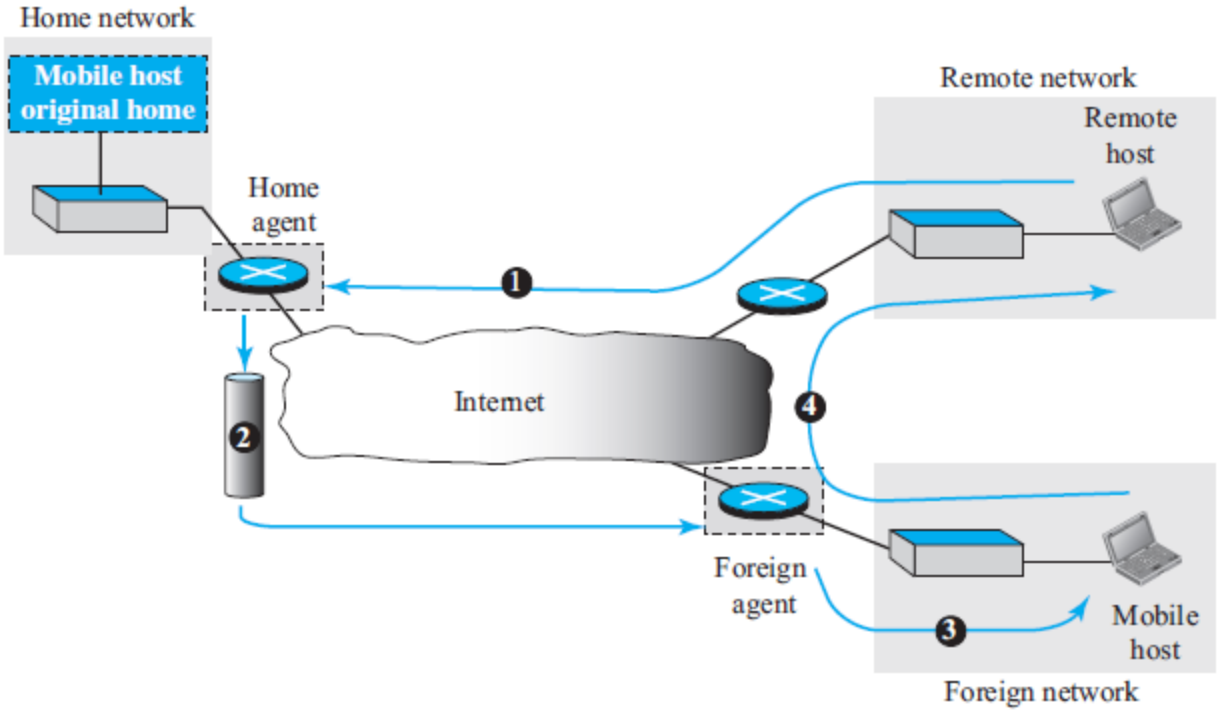
4. The mobile host must cancel its registration (deregistration) when it returns home.

Registration Request ***A registration request is sent from the mobile host to the foreign*** agent to register its care-of address and also to announce its home address and home agent address. The foreign agent, after receiving and registering the request, relays the message to the home agent. Note that the home agent now knows the address of the foreign agent because the IP packet that is used for relaying has the IP address of the foreign agent as the source address.

Registration Reply ***A registration reply is sent from the home agent to the foreign*** agent and then relayed to the mobile host. The reply confirms or denies the registration request.

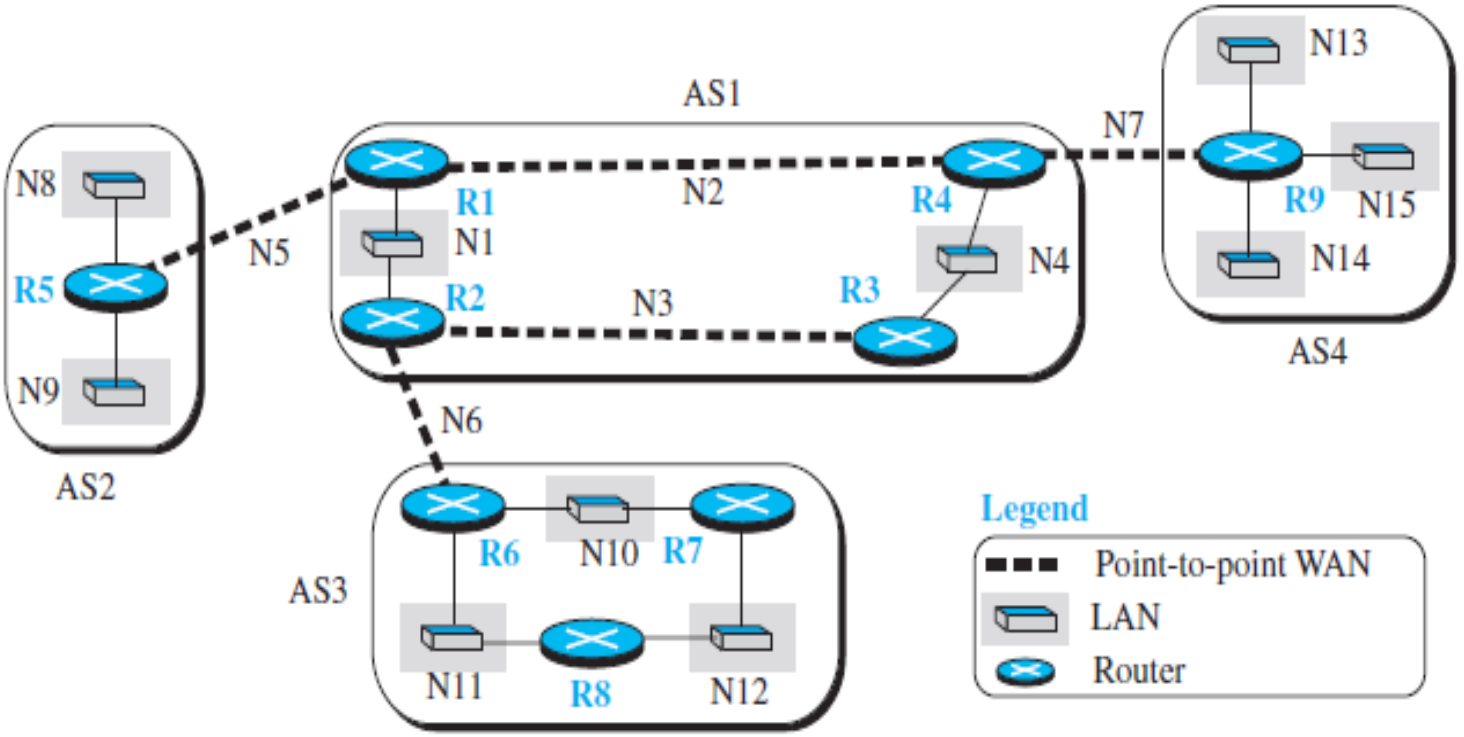
Data Transfer

After agent discovery and registration, a mobile host can communicate with a remote host.



Q 5) Explain the operation of External and Internal Border Gateway Protocol

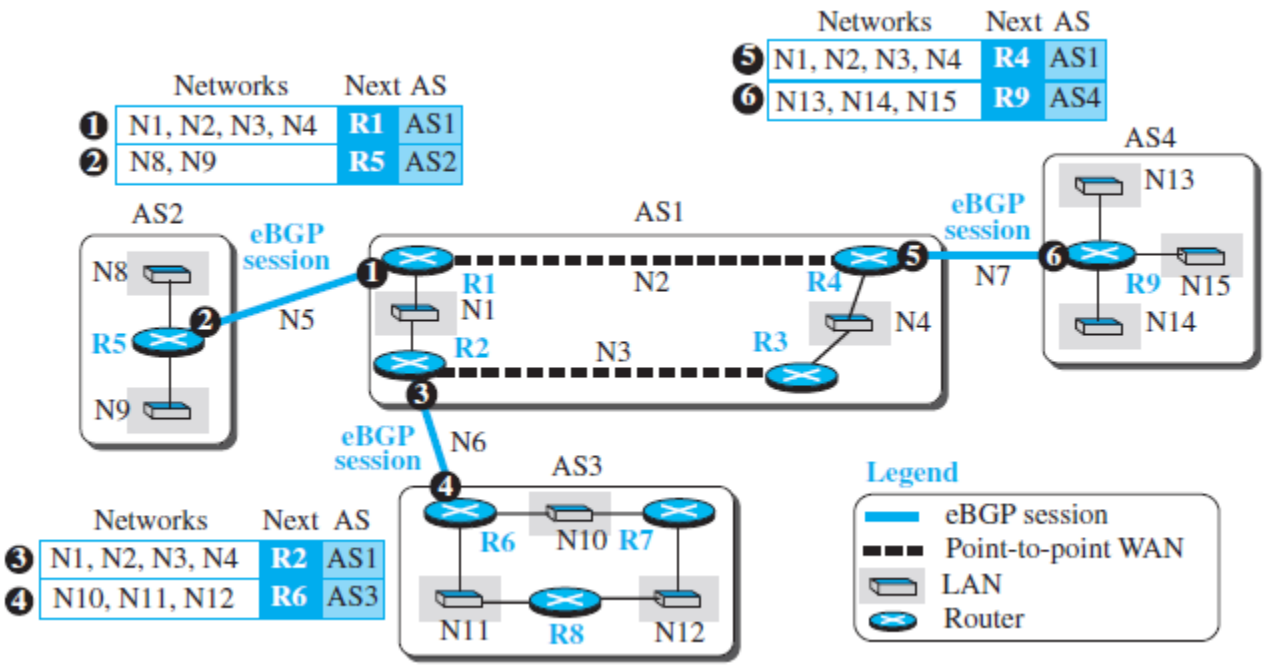
ANS: The **Border Gateway Protocol version 4 (BGP4) is the only interdomain routing protocol** used in the Internet today. BGP4 is based on the path-vector algorithm



To enable each router to route a packet to any network in the internet, BGP4, called *external BGP (eBGP) is installed on each border router.* Then install the second variation of BGP, called *internal BGP (iBGP), on all routers. This* means that the border routers will be running three routing protocols (intradomain, eBGP, and iBGP), but other routers are running two protocols (intradomain and iBGP).

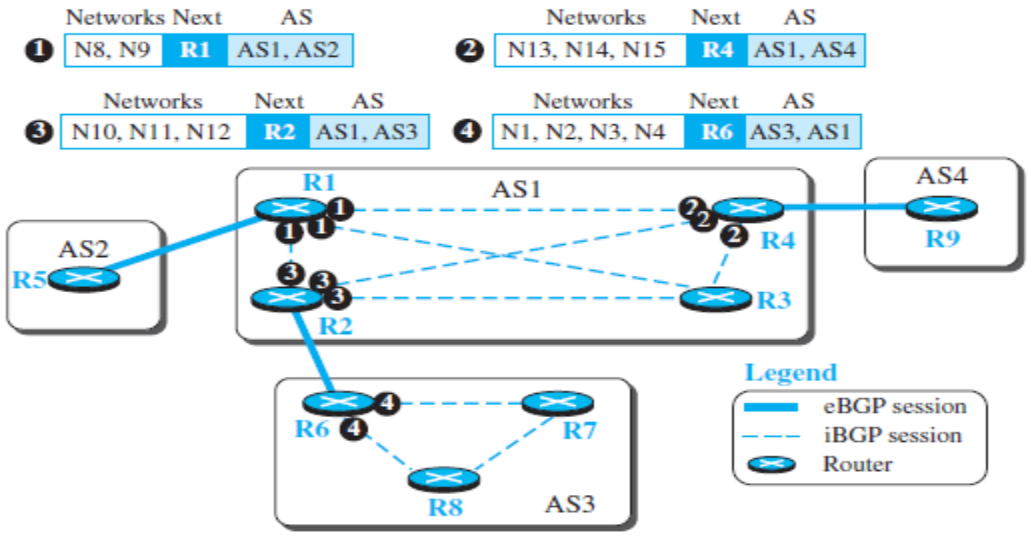
Operation of External BGP (eBGP)

The eBGP variation of BGP allows two physically connected border routers in two different ASs to form pairs of eBGP speakers and exchange messages. The routers that are eligible are in pairs as R1-R5, R2-R6, and R4-R9.



Operation of Internal BGP (iBGP)

Some border routers do not know how to route a packet destined for nonneighbor ASs. For example, R5 does not know how to route packets destined for networks in AS3 and AS4. Routers R6 and R9 are in the same situation as R5: R6 does not know about networks in AS2 and AS4; R9 does not know about networks in AS2 and AS3. Moreover **None of the nonborder routers know how to route a packet destined for any networks** in other ASs. Hence iBGP are used.



The first message (numbered 1) is sent by R1 announcing that networks N8 and N9 are reachable through the path AS1-AS2, but the next router is R1. This message is sent, through separate sessions, to R2, R3, and R4. Routers R2, R4, and R6 do the same thing but send different messages to different destinations. The interesting point is that, at this stage, R3, R7, and R8 create sessions with their peers, but they actually have no message to send.

bout the Bluetooth and also the two ed by Bluetooth.

- Bluetooth is a wireless LAN technology designed to connect devices of different functions when they are at a short distance from each other.

- A Bluetooth LAN is an ad hoc network.

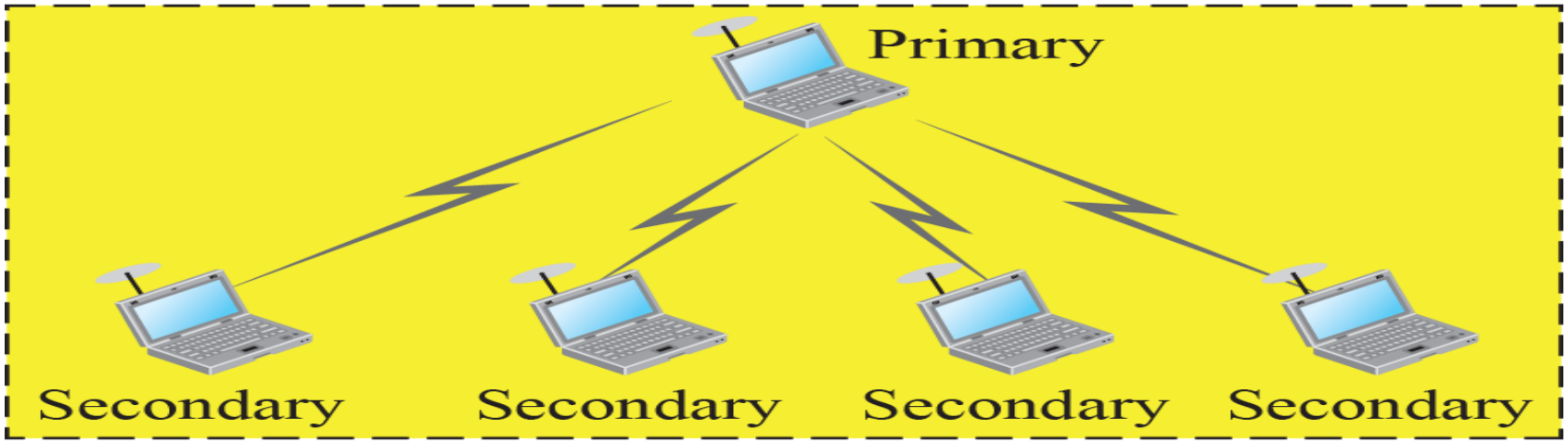
- The devices, sometimes called gadgets, find each other and make a network called a piconet.

Bluetooth Architecture

Bluetooth defines two types of networks:

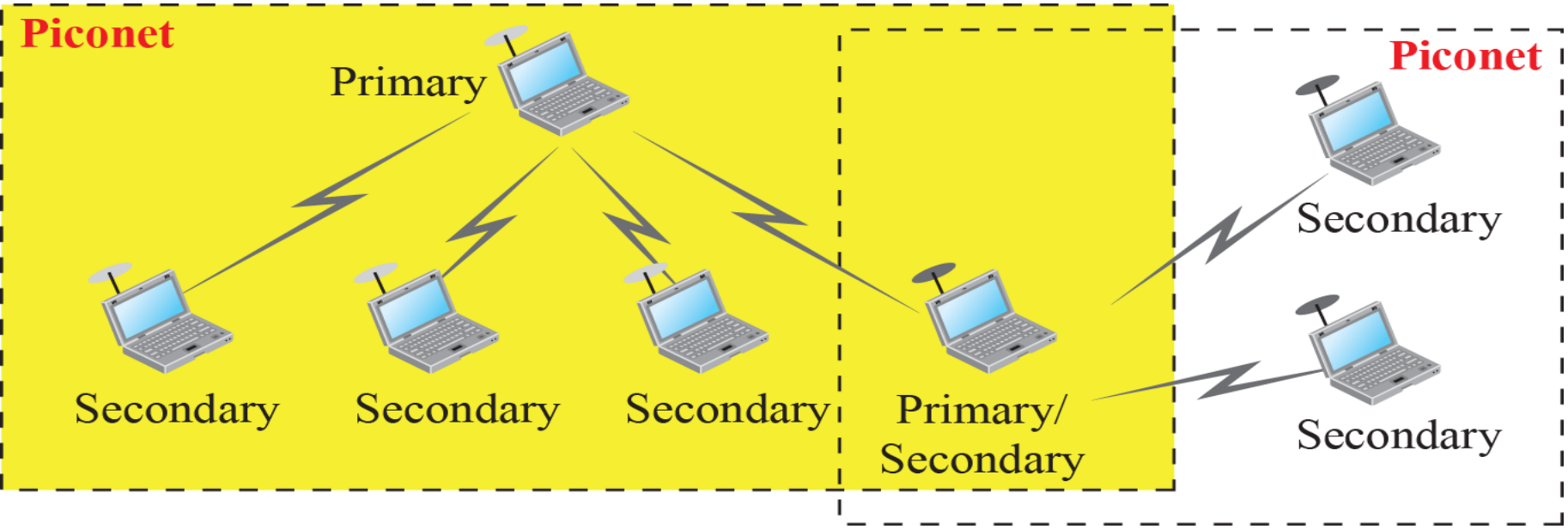
- Piconet
- Scatternet.

Piconet



- In a piconet there are maximum eight stations, one is called as the primary and the rest are called secondaries.
- There can be maximum 7 secondaries and all the secondary stations must synchronize their clocks and hopping sequence with the primary.
- The communication between the primary and secondary stations can be one-to-one or one-to-many.
- Although a piconet can have a maximum of seven secondaries and if some secondary is in parked state then they can't participate in communication untill moved from parked state to the active state.

Scatternet



- Many piconets combines to form a scatternet.
- A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.
- A station can be a member of two piconets.

Q)6 b Explain the UDP Services and TCP services

1.Process-to-Process Communication

UDP provides process-to-process communication using **socket addresses, a combination** of IP addresses and port numbers.

2. Connectionless Services

As mentioned previously, UDP provides a ***connectionless service.*** *This means that each* user datagram sent by UDP is an independent datagram.

3. Flow Control

In UDP there is **no *flow control*,** *and hence no window mechanism*

4. Error Control

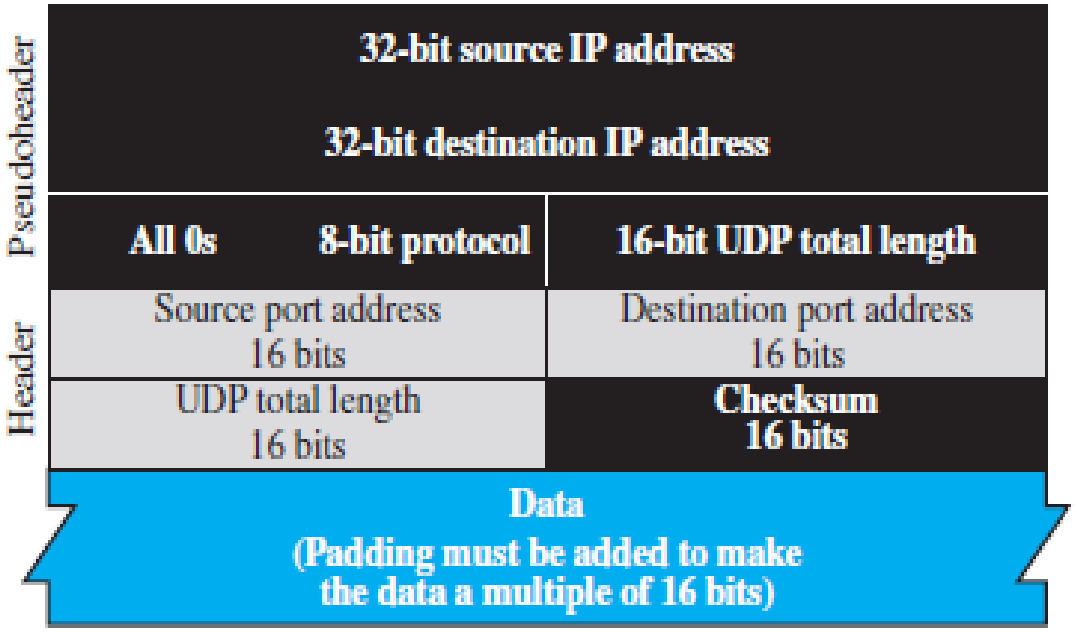
There is **no *error control mechanism*** *in UDP except for the checksum. This means that* the sender does not know if a message has been lost or duplicated. The receiver detects an error through the checksum.

Checksum

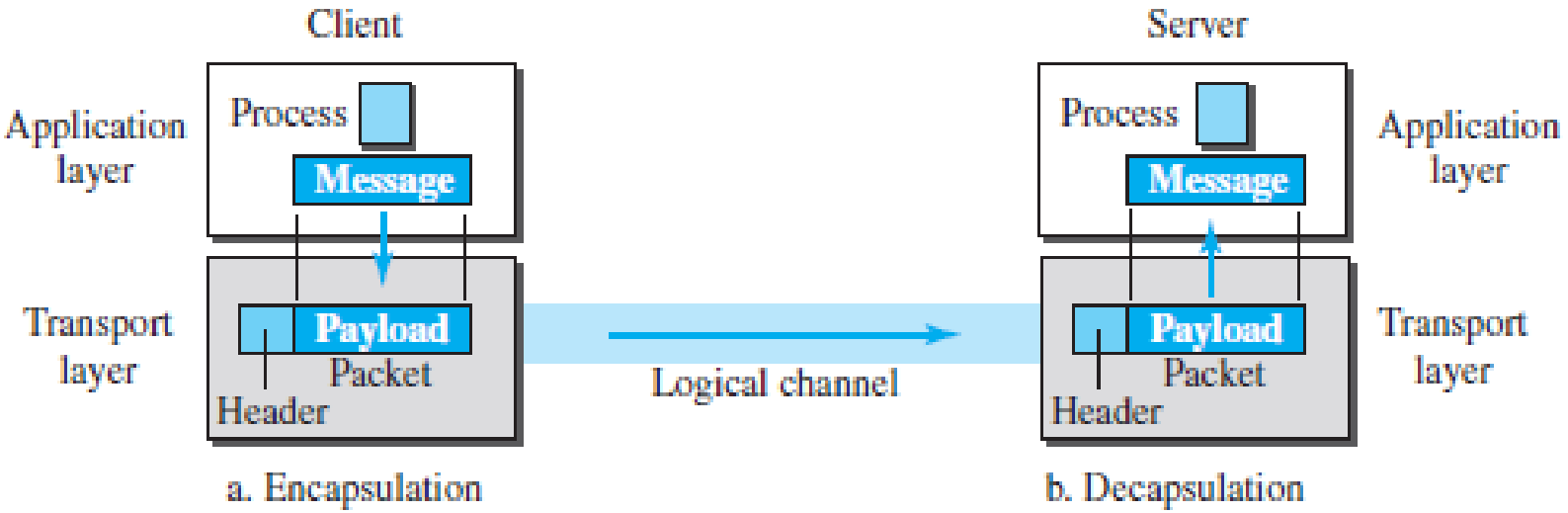
- UDP checksum calculation includes three sections:

1) A pseudoheader 2) The UDP header 3) The data coming from the application layer.

- The *pseudoheader is the part of the header of the IP packet* in which the user datagram is to be encapsulated with some fields filled with 0s



5) *Encapsulation and Decapsulation*



Encapsulation

At the the sender side, when a message is passed to transport-layer then the transport layer adds the transport-layer header. This process is called as encapsulation.

Decapsulation

At the receiver side, when the message arrives at the destination transport layer, the header is dropped and the transport layer delivers the message to the process running at the application layer.

6) Multiplexing and Demultiplexing

In a host running a TCP/IP protocol suite, there is only one UDP but possibly several processes that may want to use the services of UDP. To handle this situation, UDP multiplexes and demultiplexes.

Q) 6 b What are the different TCP services

TCP Services

1) Process-to-Process Communication

TCP provides process-to-process communication using port numbers.

2) Full-Duplex Communication:

- TCP offers full-duplex service, where data can flow in both directions at the same time.
- Therefore each TCP endpoint then has its own sending and receiving buffer, and segments move in both directions.

3) Multiplexing and Demultiplexing

TCP performs multiplexing at the sender and demultiplexing at the receiver. since TCP is a connection-oriented protocol, a logical connection is established for each pair of processes, then data are exchanged and at last connection is terminated.

4) Stream Delivery Service

The TCP segment is encapsulated in an IP datagram and can be sent out of order which may be routed over a different path to reach the destination and that can be lost or corrupted and resent. Hence **TCP creates a stream-oriented environment in which it guarantees the delivering the bytes in order at the destination.**

5) Reliable Service

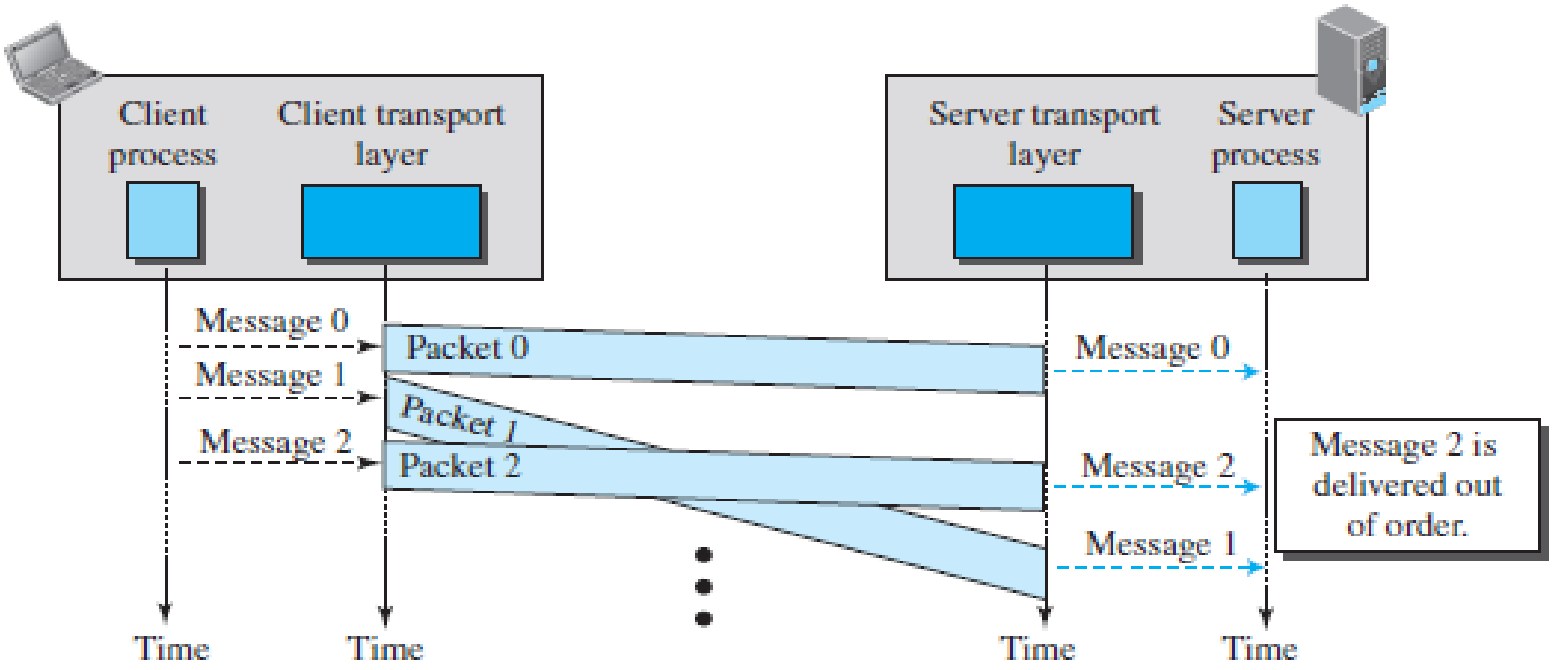
TCP is a reliable transport protocol and uses an **acknowledgment mechanism** to check the safe and sound arrival of data.

7. Error Control

1. Detecting and discarding corrupted packets.
2. Keeping track of lost and discarded packets and resending them.
3. Recognizing duplicate packets and discarding them.
4. Buffering out-of-order packets until the missing packets arrive.
5. Add sequence numbers to the packets from 0 to $2m - 1$. *like* 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ...

Q) 7 Explain connectionless and connection-oriented service represented as FSMs for transport layer

Connectionless and Connection-Oriented Protocols at transport layer



Connectionless Service

- The chunks of packets from the application layer are are handed over to the connectionless transport protocol in order.

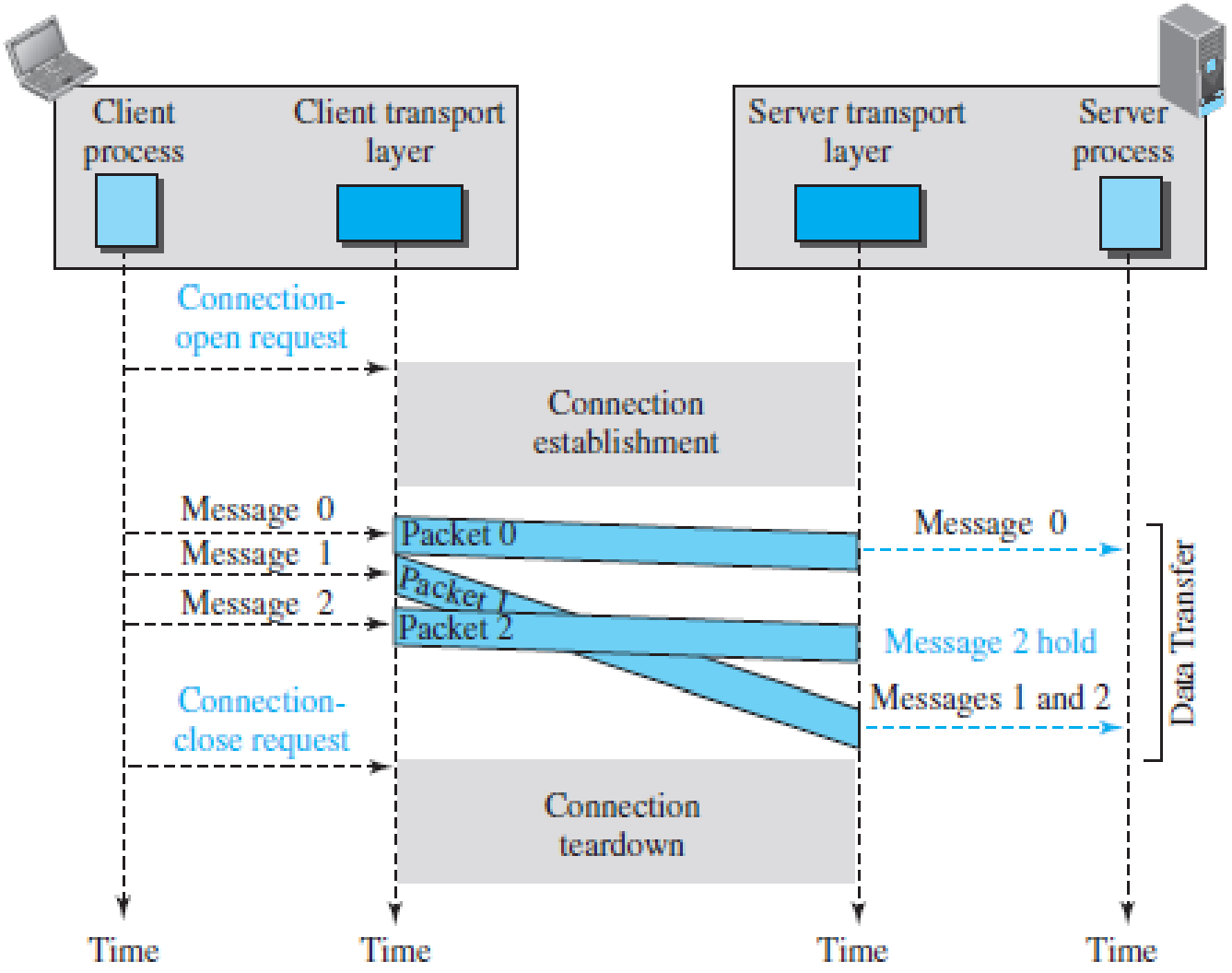
- As there is no dependency between the packets hence, the packets may arrive out of order at the destination and will be delivered out of order to the server process

- For example in the figure three chunks of messages are delivered in order (0, 1, and 2) but due to some delay the messages arrive at the server is out of order (0, 2, 1). Hence the server process a kind of strange message.

- The situation become more worse if some of the packets gets lost. As it is difficult for receiver to find the order of packets.

In connection less service there is no flow control, error control, or congestion control being implemented.

Connection-Oriented Service



Connection-Oriented Service

- Occurs in three steps

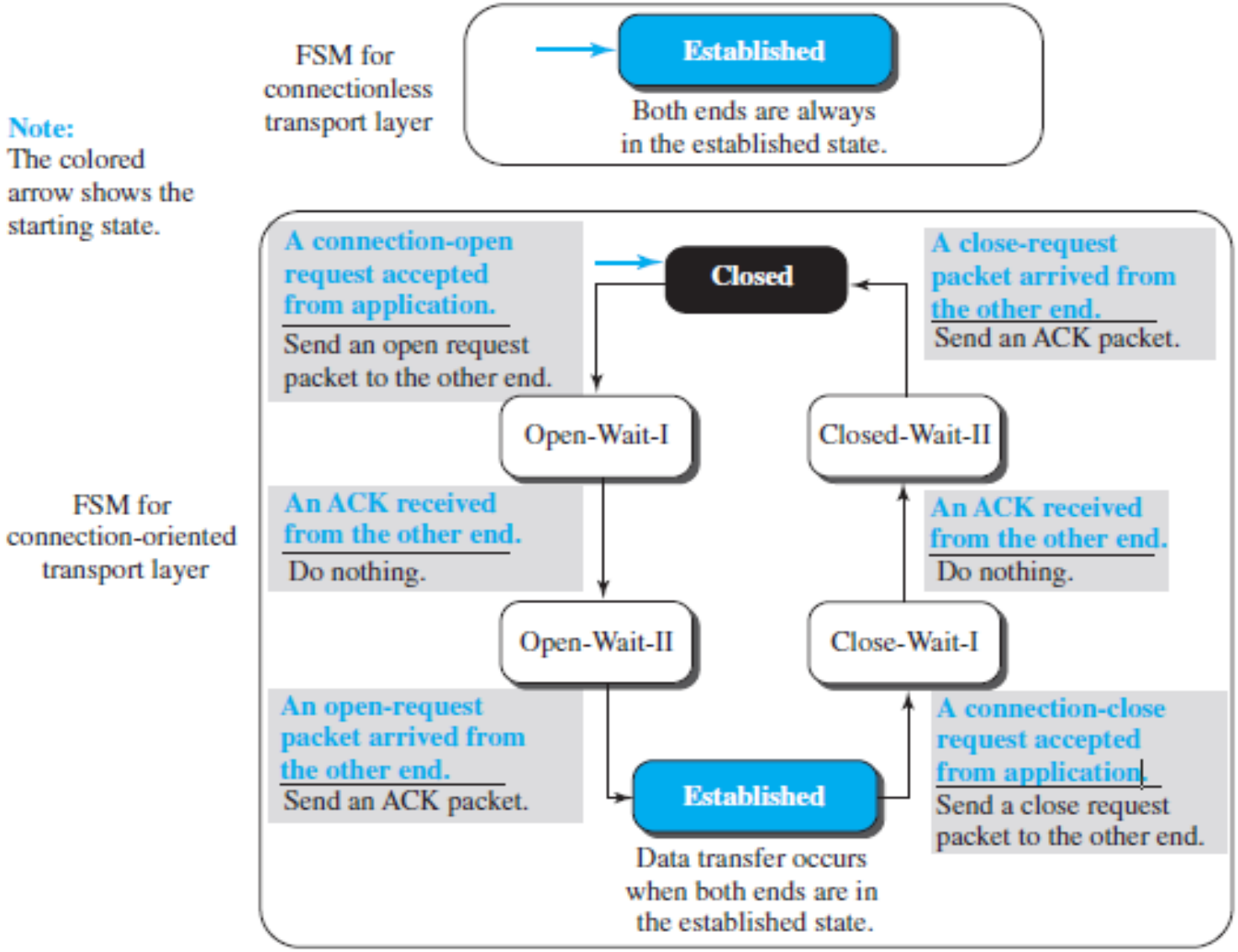
1) First the client and the server establish a logical connection.

2) Start exchanging the data.

3) After data exchange, the connection needs to be torn down.

- *The flow control, error control, and congestion control mechanism can be implemented in in a connection oriented Protocol.*

Connectionless and connection-oriented service represented as FSMs



Connectionless service represented as FSMs

- Here the FSM has only one state i.e. the established state.
- The machine on each end (client and server) is always in the established state, ready to send and receive transport-layer packets.

Connection-oriented service represented as FSMs

- It works in three phases :

1) Logical connection formation 2) Data transfer 3) Connection termination

1) logical connection formation:

- Here the FSM needs to go through three states

closed state:

- When the machine is in the **closed state** when there is no connection.

open-wait-I state:

- The machine sends an open request packet to the remote transport layer and moves to the **open-wait-I state.**

open-wait-II state:

- When an acknowledgment is received from the other end, the local FSM moves to the **open-wait-II state.**

Connection-oriented service represented as FSMs

2) Data transfer (also called as established state).

- When the request is received, the machine moves to the **established state** where the data and data ACK are exchanged between the two ends.

3) Connection termination

Goes through three phases

close-wait-I state.

- To tear down the connection, transport layer sends a close-request packet to the other end and moves to **close-wait-I state.**

close-wait-II state

- When an acknowledgment is received from the other end, the machine moves to **the close-wait-II state** and waits for the close-request packet.

closed state When the close-request packet arrives, the machine sends an acknowledgment and moves to the **closed state.**

Q) 8 Explain TCP connection establishment and connection termination using three way handshaking

A TCP Connection using three way handshaking

By three process:

1) ***Logical connection Establishment***
2) ***Data Transfer***
3) ***Connection Termination***

1) *Connection Establishment*

Three-Way Handshaking

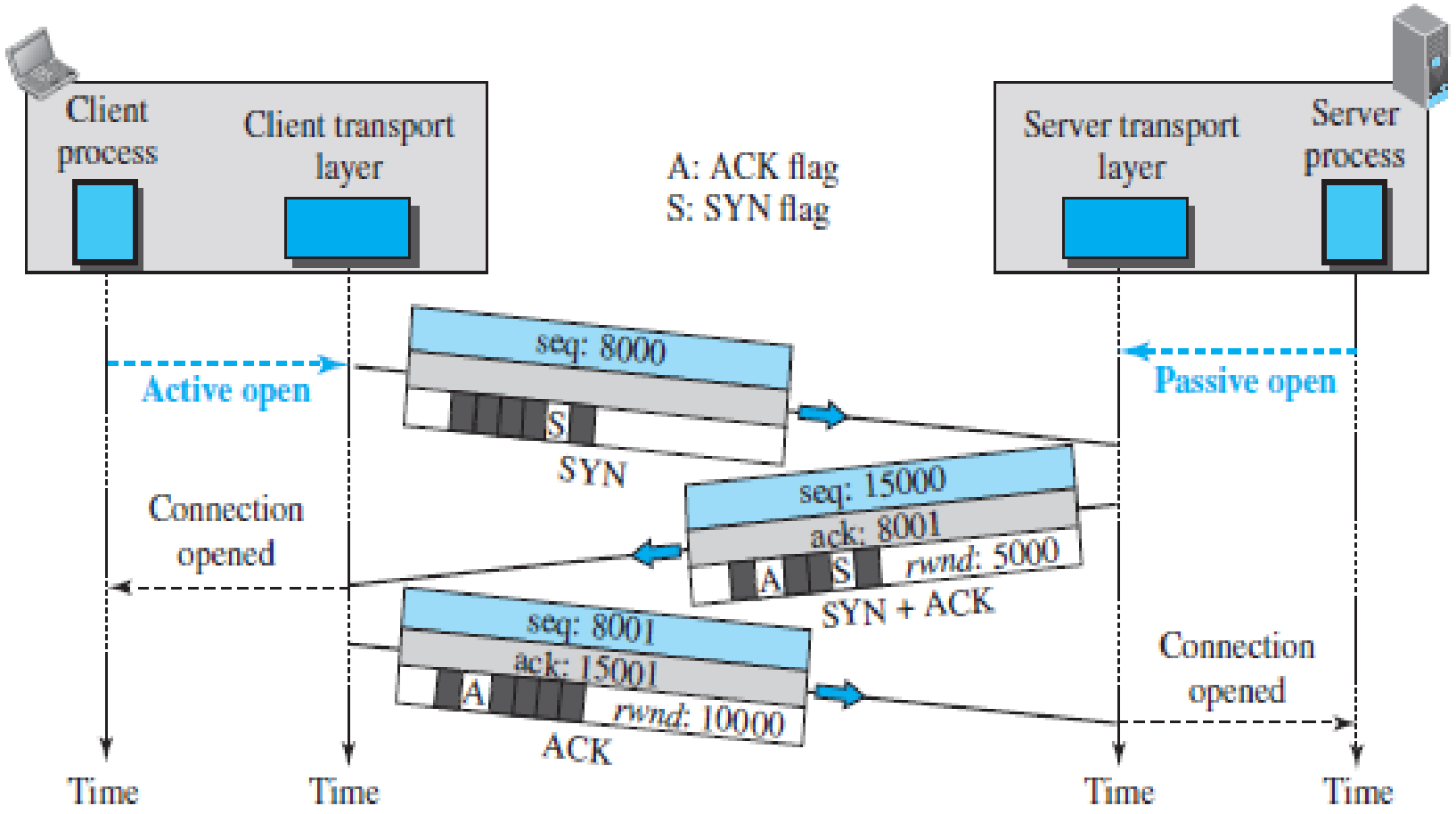
passive open request:

The server program tells its TCP that it is ready to accept a connection. This request is called a *passive open*

active open:
The client program issues a request for an *active open*. *A client that wishes to connect* to an open server tells its TCP to connect to a particular server.

Then TCP start the three-way handshaking process

Three-way handshaking process



SYN segment

1) The client sends the first segment, a SYN segment, in which only the SYN flag is set and this segment **is for synchronization of sequence numbers.**

A SYN segment cannot carry data, but it consumes one sequence number

SYN + ACK segment

- The server sends SYN + ACK segment with two flag bits set as: SYN and ACK.

- This segment has a dual purpose.

1) First, this segment to initialize a sequence number for the bytes sent from the server to the client.

2) Second the server also acknowledges the receipt of the SYN segment from the client by setting the ACK flag and displaying the next sequence number it is expecting to receive from the client.

- Because the segment contains an acknowledgment, it also needs to define the receive window size, *rwnd*.

A SYN 1 ACK segment cannot carry data, but it consumes one sequence number

ACK segment

- The client sends the third segment as an ACK segment.
- It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field

An ACK segment, if carrying no data, consumes no sequence number.

Data Transfer

- **After connection is established, bidirectional data transfer can take place**

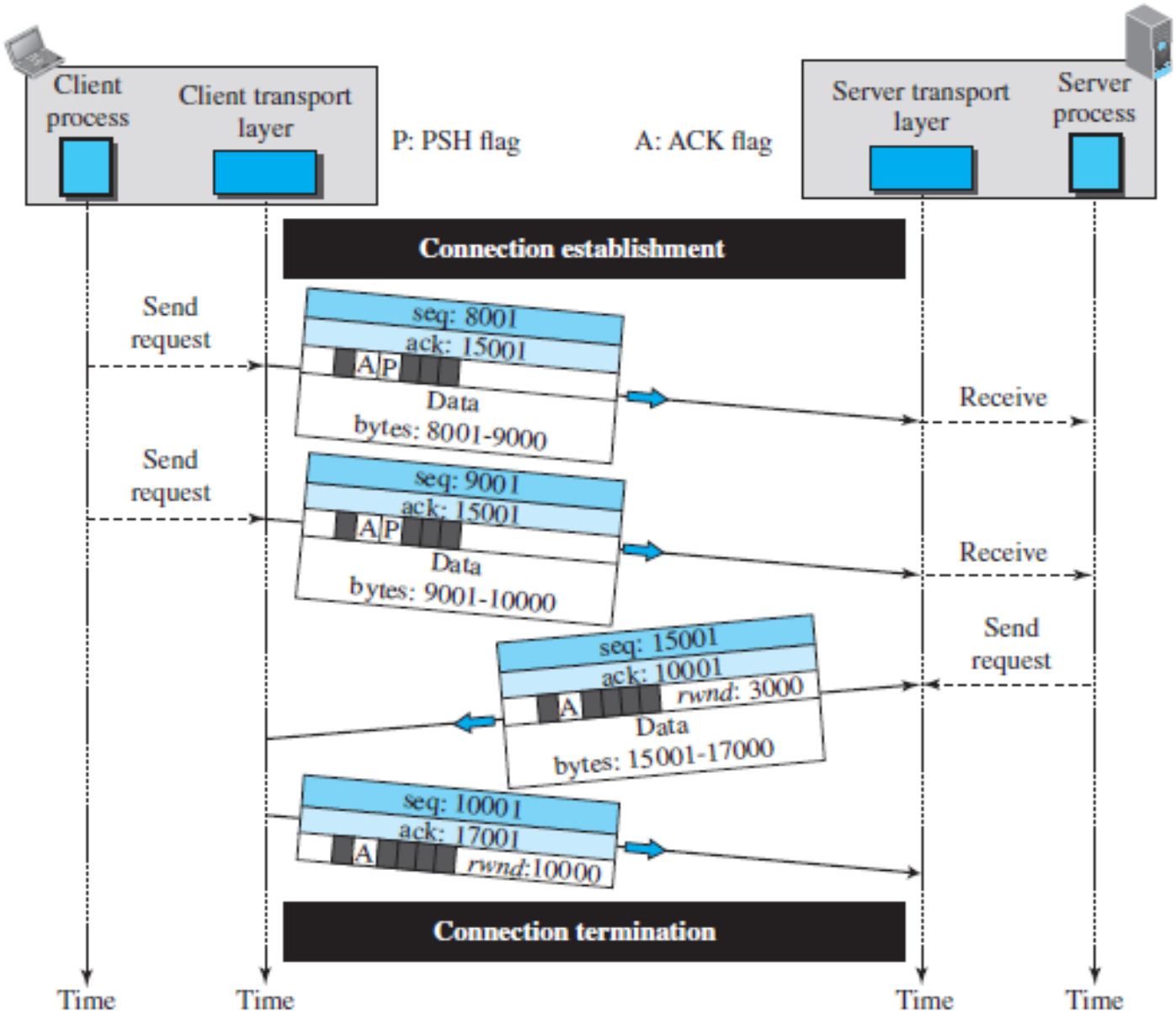
- Client client sends two segments of 1000 byte each.

- The server then sends 2,000 bytes in one segment.

- The client sets the PSH (push) flag in data segments so that the server TCP knows that data transmission is happening.

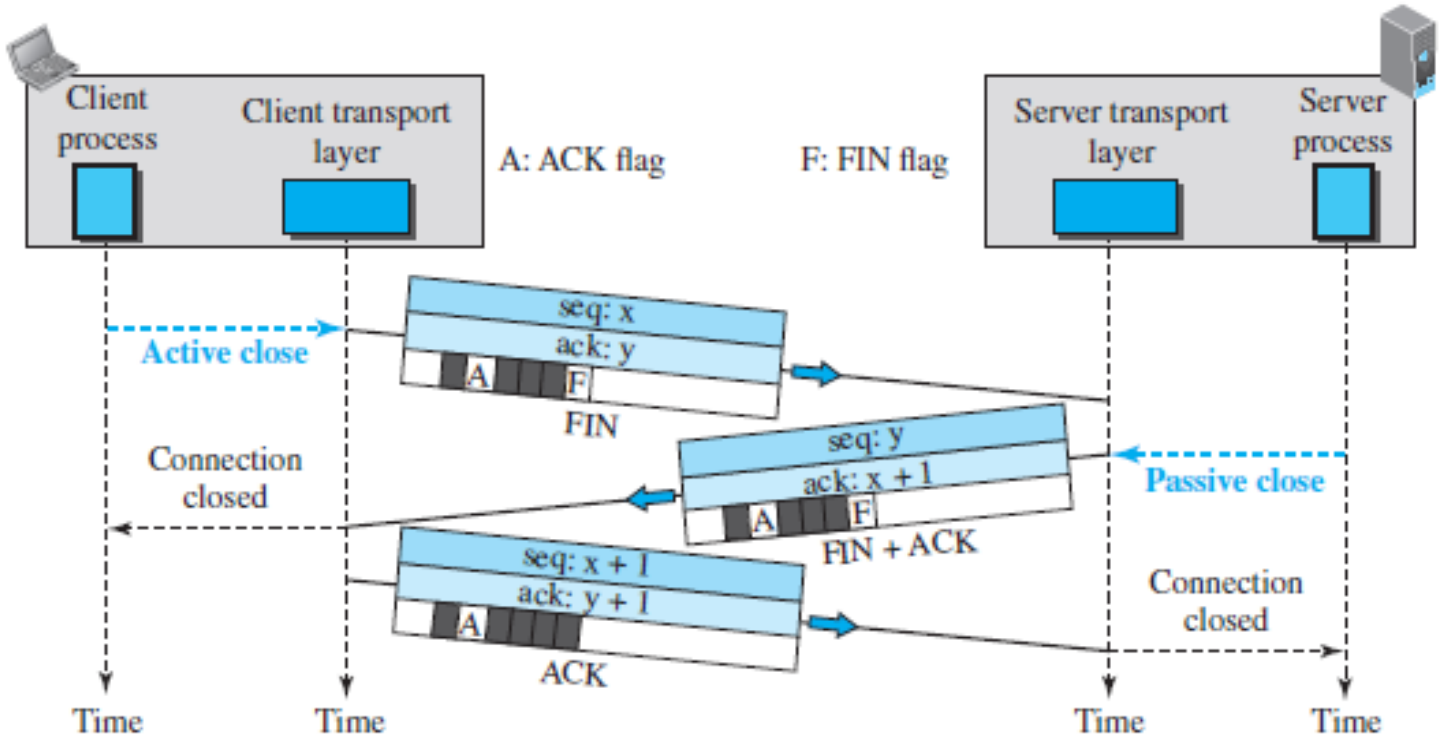
- The segment from the server, on the other hand, does not set the push flag.

Data Transfer



Connection Termination

Three-Way Handshaking



FIN segment

The client sends the FIN segment in which the FIN flag is set. FIN segment can include the last chunk of data sent by the client.

The FIN segment consumes one sequence number if it does not carry data.

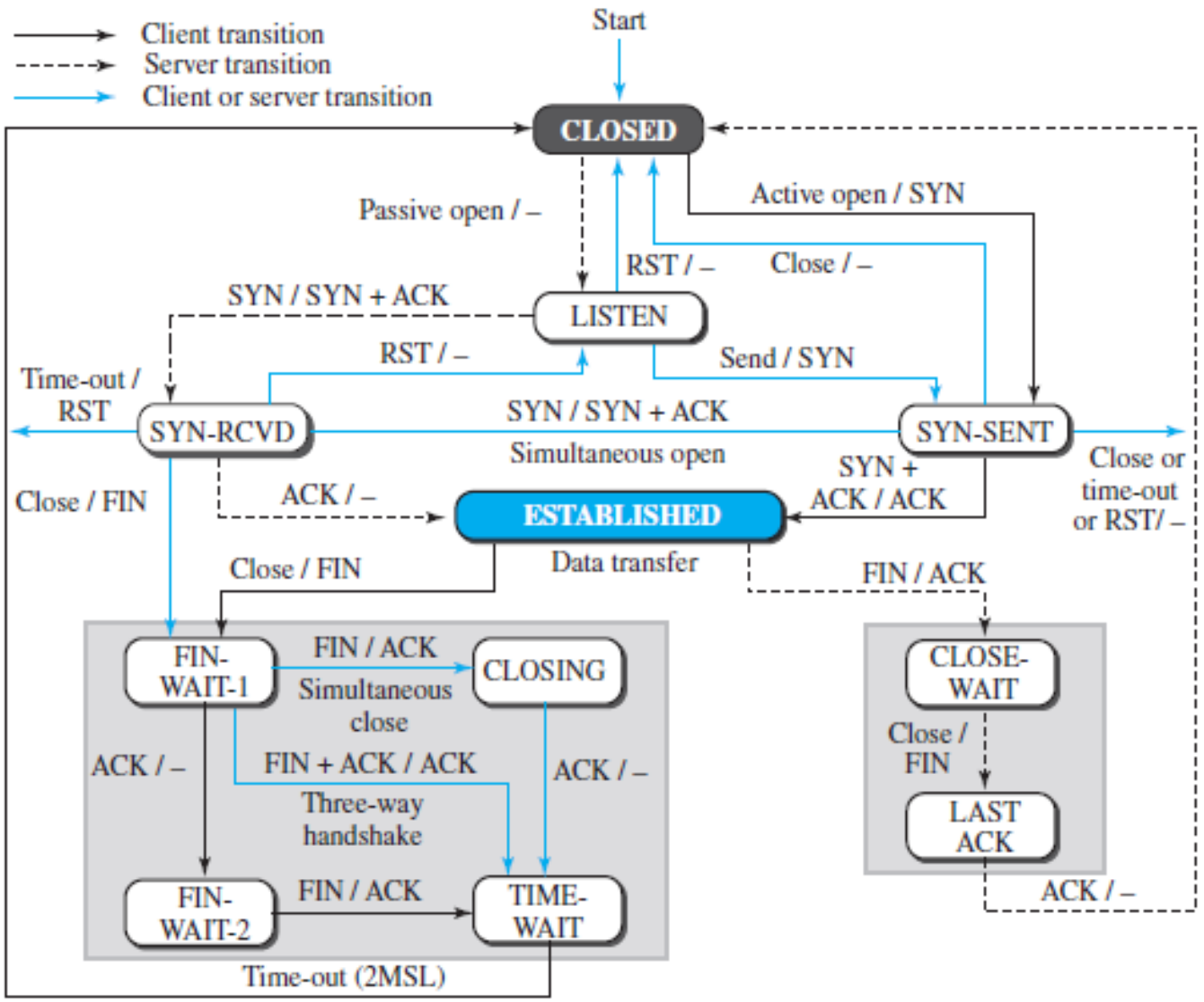
FIN + ACK segment

The server sends the FIN + ACK segment, to confirm the receipt of the FIN segment from the client and also announces the closing of the connection.

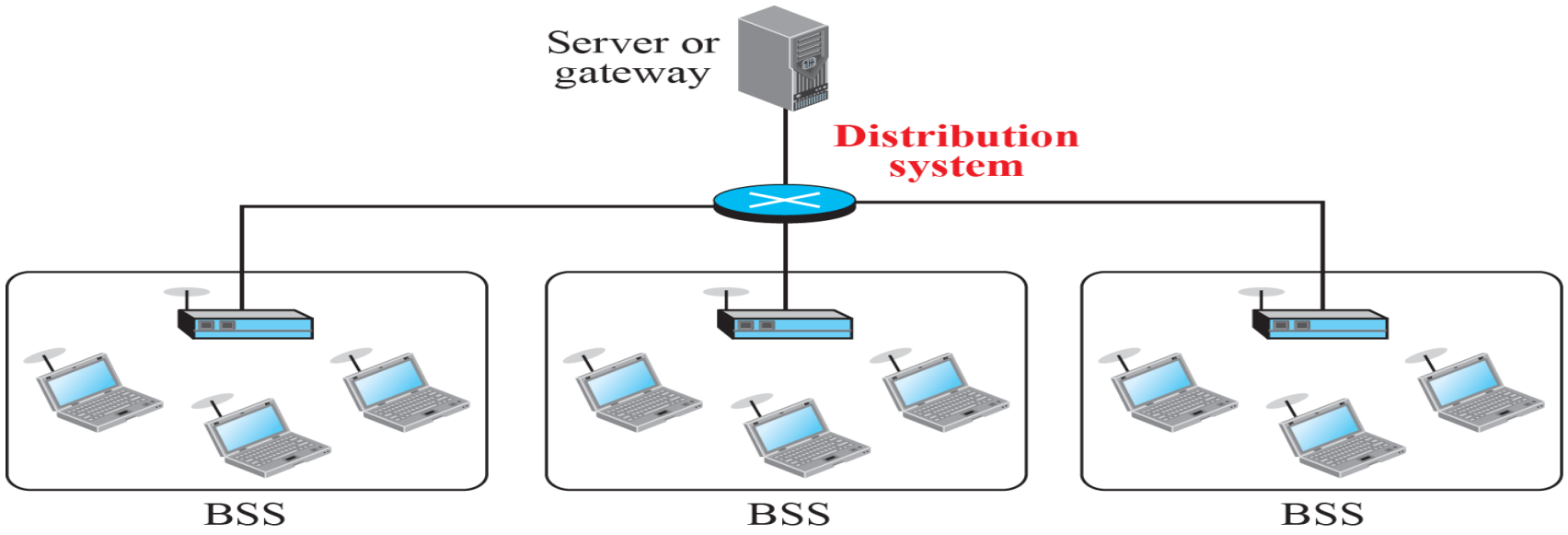
ACK segment

The client TCP sends the last ACK segment to confirm the receipt of the FIN segment from the TCP server.

State Transition Diagram



Extended service set (ESS)



Note that the extended service set uses two types of stations/nodes

a) Mobile stations/nodes
b) Stationary stations/nodes

- The mobile stations are normal stations inside a BSS.
- The stationary stations are AP stations that are part of a wired LAN.
- When BSSs are connected, the stations within reach of one another can communicate without the use of an AP.
- The communication between two or more then two BSS occurs via the AP.