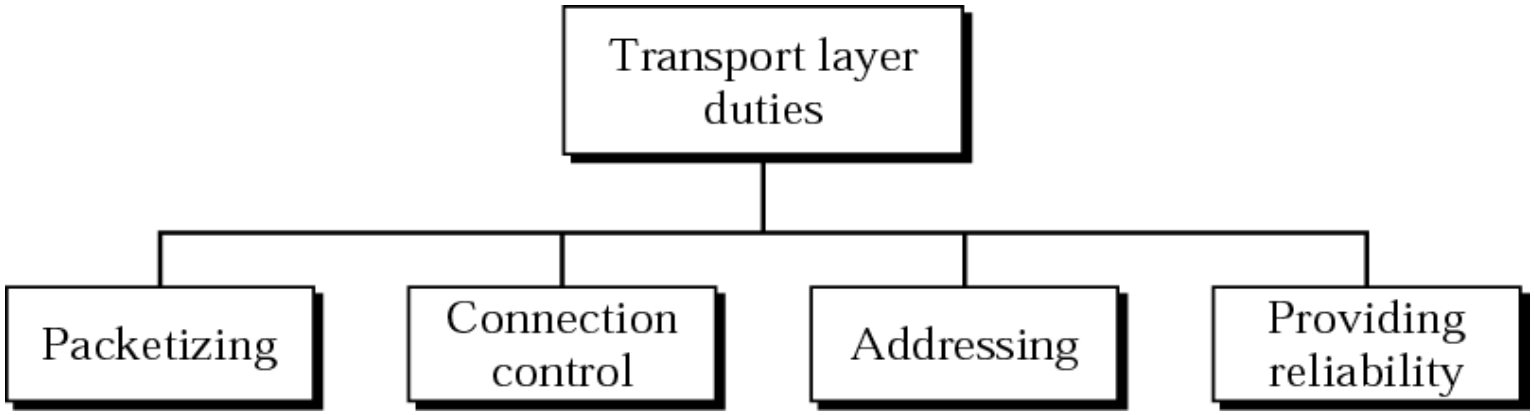
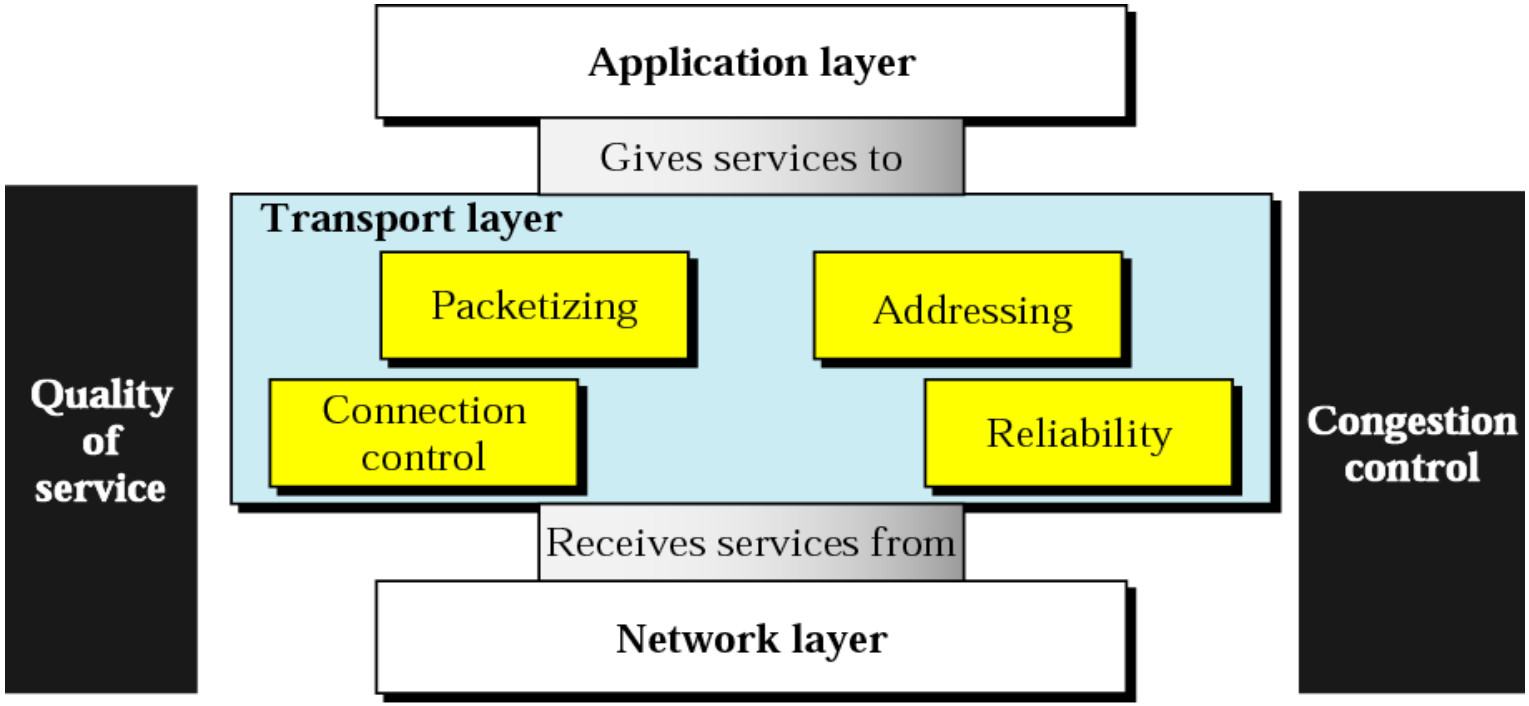
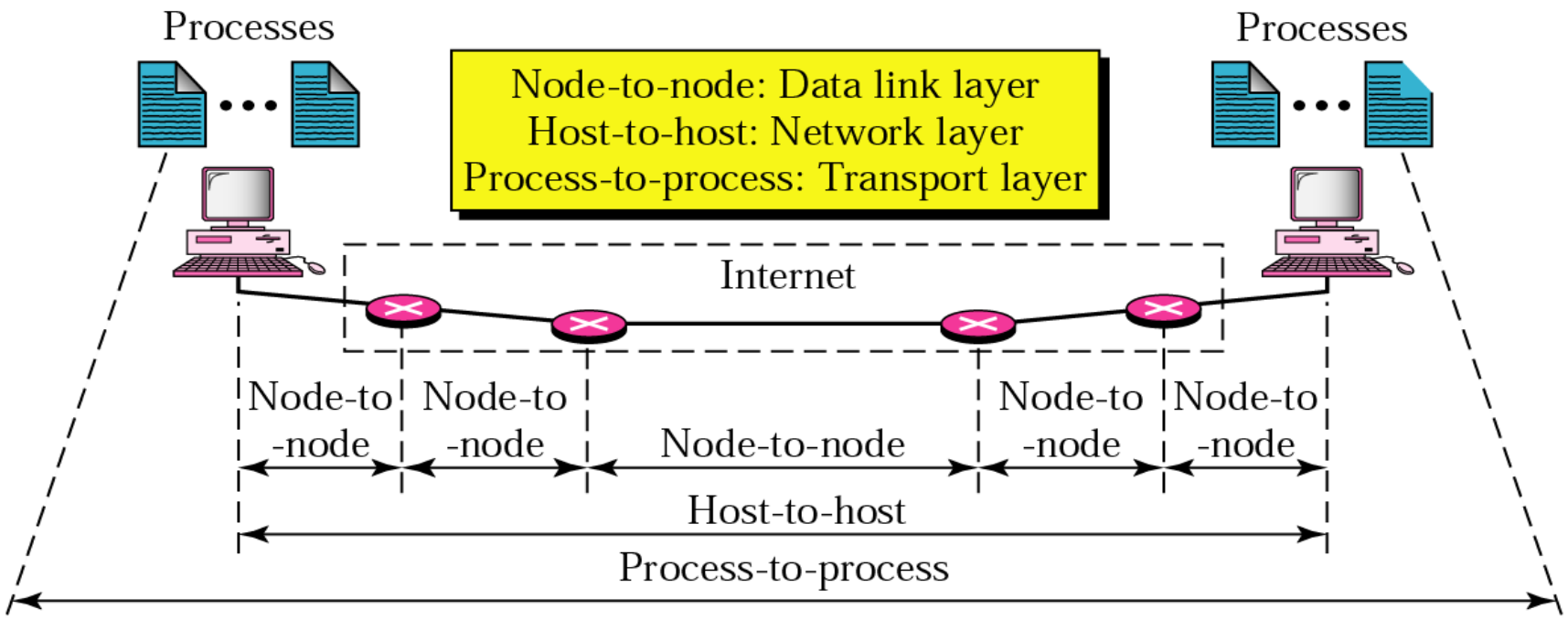
Chapter 6: Transport Layer and protocol


Transport layer duties
Packetizing
Connection control
Addressing
Providing reliability

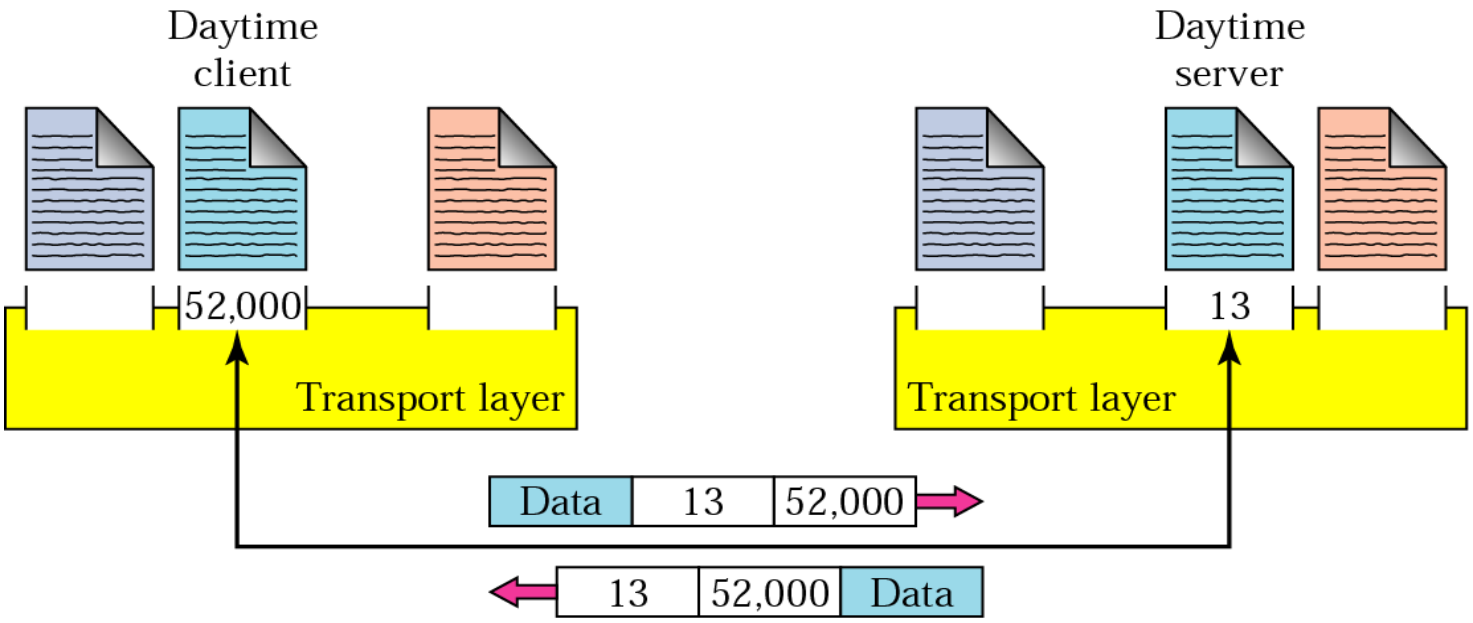
Transport Layer : Duties ??



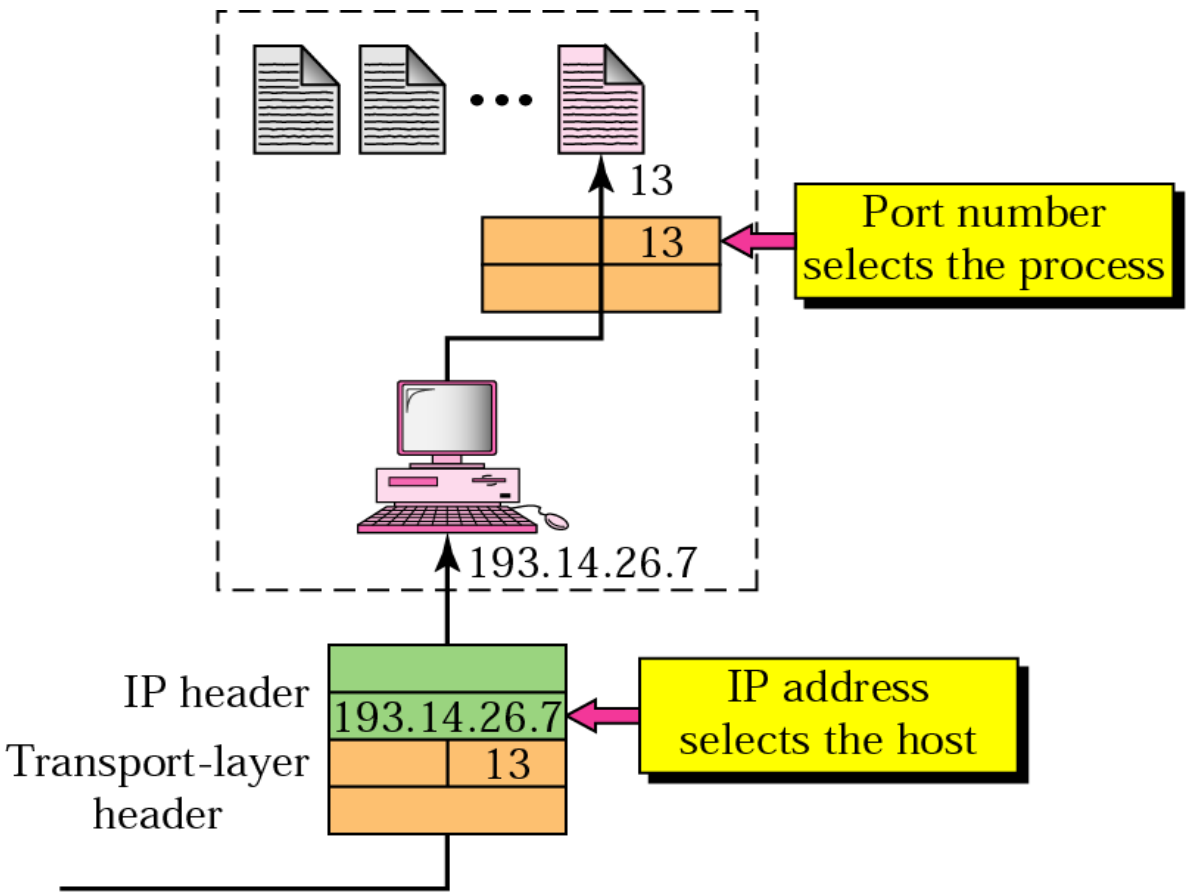
Transport Layer : Type of Data Deliveries



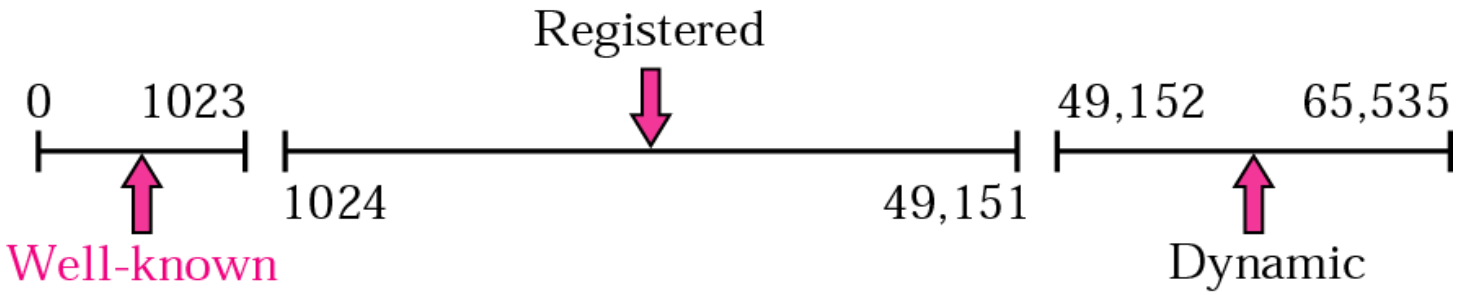
Transport Layer : Port Numbers



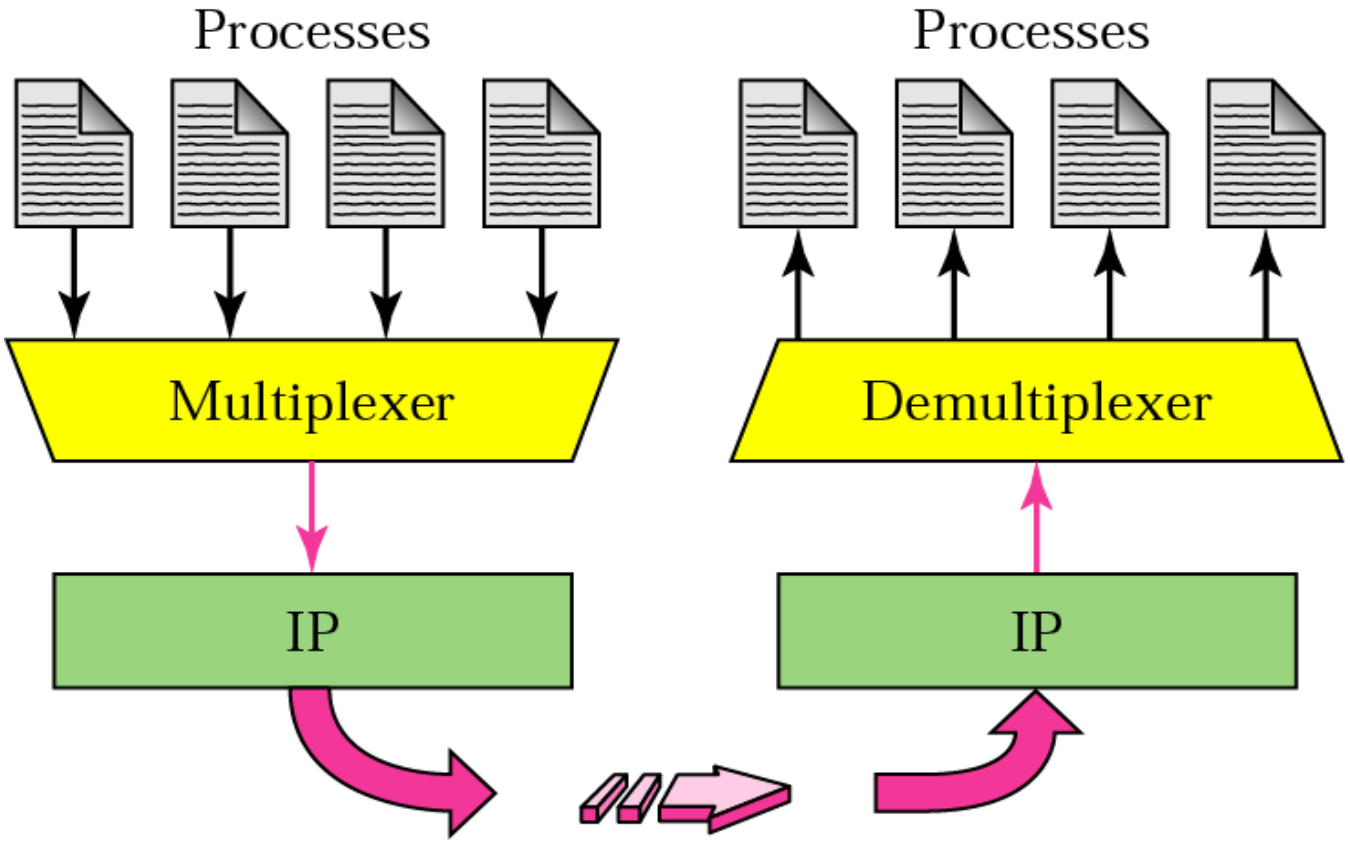
Transport Layer : IP VS Port Numbers



Transport Layer : Port Numbers (IANA Range)



Transport Layer : Multiplexing and Demultiplexing



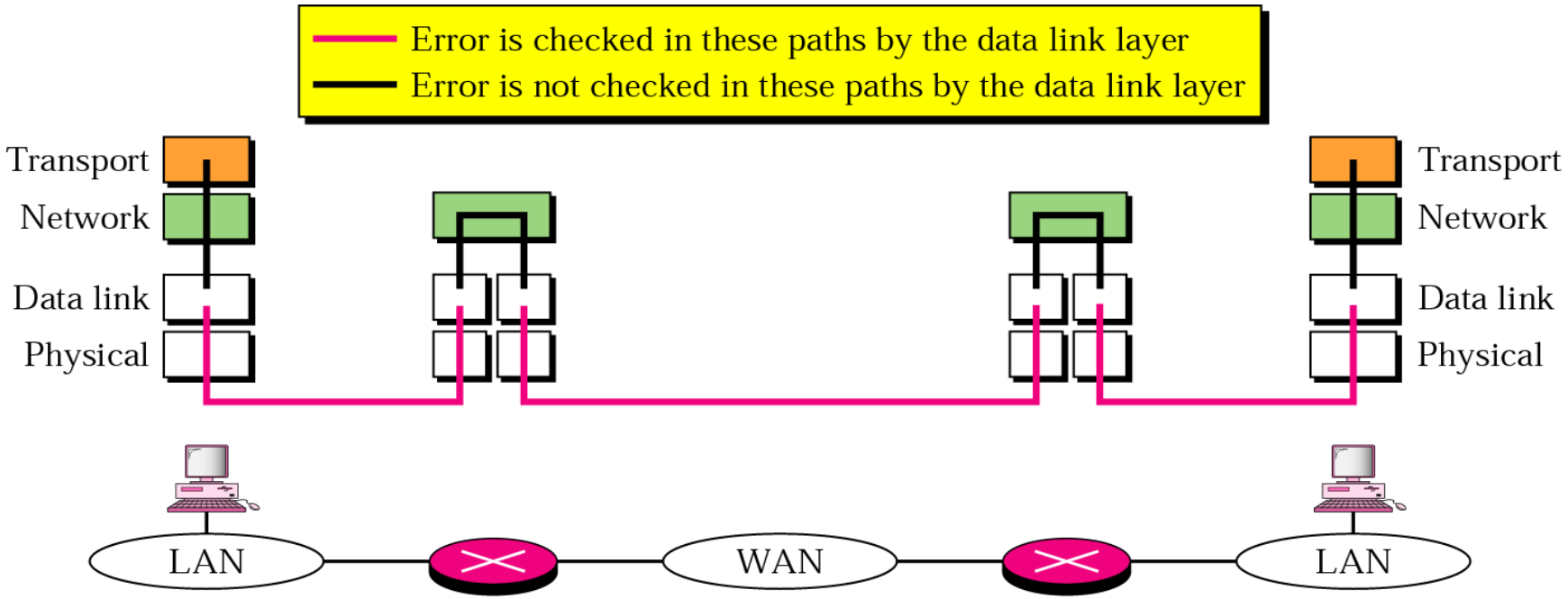
Transport Layer : Multiplexing and Demultiplexing

The technique to combine two or more data stream in one session is called Multiplexing. When a TCP client initializes a connection with Server, it always refers to a well-defined port number which indicates the application process. The client itself uses a randomly generated port number from private port number pools.

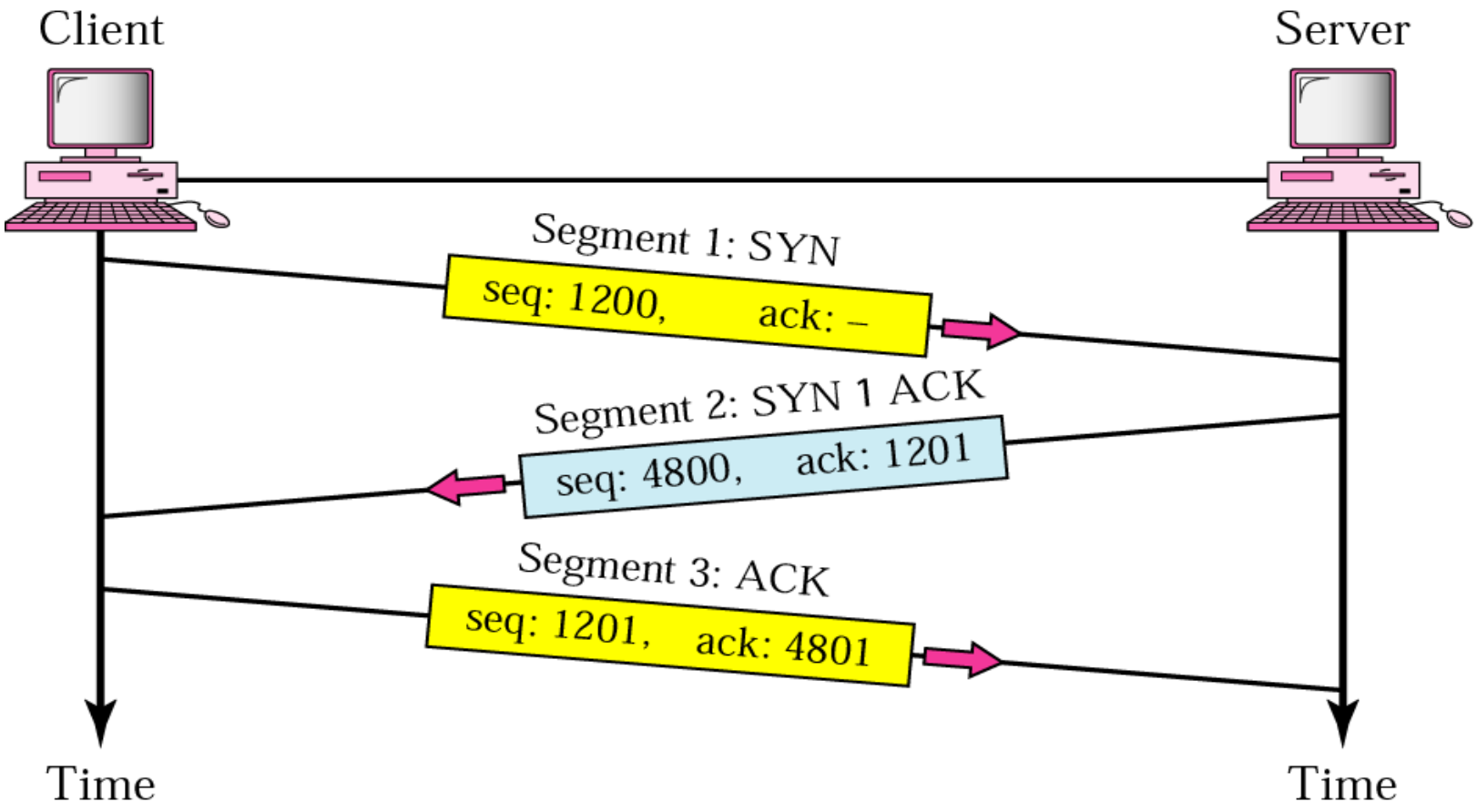
Using TCP Multiplexing, a client can communicate with a number of different application process in a single session. For example, a client requests a web page which in turn contains different type of data (HTTP, SMTP, FTP etc.) the TCP session timeout is increased and the session is kept open for longer time so that the three-way handshake overhead can be avoided.

This enables the client system to receive multiple connection over single virtual connection. These virtual connections are not good for Servers if the timeout is too long.

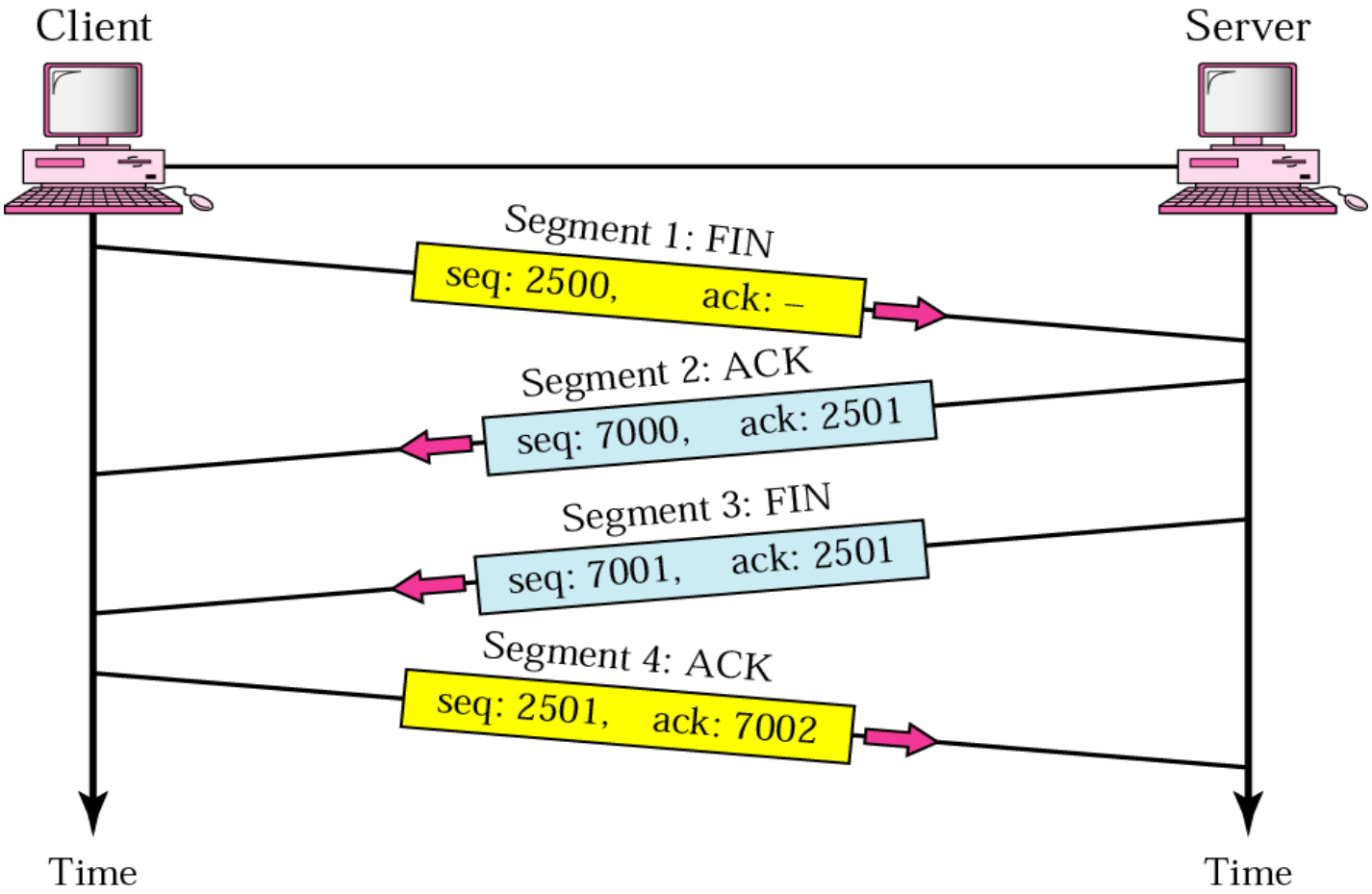
Error Control in Transport Layer



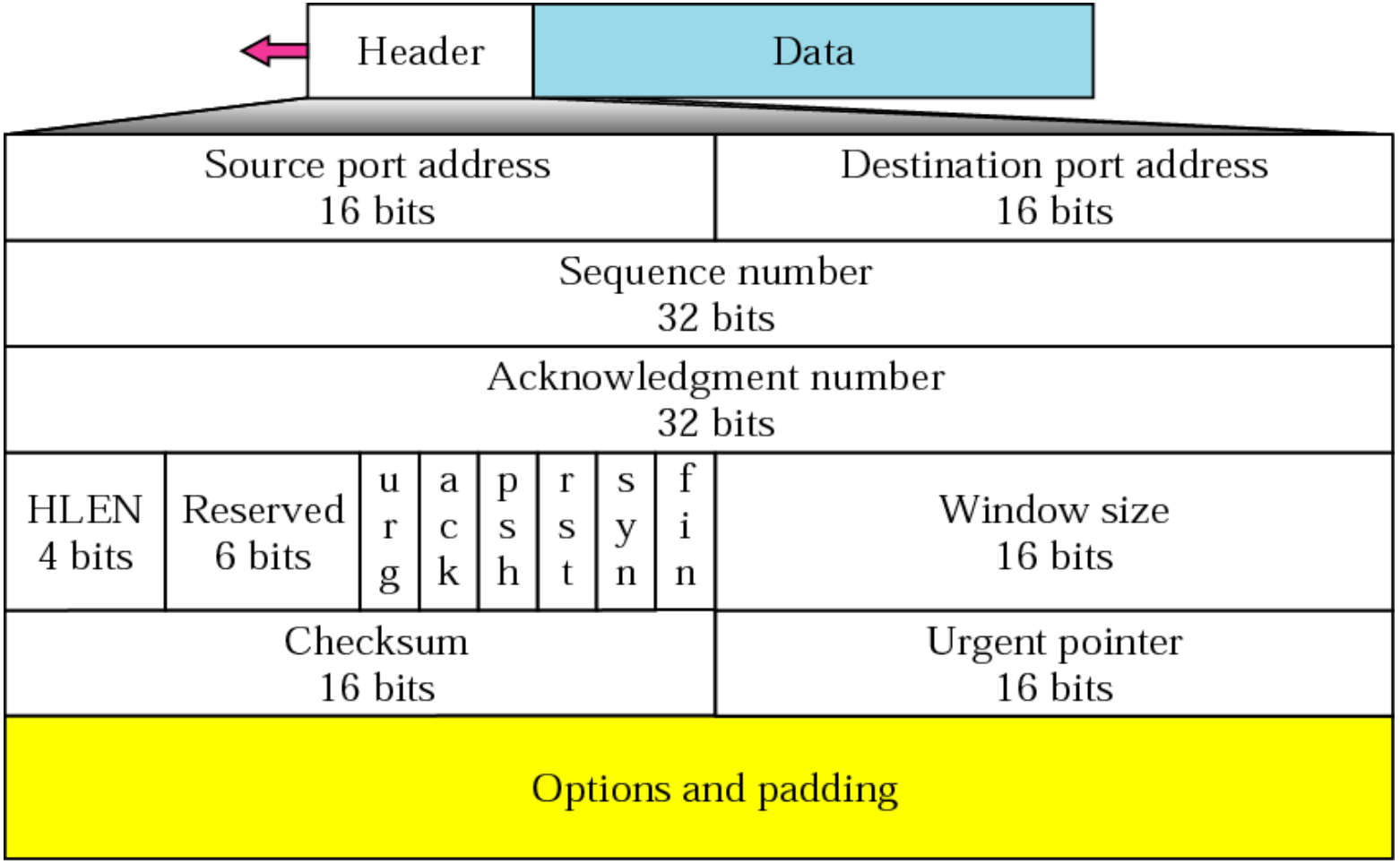
Transport Layer : Three Step Connection Establishment: Handshaking



Transport Layer : Four Step Connection Termination, Handshaking

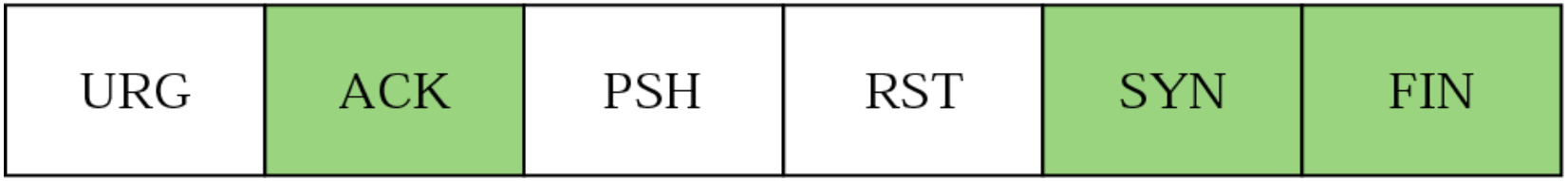


Transport Layer : TCP Segment Format

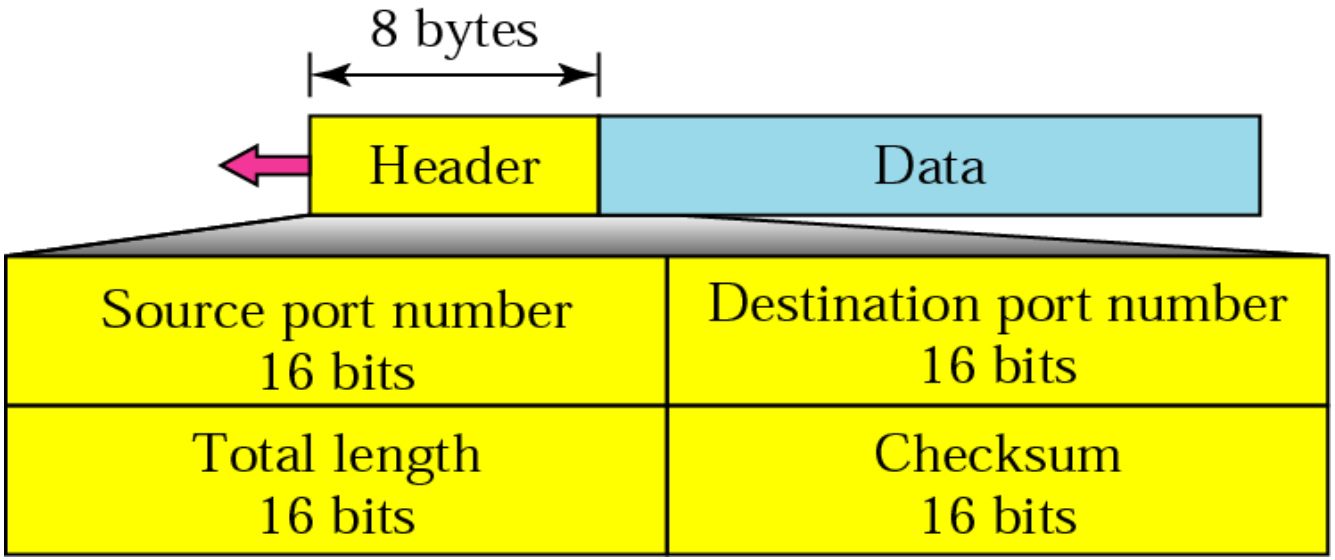


Transport Layer : TCP Segment Format (Control Fields)

URG: Urgent pointer is valid
ACK: Acknowledgment is valid
PSH: Request for push
RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: Terminate the connection



Transport Layer : UDP Segment Format



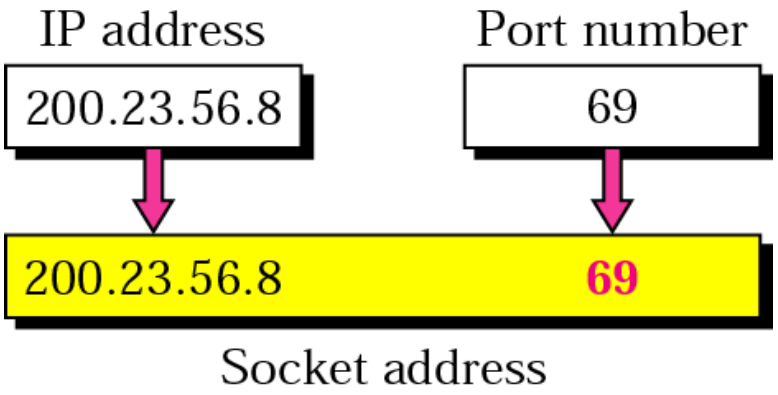
TCP Services

- TCP is reliable protocol, that is, the receiver sends an acknowledgement back to the sender, of each packet it receives. Sender is now confirmed that packet has been received and can process further packets in its queue.
- TCP ensures that data has been received in the order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can act like receiver and sender.

UDP Services

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.

Socket


IP address
Port number
200.23.56.8
69
200.23.56.8
69
Socket address

Socket

- A socket is one endpoint of a two-way communication link between two programs running on the network.
- A socket is bound to a port number so that the TCP layer can identify the application that data is destined to be sent.

- Normally, a server runs on a specific computer and has a socket that is bound to a specific port number.
- The server just waits, listening to the socket for a client to make a connection request.
- On the client-side: The client knows the hostname of the machine on which the server is running and the port number to which the server is connected.
- To make a connection request, the client tries to make contact with the server on the server's machine and port.

Socket

SOCKET PROGRAMMING

CLIENT SIDE PROGRAMMING

SERVER SIDE PROGRAMMING

Client side socket programming

```
  Socket client;


    try{
client = new Socket("127.0.0.1",5001);
        }


    catch(Exception ae1)
        {
      //Unable to Create Socket
      }
```

SERVER SIDE PROGRAMMING

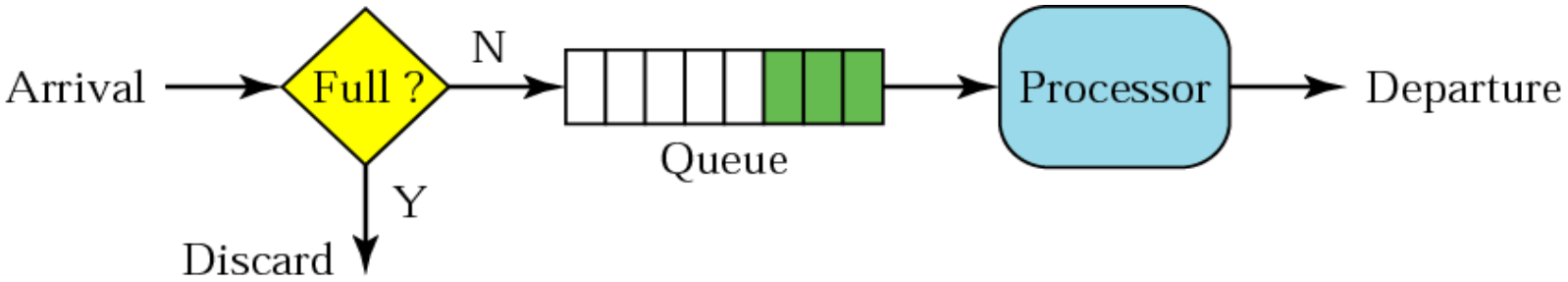
```
ServerSocket(Port No)
try{
ServerSocket server=new ServerSocket(5001);
}


catch(Exception ae1)
{
  // Cannot Start the Server
}
```

Congestion Control in TCP

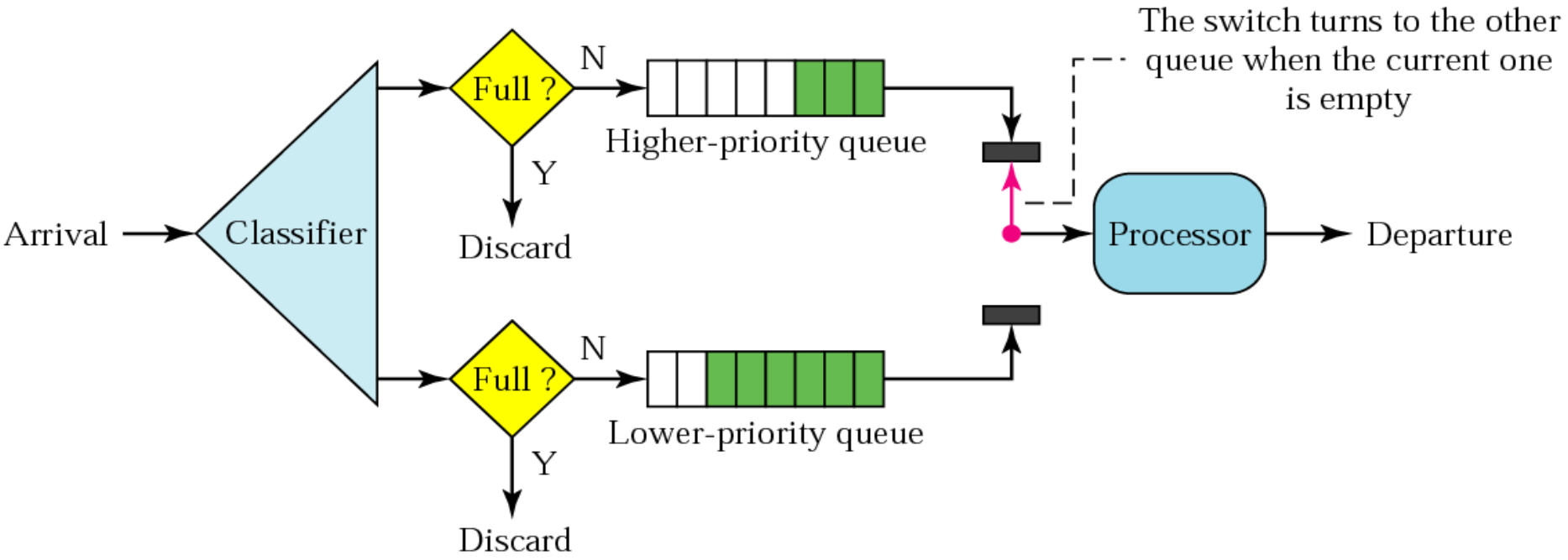
TCP assumes that the cause of a lost segment is due to congestion
in the network.

If the cause of the lost segment is congestion, retransmission of the segment does not remove
the cause—it aggravates it.

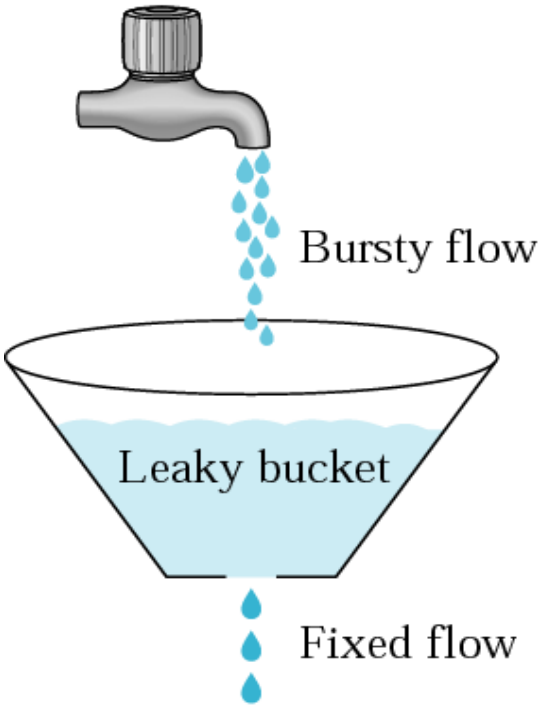
FIFO queue

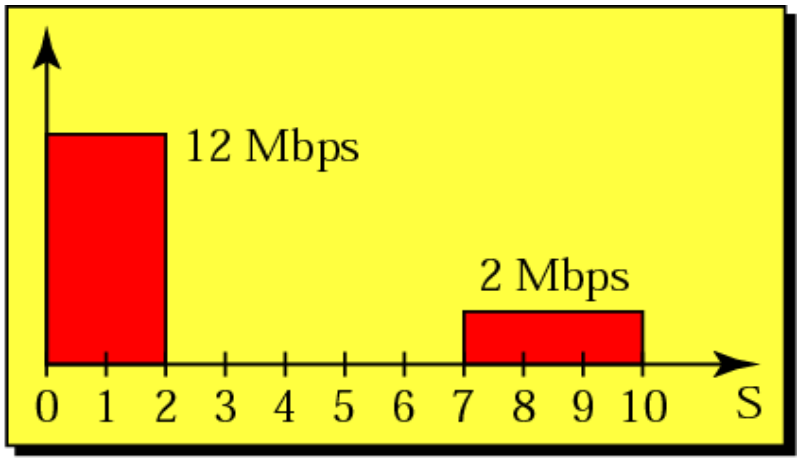


Priority queuing

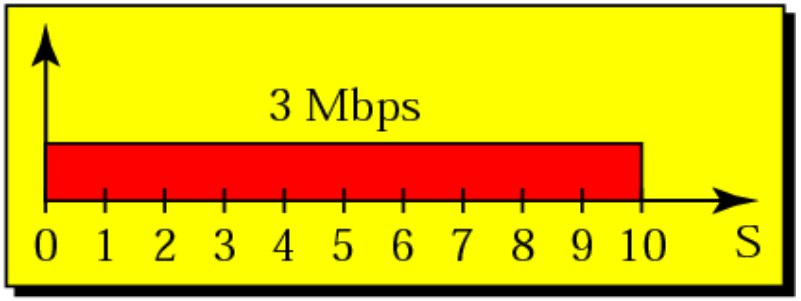


Leaky bucket



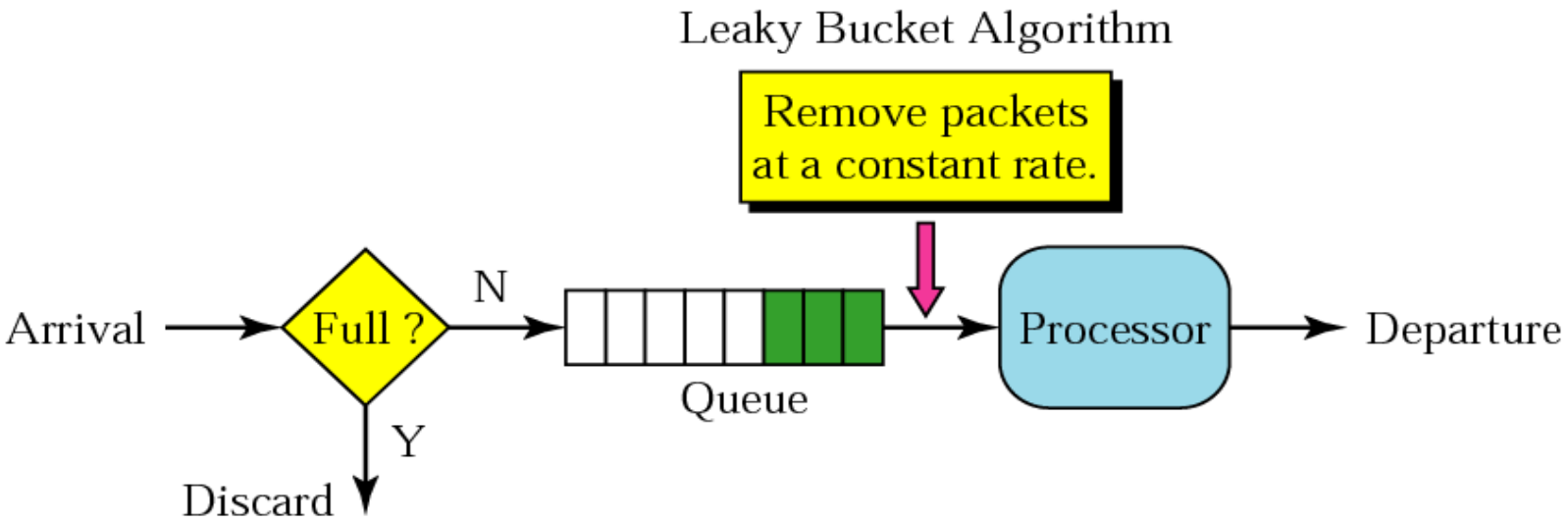


Bursty data



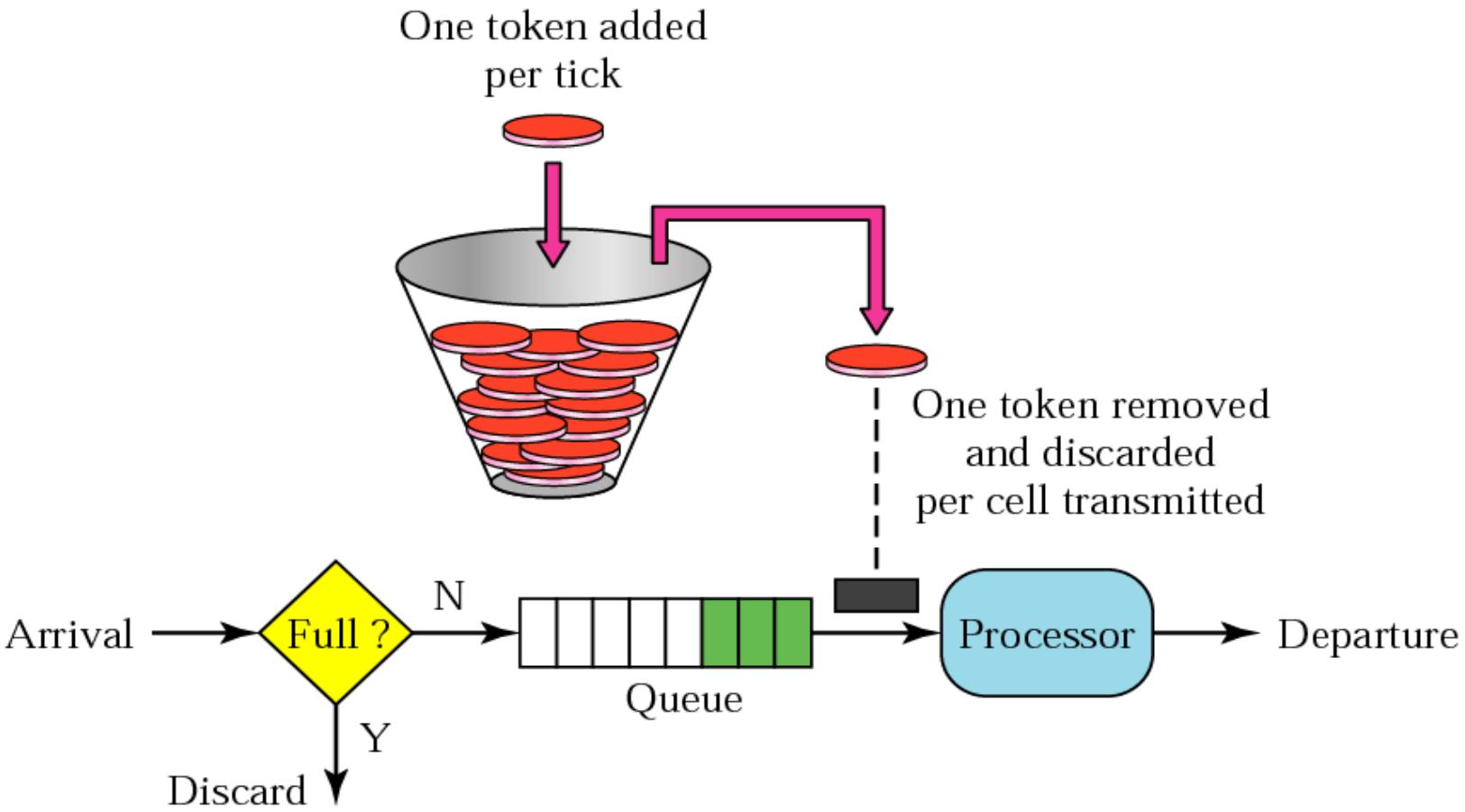
Fixed-rate data

Leaky bucket implementation

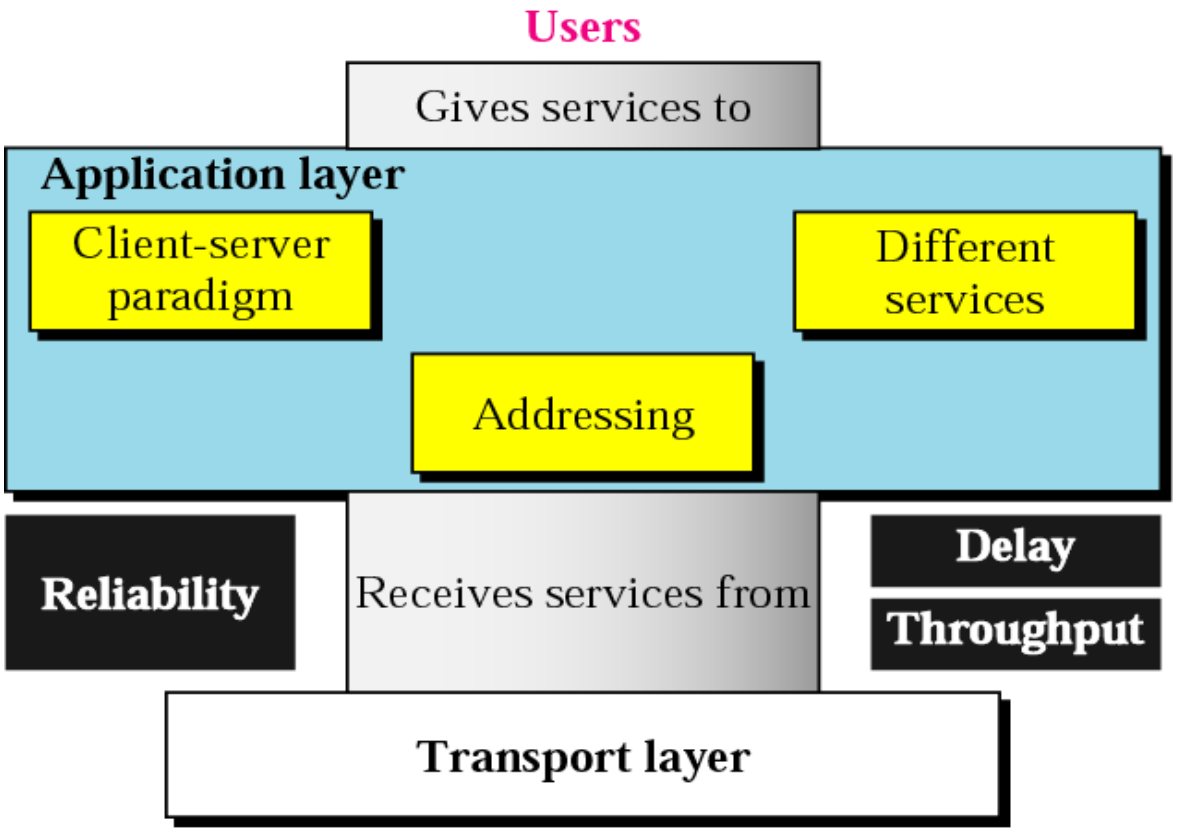


A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.

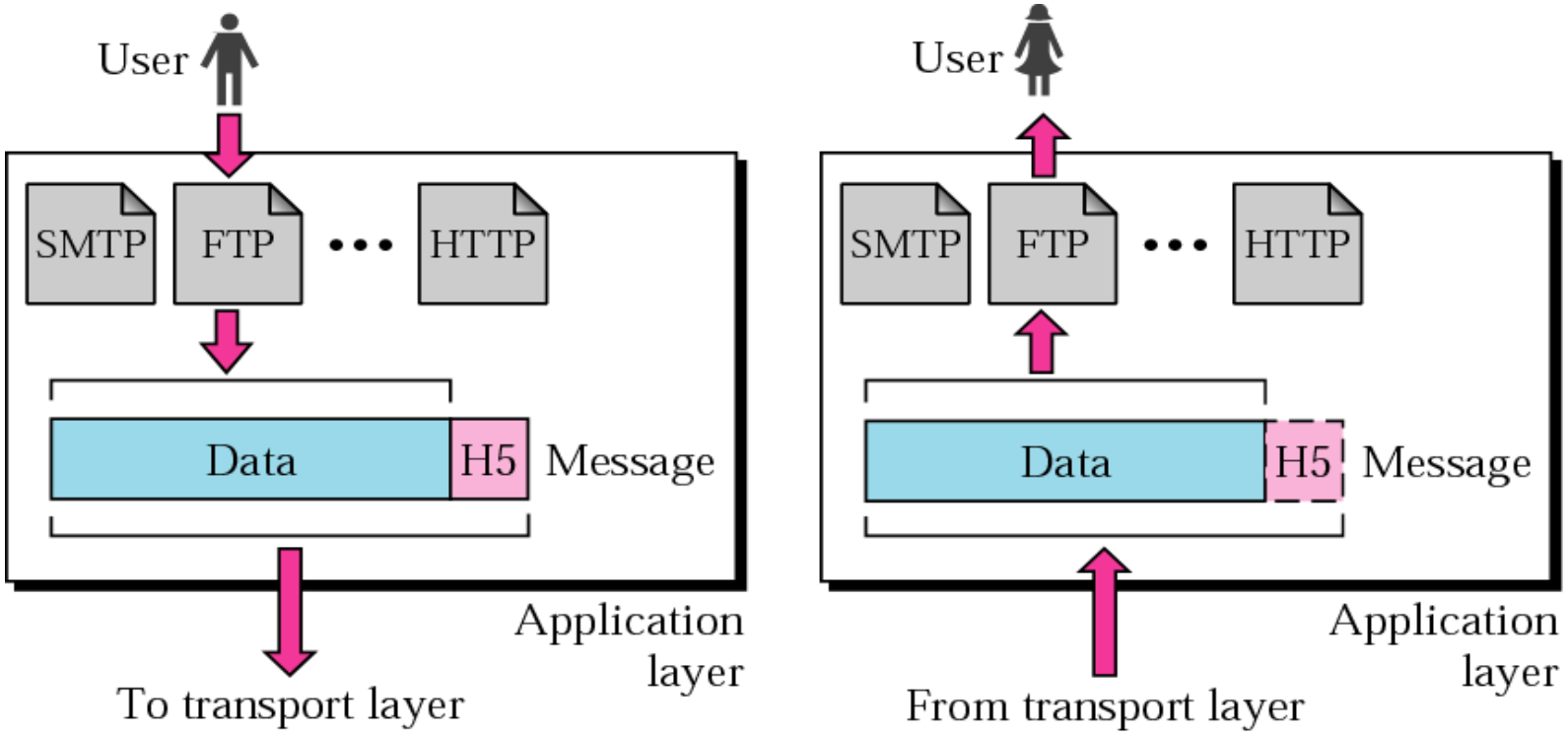
Token bucket



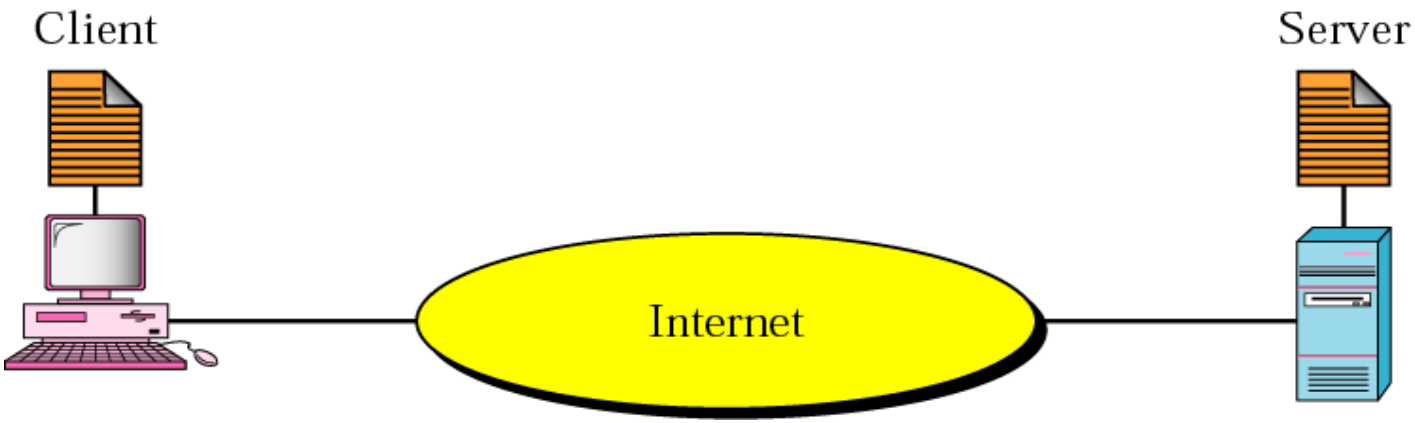
Application Layer : Duties ??



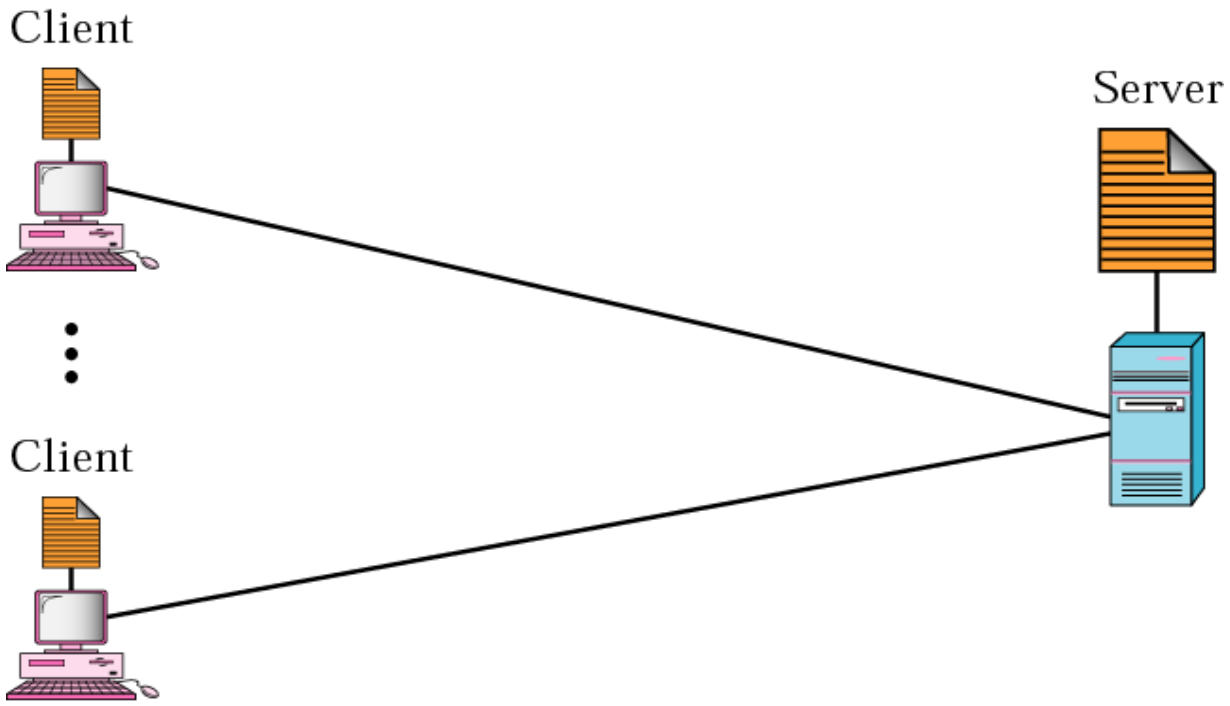
Application Layer : Application Services



Client Server Model : Generic Diagram



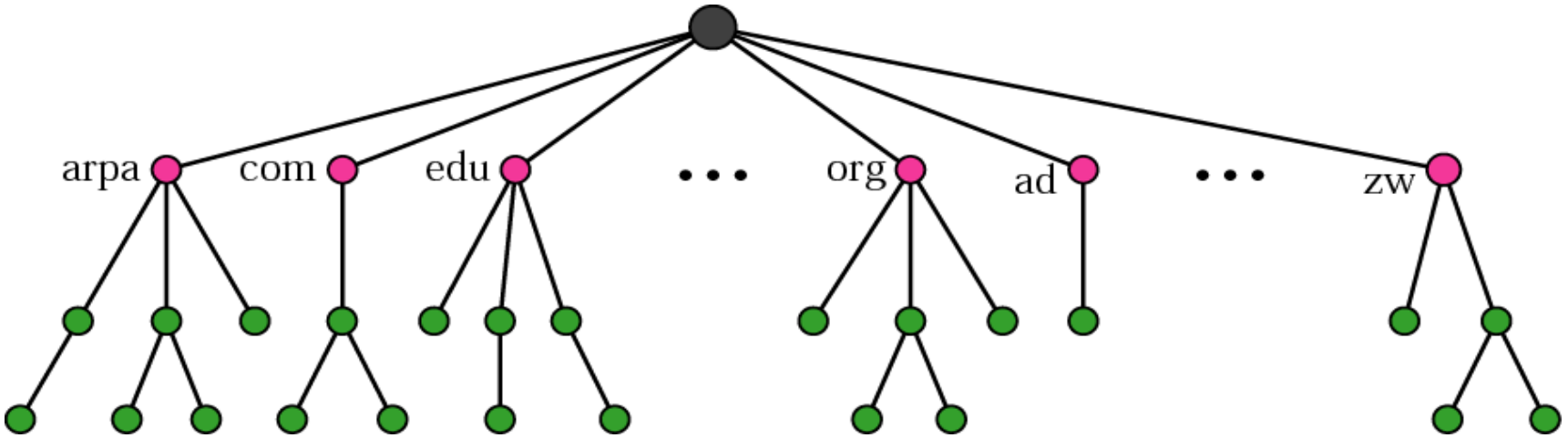
Client Server Relationship



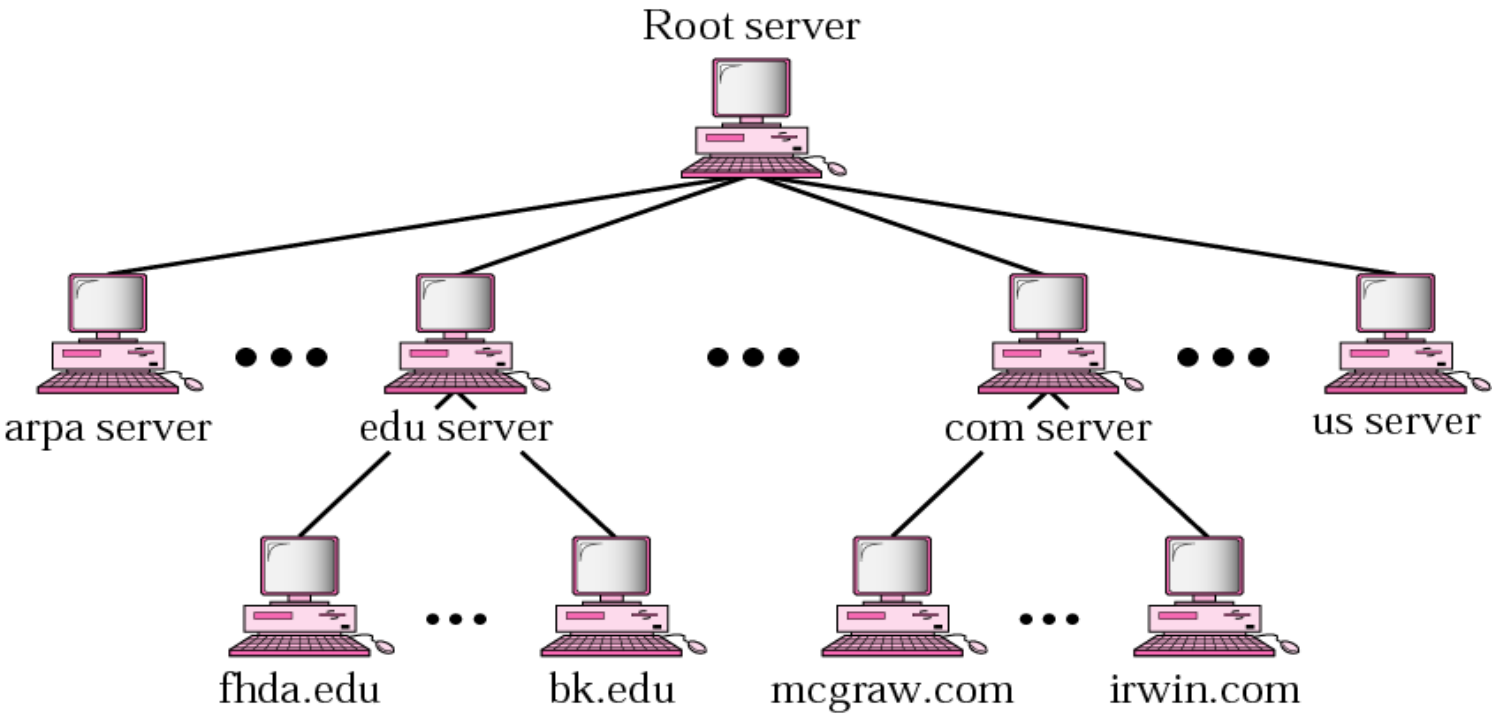
DNS : Domain Name System

- Hierarchical Naming System Built on a Distributed Database.
- Responsible to Translate Human Address into IP Address.
- Example => How To Verify ??

Domain Name System : Hierarchical Naming



Domain Name System : Hierarchy of Name Servers



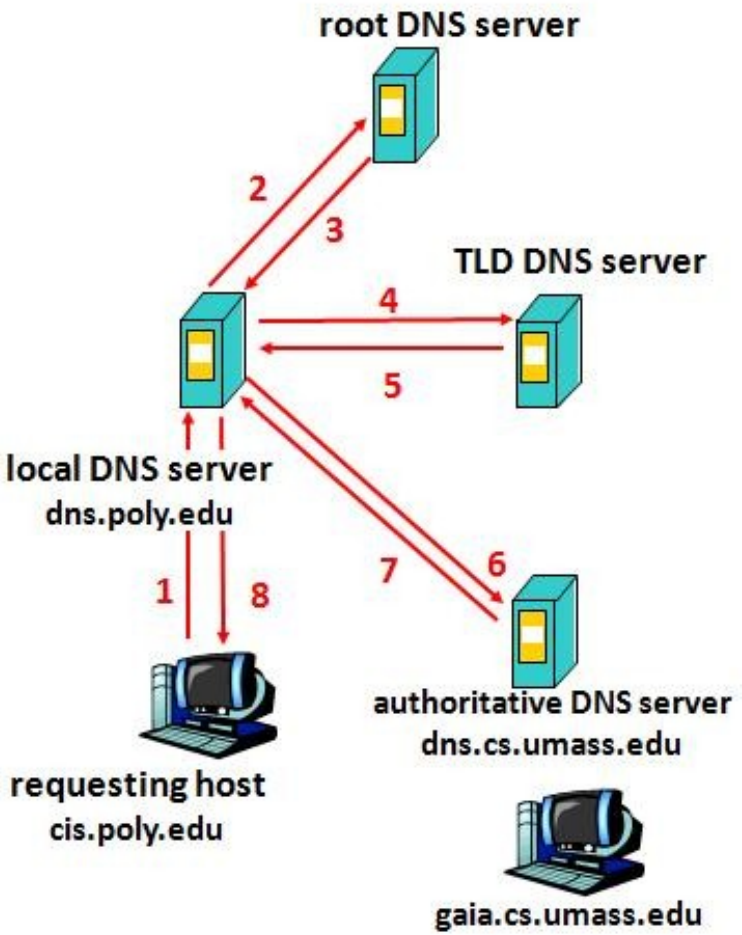
Domain Name System : Types

- Root Name Servers
  - ✓ Contracts Authoritative Name Server if Mapping Not Found.
  - ✓ Gets Mapping.
  - ✓ Returns Mapping to Local Name Server.
- Top Level Domain Servers
  - ✓ Responsible for com, org, net.
  - ✓ All top level Country domains like us, uk, fr, np, in.
- Authoritative Domain Servers
  - ✓ Organization’s DNS Servers.

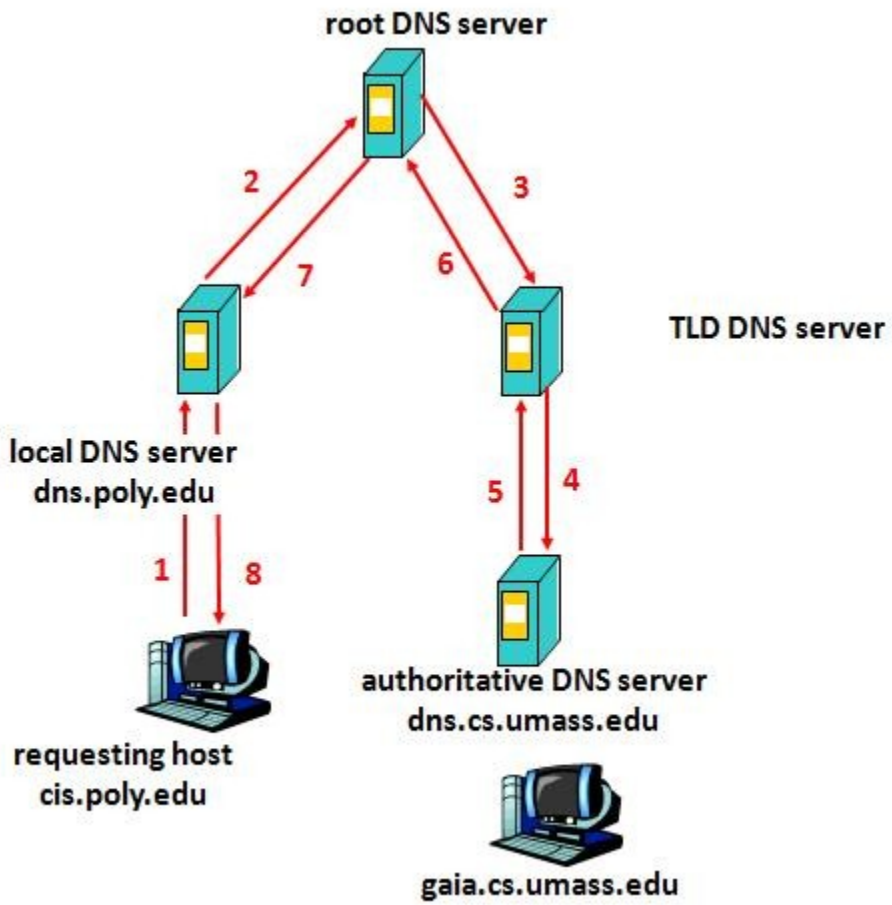
Domain Name Space : Root Name Servers

13 Root Name Servers Worldwide

DNS Name Resolution : Iterated Query



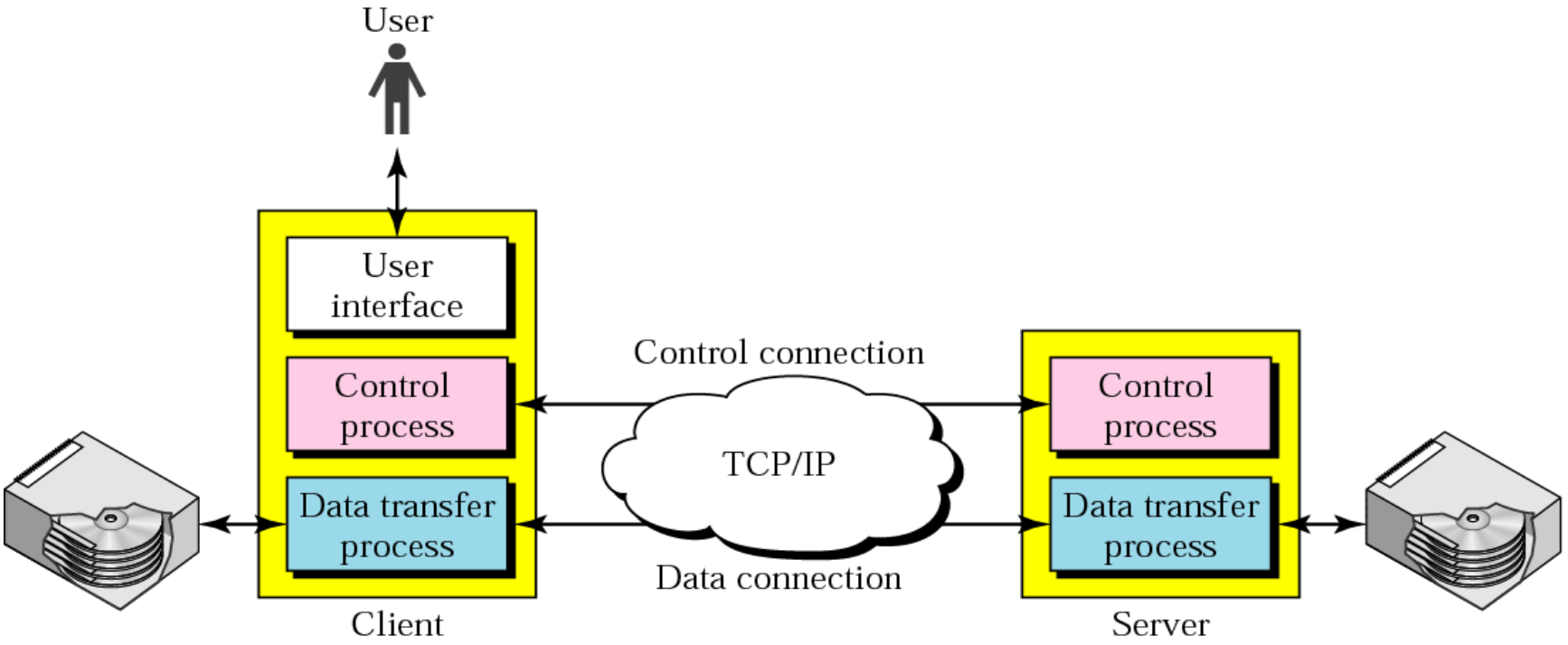
DNS Name Resolution : Recursive Query



FTP : File Transfer Protocol

- Protocol used to Copy File from One Host to Another.
- It uses the Services of TCP.
- It needs Two TCP Connections.
- The Well Known Port 21 is used for Control Connection.
- The Well Known Port 20 is used for Data Connection.

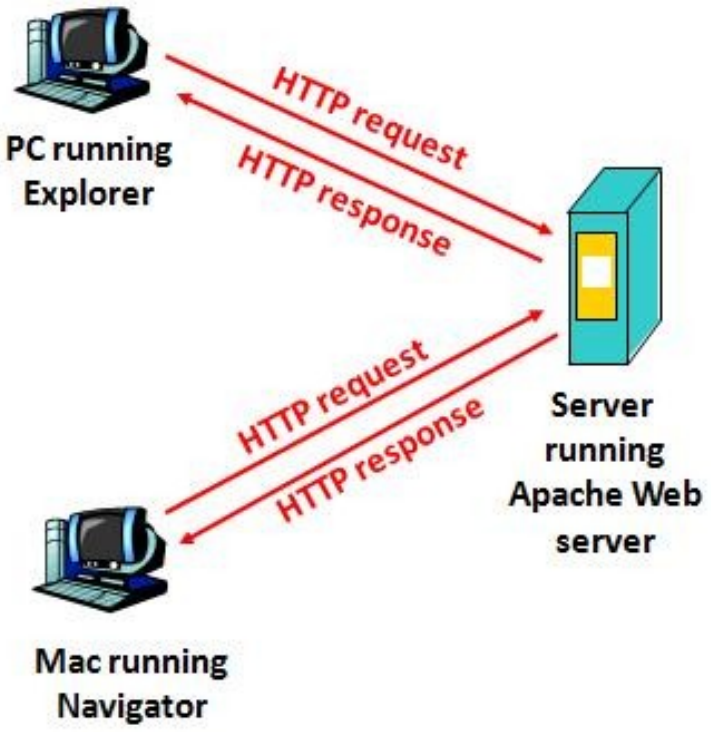
FTP : File Transfer Protocol



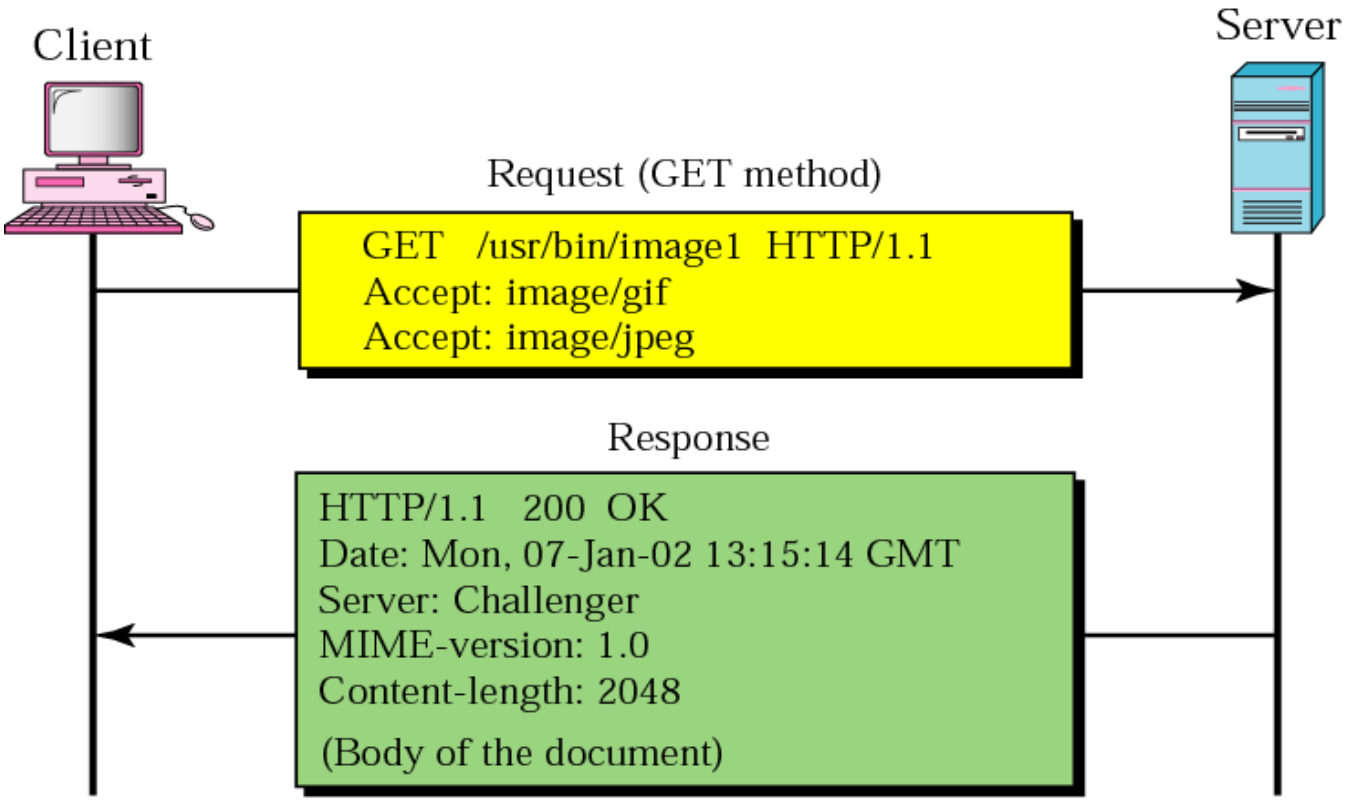
HTTP : Hyper Text Transfer Protocol

- Foundation of Data Communication For World Wide Web.
- HTTP Functions as Request/Response Protocol in Client Server Computing Model.
- Web Browser : Client
- Web Server : Apache Web Server
- HTTP is “Stateless” => No Information of Past Client Requests.
- HTTP Connections => Non Persistent and Persistent.

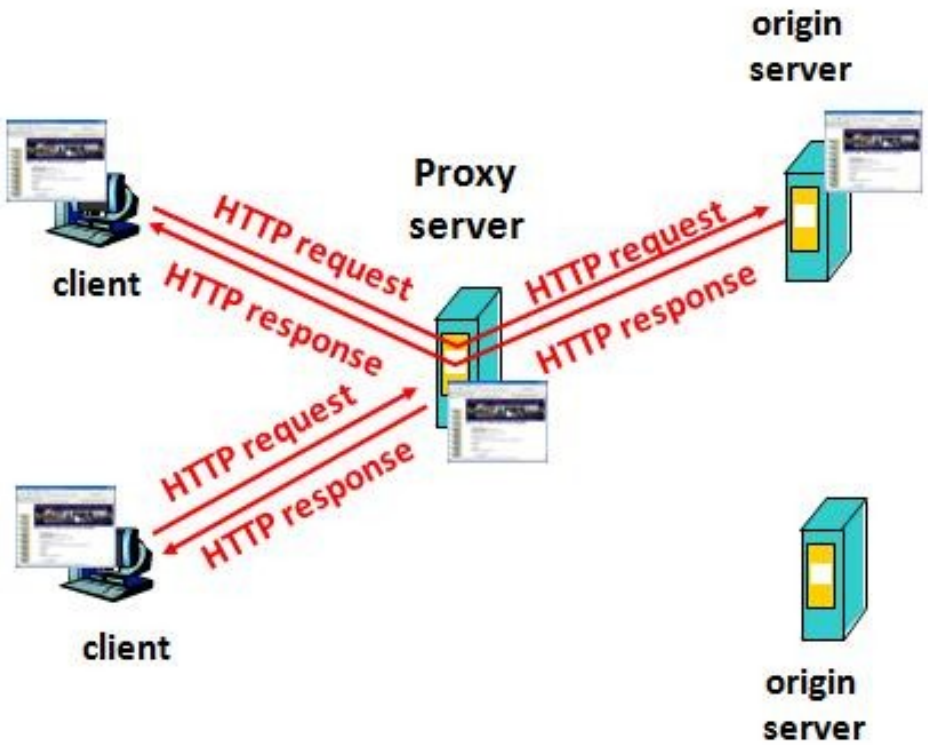
HTTP : Request/Response Protocol



HTTP : Request/Response Example

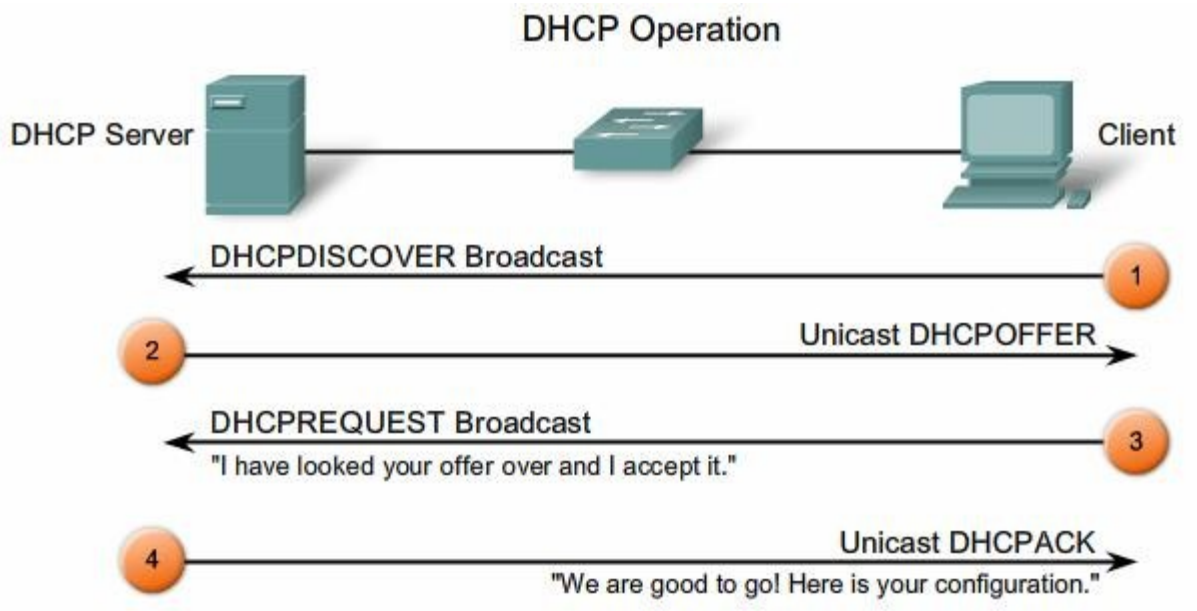


Proxy Server : Web Caching



Satisfy Client Request without Involving Origin Server

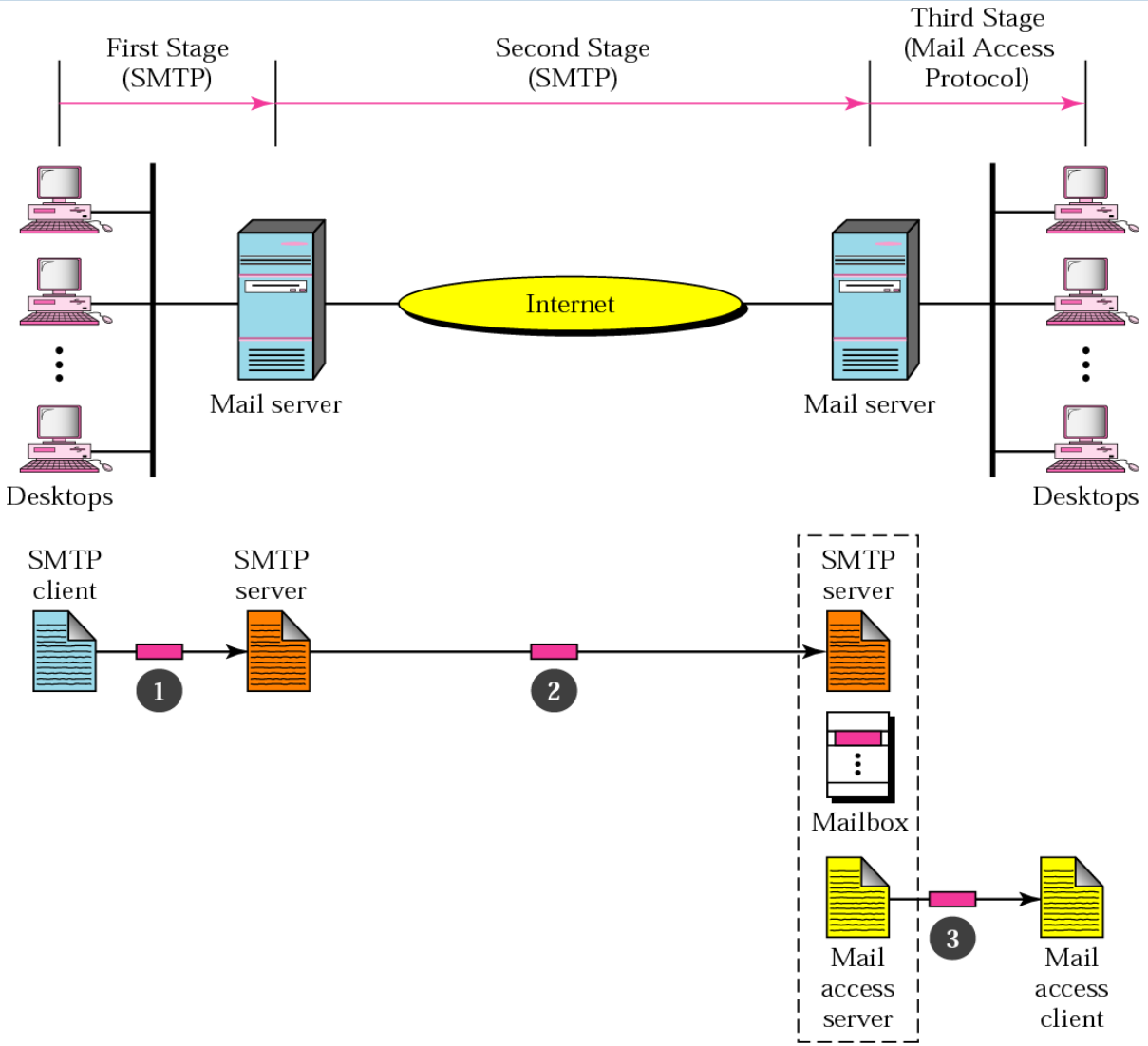
DHCP : Dynamic Host Configuration Protocol



SMTP : Simple Mail Transfer Protocol

- Internet Standard for Electronic Mail Transmission.
- It is Specified for Outgoing Mail Transport.
- Uses TCP Port No 25.
- For Receiving Messages Clients Use IMAP or POP.
  - ✓ IMAP : Internet Message Access Protocol
  - ✓ POP : Post Office Protocol

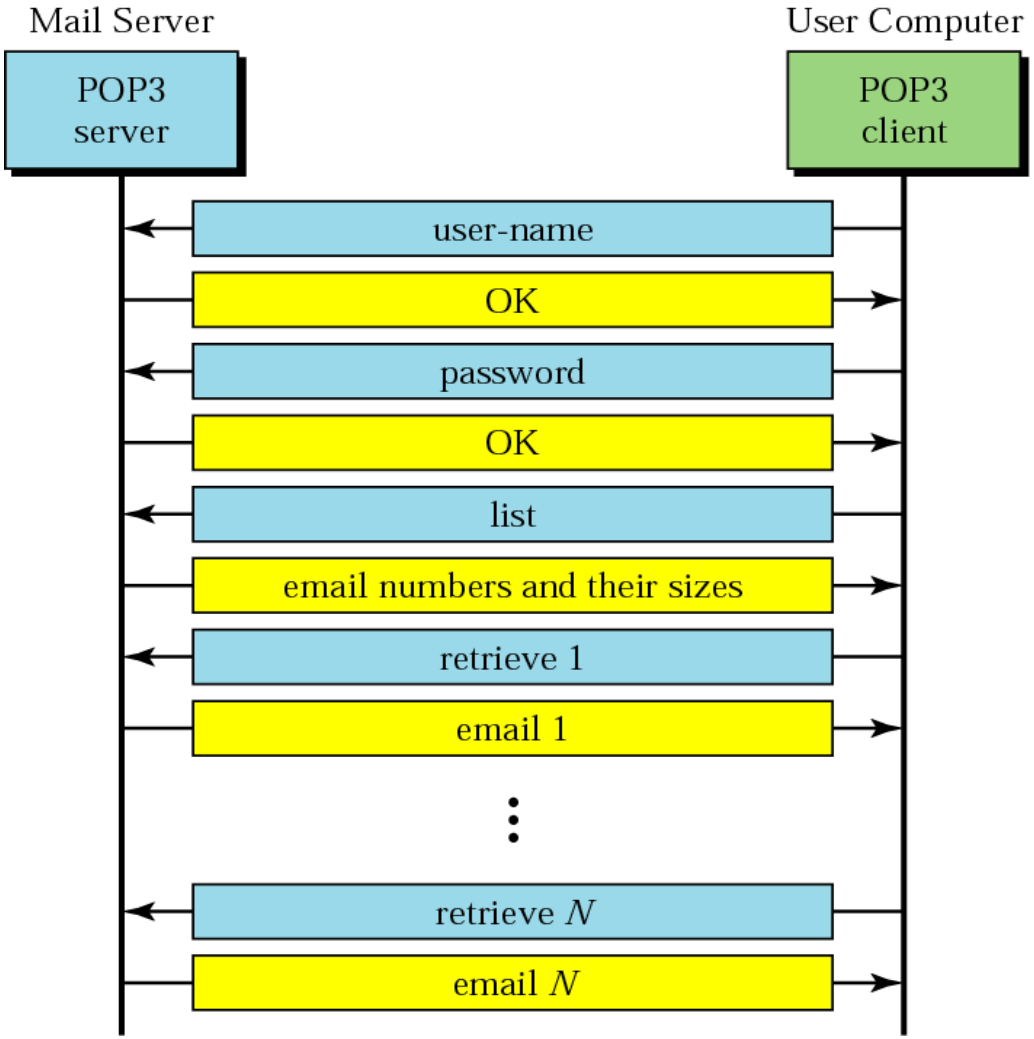
SMTP : Example



POP : Post Office Protocol

- Application Layer Protocol used by Email Clients to retrieve Email From Remote Server.
- POP Version 3 is referred as POP3.
- A POP3 Servers Listens on Well Know Port 110.
- Encryption Communication for POP3 Using SSL.
- It uses Well Known TCP Port 995 (Eg. Google Gmail).

POP3 : Post Office Protocol Version 3 (Steps)



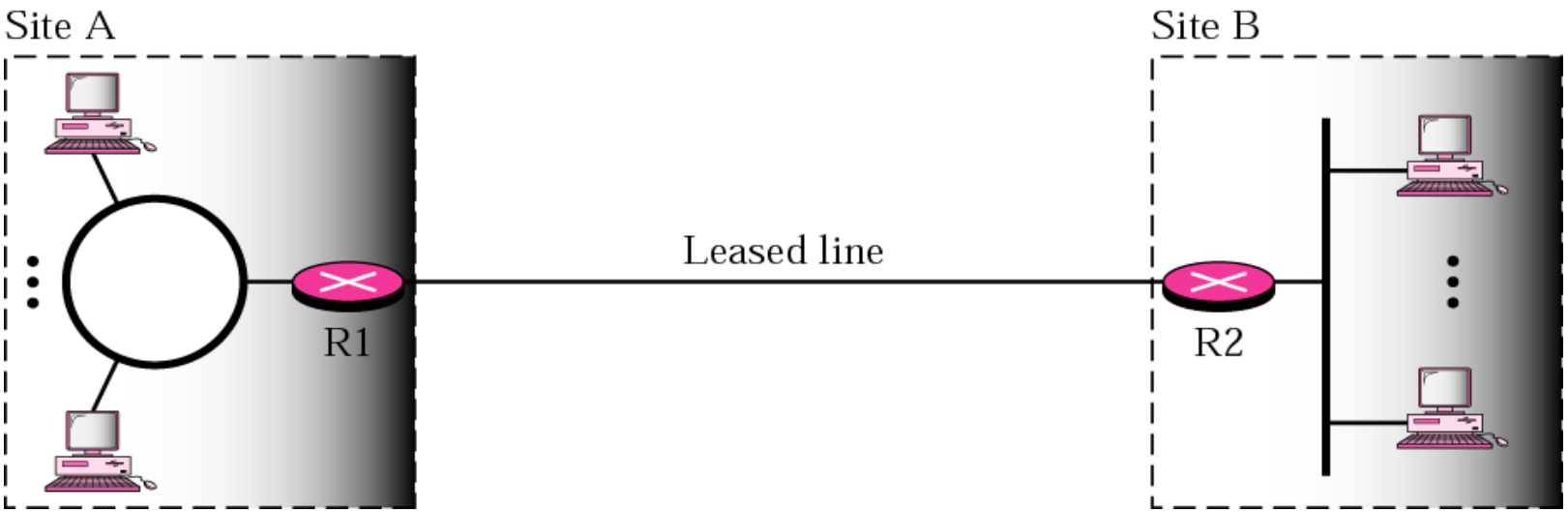
IMAP : Internet Message Access Protocol

- It is one of the Prevalent Application Layer Protocol for Email Retrieval.
- All Modern Email Clients and Servers Supports IMAP.
- An IMAP Server Listens at Port 143.
- IMAP4 is referred as IMAP Version 4.
- Multiple Clients can Simultaneously connect to Same Mailbox.
- It allows Connected and Disconnected Mode of Operation.
- Multiple Mailboxes on the Server.

Tools For Client Server:

- Web Servers and Clients
  - ✓ Apache Tomcat
  - ✓ Microsoft IIS
  - ✓ Oracle Web Tier

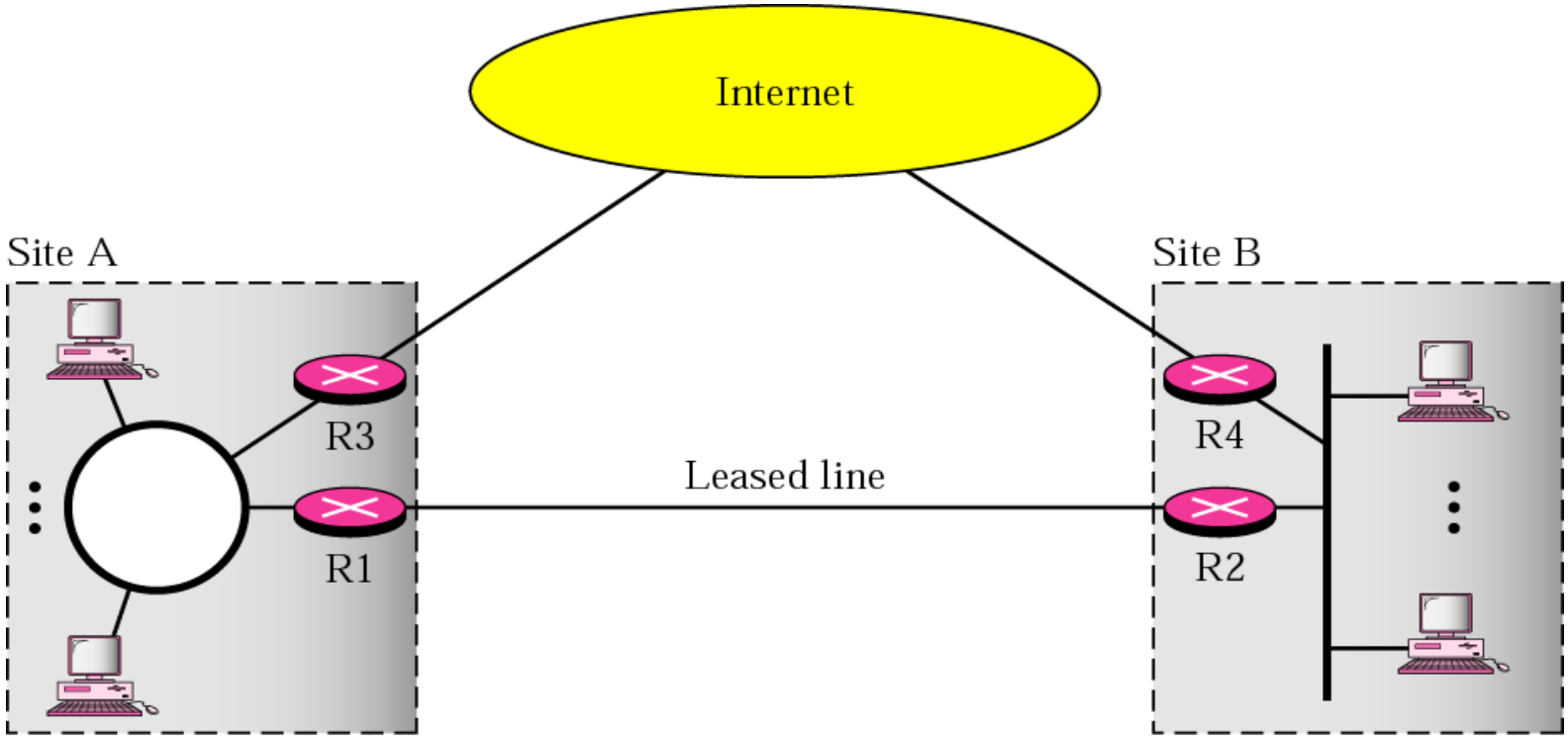
Private Networks



Hybrid Networks : What it is ??

- Two Links => Private and Public
- Private Link => Leased Line or Optical Fiber
- Private Link for Intranet
- Public Link for Internet.
- All Intraorganization data are routed through the Private Link.
- All Interorganization data are routed through the Public Link.

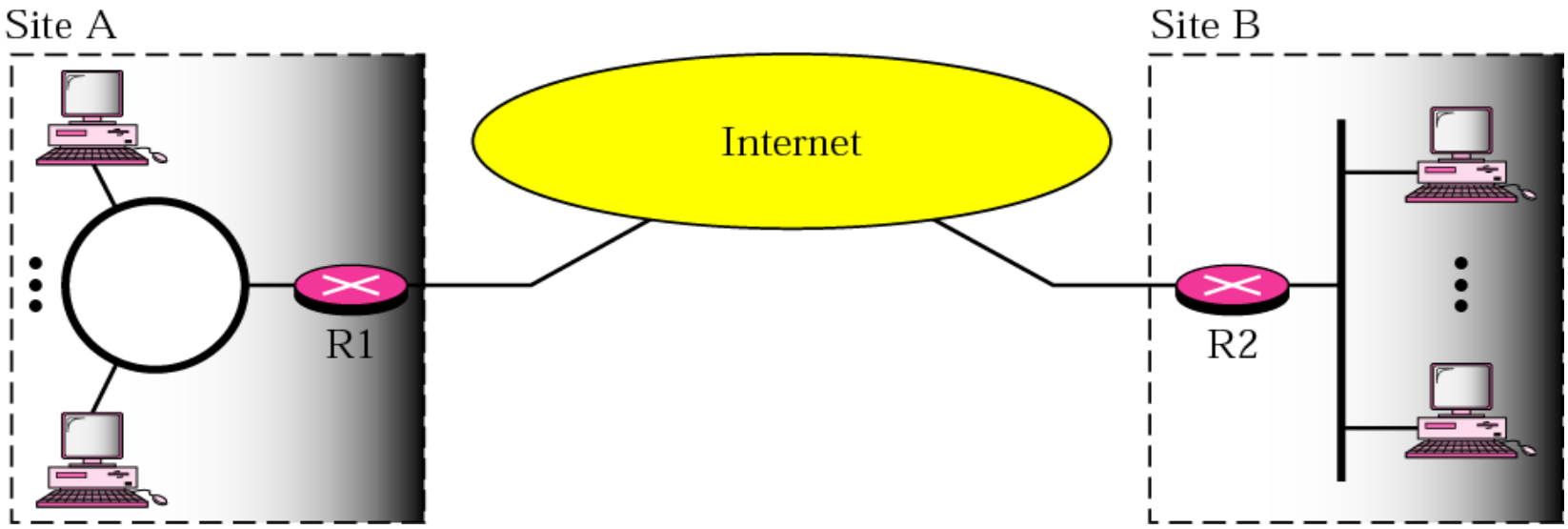
Hybrid Networks



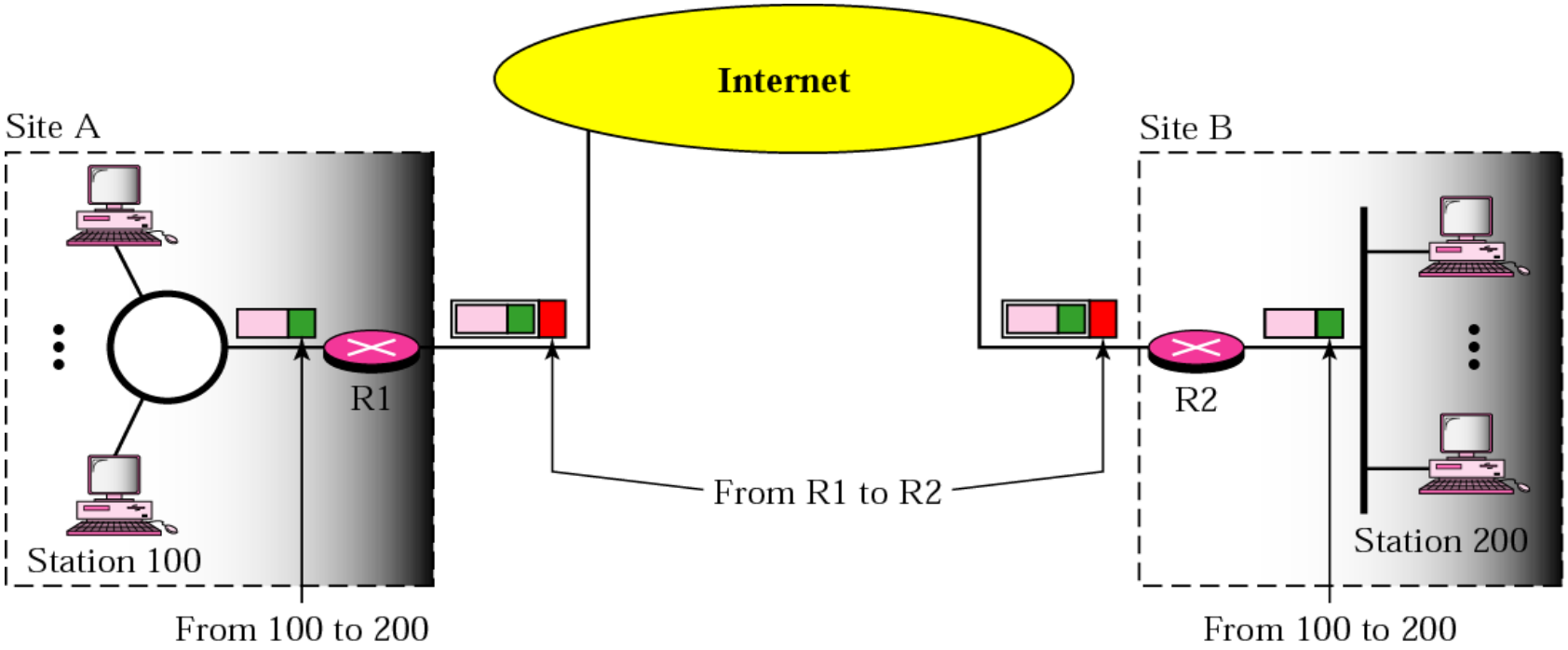
VPN : Virtual Private Networks

- Both Private and Hybrid Networks are Expensive.
- Solution to use global Internet for both Private and Public Communication => VPN
- VPN Creates a Network that is Private but Virtual.
- It is Private because it guarantees Privacy inside the Organization.
- It is Virtual because it does not use Real Private WANs.
- The Network is Physically Public but Virtually Private.
- VPN Use IPSec in the Tunnel Mode to Provide Authentication, Integrity and Privacy.

VPN：Virtual Private Networks



Addressing in VPN



To use IPSec in Tunneling mode VPN need to use Two sets of Addressing

Thank You