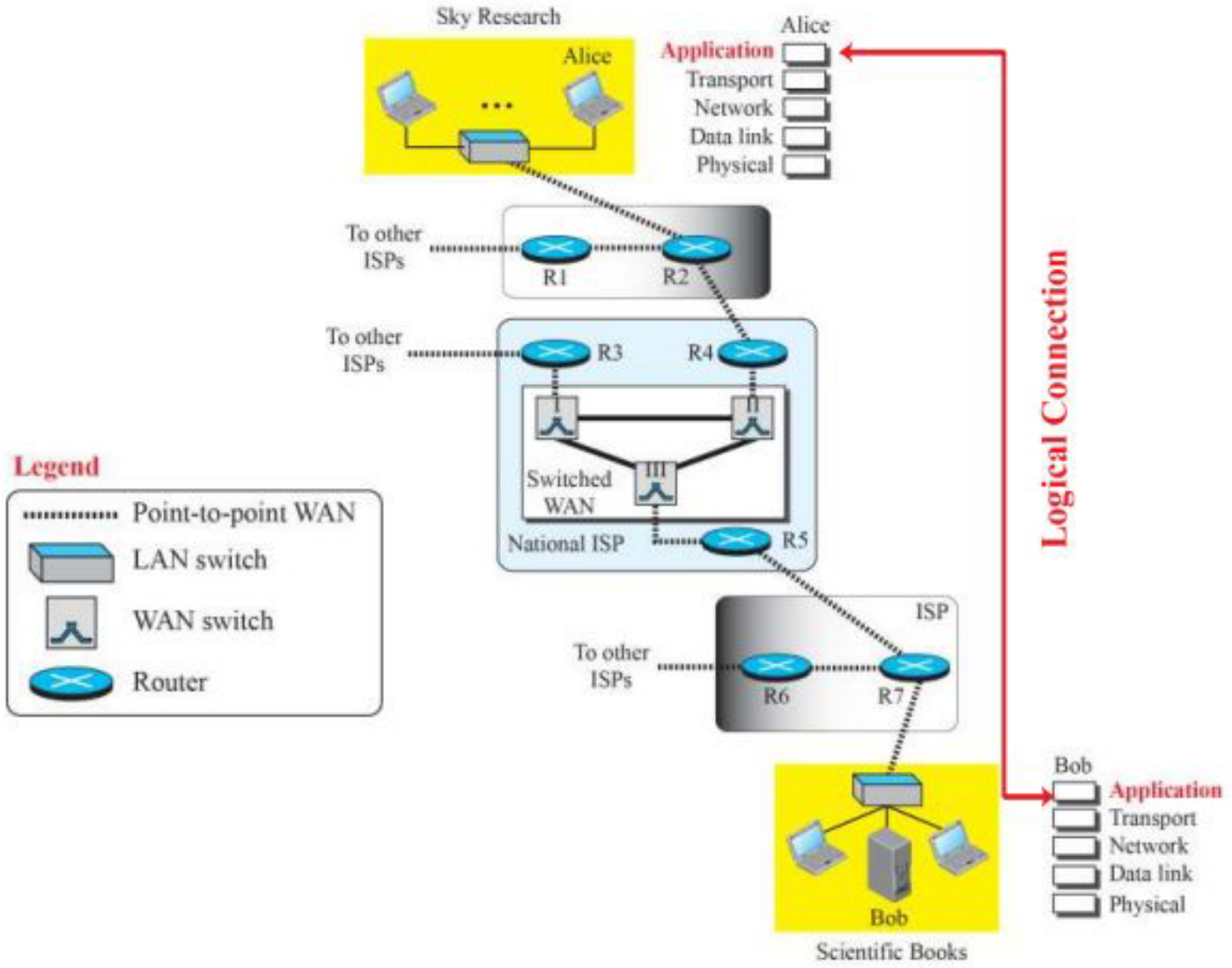
Application Layer

Client Server Paradigm: Communication using TCP and UDP

Peer to Peer Paradigm, Application Layer Protocols :Domain Name System (DNS), Hyper Text Transfer Protocol (HTTP), Email: SMTP, MIME, POP3, Webmail, FTP,TFTP, TELNET, Dynamic Host Control Protocol (DHCP), Simple Network Management Protocol (SNMP) .

Figure 25.1: Logical connection at the application layer



Providing Services

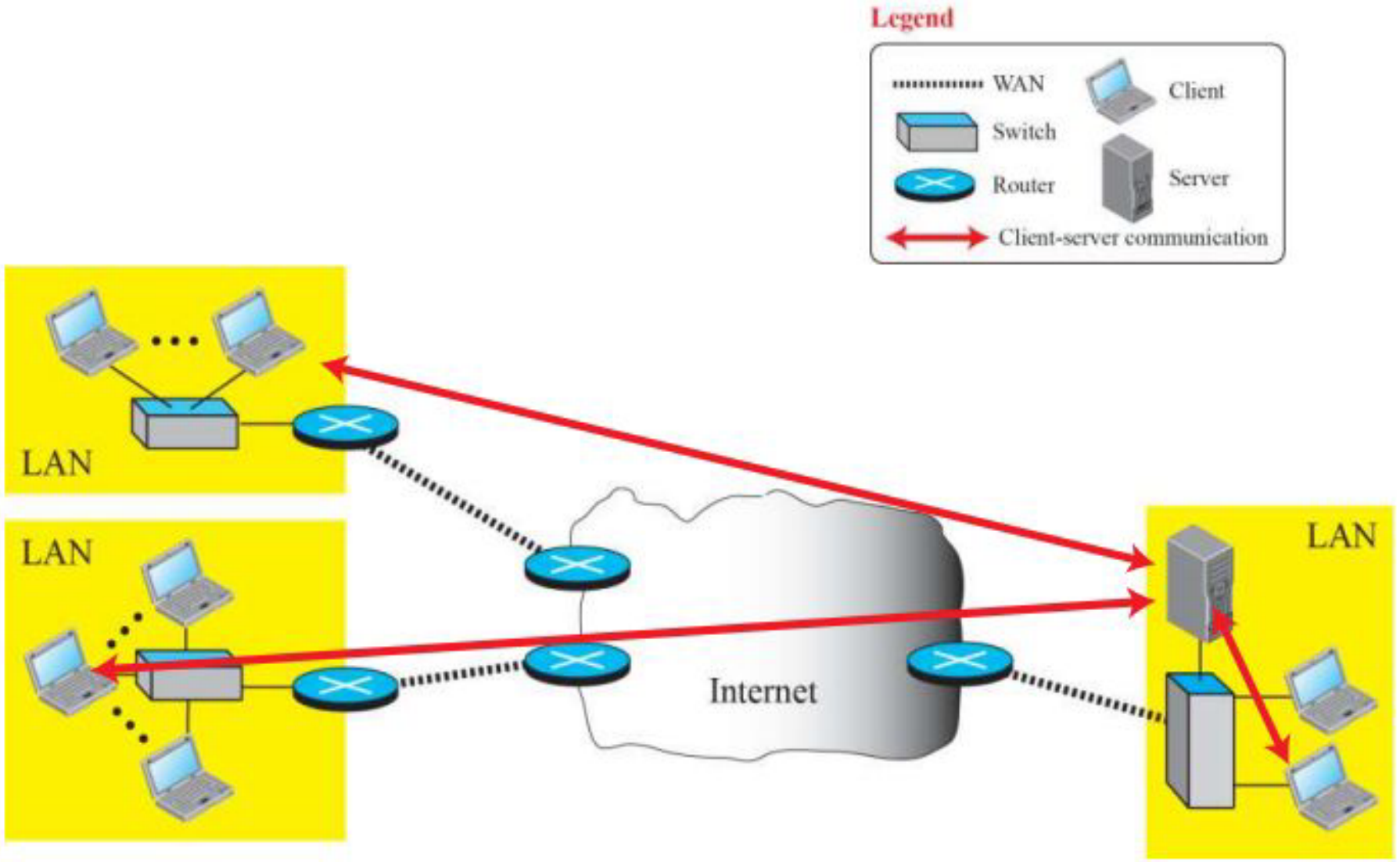
- The application layer provides services to the user.
- Communication is provided using a logical connection, which means that the two application layers assume that there is an imaginary direct connection through which they can send and receive messages. Figure 25.1 shows the idea behind this logical connection

- All communication networks that started before the Internet were designed to provide services to network users.
- For example, the telephone network was originally designed to provide voice service: to allow people all over the world to talk to each other.
- This network, however, was later used for some other services, such as facsimile (fax), enabled by users adding some extra hardware at both ends

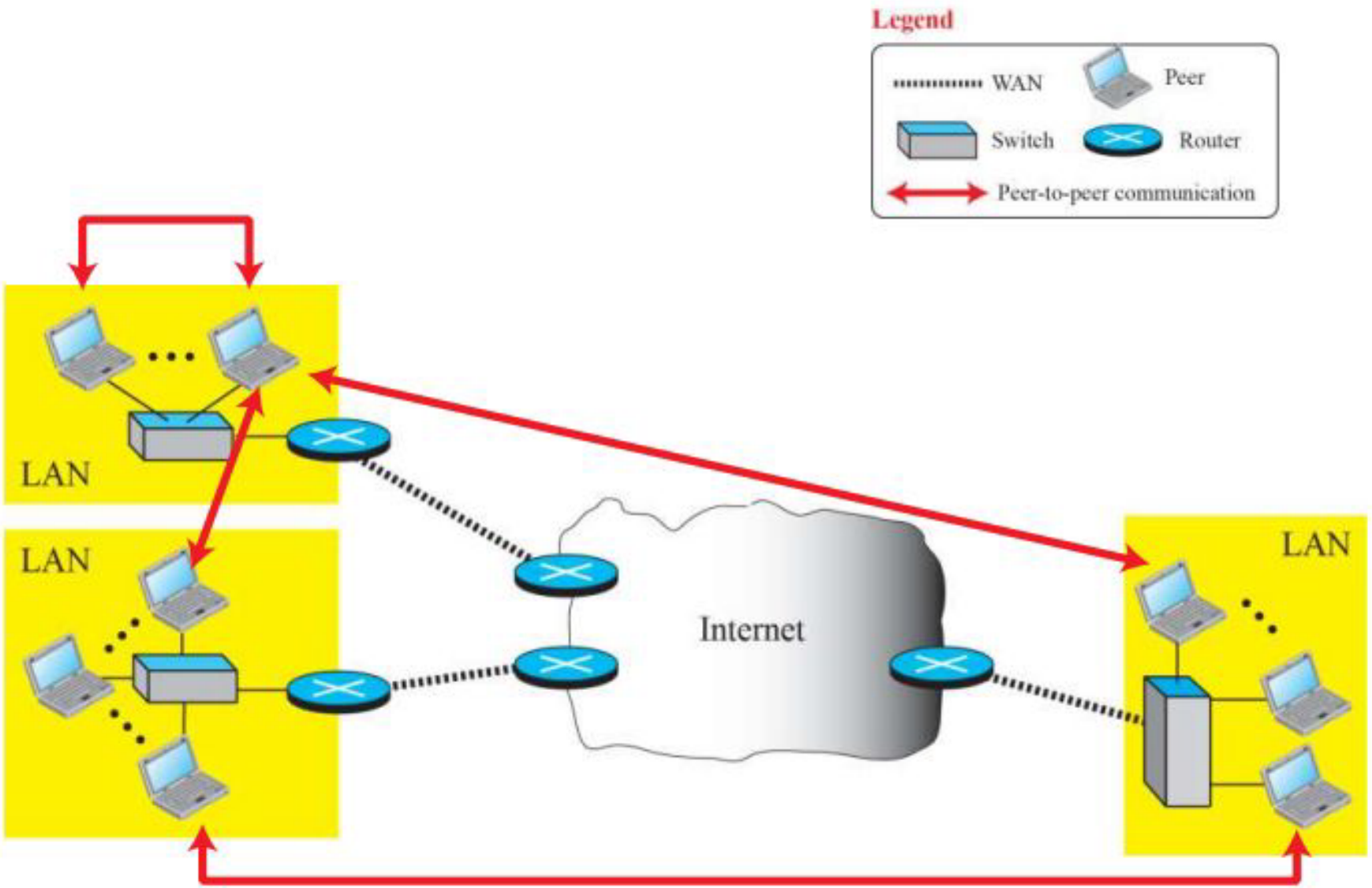
Application-Layer Paradigms

- It should be clear that to use the Internet we need two application programs to interact with each other: one running on a computer somewhere in the world, the other running on another computer somewhere else in the world.
- The two programs need to send messages to each other through the Internet infrastructure.
- However, we have not discussed what the relationship should be between these programs.
- Two paradigms have been developed : the client-server paradigm and the peer to-peer paradigm.

Example of a client-server paradigm



Example of a peer-to-peer paradigm



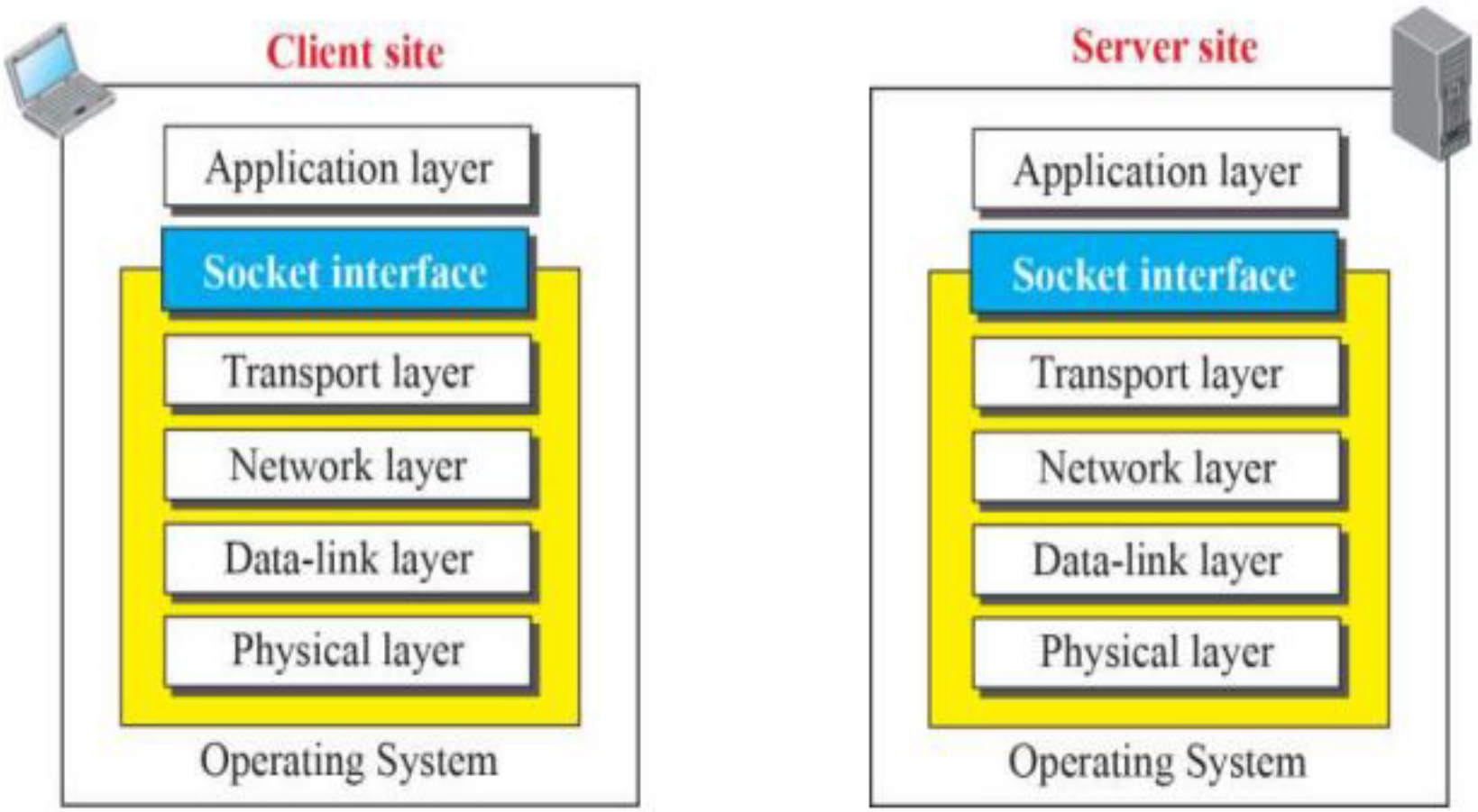
CLIENT-SERVER PROGRAMMING

- In this paradigm, communication at the application layer is between two running application programs called processes: a client and a server. A client is a running program that initializes the communication by sending a request; a server is another application program that waits for a request from a client.

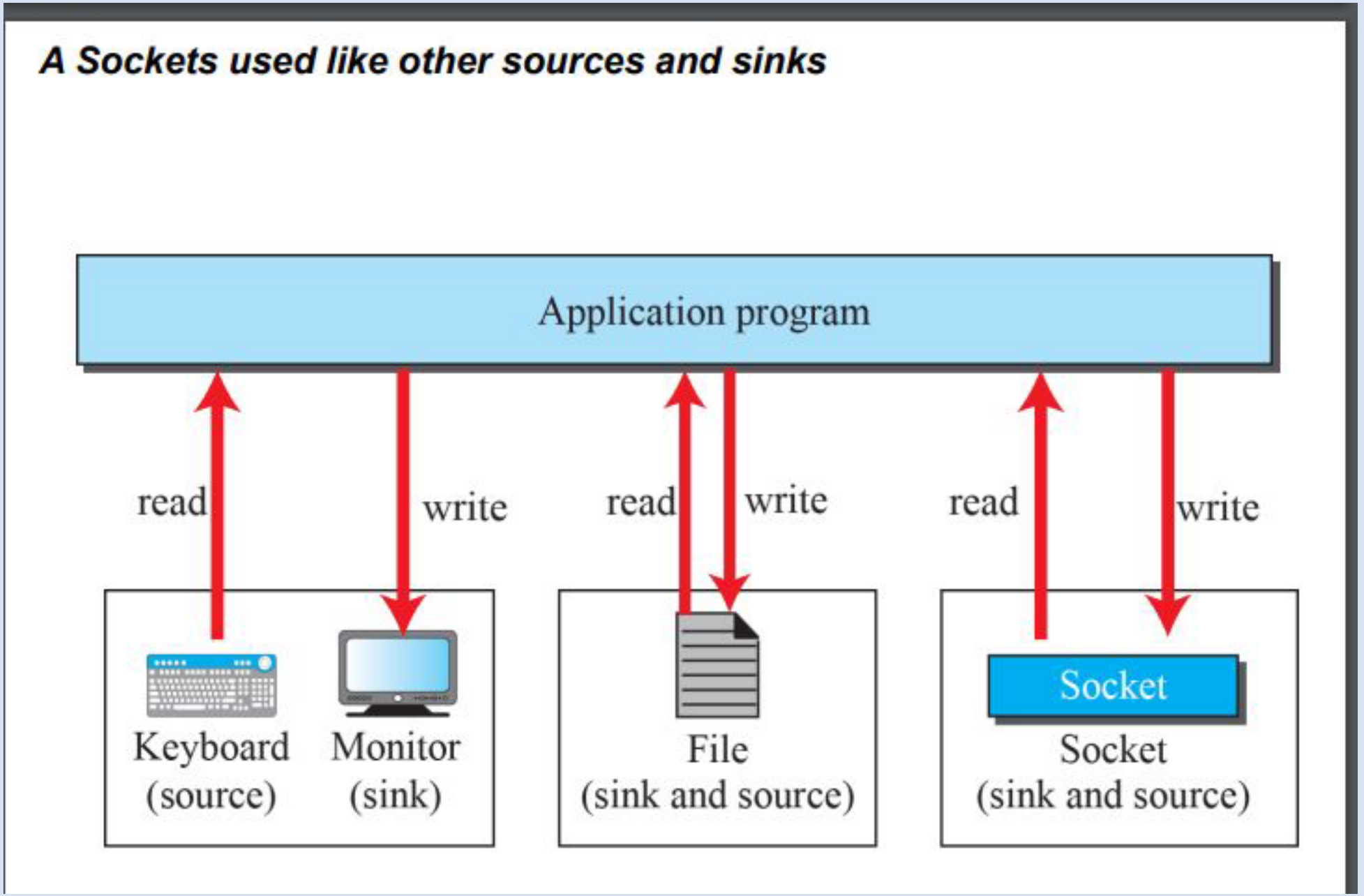
API

- How can a client process communicate with a server process? A computer program is normally written in a computer language with a predefined set of instructions that tells the computer what to do. If we need a process to be able to communicate with another process, we need a new set of instructions to tell the lowest four layers of the TCP/IP suite to open the connection, send and receive data from the other end, and close the connection. A set of instructions of this kind is normally referred to as an application programming interface (API)

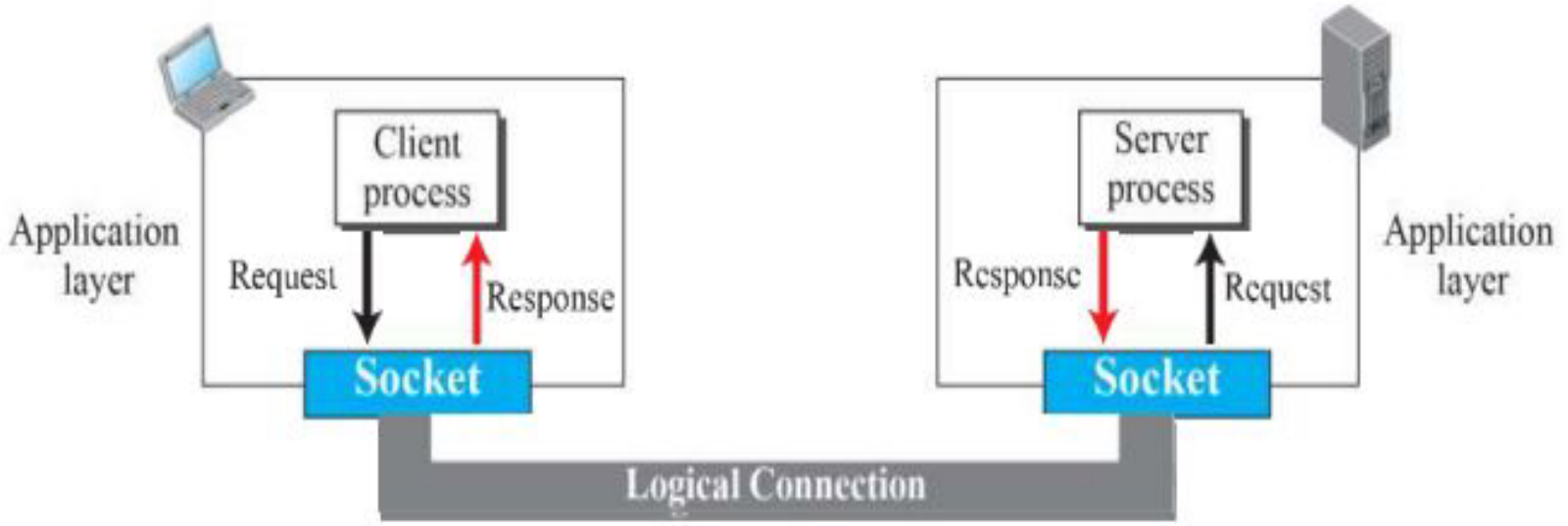
Position of the socket interface



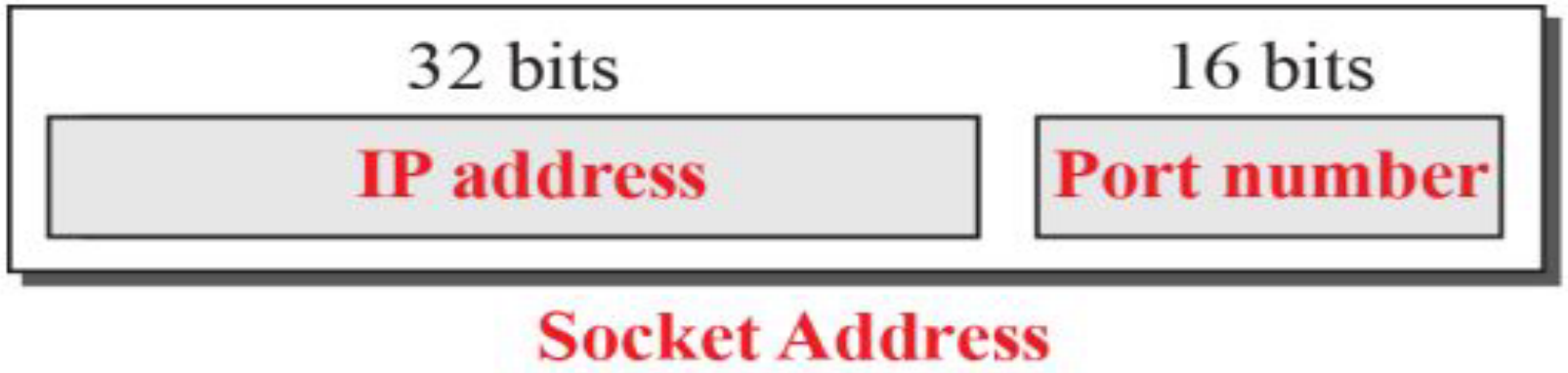
A Sockets used like other sources and sinks



Use of sockets in process-to-process communication



A socket address



An application layer protocol

- An application layer protocol defines how application processes (clients and servers), running on different end systems, pass messages to each other. In particular, an application layer protocol defines:
- The types of messages, e.g., request messages and response messages.
- The syntax of the various message types, i.e., the fields in the message and how the fields are delineated.
- The semantics of the fields, i.e., the meaning of the information that the field is supposed to contain;
- Rules for determining when and how a process sends messages and responds to messages.

Application Type	Application-layer protocol	Transport Protocol
Electronic mail	Send: Simple Mail Transfer Protocol SMTP [RFC 821]	TCP 25
	Receive: Post Office Protocol v3 POP3 [RCF 1939]	TCP 110
Remote terminal access	Telnet [RFC 854]	TCP 23
World Wide Web (WWW)	HyperText Transfer Protocol 1.1 HTTP 1.1 [RFC 2068]	TCP 80
File Transfer	File Transfer Protocol FTP [RFC 959]	TCP 21
	Trivial File Transfer Protocol TFTP [RFC 1350]	UDP 69
Remote file server	NFS [McKusik 1996]	UDP or TCP
Streaming multimedia	Proprietary (e.g., Real Networks)	UDP or TCP
Internet telephony	Proprietary (e.g., Vocaltec)	Usually UDP

- **SMTP (Simple Mail Transfer Protocol):**One of the most popular network service is electronic mail (e-mail).
- The TCP/IP protocol that supports electronic mail on the Internet is called Simple Mail Transfer Protocol (SMTP).
- SMTP transfers messages from senders' mail servers to the recipients' mail servers using TCP connections.
- Users based on e-mail addresses.
- SMTP provides services for mail exchange between users on the same or different computers.
- Following the client/server model:
  - SMTP has two sides: a client side which executes on a sender's mail server, and server side which executes on recipient's mail server.
  - Both the client and server sides of SMTP run on every mail server.
  - When a mail server sends mail (to other mail servers), it acts as an SMTP client.
  - When a mail server receives mail (from other mail servers) it acts as an SMTP server.

TELNET (Terminal Network):

- TELNET is client-server application that allows a user to log onto remote machine and lets the user to access any application program on a remote computer.
- TELNET uses the NVT (Network Virtual Terminal) system to encode characters on the local system.
- On the server (remote) machine, NVT decodes the characters to a form acceptable to the remote machine.
- TELNET is a protocol that provides a general, bi-directional, eight-bit byte oriented communications facility.
- Many application protocols are built upon the TELNET protocol
- Telnet services are used on PORT 23.

FTP (File Transfer Protocol):

- FTP is the standard mechanism provided by TCP/IP for copying a file from one host to another.
- FTP differs form other client-server applications because it establishes 2 connections between hosts.
- Two connections are: Data Connection and Control Connection.
- Data Connection uses PORT 20 for the purpose and control connection uses PORT 21 for the purpose.
- FTP is built on a client-server architecture and uses separate control and data connections between the client and the server.
- One connection is used for data transfer, the other for control information (commands and responses).
- It transfer data reliably and efficiently.

Multipurpose Internet Mail Extensions (MIME):

- It is an extension of SMTP that allows the transfer of multimedia messages.
- If binary data is included in a message MIME headers are used to inform the receiving mail agent:
  - Content-Transfer-Encoding: Header alerts the receiving user agent that the message body has been ASCII encoded and the type of encoding used.
  - Content-Type: Header informs the receiving mail agent about the type of data included in the message.

POP (Post Office Protocol):

- POP is also called as POP3 protocol.
- This is a protocol used by a mail server in conjunction with SMTP to receive and holds mail for hosts.
- POP3 mail server receives e-mails and filters them into the appropriate user folders. When a user connects to the mail server to retrieve his mail, the messages are downloaded from mail server to the user's hard disk.

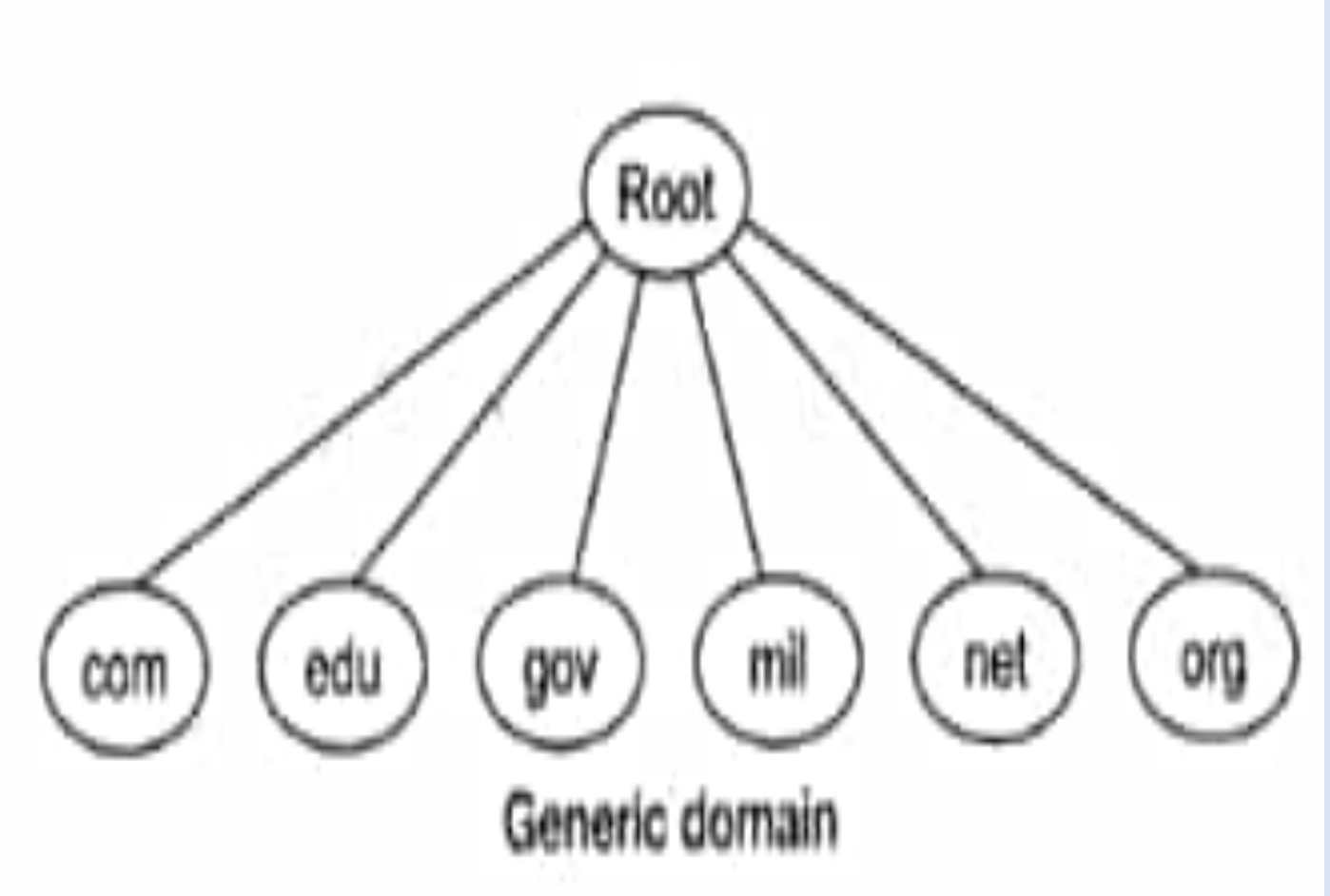
HTTP (Hypertext Transfer Protocol):

- This is a protocol used mainly to access data on the World Wide Web (www).
- The Hypertext Transfer Protocol (HTTP) the Web's main application-layer protocol although current browsers can access other types of servers
- A repository of information spread all over the world and linked together.
- The HTIP protocol transfer data in the form of plain text, hyper text, audio, video and so on.
- HTTP utilizes TCP connections to send client requests and server replies.
- it is a synchronous protocol which works by making both persistent and non persistent connections.

Domain Name System (DNS):

- To identify an entity, TCP/IP protocol uses the IP address which uniquely identifies the connection of a host to the Internet.
- DNS is a hierarchical system, based on a distributed database, that uses a hierarchy of Name Servers to resolve Internet host names into the corresponding IP addresses required for packet routing by issuing a DNS query to a name server.
- However, people refer to use names instead of address. Therefore, we need a system that can map a name to an address and conversely an address to name.
- In TCP/IP, this is the domain name system.
- DNS in the Internet: DNS is protocol that can be used in different platforms.

- Domain name space is divided into three categories.
- **Generic Domain:** The generic domain defines registered hosts according, to their generic behaviour. Each node in the tree defines a domain which is an index to the domain name space database.



- **Country Domain:** The country domain section follows the same format as the generic domain but uses 2 characters country abbreviations (e.g., US for United States) in place of 3 characters.
- **Inverse Domain:** The inverse domain is used to map an address to a name.

Dynamic Host Control Protocol (DHCP)

- It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts. There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. Port number for DHCP is 67, 68.
- Dynamic Host Configuration Protocol(DHCP) is an application layer protocol which is used to provide:

- Subnet Mask (Option 1 – e.g., 255.255.255.0)
- Router Address (Option 3 – e.g., 192.168.1.1)
- DNS Address (Option 6 – e.g., 8.8.8.8)
- Vendor Class Identifier (Option 43 – e.g., ‘unifi’ = 192.168.1.9 ##where unifi = controller)
- DHCP is based on a client-server model and based on discovery, offer, request, and ACK.
- DHCP port number for server is 67 and for the client is 68. It is a Client server protocol which uses UDP services. IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process.

- **Advantages –** The advantages of using DHCP include:

- centralized management of IP addresses
- ease of adding new clients to a network
- reuse of IP addresses reducing the total number of IP addresses that are required
- simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client
-
- The DHCP protocol gives the network administrator a method to configure the network from a centralized area.
  With the help of DHCP, easy handling of new users and reuse of IP address can be achieved.
- **Disadvantages –** Disadvantage of using DHCP is:

- IP conflict can occur

Simple Network Management Protocol (SNMP) .

- If an organization has 1000 devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used
- It stands for Simple Network Management Protocol. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. It is a way that servers can share information about their current state, and also a channel through which an administrate can modify pre-defined values. The Port number of SNMP is 161(TCP) and 162(UDP).

SNMP components –

- There are 3 components of SNMP:

- **SNMP Manager –**
  It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)

- **SNMP agent –**
  It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.

- **Management Information Base –**
  MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables

- **SNMP messages –**
  Different variables are:

- **GetRequest –**
  SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.

- **GetNextRequest –**
  This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.

- **GetBulkRequest –**
  This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.

- **SetRequest –**
  It is used by the SNMP manager to set the value of an object instance on the SNMP agent.

- **Response –**
  It is a message sent from the agent upon a request from the manager. When sent in response to Get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.

- **Trap –**
  These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.

- **InformRequest –**
  It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn’t provide.

- **SNMP security levels –**
  It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

- **noAuthNoPriv –**
  This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.

- **authNopriv –** This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.

- **authPriv –** This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses the DES-56 algorithm.