# INDIAN SCHOOLMUSCAT

## CLASS XI

## INFORMATION TECHNOLOGY(802)

## Chapter - 2 : Networking and Internet

**Teacher:** Saju Jagannath

# Some points to keep in mind…..

- Please avoid login from multiple systems.
- Kindly logout at the end of the session.
- Please turn off your mic and webcam
- If you have any doubt, write in the chat box
- If there is any technical problem, hold on – we will be back
- Since it is a lockdown situation you can use rough notebook or notepad or sheets of paper to take down notes. You may take screenshots during the course of delivery of topics.

# TCP/IP Model (4 – Layers)

| |
|---|
| APPLICATION LAYER (HTTP, FTP, SMTP, …) |
| TRANSPORT LAYER (TCP, UDP, …) |
| INTERNET LAYER (IP,ICMP,ARP,…) |
| LINK LAYER (Ethernet, Wifi, …) |

# APPLICATION LAYER

**APPLICATION LAYER:** Data/message is created at the sender's end at Application layer. At the receiving end it is examined and processed (possibly displayed) at Application layer. This layer is also responsible for enveloping the message to be sent with the header. Several protocols such as HTTP, SMTP, POP3, and TELNET (remote login) operate on this layer.

# TRANSPORT LAYER

**TRANSPORT LAYER:** Application layer passes the message to the Transport layer which appends the information about the source and destination ports of the processes at two ends. At the ends, the ports process the message. Mainly two end-to end protocols operate at this layer, namely TCP and UDP.

# TRANSPORT LAYER Continued…

TCP (Transmission Control Protocol) is a reliable connection-oriented protocol needed when timely and error free delivery of data is important.

UDP (User Datagram Protocol) is an unreliable connectionless protocol needed in a scenario such as exchange of short messages and client server request-reply messages, where immediate response is more important rather than assured delivery.

# TRANSPORT LAYER Continued…

Further, transport layer divides the message into a number of fragments, called segments, depending upon the maximum transmission size permitted.
In TCP, each segment will carry the sequence number denoting its relative position in the message, so that, the message can be assembled at the receiver end by the transport layer at recipient's end.

# INTERNET LAYER

**INTERNET LAYER:** Transport layer hands over the segments to the Internet layer which adds source and destination machine network address (also termed IP address). Internet layer is mainly responsible for packet routing and injects packets into the network that may take independent path to the destination, and thus may arrive out of order at the destination.

# INTERNET LAYER Continued…

At the receiving layer, message is reassembled in the correct order. In the Internet layer, Internet Protocol (IP) is used. IP defines the format of packets exchanged over the Internet. This protocol is usually accompanied by three other protocols, namely, Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), and Dynamic Host Configuration Protocol (DHCP).

# LINK LAYER

**LINK LAYER** is also called Host to Internet layer. This layer is responsible for adding the header containing sender and receiver physical address to the packet received from Internet layer.

The resulting message is called frame. It may be noted that recipient's physical address corresponds to the physical address of the next host on the network to which message is to be relayed, and not (necessarily) the physical address of the destination machine.

Suppose host 1 wishes to send a message Hello to host 2. Diagram in Figure 2.19 illustrates how layer by layer message is processed at the host 1 and host 2.

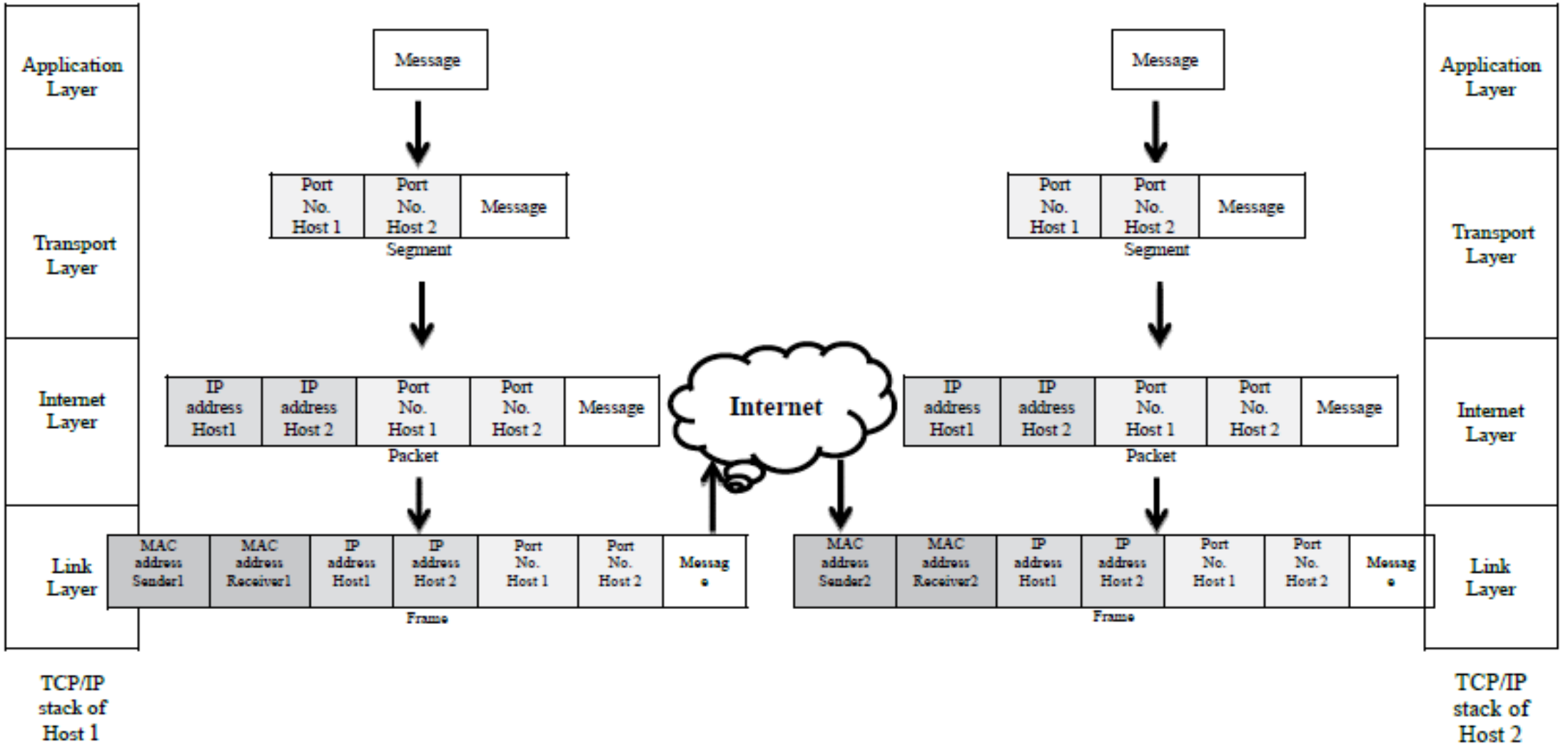


*Figure 2.19: Message transfer illustrated through TCP/IP Model*

# Network Safety Concerns

With increase in use of network for accessing data and resource sharing, security is becoming a prime concern. Large amount of data placed on the Internet and substantially increasing number of users are leading to security issues such as misuse of data, hacking, copyright issues and many more.

# Network Safety Concerns Continued….

**Malwares:** The term malware refers to malicious software (programs) designed with the intension to affect the normal functionality by causing harm to the system, or with the intension of getting unauthorized access to the system, or denying access to legitimate users of computing resources.

A malware may be virus, worm, Trojan horse, or spam.

# Network Safety Concerns Continued….

**Virus:** A virus is a software code that may harm your system by overwriting or corrupting the system files. A computer virus is similar in action to viruses in our body which replicate themselves and affect body cells. The affected part is called infected area.

# Network Safety Concerns Continued….

A computer virus may make several copies of it by inserting its code onto the system programs, files or boot sector of hard drives and thereby may corrupt them. This causes the system to slow down or even stop functioning.

The viruses are mainly categorized as boot sector virus, file infector virus, and macro virus.

# Network Safety Concerns Continued….

**Boot sector viruses** affect boot record of the disks. These are the memory resident viruses that embed themselves into the disk area and are activated when the drive is started (booted up),
for example, Michelangelo virus.

# Any Questions?