TCP/IP Model

TCP/IP MODEL

It is also called as the TCP/IP protocol suite. It is a collection of protocols.

IT is a hierarchical model, ie. There are multiple layers and higher layer protocols are supported by lower layer protocols.

It existed even before the OSI model was developed.

Originally had four layers (bottom to top):

1. Host to Network Layer
2. Internet Layer
3. Transport Layer
4. Application Layer

The figure for TCP/IP model is as follows:

Application
Transport
Network or IP
Host to Network

The structure TCP/IP model is very similar to the structure of the OSI reference model. The OSI model has seven layers where the TCP/IP model has four layers.

The Application layer of TCP/IP model corresponds to the Application Layer of Session, Presentation & Application Layer of OSI model.

The Transport layer of TCP/IP model corresponds to the Transport Layer of OSI model

The Network layer of TCP/IP model corresponds to the Network Layer of OSI model

The Host to network layer of TCP/IP model corresponds to the Physical and Datalink Layer of OSI model.

The diagram showing the comparison of OSI model and TCP/IP model along with the protocols is as shown below:

Fig: Comparison of OSI model and TCP/IP model Functions of the Layers of TCP/IP model:

A. Host to Network Layer

This layer is a combination of protocols at the physical and data link layers. It supports all standard protocols used at these layers.

B. Network Layer or IP

Also called as the Internetwork Layer (IP). It holds the IP protocol which is a network layer protocol and is responsible for source to destination transmission of data.

The Internetworking Protocol (IP) is an **connection-less** & **unreliable protocol.**

It is a best effort delivery service. i.e. there is no error checking in IP, it simply sends the data and relies on its underlying layers to get the data transmitted to the destination.

IP transports data by dividing it into **packets or datagrams** of same size. Each packet is independent of the other and can be transported across different routes and can arrive out of order at the receiver.

In other words, since there is no connection set up between the sender and the receiver the packets find the best possible path and reach the destination. Hence, the word **connection-less**.

The packets may get dropped during transmission along various routes. Since IP does not make any guarantee about the delivery of the data its call an **unreliable** protocol.

Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is required for transmitting data thereby giving maximum efficiency. Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where there is no error at all.

IP is a combination of four protocols:

1. ARP
2. RARP
3. ICMP
4. IGMP

1. ARP – Address Resolution Protocol

I. It is used to resolve the physical address of a device on a network, where its logical address is known.

II. Physical address is the 48 bit address that is imprinted on the NIC or LAN card, Logical address is the Internet Address or commonly known as IP address that is used to uniquely & universally identify a device.

2. RARP– Reverse Address Resolution Protocol

I. It is used by a device on the network to find its Internet address when it knows its physical address.

3. ICMP- Internet Control Message Protocol

I. It is a signaling mechanism used to inform the sender about datagram problems that occur during transit.

II. It is used by intermediate devices.

III. In case and intermediate device like a gateway encounters any problem like a corrupt datagram it may use ICMP to send a message to the sender of the datagram.

4. IGMP- Internet Group Message Protocol

I. It is a mechanism that allows to send the same message to a group of recipients.

C. Transport Layer

Transport layer protocols are responsible for transmission of data running on a process of one machine to the correct process running on another machine.

The transport layer contains three protocols:

1. TCP
2. UDP
3. SCTP

1. TCP – Transmission Control Protocol

I. TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted.

II. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.

2. UDP – User Datagram Protocol

I. UDP is a simple protocol used for process to process transmission.

II. It is an unreliable, connectionless protocol for applications that do not require flow control or error control.

III. It simply adds port address, checksum and length information to the data it receives from the upper layer.

3. SCTP – Stream Control Transmission Protocol

I. SCTP is a relatively new protocol added to the transport layer of TCP/IP protocol suite.

II. It combines the features of TCP and UDP.

III. It is used in applications like voice over Internet and has a much broader range of applications

D. Application Layer

I. The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and define high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

5.3 ADDRESSING IN TCP/IP The TCP/IP protocol suited involves 4 different types of addressing:

1. Physical Address
2. Logical Address
3. Port Address
4. Specific Address

APPLICATION LAYER	**Processes**			**SPECIFIC ADDRESS**
TRANSPORT LAYER	**TCP**	**UDP**	**SCTP**	**PORT ADDRESS**
NETWORK LAYER	**IP and other associated protocols**			**LOGICAL ADDRESS**
Protocols of underlying network used at physical & data link layer				
HOST TO NETWORK LAYER	**PHYSICAL ADDRESS**			

Fig: Addressing in TCP/IP model

51

Each of these addresses are described below:

1. Physical Address

i. Physical Address is the lowest level of addressing, also known as link address.

ii. It is local to the network to which the device is connected and unique inside it.

iii. The physical address is usually included in the frame and is used at the data link layer.

iv. MAC is a type of physical address that is 6 byte (48 bit) in size and is imprinted on the Network Interface Card (NIC) of the device.

v. The size of physical address may change depending on the type of network. Ex. An Ethernet network uses a 6 byte MAC address.

2. Logical Address

i. Logical Addresses are used for universal communication.

ii. Most of the times the data has to pass through different networks; since physical addresses are local to the network there is a possibility that they may be duplicated across multiples networks also the type of physical address being used may change with the type of network encountered. For ex: Ethernet to wireless to fiber optic. Hence physical addresses are inadequate for source to destination delivery of data in an internetwork environment.

iii. Logical Address is also called as IP Address (Internet Protocol address).

iv. At the network layer, device i.e. computers and routers are identified universally by their IP Address.

v. IP addresses are universally unique.

vi. Currently there are two versions of IP addresses being used:
a. **IPv4**: 32 bit address, capable of supporting 2^{32} nodes
b. **IPv6:** 128 bit address, capable of supporting 2^{128} nodes

3. Port Address

VIII. A logical address facilitates the transmission of data from source to destination device. But the source and the destination both may be having multiple processes communicating with each other.

52

Ex. Users A & B are chatting with each other using Google Talk, Users B & C are exchanging emails using Hotmail. The IP address will enable transmitting data from A to B, but still the data needs to be delivered to the correct process. The data from A cannot be given to B on yahoo messenger since A & B are communicating using Google Talk.

IX. Since the responsibility of the IP address is over here there is a need of addressing that helps identify the source and destination processes. In other words, data needs to be delivered not only on the correct device but also on the correct process on the correct device.

X. A Port Address is the name or label given to a process. It is a 16 bit address.

XI. Ex. TELNET uses port address 23, HTTP uses port address 80

4. Specific Address

i. Port addresses address facilitates the transmission of data from process to process but still there may be a problem with data delivery.

For Ex: Consider users A, B & C chatting with each other using Google Talk. Every user has two windows open, user A has two chat windows for B & C, user B has two chat windows for A & C and so on for user C Now a port address will enable delivery of data from user A to the correct process (in this case Google Talk) on user B but now there are two windows of Google Talk for user A & C available on B where the data can be delivered.

ii. Again the responsibility of the port address is over here and there is a need of addressing that helps identify the different instances of the same process.

iii. Such address are user friendly addresses and are called specific addresses.

iv. Other Examples: Multiple Tabs or windows of a web browser work under the same process that is HTTP but are identified using **Uniform Resource Locators (URL**), Email addresses.