TCP/IP and DoD Model

tutorialandexample.com/tcp-ip-model

admin July 4, 2019

Introduction to TCP/IP Model

- TCP/IP model was introduced in 1974.
- TCP/IP stands for Transmission Control Protocol/Internet Protocol.
- TCP/IP is an underlying communication protocol used by internet and commercial networks.
- The Transmission Control Protocol (TCP) handles reliable delivery of messages, and The Internet Protocol (IP) manages the routing of network transmission from the sender to the receiver.
- TCP/IP defines how electronic devices such as computers connected to the Internet and how data is transmitted between them.

Features of TCP/IP Model

A list of features of TCP/IP Model –

Support from vendors: TCP/IP receives support from many hardware and software vendors.

Interoperability: It can be installed and used on every platform.

Flexibility: An administrator can automatically assign an IP address to a host.

TCP/IP and the DoD Model

DoD stands for Department of Defense. It is a smaller version of the OSI reference model.

TCP/IP DoD model has four layers that are:

- Process/Application layer
- Host-to-Host layer
- Internet layer
- Network Access Layer

Process/Application layer

- The Application layer of the DoD model is equivalent to the upper three layers of the OSI model, i.e., Session layer, Presentation layer, and Application layer.
- The Process/Application layer of the DoD model provides the following capabilities –
- Enable applications to communicate with each other.
- Provides access to the services that operate at the lower layers of the DoD model.
- It contains a protocol that implements user-level functions such as mail delivery, file transfer, and remote login.

Host-to-Host layer

- A host-to-host layer of the DoD model performs the same functions as the Transport layer of the OSI reference model.
- It handles issues such as flow control, reliable end-to-end communication, and ensuring error-free delivery of the data.
- Protocols that operate on the Host-to-Host layer are: TCP and UDP.

Internet layer

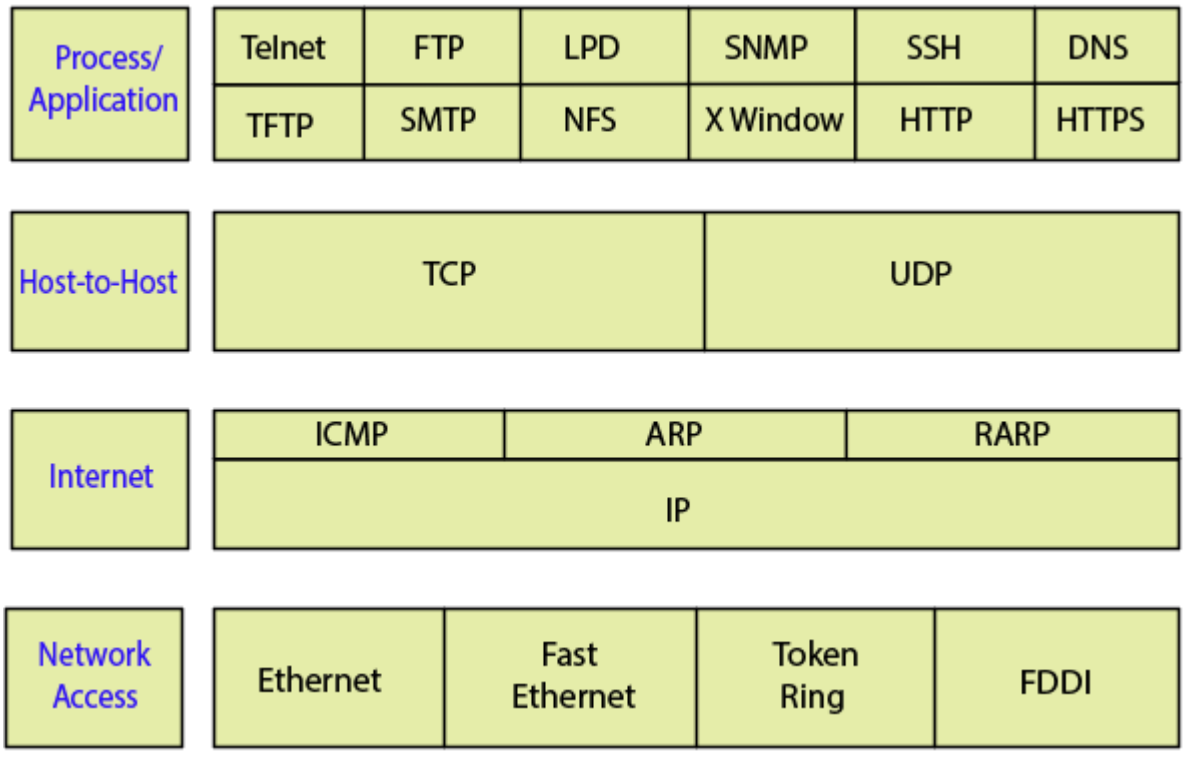
- Internet layer of the DoD model performs the same functions as the Network layer of the OSI reference model.
- It handles the packaging, addressing, and routing of packets among multiple networks.
- This layer also establishes a connection between two computers to exchange the data.

Network Access Layer

- The Network Access layer of the DoD model is equivalent to the lower two layers of the OSI model, i.e., Data link layer, and Physical layer.
- The Hardware connected to Network access layer are:
- Network medium: Cables like coaxial, twisted pair. Today, mostly, we use a wireless medium such as Bluetooth, WI-FI.
- Network Interface Card (NIC) has two types of addresses.

1. MAC Address- It is a **48 bits** physical address.
2. IP Address – It is a **32 bits** logical address.

The TCP/IP DoD Protocols



The Application Layer Protocols

There are following protocols at this layer:

- Telnet
- File Transfer Protocol (FTP)
- Line Printer Daemon (LPD)
- Simple Network Management Protocol (SNMP)
- Secure Shell (SSH)
- Domain Name Service (DNS)
- Trivial File Transfer Protocol (TFTP)
- Simple Mail Transfer Protocol (SMTP)
- Network File System (NFS)
- XWindow
- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol Secure (HTTPS)

Telnet

- Telnet stands for Telecommunication Network.
- It is also called as Remote Access Protocol because it is used to access the remote machine over the Internet.
- A user on a remote client machine called the Telnet Client.
- A machine who access to resources called the Telnet server.
- It uses **TCP port no 23**.
- It is less secure, and all data exchange without using any form of encryption.

File Transfer Protocol (FTP)

- It is the standard protocol that uses client-server architecture to transfer files between computers and servers over a network such as the Internet.
- FTP server helps you to download, upload, and delete files.
- It uses **TCP port number 21** to maintain the connection.
- It also uses **TCP port number 20** for the actual transmission of the files.
- It is a simple and secure way to exchange files.

There are two types of FTP Servers

Anonymous Server – No need of Password to access the FTP server.

Non-Anonymous Server – Need of Password to access the FTP server.

Line Printer Daemon (LPD)

This protocol designed for printer sharing. It is basically created for **Linux, and Unix** Systems.

Simple Network Management Protocol (SNMP)

- It collects and manipulates valuable network information.
- It is a UDP based network protocol.
- There are three types of SNMP version that are SNMP v1, SNMP v2, and SNMP v3. SNMP v3 provides security and remote configuration capabilities to the previous versions.

SNMP consists of 3 sub-components that are:

- **SNMP Manager** – It is a computer that monitor the network.
- **SNMP Agent** – It is a device that we want to monitor such as Router, Switches, and Servers
- **Management Information Base (MIB)** – These components make sure that the data exchange between the manager and agent remains structured.

Secure Shell (SSH)

- It is also called as a new-generation protocol that now used in a place of rsh and rlogin even Telnet.
- It is a cryptographic network protocol.
- It performs operations like logging into the system, running programs on remote systems, and moving files from one system to another. It does all these operations by maintaining a strong encrypted connection.
- It uses a secure key for transmitting data securely. Only the sender and receiver know this key.
- SSH uses TCP port number 22.

Domain Name Service (DNS)

- It is an internet directory service.
- It is an application that maps host names into their corresponding IP address.
- Mapping hostnames into their corresponding IP address is known as name resolution or name translation.
- We need DNS because it is very difficult for users to remember the IP address so, DNS provides a specific name for every IP address.

Example

If you want to open Google, You directly type www.google.com instead of given Google's IP address.

Trivial File Transfer Protocol (TFTP)

- TFTP is a simple file transfer protocol that is similar to FTP. It is also called a simplified version of FTP.
- It uses UDP port number 69 for TFTP server.
- It does not provide authentication and security while transferring the files.

Simple Mail Transfer Protocol (SMTP)

- SMTP, the acronym is associated with **Sending Mail To People**.
- It is a set of commands that authenticates and directs the transfer of Email (Electronic Mail) over the internet.
- SMTP uses TCP protocol

- The default SMTP port number is 25.
- Secondary SMTP port number is 26.
- SMTP over SSL/TLS port number is 465.

Network File System (NFS)

- It is a distributed file system protocol developed by Sun Microsystems in 1984.
- It allows a user on a client computer to access files over a network.
- NFS supports heterogeneous hardware and operating systems.
- NFS client code implements all client system calls on remote files by sending one or more RPC requests to the server.

XWindow

- XWindow was used to perform client/server operations like writing client/server applications based on a Graphical User Interface (GUI).
- It allowed the client to run a program on one computer and have to display it on window server of another computer.

Hypertext Transfer Protocol (HTTP)

- It is a protocol used for transferring hypertext, i.e. (plain text, Images, sound, and video, etc.) between two computers.
- Hypertext is the text that is specially coded using a standard coding language called Hypertext Markup Language (HTML).
- It provides standard communication between web browsers and web servers.
- It uses TCP port number 80.

Hypertext Transfer Protocol Secure (HTTPS)

- It encrypts the data that is being retrieved by HTTP.
- It makes sure that the data transfer between the client and server is secure.
- It established an encrypted connection between the browser and the web server using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols.
- It increases the speed of data transfer as compared to http.

The Host-to-Host Layer Protocols

There are the following two protocols at this layer:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

Transmission Control Protocol (TCP)

- It takes a large block of information from an application layer and breaks them into segments.
- It is a full-duplex, connection-oriented, and reliable protocol.

TCP Header

TCP header is minimum 20 bytes long. There are following fields in the TCP header:

Source Port

It is 16-bit long port number of application on the source host.

Destination port

It is also 16-bit long port number of the application on the destination host.

Sequence Number

It is a 32-bit long field. TCP access a unique sequence number for each byte of data contained in the TCP segment.

Acknowledgment Number

It is also a 32-bit field. It contains a sequence number of data that the receiver expects to receive from the sender. Once a connection is established, the receiver always sends an acknowledgment.

Data Offset (DO)

It stores the total size of the TCP header in multiples of 4 bytes. It indicates where the data begins.

RSV

It contains 6 bits that reserve for future use.

Flags

There are following six flags in the TCP header –

URG: URGENT Pointer field contains valid data.

ACK: Acknowledgment number is valid.

PSH: The receiver should pass this data to the application as soon as possible.

RST: Reset the connection.

SYN: Synchronize sequence number to initiate a connection.

FIN: The sender is finished sending data.

Window

It is a 16-bit field. It indicates the size of the receiver window. Window size changes dynamically during the transmission. It is also used in flow control to retransmit the lost packets.

Checksum

It is a 16-bit long field used for the error control mechanism. The sender adds CRC checksum in the checksum field before sending the data.

Urgent Pointer

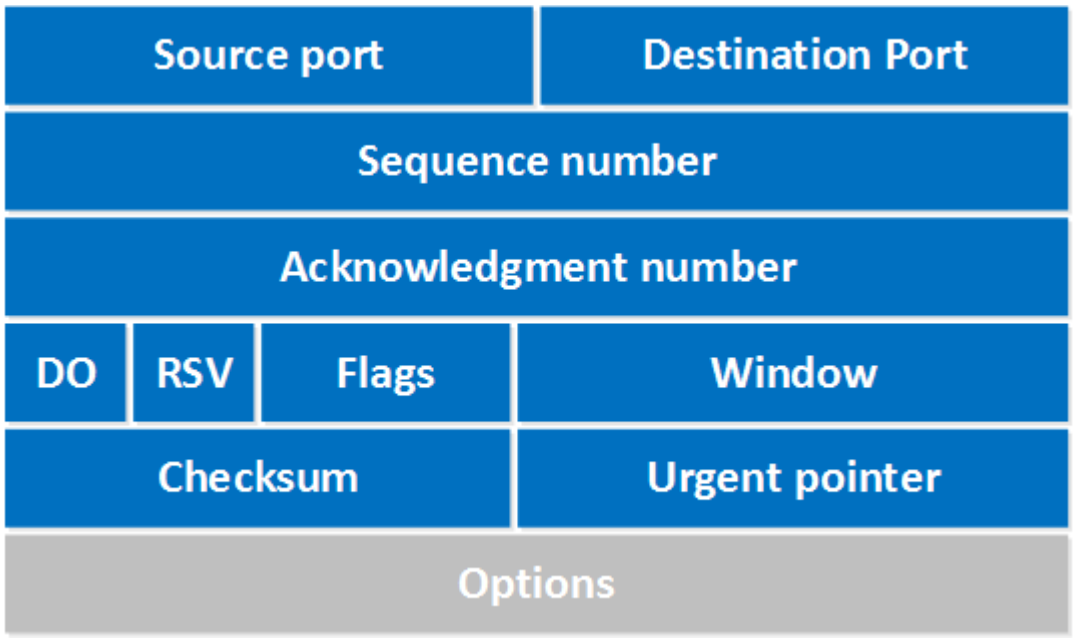
It is a 16-bit field. Urgent pointer added to the sequence number to show the end of urgent data.

Options

The size of the options field lies from 0 bytes to 40 bytes.

Options fields used for the following purposes:

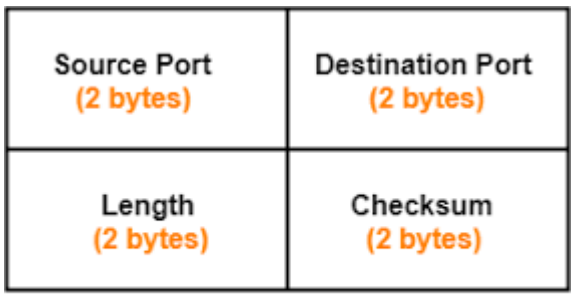
- Timestamp
- Window size extension
- Parameter negotiation
- Padding



User Datagram Protocol (UDP)

- It is fast, connectionless, and unreliable protocol.
- It has been designed to send data packets over the network.
- UDP does not provide reliability, flow control, and error recovery mechanism.

UDP Header



UDP Header

Source Port Number

It is a 16 bits field that contains the port number of the application that sends the data.

Destination Port Number

It is a 16 bits field that contains the port number of the application that receives the data.

Length

It is a 16 bits field that identifies the combination length of UDP header and encapsulated data.

Checksum

It is a 16 bits field used for the error control mechanism. In UDP checksum calculation is not mandatory.

Difference between TCP and UDP –

TCP	UDP
Sequenced	Un-Sequenced
Reliable	Unreliable
Connection-oriented	Connectionless
Acknowledgments	No acknowledgment
Windowing or flow control	No windowing or flow control

The Internet Layer Protocols

There are following protocols at this layer:

Internet Control Message Protocol (ICMP)

Address Resolution Protocol (ARP)

Reverse Address Resolution Protocol (RARP)

Internet Protocol (IP)

Internet Control Message Protocol (ICMP)

- It is a management protocol and messaging service provider for IP.
- ICMP is used to send error and control messages.

Some common ICMP events and messages are:

Destination Unreachable

If a router can't send an IP datagram to any destination device, it uses ICMP to send a message back to the sender.

Buffer Full

If a router's memory buffer is full, it will use ICMP to send out this message until congestion is decreased.

Ping

Ping stands for Packet Internet Groper. It uses ICMP echo request and replies messages to check the physical and logical connectivity of machines over the network.

Tracert

It stands for trace route. This command is used to see the exact path that the data packet is taking on its way to the destination.

Address Resolution Protocol (ARP)

It is a network protocol for mapping an IP address to a MAC address on a local area network.

192.162.10.25 -> 7A-89-76-E0-B1-23

Where the MAC address is a unique address of a device.

Reverse Address Resolution Protocol (RARP)

- RARP packet format is the same as the ARP packet.
- Its request consists of a MAC header, an IP header, and the ARP request message.
- RARP requests are broadcast, and RARP replies are unicast.

Internet Protocol (IP)

- IP is a set of rules that defines how computers communicate over a network.
- IP software performs the routing function.
- IP is unreliable and connectionless datagram protocol.

Currently, there are two versions of IP

IP version 4 (IPv4)

IP version 6 (IPv6)

The Network Access Layer

There are the following terms used in this layer:

- Ethernet
- Fast Ethernet
- Token Ring
- FDDI

Ethernet

- It is a computer network technology that is widely used by different networks like LAN, MAN, CAN, and WAN.
- It is a fast and reliable network solution.
- *Ethernet* connects computers together with cables like fiber optic, co-axial so that the computers can share information.
- Today, we also use wireless Ethernet that can handle a large number of users.
- Wireless Ethernet is less expensive than a wired Ethernet network.

Fast Ethernet

- It can transfer data at a rate of 100 Mbps.
- It uses a twisted pair and fiber optic cable for communication.

There are three types of Fast Ethernet –

- 100BASE-TX
- 100BASE-FX
- 100BASE-T4

Token Ring

- It was developed in 1980 by IBM for a Local Area Network (LAN).
- In a token ring network, all hosts are connected in a ring topology.
- The token, an empty frame, is continuously circulated on the ring. If a host doesn't have anything to transmit, it passes the token along. If it does have something to transmit, it catches the token and attaches the data and sends it back to ring.
- It transmits a larger frame than Ethernet.
- It is costly to use.

Fiber Distributed Data Interface (FDDI)

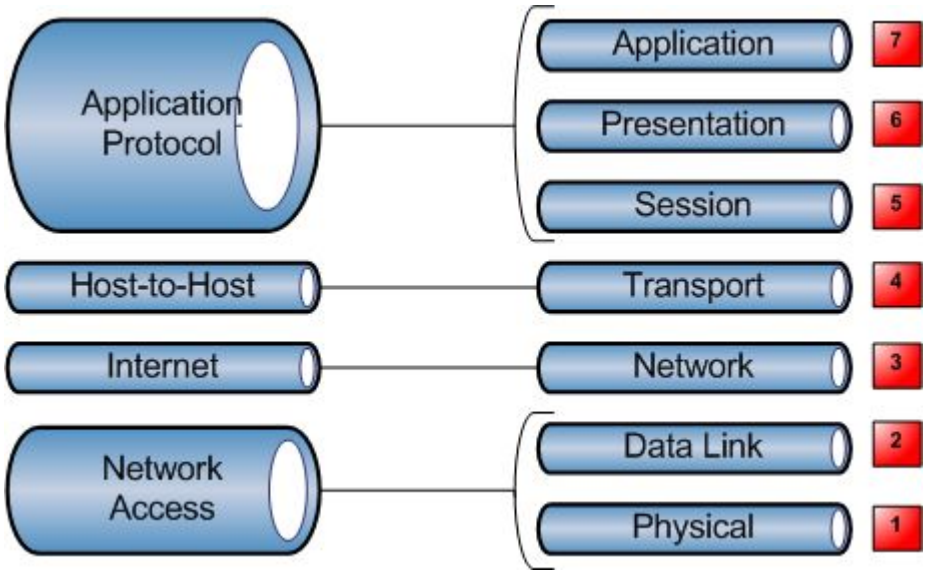
- It is developed by American Nation Standard Institute (ANSI).
- It is based on the token ring protocol.
- It transmits data on optical fibers.
- It supports the transmission rate up to 200 Mbps.

It uses two rings:

- The first ring is used to carry data at 100 Mbps.
- The second ring is used for backup and recovery in case the first ring fail. It also increases the data transmission rate up to 200 Mbps.

Difference between TCP/IP and OSI network model:

TCP/IP Model	OSI Model
It has only 4 layers.	It has seven layers.
Horizontal Approach.	Vertical Approach.
In this model, Host-to-Host layer does not guarantees delivery of packets.	In this model, transport layer guarantees delivery of packets.
Supports only connectionless communication in the Internet layer.	Supports connectionless and connection-oriented communication in the Network layer.



? Previous Next ?