Network Protocols

Presentation · December 2021

DOI: 10.13140/RG.2.2.30555.28963

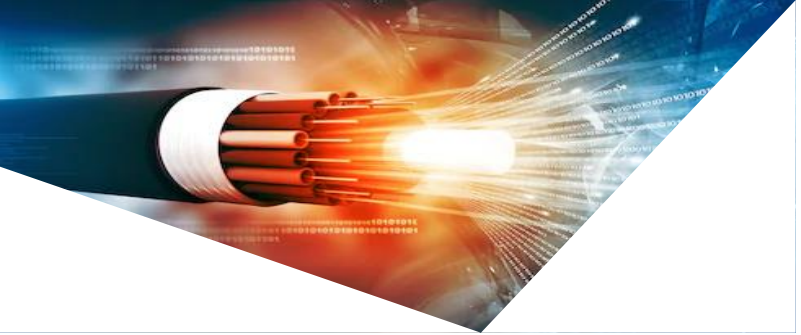
CITATIONS
0

READS
13,931

1 author:

Husam K Salih
Al-Rasheed University College
40 PUBLICATIONS **96** CITATIONS

SEE PROFILE



Network Protocols

Husam K. Salih

Outlines

- Network Protocol?
- TCP/IP
- Protocol Hierarchies
- Application Layer Protocols
- Transport Layer Protocols
- Network Layer Protocols
- References

Network Protocol

- A protocol is a set of rules that governs the communications between computers on a network.

- Functions of protocols:
  - Addressing
  - Data Packet Format
  - Segmentation (Splitting long messages into small pieces)
  - Embedding control information
  - Detecting Errors
  - Controlling data flow
  - Controlling connection

NETWORK PROTOCOL

Keep three points in mind when you think about protocols in a network environment:

1) There are many protocols.

- **While each protocol facilitates basic communications, each has different purposes and accomplishes different tasks.**
- **Each protocol has its own advantages and restrictions.**
- **A protocol can be implemented either in hardware or in software.**

NETWORK PROTOCOL

2) Some protocols work only at particular OSI layers.

- **The layer at which a protocol works describes its function. For example, a protocol that works at the physical layer ensures that the data packet passes through the network interface card (NIC) and out onto the network cable.**

3) Protocols can also work together in a protocol stack, or suite.

- **A protocol stack or protocol suite is a combination of protocols.**
- **Just as a network incorporates functions at every layer of the OSI reference model, different protocols also work together at different levels in a single protocol stack.**

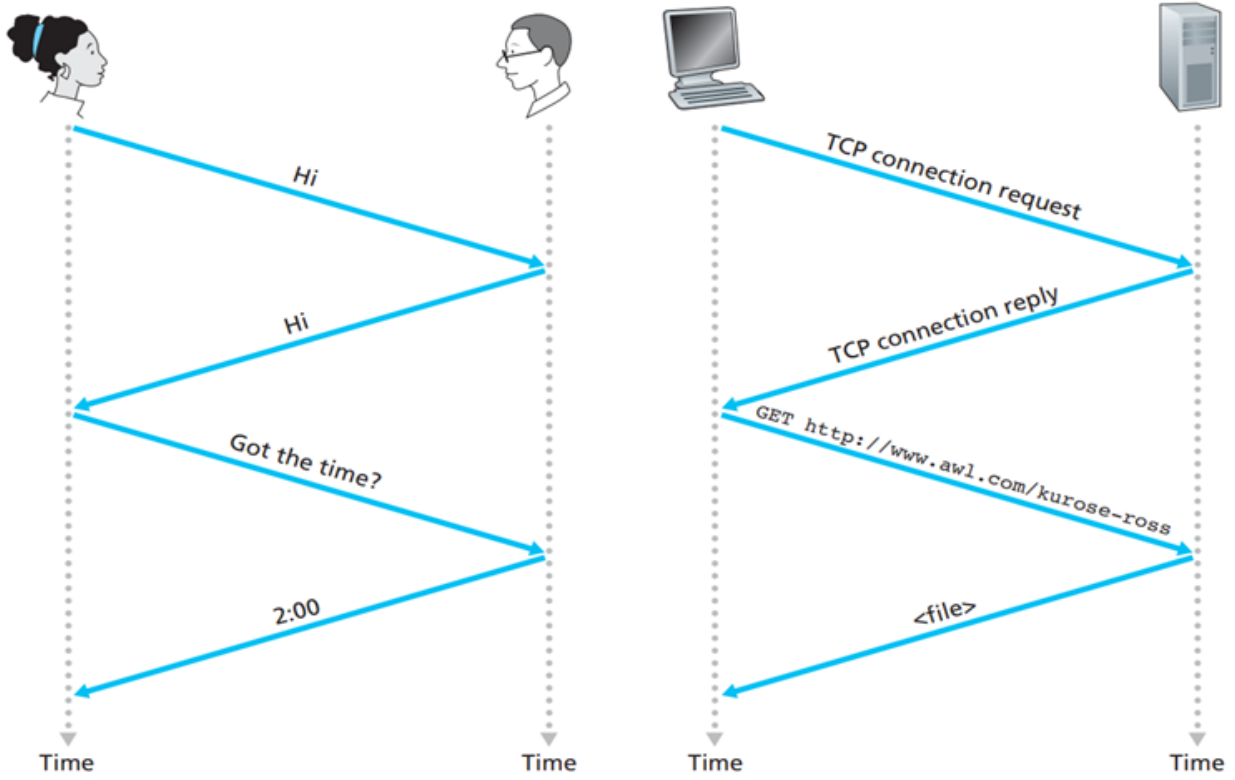
NETWORK PROTOCOL

How Protocol Works?

- As learned before, the entire technical operation by which data is transmitted over the network has to be broken down into discrete, systematic steps.
- At each step, certain actions take place that cannot take place at any other step. Each step includes its own rules and procedures, or protocol.
- The protocol steps must be carried out in a consistent order that is the same on every computer in the network.
- In the sending computer, these steps must be executed from the top down. In the receiving computer, these steps must be carried out from the bottom up.
- Both sending and receiving computers need to perform each step in the same way so that the data will have the same structure when it is received as it did when it was sent.

NETWORK PROTOCOL

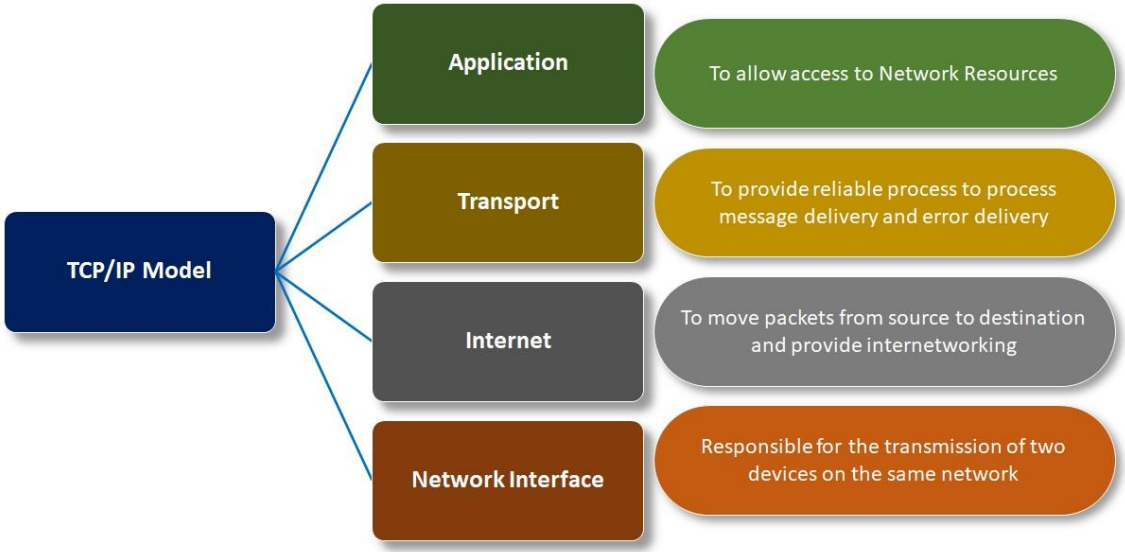
How Protocol Works?



TCP/IP

- **Is the suite of communications protocols that is used to connect hosts on the Internet and on most other computer networks as well.**
- **It is also referred to as the TCP/IP protocol suite and the Internet protocol suite.**

- **Application – client functionality**
- **Transport - moving data**
- **Network – tasks for moving data**



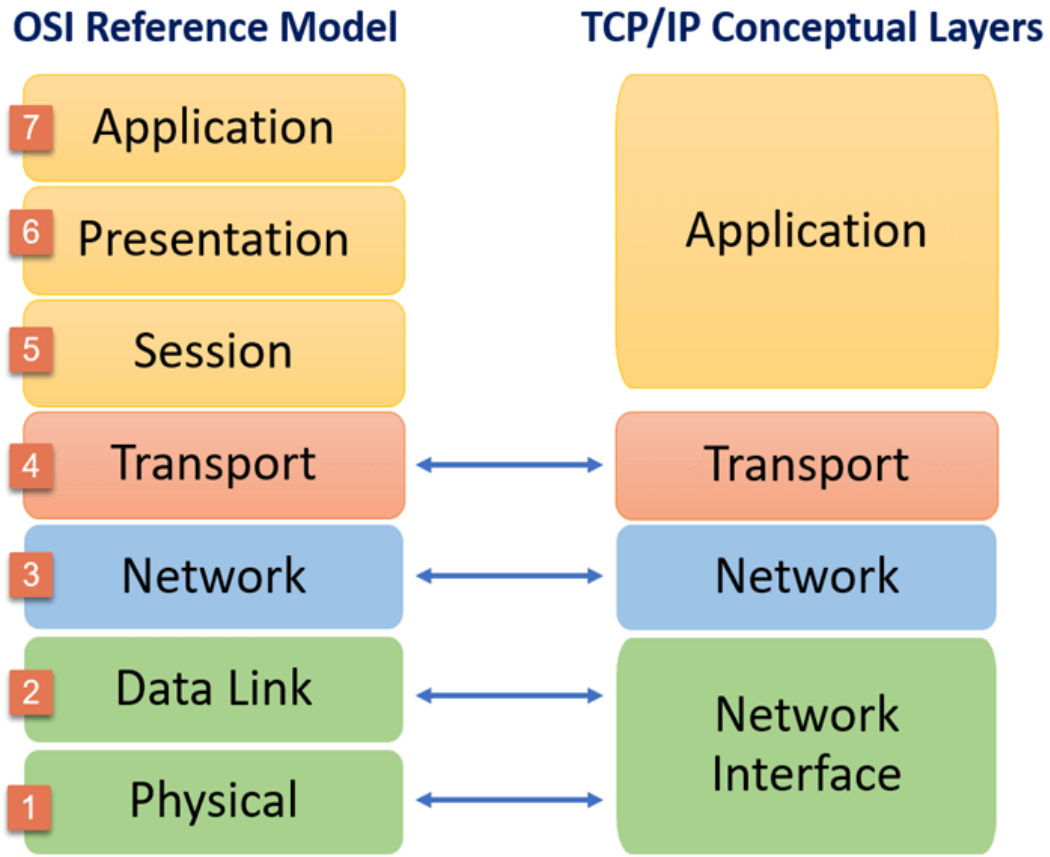
TCP/IP

Why is the TCP/IP important?

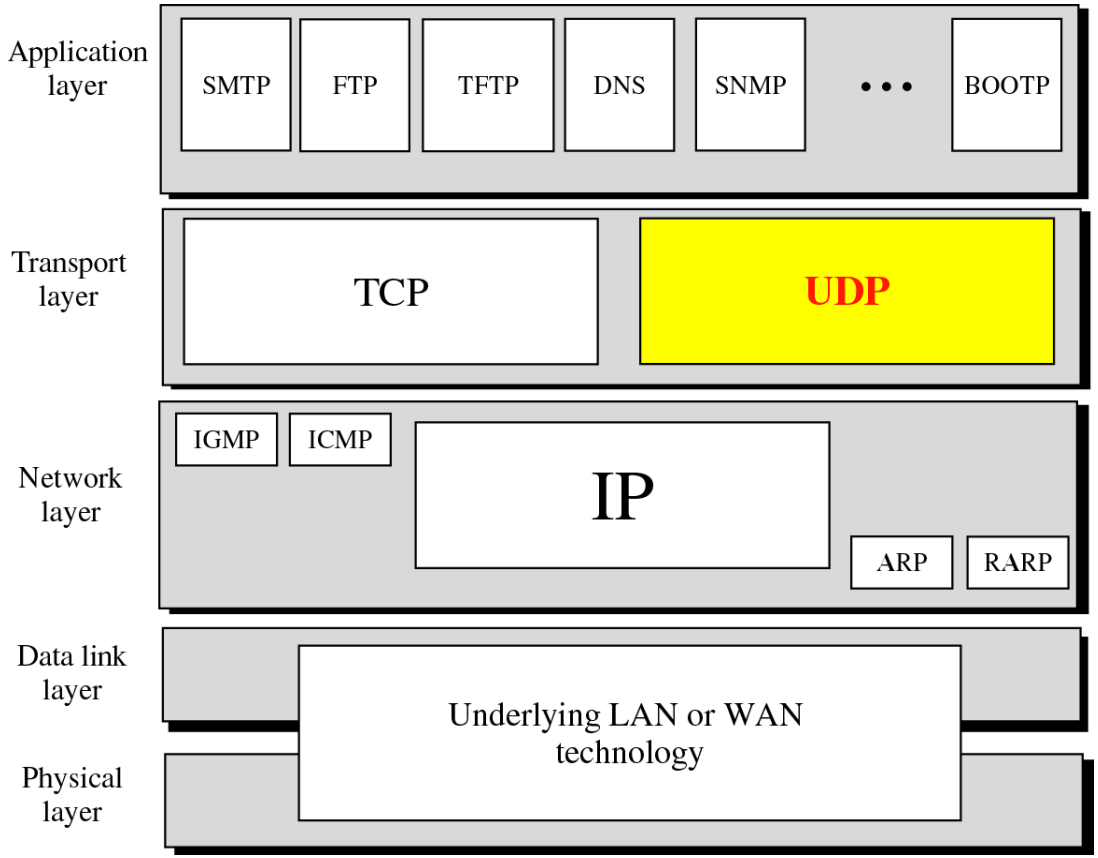
- **TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management and is designed to make networks reliable with the ability to recover automatically from the failure of any device on the network.**

- **TCP/IP is nonproprietary and, as a result, is not controlled by any single company. Therefore, the IP suite can be modified easily. It is compatible with all operating systems (OSes), so it can communicate with any other system. The IP suite is also compatible with all types of computer hardware and networks.**

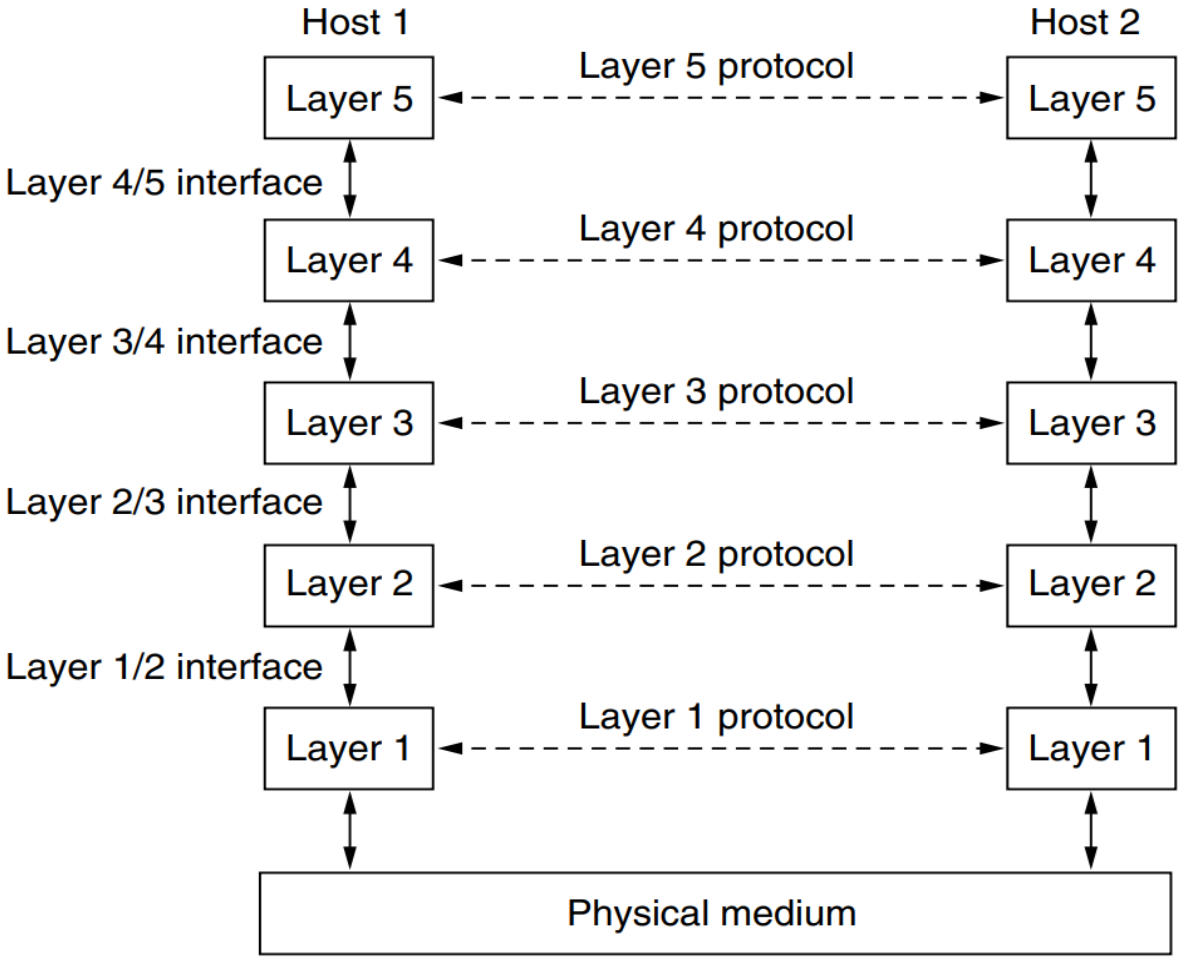
TCP/IP


OSI Reference Model
TCP/IP Conceptual Layers
7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data Link
1
Physical
Application
Transport
Network
Network Interface

TCP/IP


Application layer
SMTP
FTP
TFTP
DNS
SNMP
• • •
BOOTP
Transport layer
TCP
UDP
Network layer
IGMP
ICMP
IP
ARP
RARP
Data link layer
Underlying LAN or WAN technology
Physical layer

Protocol Hierarchies

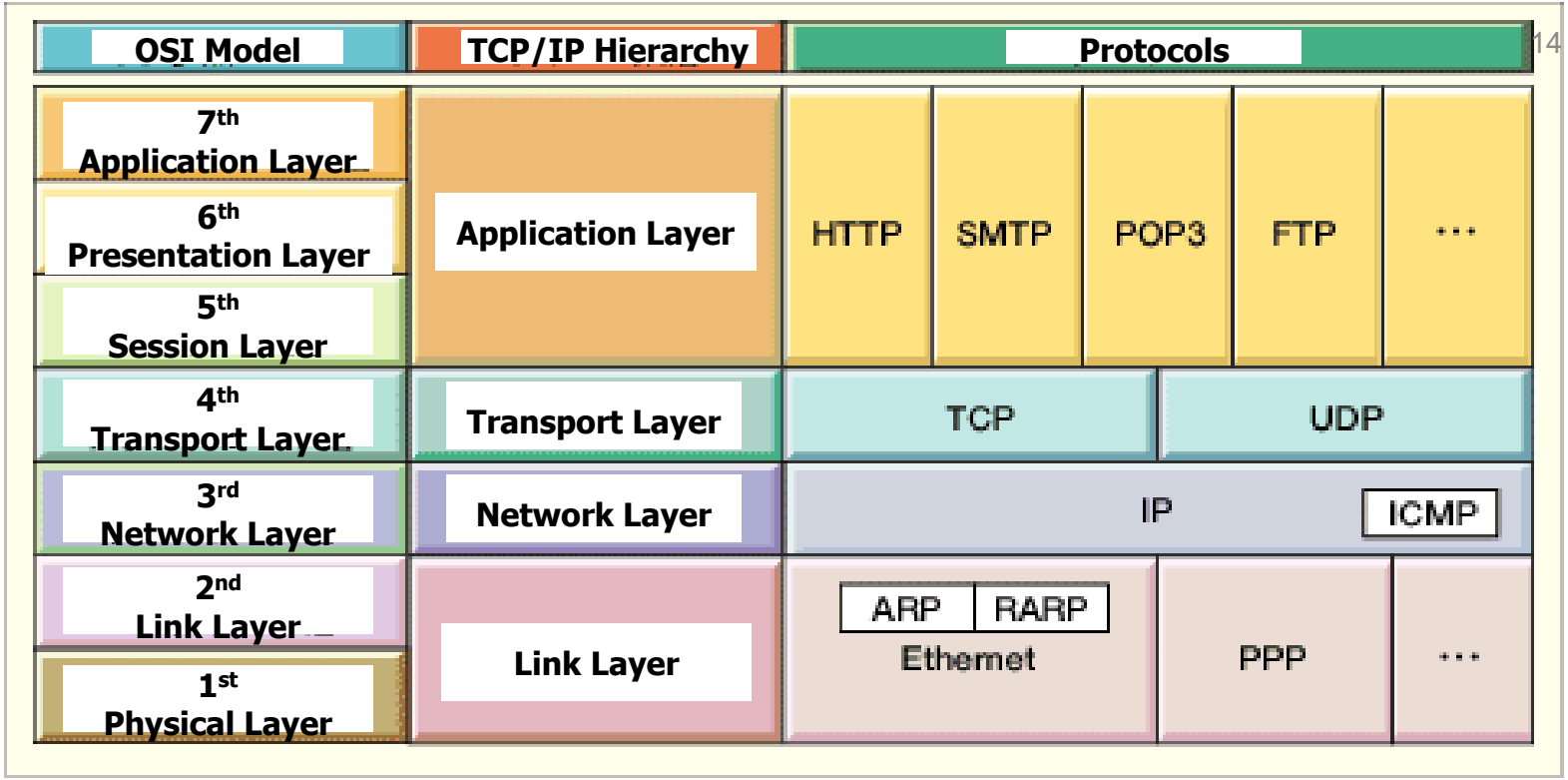


PROTOCOL HIERARCHIES

Protocols Classifications

- **By Routing Capabilities:**
  - Routable Protocols
  - Non-routable Protocols
- **By Method Orientation:**
  - Connection oriented
  - Connectionless
- **By Layer Level Tasks:**
  - Tasks on the Application Level
  - Tasks on the Transport Level
  - Tasks on the Network Level

PROTOCOL HIERARCHIES



Link Layer : Includes device driver and network interface card
Network Layer : Handles the movement of packets, i.e. Routing
Transport Layer : Provides a reliable flow of data between two hosts
Application Layer : Handles the details of the particular application

PROTOCOL HIERARCHIES

Common Protocols

- TCP
- FTP
- UDP
- TCP/IP
- DHCP
- TFTP
- DNS
- HTTP
- ARP
- SIP
- RTP
- SSH
- POP3
- NTP
- IMAP4
- TELNET
- SMTP
- SNMP
- ICMP
- IGMP
- TLS

Application Layer Protocols

- Ensure connection between user applications & the network server & exchange data between them.

- **Examples:**
  - File Transfer Protocol (FTP)
  - Hypertext Transfer Protocol (HTTP)
  - Hypertext Transfer Protocol Secure (HTTPS)
  - Domain Name System (DNS)
  - Secure Shell (SSH)
  - Secure Sockets Layer (SSL)
  - Real Time Protocol (RTP)
  - Border Gateway Protocol (BGP)
  - Simple Mail Transfer Protocol (SMTP)
  - Server Message Block (SMB)
  - Simple Network Management Protocol (SNMP)

APPLICATION LAYER PROTOCOLS

FTP

- File Transfer Protocol
- Uploading and downloading of files
- Uses TCP as a transport protocol
- Used to transfer files over the LAN
  - Popular to distribute files over the internet
- Application layer

APPLICATION LAYER PROTOCOLS

HTTP

- Hypertext Transfer Protocol
- Uses TCP
- Allows text, graphics, multimedia and other material to be downloaded
- Requests sent in clear text

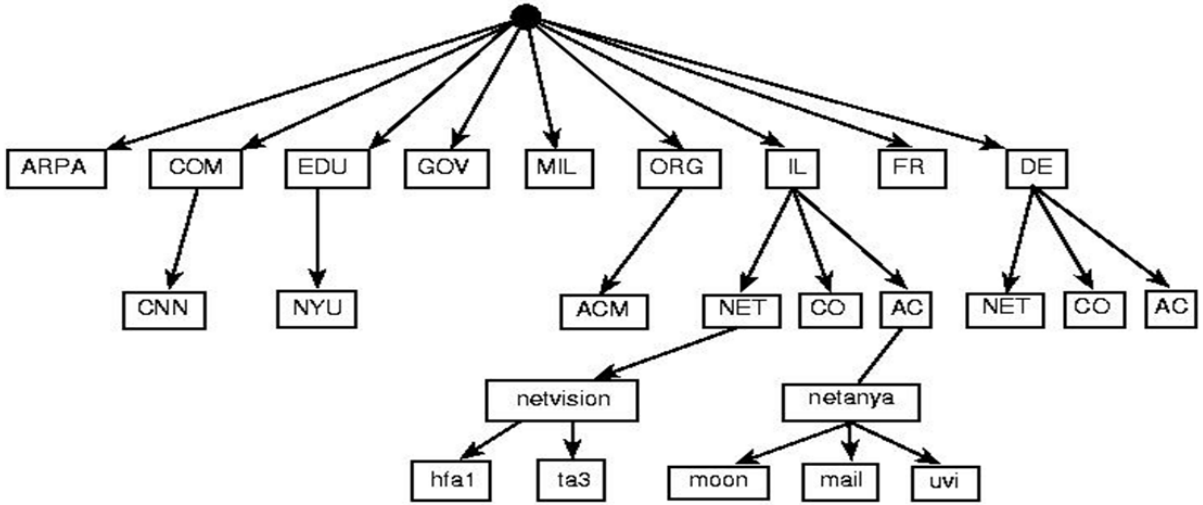
APPLICATION LAYER PROTOCOLS

DNS

- On the Internet, the DNS associates various sorts of information with domain names.
- A domain name is a meaningful and easy-to-remember "handle" for an Internet address.
- The Domain Name System protocol translates domain names into IP addresses.
- When a client wants to open a webpage at www.google.com, a query is sent to a DNS server (name server) to fetch the corresponding IP address.

APPLICATION LAYER PROTOCOLS

DNS



Top-Level Domain Name	→	EDU INT ORG GOV COM NET MIL US IT FR ...
Domain Name	→	Microsoft Volstate Thomson Yahoo IBM Cisco Florida ...
Host Name	→	www ftp www2 web ...

APPLICATION LAYER PROTOCOLS

SSL & SSH

SSL	SSH
Stands for “secure socket layer.”	Stands for “secure shell.”
SSL is a security protocol.	SSH is a network cryptographic network protocol.
Runs on port 443.	Runs on port 22.
Used primarily to establish secure connections between web servers and clients (web browsers).	Typically used for secure communication with a remote computer.
Authentication is done by employing an X.509 digital certificate (SSL/TLS certificate).	Authentication is done by a three-step process: server verification, session key generation, and client authentication.
SSL works based on SSL/TLS certificates.	SSH works based on network tunnels.
Primarily used to protect against man-in-the-middle (MiTM) attacks and identity theft.	Protects against DNS spoofing, IP source routing, data manipulation, data sniffing during transmission, Spoofing of IP addresses, etc.

APPLICATION LAYER PROTOCOLS

RTP

- Delivering audio and video over IP networks.
- Streaming media, such as telephony, video teleconference.
- RTP typically runs over User Datagram Protocol (UDP).
- used in conjunction with the RTP Control Protocol (RTCP).
- The protocol provides facilities for jitter compensation and detection of packet loss and out-of-order delivery.

Transport Layer Protocols

- **Ensure the security & the continuity of data transfer without any mistakes & is responsible for maintaining the quality & the accuracy of the exchanged information between devices.**

- **Examples:**
  - **Transmission Control Protocol (TCP)**
  - **User Data Protocol (UDP)**

TRANSPORT LAYER PROTOCOLS

TCP

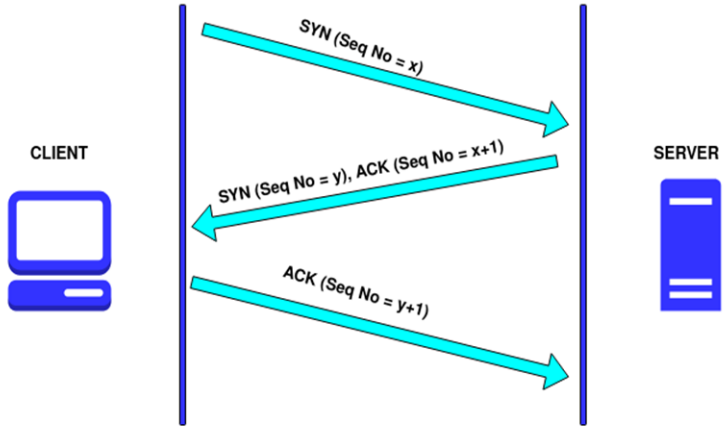
- Transmission Control Protocol
- Connection oriented – establishes a manually acknowledged session between two hosts.
- Full Duplex
- Provides reliability to IP
- Flow control, sequencing, and error detection and correction.
- Transport layer

TRANSPORT LAYER PROTOCOLS

TCP

- Sends SYN to target host
- Target opens connection and sends ACK
- Originated host sends ACK ready to transfer data
- Called three-way handshake

WWW (HTTP)
WhatsApp Messages
Email



TRANSPORT LAYER PROTOCOLS

UDP

- User Datagram Protocol
- Connectionless
- Unreliable protocol (No guarantee delivery)
- “fire and forget”
- The messages will be discarded if there is an Error
- Uses IP
- Lower overhead – low bandwidth

DNS
Voice Call & Video Call
Video Games

Network Layer Protocols

- **Ensure the security & the continuity of data transfer without any mistakes & is responsible for maintaining the quality & the accuracy of the exchanged information between devices.**

- **Examples:**
  - **Internet Protocol version 4 (IPv4)**
  - **Internet Protocol version 6 (IPv6)**
  - **Dynamic Host Configuration Protocol (DHCP)**
  - **Internet Control Message Protocol (ICMP)**
  - **Internet Group Message Protocol (IGMP)**

NETWORK LAYER PROTOCOLS

Internet Protocol (IP)

- Logical Address
- A set of requirements for addressing and routing data on the Internet.
- IP can be used with several transport protocols, including TCP and UDP.

- Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place. Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.

NETWORK LAYER PROTOCOLS

Internet Protocol (IP)

- We can also define an IP address as a numeric address assigned to each device on a network. An IP address is assigned to each device so that the device on a network can be identified uniquely. To facilitate the routing of packets, TCP/IP protocol uses a 32-bit logical address known as IPv4(Internet Protocol version 4).

- An IP address consists of two parts, i.e., the first one is a network address, and the other one is a host address.

- There are two types of IP addresses:
  - IPv4
  - IPv6

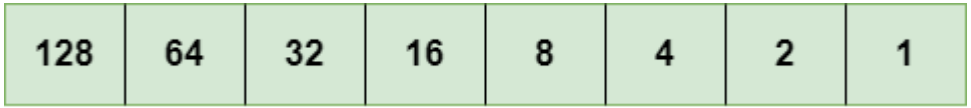
NETWORK LAYER PROTOCOLS

IPv4

- It is a current version and the most commonly used IP address.
- It is a 32-bit address written in four numbers separated by 'dot', i.e., periods called ‘Octet’.
- This address is unique for each device. For example, 66.94.29.13
- Each number in an octet is in the range from 0-255.
- This address can produce 4,294,967,296 possible unique addresses.
- IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.
- Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.
- IPv4 has five classes (A,B,C,D, and E)

IPv4

Representation of 8 Bit Octet

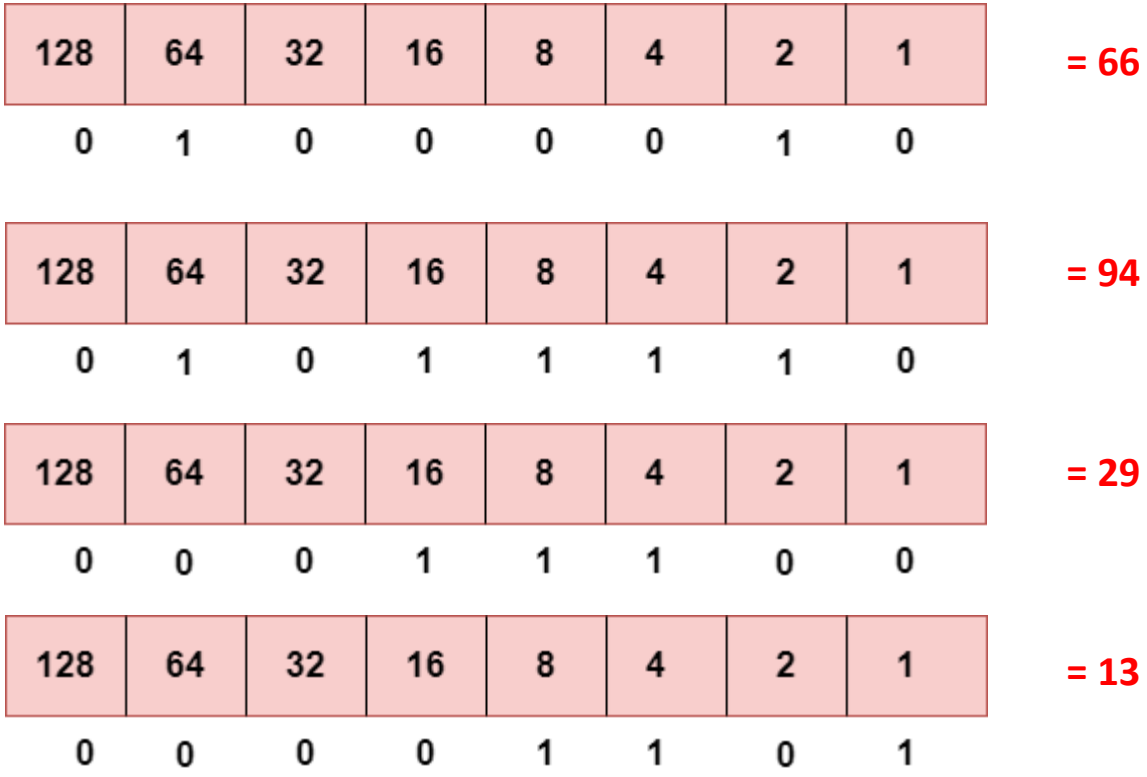


The above representation shows the structure of 8- bit octet.

Now, we will see how to obtain the binary representation of the above IP address, i.e., 66.94.29.13

NETWORK LAYER PROTOCOLS

IPv4



NETWORK LAYER PROTOCOLS

IPv4 Classes

- Class A
  - Public IP Range: 1.0.0.0 to 127.0.0.0
  - First octet value range from 1 to 127
- Class B
  - Public IP Range: 128.0.0.0 to 191.255.0.0
  - First octet value range from 128 to 191
- Class C
  - Public IP Range: 192.0.0.0 to 223.255.255.0
  - First octet value range from 192 to 223
- Class D
  - Range: 224.0.0.0 to 239.255.255.255
  - First octet value range from 224 to 239
- Class E
  - Range: 240.0.0.0 to 255.255.255.255
  - First octet value range from 240 to 255

NETWORK LAYER PROTOCOLS

Home Work 1:

A- Convert the following binary digits to IPv4 forms.

1- 01000010.01011110.00011101.00001101
2- 11000000.01000000.00000001.00000001
3- 11000000.01000000.11111111.00000000

B- Convert the following IPv4 addresses to Binary digits.

1- 192.168.1.1
2- 192.168.254.1
3- 255.255.100.0

C- Find the Class of the following IPs.

1- 192.168.1.1
2- 240.20.1.100
3- 101.0.0.1

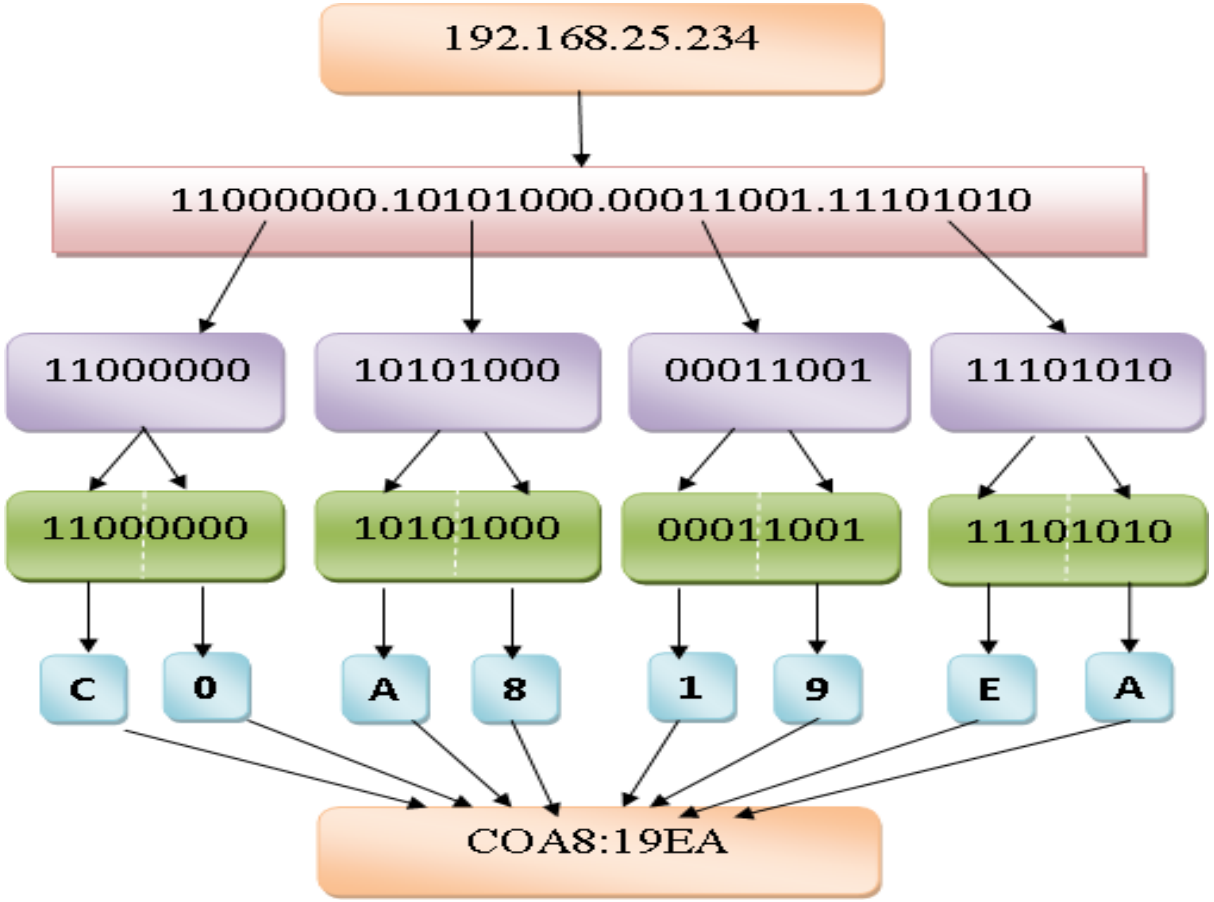
IPv6

- IPv6 is the next generation of IP addresses.
- The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

- The above diagram shows the address format of IPv4 and IPv6. An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255. Whereas an IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

NETWORK LAYER PROTOCOLS

IPv6



NETWORK LAYER PROTOCOLS

Home Work 2:

A- Convert the following binary digits to IPv6 forms.

1- 01000010.01011110.00011101.00001101
2- 11000000.01000000.00000001.00000001
3- 11000000.01000000.11111111.00000000

B- Convert the following IPv4 addresses to IPv6 forms.

1- 192.168.1.1
2- 192.168.254.1
3- 255.255.100.0

REFERENCES

[1] Behrouz A. Forouzan, ' Data Communications And Networking', 5th Edition.

[2] Andrew S. Tanenbaum, ' Computer Networks', 4th Edition.

[3] James F Kurose, Keith W Ross, ' Computer Networking A Top Down Approach', 6th Edition.

THANKS