Òco †Zvgvi cÖf‚i bv‡g whwb m„wó K‡i‡QbÓ

**OSI & DoD Models, Networking Protocols and Port Numbers**



**Abdur Razzak**

**MCSA**

**IT Professional Diploma in Networking Technologies**

**BSc (Hon’s) & MSc in Mathematics**

**Mobile: 01723090660, 01535114660**

**Email: a.razzak660@gamil.com  
Website: www.selftics.com**

|  |  |  |  |
| --- | --- | --- | --- |
| **INDEX** | | | |
| **Article** | **Topic** | | **page** |
|  | **Internetworking Models** | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | **The OSI Reference Model** | |  |
|  |  | The Application Layer |  |
|  |  | The Presentation Layer |  |
|  |  | The Session Layer |  |
|  |  | The Transport Layer |  |
|  |  | The Network Layer |  |
|  |  | The Data Link Layer |  |
|  |  | The Physical Layer |  |
|  | **Networking Protocols and Port Numbers** | |  |
|  |  | Introducing TCP/IP |  |
|  |  | Transmission Control Protocol (TCP) |  |
|  |  | User Datagram Protocol (UDP) |  |
|  |  | Port Numbers |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | **The DoD Model** | |  |
|  |  | The Process/Application Layer Protocols |  |
|  |  | The Host-to-Host Layer Protocols |  |
|  |  | The Internet Layer Protocols |  |
|  |  |  |  |
|  | **Data Encapsulation** | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**The OSI Reference Model**

1. **What is OSI Model?**

Ans. The Open Systems Interconnection (OSI) reference model was created by the International Organization for Standardization (ISO). The OSI model has seven hierarchical layers that were developed to enable different networks to communicate reliably between disparate systems.

One of the greatest functions of the OSI specifications is to assist in data transfer between Disparate. The OSI model has seven layers:

1. **Describe about of OSI Model?**

Ans. The Open Systems Interconnection (OSI) model is the primary architectural model for networks. It describes how data and network information are communicated from an application on one computer through the network media to an application on another computer. The OSI reference model breaks this approach into layers.

1. **Which year OSI model created by ISO?**

Ans: In the late 1970s, The Open Systems Interconnection (OSI) reference model was created by the International Organization for Standardization (ISO).

1. **Write down the step of OSI layer/** Write down list of OSI Model.

Ans:

1. Layer 7 : Application
2. Layer 6 : Presentation
3. Layer 5 : Session
4. Layer 4 : Transport
5. Layer 3 : Network
6. Layer 2 : Data Link
7. Layer 1 : Physical

**The Application Layer**

1. The Application Layer

Ans: An **application layer** is an abstraction layer that specifies the shared protocols and interface methods used by hosts in a communications network. The **application layer** abstraction is used in both of the standard models of computer networking; the Internet Protocol Suite (TCP/IP) and the Open Systems Interconnection model (OSI model).Although both models use the same term for their respective highest level layer, the detailed definitions and purposes are different.

**What is Application Layer?**

Application layer is the top most layers in OSI and TCP/IP layered model. This layer exists in both layered Models because of its significance, of interacting with user and user applications. This layer is for applications which are involved in communication system.

**What is the function of Application Layer?**

1. File, print, message, database and application services.
2. Provides a user interface.

**The Presentation Layer**

**What is Presentation Layer?**

In the seven-layer OSI model of computer networking, the presentation layer is layer 6 and serves as the data translator for the network. It is sometimes called the syntax layer.

1. The Presentation Layer

Ans: The presentation layer is responsible for the delivery and formatting of information to the application layer for further processing or display.[4] It relieves the application layer of concern regarding syntactical differences in data representation within the end-user systems. An example of a presentation service would be the conversion of an EBCDIC-coded text computer file to an ASCII-coded file.

**7. What is the function of Presentation Later?**

1. Data encryption, compression and translation services.
2. This layer is essentially a translator and provides coding and conversion functions.
3. data compression, decompression, encryption, and decryption are associated  
   with this layer.

**The Session Layer**

1. **What is Session Layer?**

In the seven-layer OSI model of computer networking, the session layer is layer 5. The session layer provides the mechanism for opening, closing and managing a session between end-user application processes, i.e., a semi-permanent dialogue.

The Session Layer

Ans: The session layer provides the mechanism for opening, closing and managing a session between end-user application processes,a semi-permanent dialogue. Communication sessions consist of requests and responses that occur between applications.

1. **What is the function of Session Layer?**
2. Keeps different application data separate.
3. Session layer is responsible for setting up, managing and then tearing down sessions between Presentation layer entities.
4. This layer also provides dialog control between devices, or nodes.
5. Session layer basically keeps applications data separate from other applications data.

**The Transport Layer**

1. The Transport Layer

Ans: In computer networking, the transport layer is a conceptual division of methods in the layered architecture of protocols in the network stack in the Internet Protocol Suite and the Open Systems Interconnection (OSI). The protocols of the layer provide host-to-host communication services for applications.[1] It provides services such as connection-oriented data stream support, reliability, flow control, and multiplexing.

1. **What is Transport Layer?**

In computer networking, the transport layer is a conceptual division of methods in the layered architecture of protocols in the network stack in the Internet Protocol Suite and the Open Systems Interconnection (OSI). The protocols of the layer provide host-to-host communication services for applications.

1. **What is function of Transport layer ?**
2. Transport layer provides segmentation, sequencing, and virtual circuits.
3. Provides reliable or unreliable delivery.
4. Performs error correction before retransmit.

**The Network Layer**

1. The Network Layer

Ans: In the seven-layer OSI model of computer networking, the network layer is layer 3. The network layer is responsible for packet forwarding including routing through intermediate routers, whereas the data link layer is responsible for media access control, flow control and error checking.

**2.What is the function of Network Layer ?**

1. Network layer provides logical network addressing and routing through an internetwork.
2. Provides logical addressing, which routers use for path determination.

**The Data Link Layer**

1. The Data Link Layer

Ans: The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer.

1. **What are the sublayers of the Data Link layer?**

In addition to the OSI layers, knowing the only layer that has sublayers and the functions of those sublayers is extremely important.

The Data Link layer has two sublayers: LLC and MAC.

* **LLC**: The LLC sublayer is responsible primarily for the multiplexing of Network layer protocols.
* **MAC**: The MAC sublayer is responsible for physical addressing and determining the appropriate time to place data on the network.

**4.What is function of Data Link Layer ?**

Ans:

1. Data Link layer provides framing and placing of data on the network medium.
2. Combines packets into bytes and bytes into frames.  
   Provides access to media using MAC addresses.  
   Performs error detection, not correction.
3. The *Data Link layer* provides the physical transmission of the data and handles error notification, network topology, and flow control.

**The Physical Layer**

1. The Physical Layer

Ans: The physical layer consists of the basic networking hardware transmission technologies of a network. It is a fundamental layer underlying the logical data structures of the higher level functions in a network. Due to the plethora of available hardware technologies with widely varying characteristics, this is perhaps the most complex layer in the OSI architecture.

**5. What is the function of Physical Layer?**

1. The Physical layer is responsible for taking 1s and 0s and encoding them into a digital signal for transmission on the network segment.
2. Moves bits between devices, specifies voltage, wire speed, and pin-out of cables.

Question

5.What is application Layer?

Ans: The *Application layer* of the OSI model marks the spot where users actually communicate with the computer (technically users communicate with the network stack through application processes interfaces or APIs that connect the application in use to the operating system of the computer).

1. What is presentation Layer?

Ans: The Presentation layer gets its name from its purpose: It presents data to the Application

layer and is responsible for data translation and code formatting.

1. What is Session Layer?

Ans: The Session layer is responsible for setting up, managing, and then tearing down sessions

between Presentation layer entities. This layer also provides dialog control between devices,

or nodes.

1. What is Transport Layer?

Ans: The Transport layer segments and reassembles data into a data stream.

10. Which Layer Maintaining Flow Control?

Ans: The Transport Layer by Maintaining Flow Control.

1. **Write the advantage of reference model**

Ans:

1. Reduces complexity
2. Standardizes interfaces
3. Facilitates modular engineering
4. Interoperability between Vendors
5. Ensures interoperable technology
6. Accelerates evolution
7. Simplifies teaching and learning
8. **Advantages of Reference Models**  
   The OSI model is hierarchical, and the same benefits and advantages can apply to any  
   layered model. The primary purpose of all such models, especially the OSI model, is to  
   allow different vendors’ networks to interoperate.  
   Advantages of using the OSI layered model include, but are not limited to, the following:

* The OSI model divides the network communication process into smaller and simpler  
  components, thus aiding component development, design, and troubleshooting.
* It allows multiple-vendor development through standardization of network components.
* It encourages industry standardization by defining what functions occur at each layer  
  of the model.
* It allows various types of network hardware and software to communicate.
* It prevents changes in one layer from affecting other layers, so it doesn’t hamper development and makes application programming easier.

**3.** Which layer chooses and determines the availability of communicating partners  
along with the resources necessary to make the connection, coordinates partnering  
applications, and forms a consensus on procedures for controlling data integrity and  
error recovery?

**Answer**: The Application layer is responsible for finding the network resources broadcast from a  
server and adding flow control and error control (if the application developer chooses).

**4.** Which layer is responsible for converting frames from the Data Link layer into  
electrical signals?

**Answer**: The Physical layer takes frames from the Data Link layer and encodes the 1s and 0s  
into a digital signal for transmission on the network medium.

**5.** At which layer are routing implemented, enabling connections and path selection  
between two end systems?

**Answer**: The Network layer provides routing through an internetwork and logical addressing.

**6.** Which layer defines how data is formatted, presented, encoded, and converted?

**Answer**: The Presentation layer makes sure that data is in a readable format for the Application layer.

**7.** Which layer is responsible for creating, managing, and terminating sessions between  
applications?

**Answer**: The Session layer sets up, maintains, and terminates sessions between applications.

**8.** Which layer manages the transmission of data across a physical link and is primarily  
concerned with physical addressing and the ordered delivery of frames?

Answer: Protocol Data Units (PDUs) at the Data Link layer are called frames. As soon as you  
see *frame* in a question, you know the answer.

**9.** Which layer is used for reliable communication between end nodes over the network  
and provides mechanisms for establishing, maintaining, and terminating virtual circuits as well as controlling the flow of information?

Answer: The Transport layer uses virtual circuits to create a reliable connection between two hosts.  
  
**10.** Which layer provides logical addressing that routers use for path determination?  
Answer: The Network layer provides logical addressing, typically IP addressing, and routing.

**11.** Which layer specifies voltage, wire speed, and connector pin-outs and moves bits  
between devices?

Answer: The Physical layer is responsible for the electrical and mechanical connections  
between devices.

**12.** Which layer combines bits into bytes and bytes into frames and uses MAC addressing?

Answer: The Data Link layer is responsible for the framing of data packets.

1. What do you mean connection oriented communication?

Ans; Connection-oriented (CO-mode[1]) communication is a network communication mode in and computer networking, where a communication session or a semi-permanent connection is established before any useful data can be transferred, and where a stream of data is delivered in the same order as it was sent.’

1. What is flow control?

Ans: In data communications, flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node.

1. What is windowing?

Ans: In computing, a windowing system (or window system) is a type of graphical user interface (GUI) which implements the WIMP (windows, icons, menus, pointer) paradigm for a user interface. Each currently running application is assigned a usually resizeable and usually rectangular shaped surface of the display to present its graphical user interface to the user; these windows may overlap each other, as opposed to a tiling interface where they are not allowed to overlap.

1. What is acknowledgement?

Ans: Reliable data delivery ensures the integrity of a stream of data sent from one machine to the other through a fully functional data link. It guarantees that the data won’t be duplicated or lost. This is achieved through something called positive acknowledgment with retransmission—a technique that requires a receiving machine to communicate with the transmitting source by sending an acknowledgment message back to the sender when it receives data.

**Networking Protocols and Port Numbers**

1. What is protocol?

Ans:

1. Components of protocol
2. Syntax
3. Semantics
4. timing

**Introducing TCP/IP**

**Transmission Control Protocol (TCP)**

**User Datagram Protocol (UDP)**

**Port Numbers**

**The DoD Model**

The DoD model is basically a condensed version of the OSI model; it’s composed of four, instead of seven, layer:

4. Process/Application layer

3. Host-to-Host layer

2. Internet layer

1. Network Access layer

**The Process/Application Layer Protocols**

**The Host-to-Host Layer Protocols**

1. What is the difference between TCP and UDP?

### Ans. Difference between TCP and UDP

|  |  |
| --- | --- |
| **TCP** | **UDP** |
| Reliability: TCP is connection-oriented protocol. When a file or message send it will get delivered unless connections fails. If connection lost, the server will request the lost part. There is no corruption while transferring a message. | Reliability: UDP is connectionless protocol. When you a send a data or message, you don’t know if it’ll get there, it could get lost on the way. There may be corruption while transferring a message. |
| Ordered: If you send two messages along a connection, one after the other, you know the first message will get there first. You don’t have to worry about data arriving in the wrong order. | Ordered: If you send two messages out, you don’t know what order they’ll arrive in i.e. **no ordered** |
| Heavyweight: – when the low level parts of the TCP “stream” arrive in the wrong order, resend requests have to be sent, and all the out of sequence parts have to be put back together, so requires a bit of work to piece together. | Lightweight: No ordering of messages, no tracking connections, etc. It’s just fire and forget! This means it’s a lot quicker, and the network card / OS have to do very little work to translate the data back from the packets. |
| Streaming: Data is read as a “stream,” with nothing distinguishing where one packet ends and another begins. There may be multiple packets per read call. | Datagrams: Packets are sent individually and are guaranteed to be whole if they arrive. One packet per one read call. |
| Examples: World Wide Web (Apache TCP port 80), e-mail (SMTP TCP port 25 Postfix MTA), File Transfer Protocol (FTP port 21) and Secure Shell (OpenSSH port 22) etc. | Examples: Domain Name System (DNS UDP port 53), streaming media applications such as IPTV or movies, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) and online multiplayer games etc |

|  |  |
| --- | --- |
| **Key features of TCP and UDP** | |
| TCP | UDP |
| Sequenced | Unsequenced |
| Reliable | Unreliable |
| Connection-oriented | Connectionless |
| Virtual circuit | No virtual circuit |
| Hit overhead | Low overhead |
| Acknowledgment | No acknowledgment |
| Windowing flow control | No windowing or flow control |

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) is a transportation protocol that is one of the core protocols of the Internet protocol suite. Both TCP and UDP work at transport layer TCP/IP model and both have very different usage.

**The Internet Layer Protocols**

**What is TCP/IP?**

TCP/IP stands for Transmission Control Protocol / Internet Protocol. It defines how electronic devices (like computers) should be connected over the Internet, and how data should be transmitted between them. TCP/IP provides end-to-end connectivity. TCP/IP is the basic communication language or protocol of the Internet.

It can also be used as a communications protocol in a private network (either an [intranet](http://searchwindevelopment.techtarget.com/definition/intranet) or an [extranet](http://searchenterprisewan.techtarget.com/definition/extranet)). TCP/IP is a two-layer program. The higher [layer](http://searchsoftwarequality.techtarget.com/definition/layer), Transmission Control Protocol, manages the assembling of a message or file into smaller [packet](http://searchnetworking.techtarget.com/definition/packet)s that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, [Internet Protocol](http://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol), handles the [address](http://searchnetworking.techtarget.com/definition/address) part of each packet so that it gets to the right destination.

**TCP - Transmission Control Protocol**

TCP is responsible for breaking data down into small packets before they can be sent over a network, and for assembling the packets again when they arrive.

**IP - Internet Protocol**

IP is a "connection-less" communication protocol. IP takes care of the communication between computers. It is responsible for addressing, sending and receiving the data packets over the Internet. IP is rule for addressing of computer. IP is responsible for "routing" each packet to the correct destination.

## What is IP Addresses?

IP uses 32 bits, or four numbers between 0 and 255, to address a computer.

IP addresses are normally written as four numbers separated by a period, like this: 192.168.1.50.

Each computer must have an unique IP address before it can connect to the Internet.

Each IP packet must have an address before it can be sent to another computer.

In computer terms, TCP/IP uses 32 bits addressing. It uses 4 **bytes**. One byte is**8 bits**. One byte can contain 256 different values:

00000000, 00000001, 00000010, 00000011, 00000100, 00000101, 00000110, 00000111, 00001000 .......and all the way up to 11111111.

## Three of the most common TCP/IP protocols OR TCP/IP Protocols for the Web.

Web browsers and servers use TCP/IP protocols to connect to the Internet. Common TCP/IP protocols are:

**HTTP - Hyper Text Transfer Protocol**

HTTP takes care of the communication between a web server and a web browser. HTTP is used for sending requests from a web client (a browser) to a web server, returning web content (web pages) from the server back to the client.

**HTTPS - Secure HTTP**

HTTPS takes care of secure communication between a web server and a web browser. HTTPS typically handles credit card transactions and other sensitive data.

**FTP - File Transfer Protocol**

FTP takes care of transmission of files between computers. FTP is not just a protocol; it’s also a program.

## What is Domain Names Server?

A name is much easier to remember than a 12 digit number.

Names used for TCP/IP addresses are called domain names.

www.google.com is a domain name.

When you address a web site, like http:// www.google.com, the name is translated to a number by a Domain Name Server (DNS).

All over the world, DNS servers are connected to the Internet. DNS servers are responsible for translating domain names into TCP/IP addresses.

When a new domain name is registered together with a TCP/IP address, DNS servers all over the world are updated with this information.

## All TCP/IP Protocols

## TCP/IP Protocols for Email

E-mail programs use TCP/IP for sending and receiving e-mails. The TCP/IP protocols for email are:

**SMTP - Simple Mail Transfer Protocol**

SMTP takes care of sending emails. Often emails are sent to an email server (SMTP server), then to other servers, and finally to its destination. SMTP can only transmit pure text. It cannot transmit binary data like pictures, sounds or movies.

**MIME - Multi-purpose Internet Mail Extensions**

The MIME protocol lets SMTP transmit multimedia files including voice, audio, and binary data across TCP/IP networks. The MIME protocol converts binary data to pure text, before it is sent.

**POP - Post Office Protocol**

The POP protocol is used by email programs to retrieve emails from an email server. If your email program uses POP, all your emails are downloaded to your email program (also called email client), each time it connects to your email server.

**IMAP - Internet Message Access Protocol**

The IMAP protocol works much like the POP protocol. The main difference is that the IMAP protocol will not automatically download all your emails each time your email program connects to your email server.

The IMAP protocol allows you to look through your email messages at the email server before you download them. With IMAP you can choose to download your messages or just delete them. This way IMAP is perfect if you need to connect to your email server from different locations, but only want to download your messages when you are back in your office.

## Other TCP/IP Protocols

**ARP - Address Resolution Protocol**

ARP is used by IP to find the hardware address of a computer network card based on the IP address.

**BOOTP - Boot Protocol**

BOOTP (Boot Protocol) is a simple connection-less protocol, typically used by a disc less workstation to discover its Internet address and/or the name of its bootstrap file. BOOTP operates over UDP (User Datagram Protocol). BOOTP simply discovers the parameters needed for the bootstrap procedure. *BOOTP is used for booting (starting) computers from the network.*

**DHCP - Dynamic Host Configuration Protocol**

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. *DHCP is used for allocation of dynamic IP addresses to computers in a network.*

**ICMP - Internet Control Message Protocol**

The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. *ICMP takes care of error-handling in the network.*

**LDAP - Lightweight Directory Access Protocol**

LDAP is used for collecting information about users and e-mail addresses from the internet.

**NTP - Network Time Protocol**

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use. *NTP is used to synchronize the time (the clock) between computers.*

**PPTP - Point to Point Tunneling Protocol**

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. *PPTP is used for setting up a connection (tunnel) between private networks.*

**RARP - Reverse Address Resolution Protocol**

RARP is used by IP to find the IP address based on the hardware address of a computer network card.

**SNMP - Simple Network Management Protocol**

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. *SNMP is used for administration of computer networks.*

**SSL - Secure Sockets Layer**

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. *The SSL protocol is used to encrypt data for secure data transmission.*

**TLS - Transport Layer Security**

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). *The TLS protocol is a newer and more secure version of SSL.*

**Telnet**

Telnet is a network protocol that allows a user on one computer to log onto another computer that is part of the same network. It is an [application layer](https://en.wikipedia.org/wiki/Application_layer) protocol used on the [Internet](https://en.wikipedia.org/wiki/Internet) or [local area networks](https://en.wikipedia.org/wiki/Local_Area_Network).

**SFTP – Secure File Transfer Protocol**

In computing, the SSH File Transfer Protocol (also Secure File Transfer Protocol, or SFTP) is a network protocol that provides file access, file transfer, and file management over any reliable data stream.

**TFTP – Trivial File Transfer Protocol**

Trivial File Transfer Protocol (TFTP) is a simple, lockstep, File Transfer Protocol which allows a client to get from or put a file onto a remote host. One of its primary uses is in the early stages of nodes booting from a local area network.

IT pros and Sys Admins typically use TFTP configuration for:

* Transferring files
* Remote-booting without hard drives
* Upgrading codes
* Backing up network configurations
* Backing up router configuration files
* Saving IOS images
* Booting PCs without a disk

**RDP – Remote Desktop Protocol**

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

**SIP (VoIP) – Session Initiation Protocol**

The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging, over Internet Protocol (IP) networks.

**RTP (VoIP) – Real-time Transport Protocol**

The Real-time Transport Protocol (RTP) is a network protocol for delivering audio and video over IP networks. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications, television services and web-based push-to-talk features.

**SSH - Secure Shell**

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely.

**SCP - Secure Copy Protocol**

Secure copy or SCP is a means of securely transferring computer files between a local host and a remote host or between two remote hosts. It is based on the Secure Shell (SSH) protocol. "SCP" commonly refers to the: Secure Copy Protocol.

**IGMP – Internet Group Management Protocol**

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast.

**TCP – Transmission Control Protocol**

TCP is one of the main protocols in TCP/IP networks. Whereas the IPprotocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

**UDP – User Datagram Protocol**

UDP (User Datagram Protocol) is an alternative communications protocol to Transmission Control Protocol ([TCP](http://searchnetworking.techtarget.com/definition/TCP)) used primarily for establishing low-latency and loss tolerating connections between applications on the Internet. Both UDP and TCP run on top of the Internet Protocol (IP) and are sometimes referred to as UDP/IP or TCP/IP. Both protocols send short packets of data, called [datagrams](http://searchnetworking.techtarget.com/definition/datagram).

**Data Encapsulation**

1. Encapsulation

Ans: encapsulation is a method of designing modular communication protocols in which logically separate functions in the network are abstracted from their underlying structures by inclusion or information hiding within higher level objects.

1. What is data encapsulation?

Ans. Data encapsulation, sometimes referred to as data hiding, is the mechanism whereby the implementation details of a class are kept hidden from the user. The user can only perform a restricted set of operations on the hidden members of the class by executing special functions commonly called methods. The actions performed by the methods are determined by the designer of the class, who must be careful not to make the methods either overly flexible or too restrictive.

This idea of hiding the details away from the user and providing a restricted, clearly defined interface is the underlying theme behind the concept of an abstract data type.

Data encapsulation, also known as data hiding, is the mechanism whereby the implementation details of a class are kept hidden from the user. The user can only perform a restricted set of operations on the hidden members of the class by executing special functions commonly called *methods*. **Data encapsulation** may refer to:

* The wrapping of private data in classes in object-oriented programming languages: see [Encapsulation (object-oriented programming)](https://en.wikipedia.org/wiki/Encapsulation_%28object-oriented_programming%29), [information hiding](https://en.wikipedia.org/wiki/Information_hiding), [separation of concerns](https://en.wikipedia.org/wiki/Separation_of_concerns)
* [OSI model](https://en.wikipedia.org/wiki/OSI_model) in network protocol design

Data Encapsulation

When a host transmits data across a network to another device, the data goes through *encapsulation*: It’s wrapped with protocol information at each layer of the OSI model. Each layer communicates only with its peer layer on the receiving device.

To communicate and exchange information, each layer uses *Protocol Data Units (PDUs)*.  
These hold the control information attached to the data at each layer of the model. They’re  
usually attached to the header in front of the data field but can also be in the trailer, or end,  
of it.

At a transmitting device, the data-encapsulation method works like this:  
**1.** User information is converted to data for transmission on the network.  
**2.** Data is converted to segments, and a reliable connection is set up between the transmitting and receiving hosts.  
**3.** Segments are converted to packets or datagrams, and a logical address is placed in the  
header so each packet can be routed through an internetwork.  
**4.** Packets or datagrams are converted to frames for transmission on the local network.  
Hardware (Ethernet) addresses are used to uniquely identify hosts on a local network segment.  
**5.** Frames are converted to bits, and a digital encoding and clocking scheme is used.  
To explain this in more detail using the layer addressing, I’ll use Figure 6.12.

Remember that a data stream is handed down from the upper layer to the Transport  
layer. As technicians, we really don’t care who the data stream comes from because that’s  
a programmer’s problem. Our job is to rebuild the data stream reliably and hand it to the  
upper layers on the receiving device.