Q2 (a) Explain the functioning layers in OSI model. Mention the necessity of usin layer concept in OSI model.

Answer

When computers were first linked together into networks, moving information between different types of computers was a very difficult task.

In the early 1980s, the International Standards Organization (ISO) recognized the need for a standard network model. This would help vendors to create interpretable network devices. The Open Systems Interconnection (OSI) reference model, released in 1984, addressed this need.

The OSI model describes how information makes its way from application programs through a network medium to another application program in another computer. It divides this one big problem into seven smaller problems.

Each of these seven problems is reasonably self-contained and therefore more easily solved without excessive reliance on external information. Each problem is addressed by one of the seven layers of the OSI model. The seven layers of the OSI model are:-

- Application
- Presentation
- Session
- Transport
- Network
- Data-link
- Physical

The acronym used to remember these layers is: All People Seem to Need Data Processing. The lower two OSI model layers are implemented with hardware and software. The upper five are generally implemented only in software.

Advantages of Layered Approach

The layered approach to network communications provides the following benefits:

- reduced complexity
- Improved teaching and learning
- Modular engineering
- accelerated evolution
- Interoperable technology
- Standard interfaces

As the information to be sent descends through the layers of a system it looks less and less like human language and more and more like the 1s and 0s that a computer understands.

Example

Let's look at an example of OSI-type communication. Assume that System A has information to send to System B. System A's application program communicates with System A's layer seven (Application Layer). Layer seven communicates with layer six which communicates with layer five and so on until System A's layer one is reached. The information traverses the physical medium and is received by System B's layer one.

It then ascends through System B's layers in reverse order until it finally reaches Syste B's application program.
Each of System A's layers has certain tasks it must perform. Each layer communicates directly with its adjacent layers. However, its primary concern in carrying out its tasks is to communicate with its peer layer in System B.
For example, the primary concern of layer six in System A is to communicate with layer six in System B. It does this using its own layer protocol. Each layer's protocol exchanges information, called protocol data units (PDUs), between peer layers. Each layer uses a specific term for its PDU.
For example, in TCP/IP the transport layer, TCP communicates to the peer TCP function using "segments".
Each layer in System A must rely on services provided by its lower layers for it to communicate with its System B peer. The upper layer is said to be the service user while the lower layer is the service provider. The lower layer services are provided to the upper layer at a service access point (SAP).

Layers - Functions - Devices

The application layer
The application layer of the OSI model is the layer that is closest to the user. Instead of providing services to other OSI layers, it provides services to application programs outside the scope of the OSI model. Its services are often part of the application process.
Main functions are:-
• identifies and establishes the availability of the intended communication partner.
• synchronizes the sending and receiving applications.
• establishes agreement on procedures for error recovery and control of data integrity.
• determines whether sufficient resources for the intended communications exist.
Devices:-
• Browsers
• Search engines
• E-mail programs
• Newsgroup and chat programs
• Transaction services
• Audio/video conferencing
• Telnet
• SNMP

The presentation layer
It ensures that information sent by the application layer of one system will be readable by the application layer of another system. It provides a common format for transmitting data across various systems, so that data can be understood, regardless of the types of machines involved.
The presentation layer concerns itself not only with the format and representation of actual user data, but also with data structure used by programs. Therefore, the presentation layer negotiates data transfer syntax for the application layer.
Devices:-

• Encryption
• EBCDIC and ASCII
• GIF & JPEG

The Session Layer

The main function of the OSI model's session layer is to control "sessions", which are logical connections between network devices. A session consists of a dialog, or data communications conversation, between two presentation entities. Dialogs can be
• Simplex (one-way)
• Half-duplex (alternate)
• Full-duplex (bi-directional)

Simplex conversations are rare on networks. Half-duplex conversations require a good deal of session layer control, because the start and end of each transmission need to be monitored.

Most networks are of course capable of full-duplex transmission, but in fact many conversations are in practice half-duplex.

Some examples of session layer protocols and interfaces are:
• Network File System (NFS)
• Concurrent database access
• X-Windows System
• Remote Procedure Call (RPC)
• SQL
• NetBIOS Names
• AppleTalk Session Protocol (ASP)
• Digital Network Architecture

The Transport Layer

You can think of the transport layer of the OSI model as a boundary between the upper and lower protocols. The transport layer provides a data transport service that shields the upper layers from transport implementation issues such as the reliability of a connection.

The transport layer provides mechanisms for:-
• multiplexing upper layer applications
• The establishment, maintenance, and orderly termination of virtual circuits
• Information flow control
• transport fault detection and recovery
• TCP, UDP, SPX and Sliding Windows.

Multiplexing & De-multiplexing

The transport layer uses a technique called multiplexing to segment and reassemble data from several upper layer applications onto the same transport layer data stream.

When data is being sent, the source machine includes extra bits with the data that encode the message type, originating application, and protocols used.

The destination machine de-multiplexes the data stream, and reassembles the data so that it can be passed up to the destination peer application.

The transport layer data stream provides end-to-end transport services.

It constitutes a logical connection between the end points of an internetwork, that is, the originating host and the destination host. Before data transfer can begin, both the sending and receiving applications inform their respective operating systems that a connection is going to be initiated. In essence, one machine places a call that must be accepted by the other. Protocol software modules in the two operating systems communicate by sending messages across the network to verify that the transfer is authorized and that both sides are ready. After all the synchronization has occurred, a connection is said to be established and data transfer can begin.

Sequencing - Acknowledgements - Flow Control (Windowing)

During a transfer using TCP, the two machines continue to communicate with their protocol software to verify that data is received correctly. Once data transfer is in progress, congestion can occur for two reasons.
First, the sending device might be able to generate traffic faster than the network can transfer it. Second, if multiple devices need to send data through the same gateway, or to the same destination, the gateway or destination may experience congestion.
When data grams arrive too quickly for a device to process, it temporarily stores them in memory and the process being called as buffering. If the data grams are part of a small burst, this buffering solves the problem.
However, if the traffic continues to arrive at this rate, the device eventually exhausts its memory and must discard additional data grams that arrive. Instead of losing data, the transport function can issue a "not ready" indicator to the sender. This acts like a stop sign and signals the sender to discontinue sending segment traffic to its peer.
After the receiving device has processed sufficient segments to free space in its buffers, the receiver sends a ready transport indicator - which is like a go signal. When it receives this indicator, the sender can resume segment transmission. The transport layer may provide a reliable service regardless of the quality of the underlying network. One technique that is used to guarantee reliable delivery is called "positive acknowledgement with retransmission". This requires the receiver to issue an acknowledgement message to the sender when it receives data. The sending device keeps a record of each packet it sends and it waits for an acknowledgement before sending another packet. The sender also starts a timer when it sends a packet. It retransmits the packet if the timer expires before an acknowledgement is received.

Acknowledging every data segment, however, has its drawbacks. If the sender has to wait for an acknowledgement of each data segment, the throughput will be very low.
A technique called "windowing" is used to increase the throughput. Time is available after the sender finishes transmitting the data segment, but before the sender finishes processing any received acknowledgement. This is used for transmitting more data. The number of data elements the sender is allowed to have outstanding is known as the "window". For example, with a window size of three the sender can transmit three data segments before expecting an acknowledgement.
In reality, the acknowledgements and data segments will intermix as they communicate across the network. This is known as "piggyback acknowledgement".

The Network Layer

Layer three of the OSI model is the network layer.
• The network layer sends packets from source network to destination network.
• It provides consistent end-to-end packet delivery services to its user, the transport layer.
In wide area networking a substantial geographic distance and many networks can separate two end systems that wish to communicate. Between the two end systems the data may have to be passed through a series of widely distributed intermediary nodes. These intermediary nodes are normally routers.
Routers are special stations on a network, capable of making complex routing decisions.
• The network layer is the domain of routing.
Routing protocols select optimal paths through the series of interconnected networks.
Network layer protocols then move information along these paths.
• One of the functions of the network layer is "path determination".
Path determination enables the router to evaluate all available paths to a destination and determine which to use. It can also establish the preferred way to handle a packet.
After the router determines which path to use it can proceed with switching the packet.
It takes the packet it has accepted on one interface and forwards it to another interface or port that reflects the best path to the packet's destination.

Devices:-

• IP, IPX, Routers, Routing Protocols (RIP, IGRP, OSPF, BGP etc), ARP, RARP, ICMP.

The Data-Link Layer
Layer two of the OSI reference model is the data-link layer. This layer is responsible for providing reliable transit of data across a physical link. The data-link layer is concerned with
• Physical addressing; Bridges, Transparent Bridges, Layer 2 Switches
• Network topology; CDP
• Line discipline (how end systems will use the network link)
• Error notification
• ordered delivery of frames
• flow control
• Frame Relay, PPP, SDLC, X.25, 802.3, 802.3, 802.5/Token Ring, FDDI.

At the data-link layer, the bits that come up from the physical layer are formed into data frames, using any of a variety of data-link protocols. Frames consist of fields, containing bits. The data-link layer is subdivided into two sub layers:
• The logical link control (LLC) sub layer
• The media access control (MAC) sub layer

The LLC sub layer provides support for
• Connections between applications running on a LAN
• flow control to the upper layer by means of ready/not ready codes
• Sequence control bits.
The MAC sub layer provides orderly access to the LAN medium. For multiple stations to share the same medium and still uniquely identify each other, the MAC sub layer defines

hardware, or data-link address called the "MAC address". The MAC address is unique fo each LAN interface. On most LAN interface cards the MAC address is burned into ROM. The ROM MAC address is sometimes known as the burned-in address (BIA).
Before a frame is exchanged with a device on the same LAN, the sending device needs to have a MAC address it can use as a destination address.
The sending device may use an address resolution protocol (such as TCP/IP's address resolution protocol (ARP)) to discover the destination's MAC address. In other protocols

The Physical Layer
Layer one of the OSI model is the physical layer. The physical layer is concerned with the interface to the transmission medium. At the physical layer, data is transmitted onto the medium (e.g. coaxial cable or optical fiber) as a stream of bits.
So, the physical layer is concerned, not with networking protocols, but with the transmission media on the network.
The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems. This layer puts 1's & 0's onto the wire.
Characteristics specified by the physical layer include
• Voltage levels
• Timing of voltage changes
• Physical data rates
• Maximum transmission distances
• Physical connectors

Devices:-
• Hubs, FDDI Hardware, Fast Ethernet, Token Ring Hardware.

Q2 (b) Define the following:-

(i) Bandwidth **(ii) Channel capacity**
(iii) Multiplexing **(iv) LAN**

Answer
1) In computer networks, bandwidth is often used as a synonym for data transfer rate - the amount of data that can be carried from one point to another in a given time period (usually a second). This kind of bandwidth is usually expressed in bits (of data) per second (bps). Occasionally, it's expressed as bytes per second (Bps). A modem that works at 57,600 bps has twice the bandwidth of a modem that works at 28,800 bps. In general, a link with a high bandwidth is one that may be able to carry enough information to sustain the succession of images in a video presentation.

2) In electronic communication, bandwidth is the width of the range (or band) of frequencies that an electronic signal uses on a given transmission medium. In this usage, bandwidth is expressed in terms of the difference between the highest-frequency signal component and the lowest-frequency signal component. Since the frequency of a signal is measured in hertz (the number of cycles of change per second), a given bandwidth is the difference in hertz between the highest frequency the signal uses and the lowest

frequency it uses. A typical voice signal has a bandwidth of approximately three kilohertz (3 kHz); an analog television (TV) broadcast video signal has a bandwidth of six megahertz (6 MHz) -- some 2,000 times as wide as the voice signal

ii) In electrical engineering, computer science and information theory, channel capacity is the tightest upper bound on the amount of information that can be reliably transmitted over a communications channel. By the noisy-channel coding theorem, the channel capacity of a given channel is the limiting information rate (in units of information per unit time) that can be achieved with arbitrarily small error probability.

Information theory, developed by Claude E. Shannon during World War II, defines the notion of channel capacity and provides a mathematical model by which one can compute it. The key result states that the capacity of the channel, as defined above, is given by the maximum of the mutual information between the input and output of the channel, where the maximization is with respect to the input distribution.

iii.) Multiplexing is sending multiple signals or streams of information on a carrier at the same time in the form of a single, complex signal and then recovering the separate signals at the receiving end. In analog transmission, signals are commonly multiplexed using frequency-division multiplexing (FDM), in which the carrier bandwidth is divided into sub channels of different frequency widths, each carrying a signal at the same time in parallel. In digital transmission, signals are commonly multiplexed using time-division multiplexing (TDM), in which the multiple signals are carried over the same channel in alternating time slots. In some optical fiber networks, multiple signals are carried together as separate wavelengths of light in a multiplexed signal using dense wavelength division multiplexing (DWDM).

Multiplexing is the process where multiple channels are combined for transmission over a common transmission path.

There are two predominant ways to multiplex:

- Frequency Division Multiplexing
- Time Division Multiplexing

Frequency Division Multiplexing (FDM)

In FDM, multiple channels are combined onto a single aggregate signal for transmission. The channels are separated in the aggregate by their FREQUENCY.

There are always some unused frequency spaces between channels, known as "guard bands". These guard bands reduce the effects of "bleed over" between adjacent channels, a condition more commonly referred to as "crosstalk".

FDM was the first multiplexing scheme to enjoy widescale network deployment, and such systems are still in use today. However, Time Division Multiplexing is the preferred approach today, due to its ability to support native data I/O (Input/Output) channels.

FDM Data Channel Applications

Data channel FDM multiplexing is usually accomplished by "modem stacking". In this case, a data channel's modem is set to a specific operating frequency. Different modems

with different frequencies could be combined over a single voice line. As the number of these "bridged" modems on a specific line changes, the individual modem outputs need adjustment ("tweaking") so that the proper composite level is maintained. This VF level is known as the "Composite Data Transmission Level" and is almost universally -13 dBm0.

Time Division Multiplexing
In Time Division Multiplexing, channels "share" the common aggregate based upon time! There are a variety of TDM schemes, discussed in the following sections:

Conventional Time Division Multiplexing
Statistical Time Division Multiplexing
Cell-Relay/ATM Multiplexing

Conventional Time Division Multiplexing (TDM)
Conventional TDM systems usually employ either Bit-Interleaved or Byte-Interleaved multiplexing schemes as discussed in the subsections below.

Clocking (Bit timing) is critical in Conventional TDM. All sources of I/O and aggregate clock frequencies should be derived from a central, "traceable" source for the greatest efficiency.

iv) Page Number 32 of Text Book

Q2 (c) Give the applications of TCP/IP. Mention any 3 protocols that operate in
(i) TCP (ii) I/P

Answer Page Number 59-60 of Text Book

Q3 (a) Compare the following:
(i) Twisted pair (ii) Coaxial pair
(iii) Optical fiber

Answer Page Number 112-121 of Text Book

Q3 (b) Explain the following transmission impairments and mention how it affects the Communication System:-
(i) Attenuation (ii) Delay distortion
(iii) Noise

Answer Page Number 92 – 95 of Textbook

Q3 (c) Define Nyquist bandwidth and Shannon's Capacity. Give their equations.

Answer Page Number 99 – 100 of Textbook

Q4 (a) Discuss any two methods to transform analog data to digital signal with a block diagram.

Answer Page Number 168-171 of Text Book

Q4 (b) Give an example of CRC method in error detection.

Answer

To compute an *n*-bit binary CRC, line the bits represent the input in a row, and position the (*n*+1)-bit pattern representing the CRC's divisor (called a "polynomial") underneath the left-hand end of the row.

Start with the message to be encoded:

```
11010011101100
```

This is first padded with zeroes corresponding to the bit length *n* of the CRC. Here is the first calculation for computing a 3-bit CRC:

```
11010011101100 000 <--- input left shifted by 3 bits
1011               <--- divisor (4 bits) = x³+x+1
------------------
01100011101100 000 <--- result
```

If the input bit above the leftmost divisor bit is 0, do nothing. If the input bit above the leftmost divisor bit is 1, the divisor is XORed into the input (in other words, the input bit above each 1-bit in the divisor is toggled). The divisor is then shifted one bit to the right, and the process is repeated until the divisor reaches the right-hand end of the input row. Here is the entire calculation:

```
11010011101100 000 <--- input left shifted by 3 bits
1011               <--- divisor
01100011101100 000 <--- result
 1011              <--- divisor...
00111011101100 000
  1011
00010111101100 000
   1011
00000001101100 000
       1011
00000000110100 000
        1011
00000000011000 000
         1011
00000000001110 000
          1011
00000000000101 000
           101 1
-----------------
00000000000000 100 <---remainder (3 bits)
```

Since the leftmost divisor bit zeroed every input bit it touched, when this process ends the only bits in the input row that can be nonzero are the n bits at the right-hand end of the row. These *n* bits are the remainder of the division step, and will also be the value of the CRC function (unless the chosen CRC specification calls for some postprocessing).

The validity of a received message can easily be verified by performing the above calculation again, this time with the check value added instead of zeroes. The remainder should equal zero if there are no detectable errors.

```
11010011101100 100 <--- input with check value
1011               <--- divisor
01100011101100 100 <--- result
 1011              <--- divisor ...
00111011101100 100


......


00000000001110 100
          1011
00000000000101 100
           101 1
-----------------
          0 <--- remainder
```

Q4 (c) Compare synchronous and asynchronous transmission. Give their respective applications.

Answer Page Number 189 – 191 of Textbook

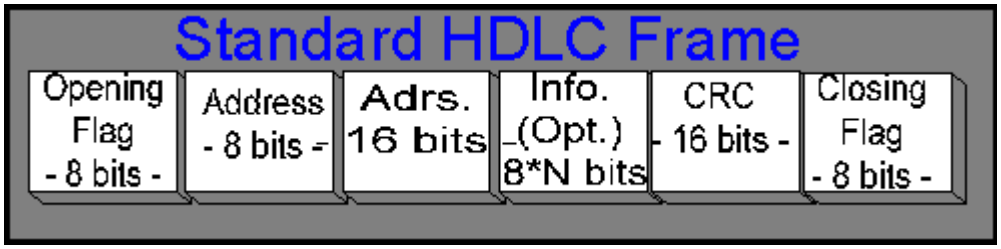
Q5 (a) Explain the role of flow control and error control in data link protocols.

Answer Page Number 225-236 of Textbook

Q5 (b) Explain the HDLC Frame format with a diagram.

Answer

The standards frame of the HDLC protocol handles both data and control messages. It has the following format: The length of the address field is commonly 0, 8 or 16 bits, depending on the data link layer protocol.



For instance the SDLC use only 8 bit address, while SS#7 has no address field at a because it is always used in point to point links.

The 8 or 16 bit control field provides a flow control number and defines the frame type (control or data). The exact use and structure of this field depends upon the protocol using the frame.

Data is transmitted in the data field, which can vary in length depending upon the protocol using the frame. Layer 3 frames are carried in the data field.

Error Control is implemented by appending a cyclic redundancy check (CRC- The Frame Control Sequence (FCS) is the HDLC frame is in most cases - 16 bit wide , the generator polynomial used is normally CRC-CCITT: x^16+x^12+x^5+1) to the frame, which is 16 bits long in most protocols.

Frame Classes:

In the HDLC protocol, three classes of frames are used:

Unnumbered frames - (Unnumbered frames are used for link management, for example they are used to set up the logical link between the primary station and a secondary station, and to inform the secondary station about the mode of operation which is used.) are used for link management.

Information frames - (Information frames are those who carry the actual data. The Information frames can be used to piggyback acknowledgment information relating to the flow of Information frames in the reverse direction when the link is being operated in ABM or ARM.) are used to carry the actual data.

Supervisory frames - are used for error and flow control.

Frame types: Three classes of secondary station and to inform the secondary station of the mode of operation to be used.) Frames, for example, are used both to set up logical link between the primary and the secondary station and to inform the secondary station of the mode of operation to be used. A logical link is subsequently cleared by the primary station sending a DISC (DISC is one kind of unnumbered frame. It is used to clear a logical link) frame. The UA (UA is one kind of unnumbered frame. It is used as an acknowledgment to other frames) frame is used as an acknowledgment to the other frames in this class.

There are four types of supervisory frames but only RR (A kind of a supervisory frame, which means: Receiver Ready. The Receiver signals the the transmitter that both, the physical layer and the application layer above it are ready to process messages.) and RNR (A kind of a supervisory frame , which means receiver not ready. This response is initiated by the application, if it is not ready, to process message. It means that layer 0 (the physical layer) is

functional, but the application above it is not.) are used in both NRM an ABM These frames are used both to indicate the willingness or otherwise of a secondary station to receive an information frame from the primary station, and for acknowledgment purposes. REJ (A kind of frame that is used only in ABM which permits simultaneous two-way communication across a point to point link. It is used with the go back N procedure) and SREJ (A kind of frame that is used only in ABM which permits simultaneous two-way communication across a point to point link. It is used with a selective repeat transmission procedure) frames are used only in ABM which permits simultaneous two-way communication across a point to point link. The two frames are used to indicate to the other station that a sequence error has occurred, that is an information frame containing an out of sequence N(s) has been received. the SREJ frame is used with a selective repeat transmission procedure, whereas the REJ frame is used with a go back N procedure. Unnumbered frames are used for link management.

Q5 (c) How is statistical TDM different from Synchronous TDM? Explain

Answer

In synchronous TDM, each input has a reserved slot in the output frame. This can be inefficient if some input lines have no data to send. In statistical time-division multiplexing, slots are dynamically allocated to improve bandwidth efficiency. Only when an input line has a slot's worth of data to send is it given a slot in the output frame. In statistical multiplexing, the number of slots in each frame is less than the number of input lines. The multiplexer checks each input line in round robin fashion; it allocates a slot for an input line if the line has data to send; otherwise, it skips the line and checks the next line. Some slots are empty in the former because the corresponding line does not have data to send. In the latter, however, no slot is left empty as long as there are data to be sent by any input line.

Q6 (a) Define Choke packet. Explain implicit Congestion Signaling and explicit Congestion Signaling in Congestion control.

Answer Page Number 418 to 420 of Textbook

Q6 (b) Mention routing parameters in packet switching networks. Mention features of adaptive routing.

Answer Page Number 387 to 394 of Textbook

Q7 (a) Explain LAN Protocol architecture. Mention LLC Services.

Answer Page Number 491- 494 of Textbook

Q7 (b) Draw IEEE 802.3 frame format used in Ethernet. Mention the features o each field.

Answer Page Number 524 of Textbook

Q7 (c) Draw the architecture of IEEE 802.11 and explain its services.

Answer Page Number 571 of Text Book

Q8 (a) Draw the IP address formats for Class A to Class E.

Answer Page Number 611 of Text Book

Q8 (b) Draw IPv6 header format and explain its fields.

Answer Page Number 620-621 of Text Book

Q8 (c) Explain the working of IP (Internet Protocol).

Answer Page Number 601 – 602 of Text Book

Q9 (a) Describe and compare the following routing algorithms:
(ii) Border Gateway Protocol

Answer Page Number 645 – 656 of Textbook

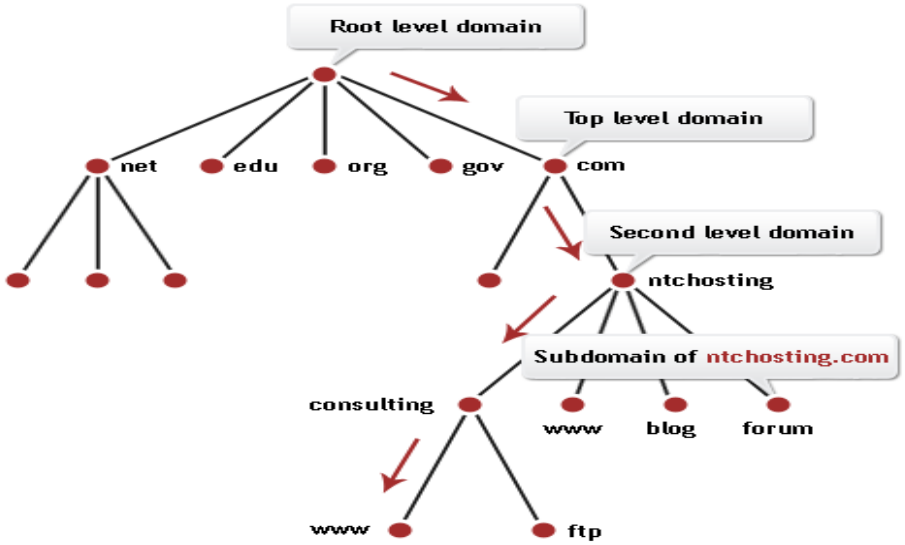
Q9 (b) Give a short note on DNS and explain its working.

Answer

Short for Domain Name System (or Service or Server), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

What does actually stand behind that almighty 3-letter abbreviation - DNS? DNS refers to Domain Name System and represents a powerful Internet technology for converting domain names to IP addresses. Its special mission is to be a mediator between the IP addresses, the system-side names of the websites and their respective domains, and their user-side alpha-numeric titles. Another important function of the DNS is to control the delivery of email messages. Behind every site, there is an IP address. But, while it's easy to remember the name of a website, it's quite hard to remember the exact IP address. For example, everybody knows about Google.com, but if you had to remember "74.125.45.100", things would have been much harder.

How does DNS work? A DNS program works like this - every time a domain name is typed in a browser it is automatically passed on to a DNS server, which translates the name into its corresponding IP address (e.g. the domain name NTC Hosting.com is translated to 66.40.65.49). Thanks to the DNS, we do not need to bother to remember complicated numeric combinations to reach a certain website - we can use its meaningful and much easier to remember domain name instead.
Hierarchy of domain names



Q9 (c) Differentiate between TCP and UDP.

Answer Page Number 699-720 of Text Book

Text Books

Data and Computer Communications, Eight Edition (2007), William Stallings, Pearson Education Low Price Edition.