Green University

Midterm Exam Assignment

Course Title: Data Communication

Course Code: CSE 307

Section: PC DA

Submitted to

Farhana Akter Sunny

Lecturer & Program Coordinator

Dept. of CSE

Green University of Bangladesh

Submitted by:

Mohammad Nazmul Hossain

ID:193902031

Dept. of CSE

Ans to the Questions No:01

Logical addresses are generated by the CPU. A logical address is an IP address that is not fixed and regularly changes and it depends upon the Network layer. If a packet is going from one network to another, need another addressing system to help distinguish source and destination systems. Network layer adds Header to the data coming from upper layers that among other things include LOGICAL ADDRESS of the sender and receiver. Logical addresses are created and used by Network layer protocols such as IP or IPX. The Network layer protocol translates logical addresses to MAC addresses. For example, I'm using an IP as the network layer protocol, devices on the network are assigned IP addresses such as 207.120.67.30. Because the IP protocol must use a Data Link layer protocol to actually send packets to devices, IP must know how to translate the IP address of a device to the device's MAC address.

The physical address is the location of memory/storage. The physical address is Called a MAC address which is fixed for every system and depends upon the network layer.No sus MAC address is used in the data link layer. which works locally.Means in node to node connection. The physical address is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. The physical address uniquely defines a host on the internet.
For example, "192.168. 1.67:80" shows the IP address Now this IP address is converted to a physical address by a resolution protocol.

A port address is a feature of a network device that translates TCP or UDP communications made between a host and port on an outside network. Port address is used for each process from client to server and it depends on the transport layer. It allows a single IP address to be used for many internal hosts. The port number is "tacked on" to the end of the IP address, for example, "192.168. 1.67:80" shows both the IP address and port number. host server listening to default port 80.

A real-life example where port address, logical address, and physical address is our pc Desktop. Its have a logical address, The physical address, and the port address as well.

Ans to the Questions No:02

The data link layer can detect errors between hops (nodes), but the error at the hope of the hope cannot be detected by the data link layer. So, we need another checking mechanism at the transport layer.

The real problem exists at the data link layer.

Packets have a maximum size of 65535 bytes. Whereas the maximum size of frames (take the example of ethernet) is 1500 bytes. The network layer does not know these parameters. It might send a large packet that is broken up into, say, 10 frames, of which 2 are lost on average. It would then take a very long time for the packet to get through. Instead, if individual frames are acknowledged and retransmitted, then errors can be corrected more directly and more quickly. On reliable channels, such as fiber, the overhead of a heavyweight data link protocol may be unnecessary, but on (inherently unreliable) wireless channels it is well worth the cost.

Ans to the Questions No:03

TCP and UDP protocols are used in the applications. Both UDP and TCP are based on the requirement of the application.

What is TCP?

TCP, or Transmission Control Protocol, is the most common networking protocol online. TCP is extremely reliable and is used for everything from surfing the web (HTTP), sending emails (SMTP), and transferring files (FTP).

TCP is used in situations where it's necessary that all data being sent by one device is received by another completely intact.

For example, when we visit a website, TCP is used to guarantee that everything from the text, images, and code needed to render the page arrives. Without TCP, images or text could be missing, or arrive in the incorrect order, breaking the page.

TCP is a connection-oriented protocol, meaning that it establishes a connection between two devices before transferring data, and maintains that connection throughout the transfer process.

What is UDP?

UDP, or User Datagram Protocol, is another one of the major protocols that make up the internet protocol suite. UDP is less reliable than TCP but is much simpler.

UDP is used for situations where some data loss is acceptable, like live video/audio, or where speed is a critical factor like online gaming.

While UDP is similar to TCP in that it's used to send and receive data online, there are a couple of key differences.

First, UDP is a connectionless protocol, meaning that it does not establish a connection beforehand as TCP does with its three-way handshake.

Next, UDP doesn't guarantee that all data is successfully transferred. With UDP, data is sent to any device that happens to be listening, but it doesn't care if some of it is lost along the way. This is one of the reasons why UDP is also known as the "fire-and-forget" protocol.

Which is Faster – TCP or UDP?

In general, UDP is the faster protocol.

UDP is much simpler and doesn't try to establish a connection between devices before sending data, or verify that all the data even arrived. It simply sends out data to any device that requests it and keeps doing that until the other device disconnects or there is no more data left to send.

But being faster doesn't mean that UDP is the better protocol overall. It just means that it's better in certain situations.

As mentioned earlier, TCP is necessary in situations where it's vital that all data packets are sent in order, and that all packets arrive. The web just wouldn't function without TCP.

And while TCP is slower because of the way it establishes connections, and due to the checks for missing packets, it can still be blazing fast. Because they're on the web and use HTTP, sites like YouTube or Netflix all use TCP to send data to your devices.

TCP also allows for buffering, so your browser can request and load more data as you watch, allowing for smooth playback and for you to skip ahead to other parts of the video.

UDP is the better choice for live video and audio or online games where speed is more important than potential data loss.

Ans to the Questions No:04

How wave propagation occurs in Earth and Freespace:

Ground wave propagation is a type of radio propagation that is also known as a surface wave. The waves follow the curvature of the earth, enabling them to cover beyond the horizon. Beyond the horizon, the waves get blocked by the curvature of the earth and the signals are produced by the diffracted surface wave.

Space wave propagation takes place when the radio waves from a transmitting antenna propagate through the space around the earth to reach a receiving antenna. The radio waves here can propagate either directly or after reflection from the ground or in the troposphere. It comprises direct or reflected waves.

Now, let's compare the Earth and space Wave propagation by some of their characteristics:

1. Ground wave Propagation:

i. Ground wave propagation takes place between the Earth's surface and ionosphere, so we can call it surface wave propagation.
ii. The wave travels with low and medium frequencies of the radio spectrum.
iii. It is the addition of all the waves that are reflected from the earth's surface, so it is called surface wave propagation.

2. Space wave propagation:
Space wave propagation occurs within the troposphere, mostly within 20kms from the earth's surface, so it is often called tropospheric propagation.