LÝ THUYẾT NWC203c cơ bản cần nhớ – Part 1

1. List the functions of a reliable communication service.

The reliability of a communications network is its ability to transport data from node to node with the expectation of the data to arrive with minimal errors. The packets are guaranteed to remain intact. In this case, TCP is considered as reliable compared to UDP. For a system to be reliable, the protocol must include several functions and characteristics:

- Error detection - there must be a method to account for all packets in a message. If some packets are lost, the packet must be re-transmitted. The packets must be reassembled in the correct order.
- Flow control – the flow of data is managed such that the devices can efficiently handle it. TCP uses a Sliding window protocol for flow control.
- Congestion control – TCP uses window flow controls (rwnd and cwnd) for congestion controls.
- Larger header size – reliable protocols have larger headers. For example, TCP has at least 20 bytes compared to 8 bytes in UDP.
- Packet size – reliable protocols have larger packets.
- Connection type – Reliable communication service utilizes connection-oriented protocol. TCP does a 3-way hand shake (SYN, SYN-ACK, ACK) to establish a connection [2].

2. List the functions of an unreliable communication service.

An unreliable communication is determined in the lack of necessity of packets being received as error-free. Tolerance of some errors is acceptable. There is no guarantee of packet integrity. In this case, UDP is considered unreliable as compared to TCP. Unreliable functions and characteristics include:

- Speed – speed is one of the primary benefits of giving up reliability. UDP is faster than TCP.
- Smaller header size – Unreliable communication service have a smaller header size. For example, the UDP header is 8 bytes.
- Smaller packet size – UDP has smaller packet sizes since the overhead is much smaller.
- Connection type – Unreliable communication service use a connectionless protocol. There is type of hand shake, such as the 3-way hand shake in TCP. UDP is a connectionless protocol [2].

3. For each of the following pairs of terms, define each term, making sure to clarify the key difference(s) between the two terms

a. “flow control” and “congestion control”

Flow control is a process in which the packets being sent will not exceed the limit in which the receiving node can receive. It is initiated by the sending node and controlled by the receiving node. Flow control is isolated to the congestion between the sender and receiver [3].

Congestion control is initiated from the sending node but is controlled by the router. This control considers the entire network, not just the path from sender to receiver. This is to avoid a loss of packets from the router buffer overflow [4].

b. “stop and wait protocol” and “sliding window protocol”

In Stop and Wait protocol, the sending node will send one packet and wait for an acknowledgement from the receiving node. Once it received that packet it will send another and wait again. It will continue this cycle until complete. The time it takes for the sender to send a packet to the time it receives an acknowledgement is the Round-Trip Time (RTT), which is twice the propagation delay. This is a very inefficient method of sending data [6].

In Sliding Window protocol, a group of packets are sent. Once the receiving node gets the packets, an acknowledgement is sent. The sending node keeps the group of packets buffered until it receives the acknowledgment. Once the acknowledgment is received, the sending node will “slide’ to the next group of packets. This number of packets can increase to send a larger group. If the acknowledgement is not received, the sender will re-transmit. This method is much more efficient that Stop and Wait protocol [6].

4. There is a choice of transport-layer protocol available in the Internet protocol stack. One choice is the Transmission Control Protocol (TCP). Another choice is the User Datagram Protocol (UDP).

a. What are the header similarities, if any, between these two protocols?

Both have a 2-byte source and a 2-byte destination port number and are used in the same way. Both have a 2-byte checksum to detect corrupted bits [5].

b. What are the functional differences, if any, between these two protocols?

TCP is connection-based, slower, and reliable. TCP has a larger and a more complex packet header.

UDP is connectionless, faster, and less reliable. UDP has a simpler and a smaller packet header.

c. Give two examples of Internet applications that use TCP. Give two examples of Internet applications that use UDP.

Two examples of applications that use TCP are websites (HTTP) and email (SMTP).

Two examples of applications that use UDP are online gaWming and streaming music.

5. What are some of the network elements that you must consider when transitioning to IPv6?

When assessing the transition from IPv4 to IPv6, all elements on the network need to be considered, from end-to-end.

- Router – the router needs to be considered when transitioning since it will the gateway for your network. Since there is still a multitude of IPv4 devices still connected, the router should facilitate IPv6 and IPv4 (Dual Stack).

d

- Hosts – all hosts on the network need to IPv6 compatible. Most newer computers and laptops devices are already IPv6 capable.

- DNS Servers – quad-A (AAAA) records need to be issued instead of A-records to map host names to IPv6 address.

- Switches – some functions operating on layer 3 or higher need to be considered, such as Multicast Listener Discovery (MLD), VLANS, and Dynamic ARP Inspection (DAI) [7].