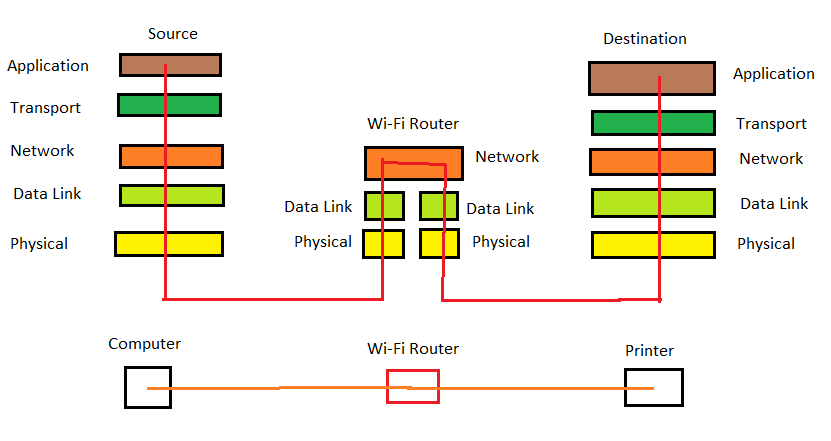
Student Name : Rakyan Satrya Adhikara

Student ID : 219548135

Problem Based Learning Task 1

***Question 1***:

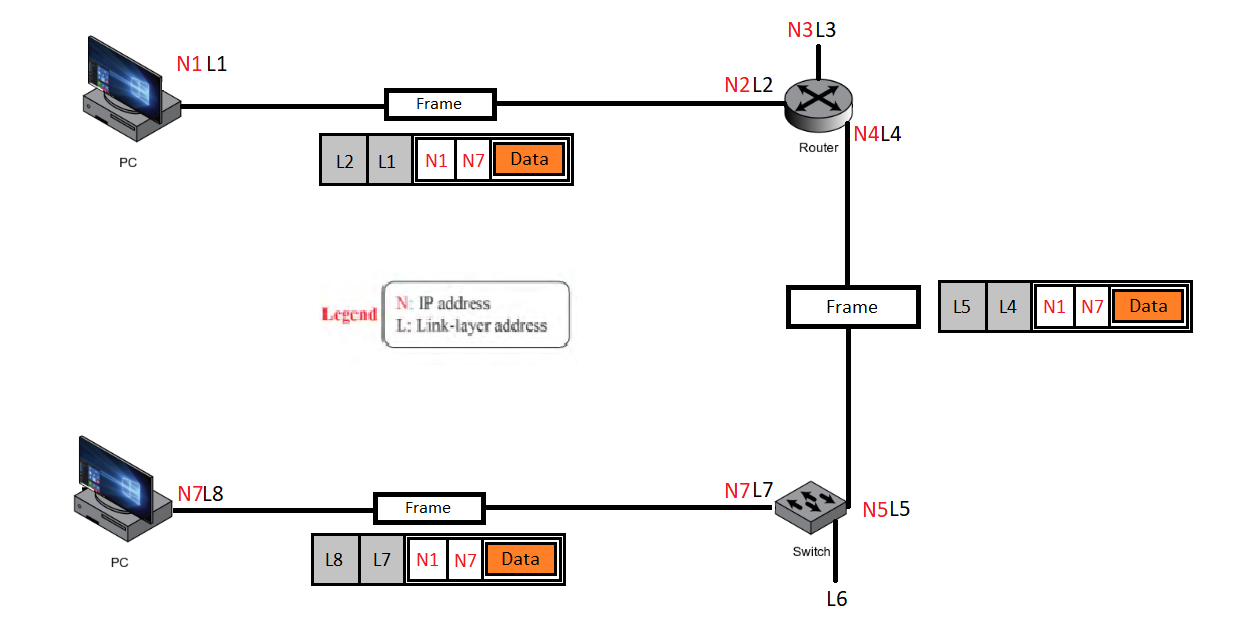
1. Layering simplifies the protocols used in networks and intermediary devices by dividing the task into several smaller and simpler task. This can be achieved by each layer provided with different functions / features.
2. Encapsulation and decapsulation mechanisms achieved logical communication between peer layers by **adding** information in the form of header and/or footer (*Encapsulation*) at a sending layer *n*, which then will be processed and **removed** (*Decapsulation*) by the peer layer *n* at the receiver.
3. A layer needs to communicate with its peer layer at the receiving node, and a protocol for passing information to the layer above and below it. A layer’s header will often include a protocol field, for example to describe which protocol the next layer up is using. It will Include address information targeting the peer layer at the receiving node, and maybe a checksum, or a length field to help with message integrity. Replacing the layer’s protocol with another has less impact on the adjacent layers than it does for the receiving layer at the other node. The peer layers must be the same, but as long as the adjacent layers are compatible with it, it is a non-issue.
4. **For HD task**:



***Question 2***:

1. The delays for Datagram switching are non-uniform due to the volume of packets at any one time. While for Virtual-Circuit switching, the delays are depending on the resource reservation. Thus, Compared to Virtual-Circuit, the delays for Datagram switching can be higher.
2. For the packets that would arrive at the receiver, for Datagram switching, all packets are free to use any available path. While for Virtual-Circuit, it will use a specific path.
3. On how reliable, Virtual-Circuit switching are much more reliable compared to Datagram switching since it ensures that all packets successfully reach the receiver.

***Question 3***:

1. 
2. Some address changed because the frame moved from one link to another. The encapsulation happened at the sender (PC1, Router, Switch) and decapsulation happened at the receiver (Router, Switch, PC2)

***Question 4***:

1. The physical characteristics of WiFi make it impossible and impractical for the CAMA/CD mechanism to be used. This is due to CSMA/CD's nature of 'listening' if the medium is free before transmitting packets. Using CSMA/CD, if a collision is detected on the medium, end-devices would have to wait a random amount of time before they can start the retransmission process. For this reason, CSMA/CD works well for wired networks, however, in wireless networks, there is no way for the sender to detect collisions the same way CSMA/CD does since the sender is only able to transmit and receive packets on the medium but is not able to sense data traversing that medium. Therefore, CSMA/CA is used on wireless networks. CSMA/CA doesn't detect collisions (unlike CSMA/CA) but rather avoids them through the use of a control message. Should the control message collide with another control message from another node, it means that the medium is not available for transmission and the back-off algorithm needs to be applied before attempting retransmission.

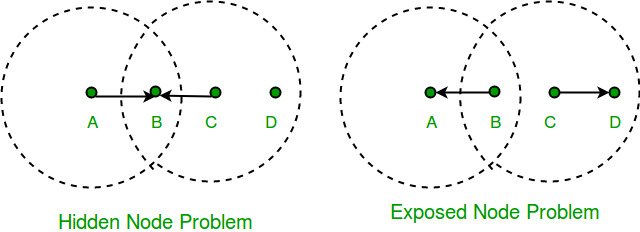


Figure 1: each of four nodes is able to send and receive signals that reach just the nodes to its immediate left and right.

Based on the figure above, for example, B can exchange frames with A and C but it cannot reach D, while C can reach B and D but not A. (A and D's reach is not shown in the figure.) Suppose both A and C want to communicate with B and so they each send it a frame. A and C are unaware of each other since their signals do not carry that far. These two frames collide with each other at B, but unlike an Ethernet, neither A nor C is aware of this collision. A and C are said to be hidden nodes with respect to each other.

"In wireless networking, the hidden node problem or hidden terminal problem occurs when a node is visible to a wireless access point (AP), but not to other nodes communicating with that AP."

Collision cannot be detected in hidden node problem

This is because the nodes A and C are out of range of each other(and so cannot detect a collision while transmitting). Thus, Carrier sense multiple access with collision detection (CSMA/CD) does not work, and collisions occur. The data received by the access point is corrupted due to the collision. To overcome the hidden node problem, RTS/CTS handshaking (IEEE 802.11 RTS/CTS) is implemented in addition to the Carrier sense multiple access with collision avoidance (CSMA/CA) scheme.

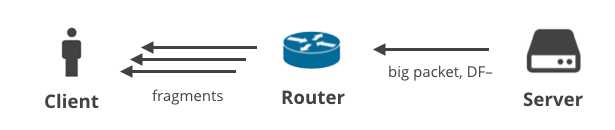
A related problem, called the exposed node problem, occurs under the following stated circumstances:

* Suppose B is sending to A (as in the above Figure).
* Node C is aware of this communication because it hears B's transmission.
* It would be a mistake for C to conclude that it cannot transmit to anyone just because it can hear B's transmission.

For example, suppose C wants to transmit to node D. This is not a problem since C's transmission to D will not interfere with A's ability to receive from B.

We address these problems by an algorithm known as Multiple Access with Collision Avoidance (MACA). The sender and receiver exchange frames with each other before transmitting data. This informs all nearby nodes that a transmission is about to begin. Sender transmits Request to Send (RTS) frame to receiver . The receiver then replies with clear to send (CTS) frame back to the sender. Any node that receives CTS frame knows that it is close to the receiver, therefore, cannot transmit a frame. Any node that receives RTS frame but not the CTS frame knows that is not close to the receiver to interfere with it, so it is free to transmit data.

***Question 5***:

1. 
2. A Router may connect different physical networks. Incoming IP datagram may be encapsulated inside an Ethernet frame. Outgoing same IP datagram may be encapsulated in a Token Ring frame. Each type of frame may have its Maximum Transfer Unit.

The size of an IP datagram may be up to 65,535. This is too big for some physical networks. The IP datagram must be fragmented into smaller units to pass through. It could even be further fragmented by other routers ahead. Each fragment becomes a datagram with its own header. Reassembly is done at destination host.

Identification: Set by the source host (a counter incremented each time a datagram is emitted). Together with the source IP address, it uniquely identifies the datagram. All fragments of this datagram will copy the same Identification.

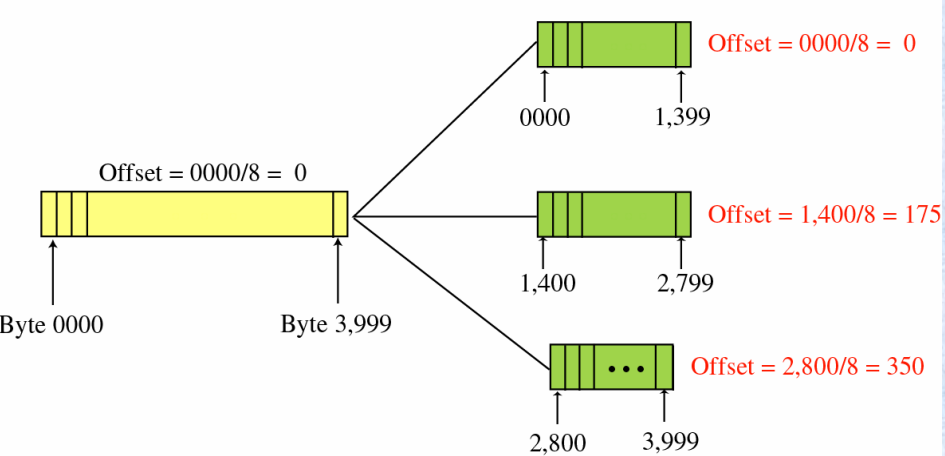


Figure 2: The refined explanation of fragmentation