OSI MODEL, FUNCTIONS OF EACH LAYER, Unit1

Nithya Mam, CSPC53 Networks

PHYSICAL LAYER

Data is in the form of 0s and 1s. Physical layer takes the responsibility of transmitting bit streams through coaxial cables, twisted pair cables or fibre optic cables. Its functionality is entirely implemented in hardware – each device has their layer in the form of network adapter / serial port. The physical layer needs to define the characteristics of the interface between the device and the medium.

Line Configuration: The physical layer needs to take care of the line configuration.

Physical Topologies: The physical layer considers how devices are connected to make a network. Source, destination, and intermediates may each have different types of topologies.

Transmission Mode: Physical layer needs to transmit data both unidirectionally (simplex), bidirectionally (half-duplex) and simultaneously (full-duplex).

Representation of Bits: Since the physical layer is going to transmit only 0s and 1s along the medium, which contains only electric signals, the physical layer must decide how much voltage is needed to represent the bits 0 and 1. The destination also needs to follow the same. This conversion is known as encoding – there are different encoding mechanisms.

The physical layer needs to take care of the data rate also – the number of bits transferred per second.

The physical layer also needs to decide the duration of the bit – for how long a single bit must be transmitted.

Synchronization – the physical layer must ensure synchronization between the source and destination.

DATA LINK LAYER

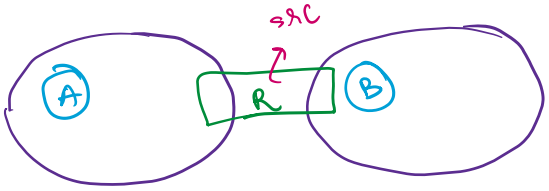
(Both header and tailer are added)

SENDER SIDE:

Framing – In the sender side, the data link layer receives information from the network layer. After receiving the data, the frame needs to be constructed from the received data – where to start and where to stop – the size of the frame, and how to identify the frame starting – all is taken care of by the DLL.

Physical Addressing / Mac Addressing – In a network, a source and destination address is present. If the destination is in the same network, then no problem occurs – we can have the same physical address as the destination address. But if the destination is in another network and there is a connecting device between the networks – the source address will be 'A' and the destination address will be 'R'. A,

R and B are the physical addressing of the devices. Then source address will be 'R' and destination address will be 'B'.



Flow Control – If the receiving rate is lesser than the transmitting rate, then proper flow control is needed. Sometimes the flow control techniques may be very simple, for example, the receiver may not send any acknowledgement to the transmitter – so the transmitter must wait – there will not be any data transmission during this period.

Access Control – If the transmitting media is shared by 2 devices, then proper access control is needed. If there is a dedicated link between 2 devices, then access control will not be required. But otherwise, it is needed, to know which device will transmit next and for what period.

RECEIVER SIDE:

Error Control:

Before removing the header and tailer, framing needs to be done. Data (bit streams) need to be converted back to frames, based on the framing techniques used. The receiver must know how to do framing (where to start) – Assuming we have 10 bits and receiver has 3 bits per frame, the receiver must do proper framing.

After framing, it must check for transmission error. Once error is detected, it needs to be changed. If there is a single bit error (a 0 becomes a 1 or a 1 becomes a 0) – the error correction is simple. But if there are continuous bits with error – proper error correction techniques become necessary.

If the service is reliable, there are no transmission errors, and the receiver must send acknowledgement. Once the acknowledgement is received, the transmitter knows that the data is successfully received without any error and will transmit the remaining bits.

If acknowledgement is lost, delay occurs, and the same data is retransmitted to the receiver – the packet is now a repeating packet – identification of repeating packets is also a part of error control techniques. These functionalities are implemented using network adapters and their drivers (hardware and software).

NETWORK LAYER

It is responsible for transmitting data from 'A' to 'B'.

In DLL, physical addressing / mac addressing is present. It is not possible to have a unique mac addressing for each device. Different devices on the same network

may have the same mac addressing. To avoid these types of problems, we can use logical addressing provided by the network layer.

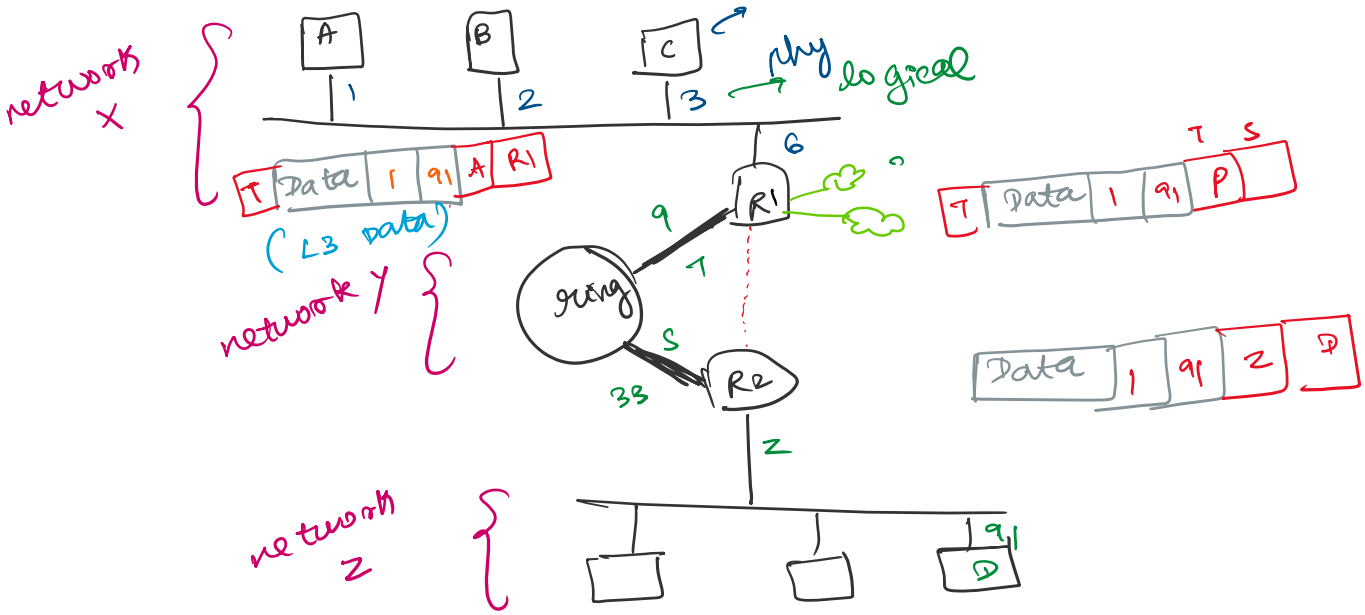
In DLL, the addressing problem is controlled locally. If the packet however is to be transmitted from one network to another, we need to have proper logical addressing between the source and destination.

Logical addresses are unique. It is not possible to have duplicates, otherwise the reception of data will not be performed correctly.

Eg: data transmitted from A to D. First data is transmitted from A to R1, then it must be decided as to from which interface (path) data must be forwarded.

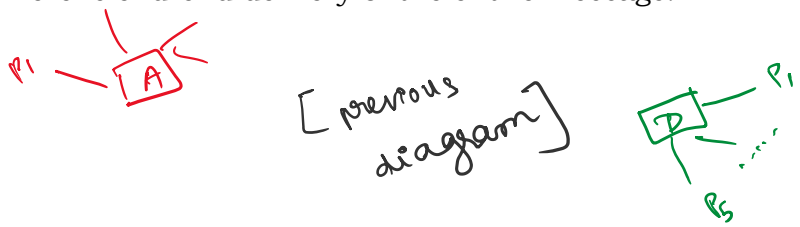
DLL – node to node delivery, NL – source to destination delivery – main difference

The connecting devices must have exact information about the entire network, to decide the best path. In broadcast network, only one device transmits, and all other devices receive the data – therefore there aren't many problems in terms of routing.



TRANSPORT LAYER

There is end-end delivery of the entire message.



The transport layer is responsible for transmitting data from process P1 running on A to process P5 running on D – transmission of the entire message is considered.

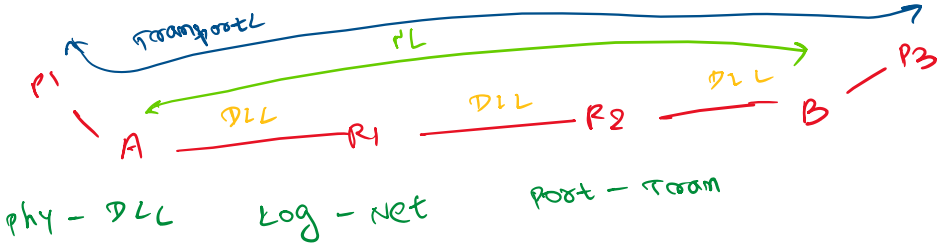
Network layer – responsibility is only within the packets – it doesn't know about the relationship between the packets. It treats each packet independently. But the transport layer – all packets are assumed to be dependent and from the same message. They must be transported from the source process to the destination process.

One more addressing is required here – for the processes, known as port addressing or service point addressing. To transmit a single packet, we now need 3 levels of addressing - physical addressing, logical addressing and port addressing. Port addressing is provided by the transport layer.

Segmentation and Re-assembling of packets: Segmentation involves breaking a message into messages of smaller sizes. Since the packet needs to be transmitted across different networks, the connecting devices and other intermediate devices may have their own restrictions on the message size based on the cable used. Segmentation is done by the sender and re-assembling is done by the receiver.

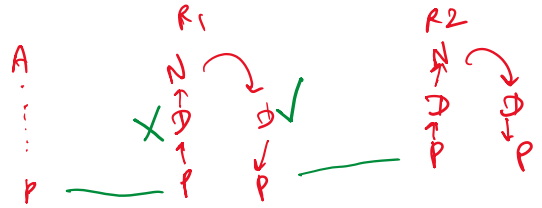
Connection-Control: The transport layer provides either connection-oriented or connectionless service.

Flow and Error Control: Flow and error control in the network layer is only for control between 2 nodes. Here it is applicable to the whole path, from the starting source process to the destination process.



In DLL, we have F and E control. In TL also, we have F and E control. Why?

Everything is fine between node to node, but still, we need F and E control from point to point. From R1 to R2, if any error is present, the R2 DLL needs to identify the error.



After receiving data, the DLL verifies for error and passes the data to the network layer. If the logical addresses do not match, R1 assumes that it is not the intended destination and takes a decision to forward. Based on routing tables and other algorithms, R1 finds the next node to be used and again resends the data to the DLL. One DLL is crossed twice.

Errors may appear during transmission through the transport layer which R1 and R2 cannot catch – this is why Flow and Error Control is provided with flow and error control.

SESSION LAYER

It is the network dialog controller. It is mainly used to maintain and synchronize the interaction between the devices. It performs dialog control – the source and destination must enter a dialogue and the session layer helps to synchronize between the devices. Communication may be full duplex or half duplex.

It provides synchronization by adding checkpoints in the data. Eg a file with 100 pages is transmitted without any checkpoints. Then if there is any error, for example in page number 75, or 99, then the entire page set starting from 1 must be retransmitted – we don't know from where the file corruption has started. To avoid this, checkpoints are added, say after every 10 pages. If there is any error, retransmission can be done only from the previous checkpoint instead of from the beginning. If there is an error at page 75, we only need to retransmit from page 70.

PRESENTATION LAYER

It mainly controls the syntax and semantics of the information.

1. *Translation*: Communication may occur between different kinds of systems. In the source machine, it may use one type of character encoding system, while the destination may use another type of character encoding system [ASCII, extended ASCII are some examples]. In such cases, inter-operability is taken care of by the presentation layer.

The presentation layer in the source converts the sender specific encoded characters into common format. Then, the presentation layer in the destination device converts the common format characters into the destination specific encoded characters.

2. *Encryption and Decryption*: Sender information is encrypted by the presentation layer in the source network so that no one else can understand the message being transmitted. The encrypted information is then transmitted to the receiver network. Then, the presentation layer in the receiver network decrypts the message. These encryption and decryption algorithms are responsible for secure communication.

3. *Compression*: The number of bits to be transmitted is reduced. This is highly useful when multi-media data is transmitted.

APPLICATION LAYER

It provides user interfaces and supports email system, remote file accessing and other types of distributed information services. It provides support for FTP (file transfer protocol).

Why is layered architecture needed – By distributing the work of various functions between various layers, more modularity is achieved, and clear interfaces can be provided between the modules. It becomes very easy to identify where errors have occurred. This also helps in better understanding. We also need to ensure the independence of the layers – if one of the layers is enhanced or modified, it must not affect the other layers.