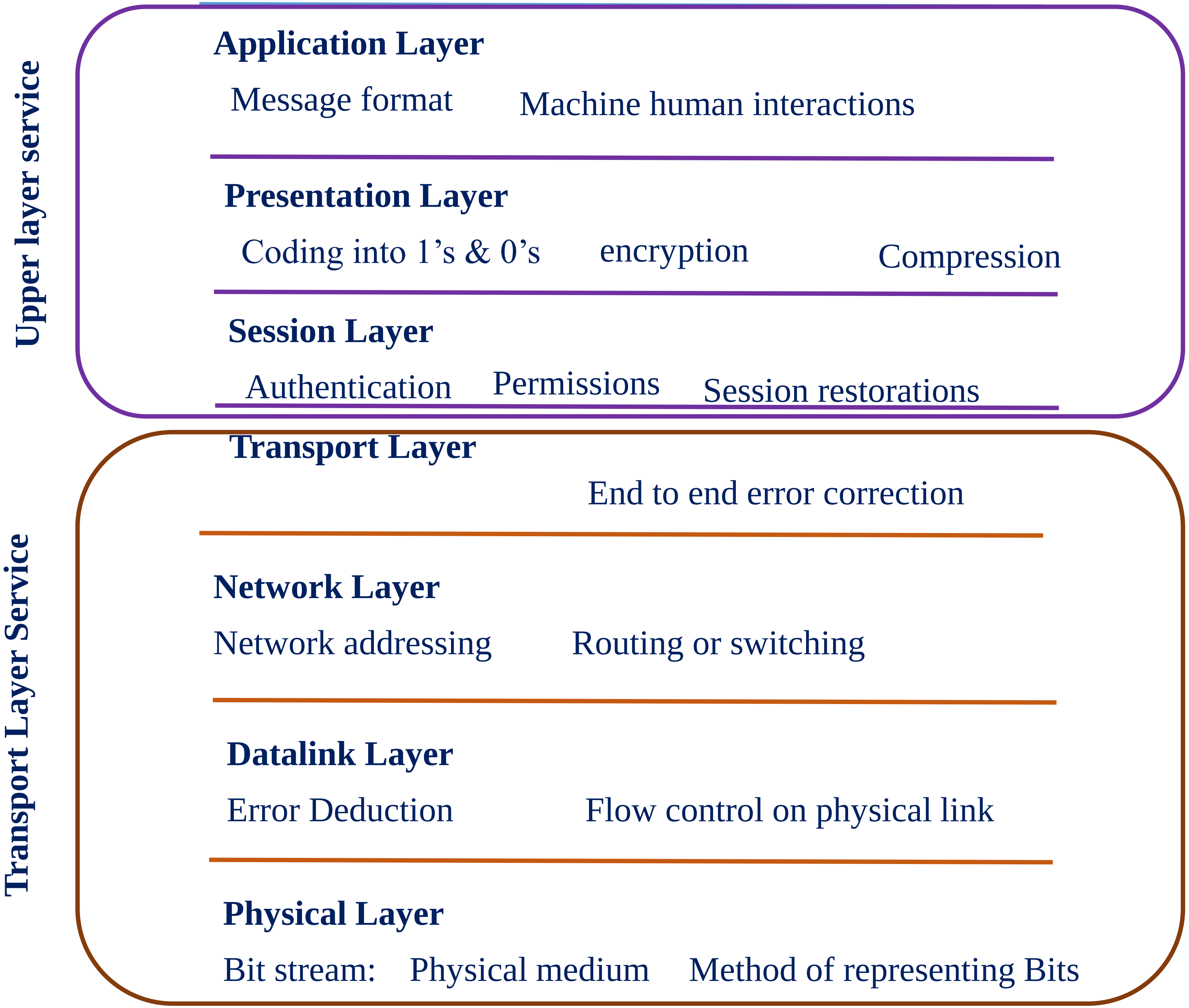
Communication Protocols for IoT

- IoT is about connectivity and interoperability,
- The standards for protocols and media are heavily fragmented.
- The key communications protocols required for IoT to be successful. It also covers the main wireless offerings that provide the pervasive coverage essential to IoT and touches on some essential wired ones.
- Overview of the key communications protocols to understand what is required from a platform connectivity perspective, especially at the edge and fog layers of the system.

- Many emerging and competing networking technologies are being adopted for IoT.
- Various consortia/alliances, vertical markets, and vendors offer differing technologies for IoT connectivity.
- Traditional enterprise technologies such as Wi-Fi and Ethernet can be applied for IoT.
- New technologies are being developed specifically to meet the challenges of IoT, especially closer to the edge where specific device, distance, or bandwidth challenges need to be addressed.

- Communication protocols are a set of rules that allow two or more devices in hardware or software to establish a reliable communication system that allows data to be transmitted between them.
- Rules include syntax, semantics, and synchronization, as well as error recovery mechanisms.

- The most common communications model is the Open Systems Interconnection (OSI) model, which breaks communications into seven functional layers for easier implementation of scalable and interoperable networks.
- Each layer delivers a specific function and handles clearly defined tasks while interfacing with the layers located directly above and below it.
- The model is the most widely used in network communications today, with clearly defined layers allowing easier implementation of interoperable and scalable networks.



Upper layer service

Application Layer

Message format   Machine human interactions

Presentation Layer

Coding into 1’s & 0’s   encryption   Compression

Session Layer

Authentication   Permissions   Session restorations

Transport Layer Service

Transport Layer

End to end error correction

Network Layer

Network addressing   Routing or switching

Datalink Layer

Error Deduction   Flow control on physical link

Physical Layer

Bit stream: Physical medium   Method of representing Bits

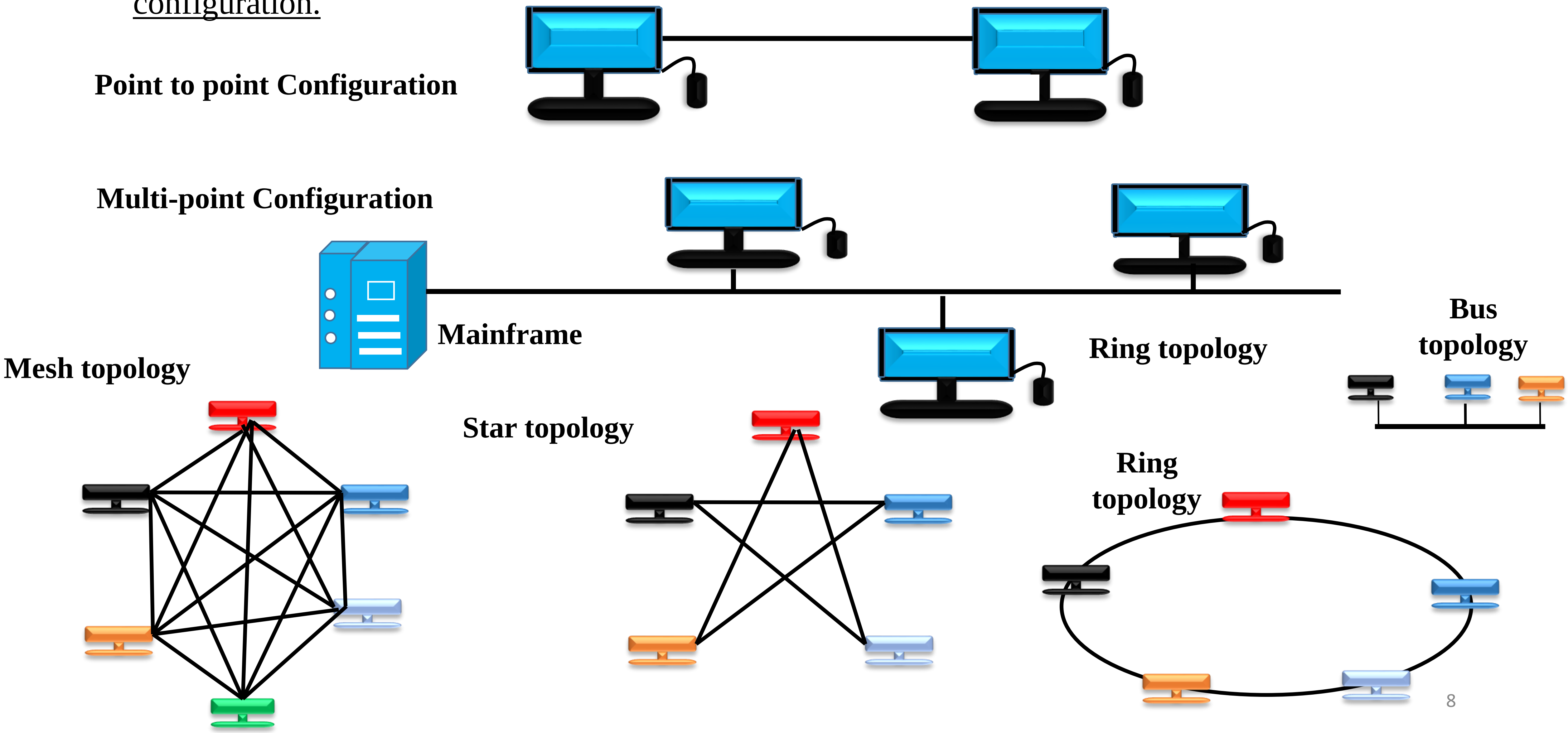
Functions of Different Layers:

Layer 1: The Physical Layer:

1. It is the lowest layer of the OSI Model.
2. It ***activates, maintains*** and ***deactivates*** the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. **Data rates** needed for transmission is defined in the physical layer.
5. It converts the bits into electrical signal (digital / analog) or optical signals (light).
6. Data encoding (Encoding is the **process of using various patterns of voltage or current levels to represent 1s and 0s of the digital signals** on the transmission link.) is also done in this layer.

Line Configuration:

- This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.



Point to point Configuration

Multi-point Configuration

Mainframe

Mesh topology

Star topology

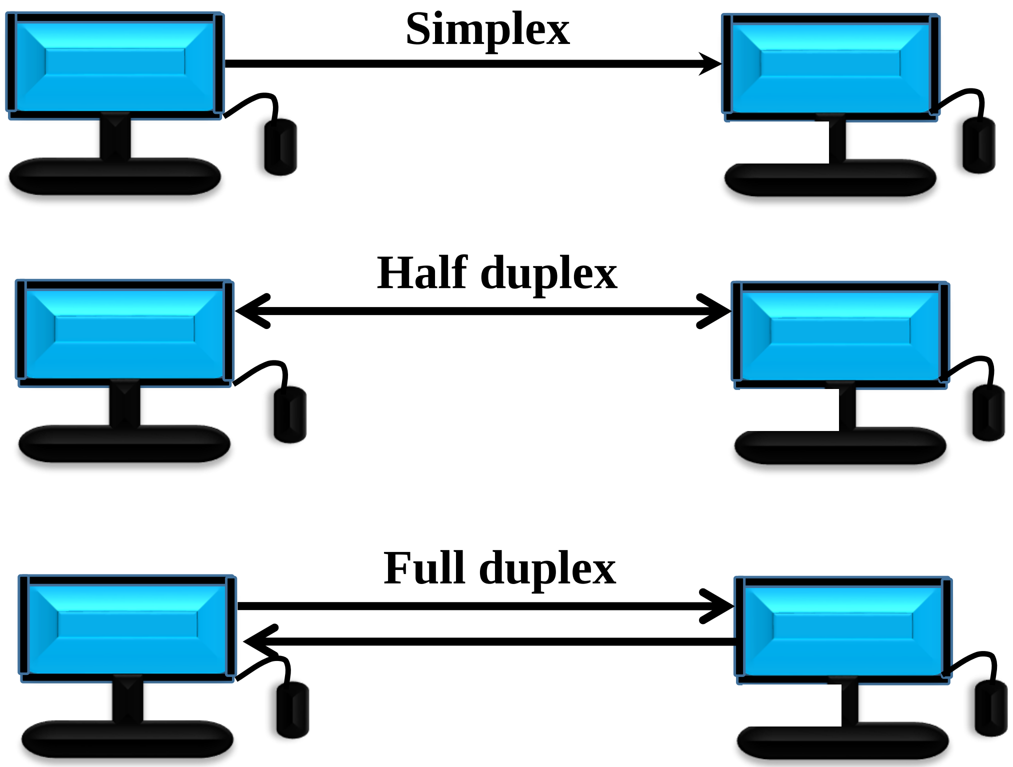
Ring topology

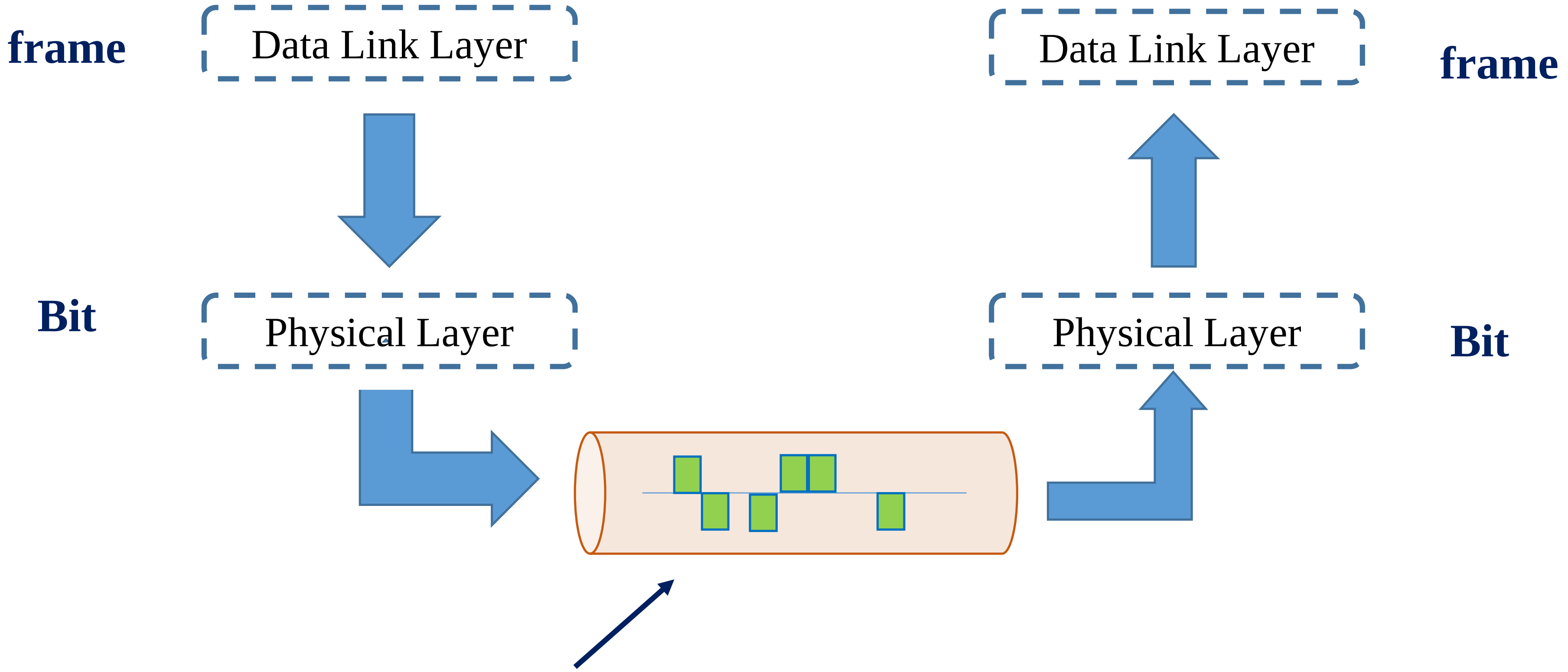
Bus topology

Ring topology

Transmission Modes:

- Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex and Full Duplex
- Deals with baseband and broadband transmission.





frame

Data Link Layer

Bit

Physical Layer

Data Link Layer

frame

Physical Layer

Bit

Transmission medium / channel (cable)

or

Air

Layer 2: The Datalink Layer:

Framing

- Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.

Physical Addressing

- The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame.

Flow Control:

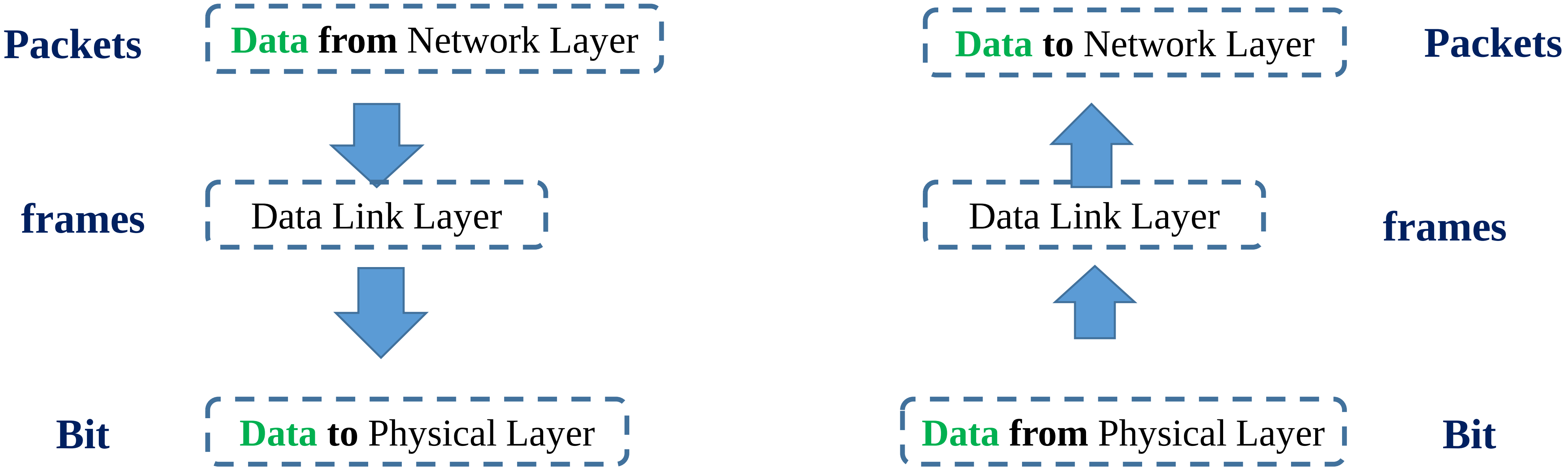
- A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.

Error Control

- Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism.
- Data Link Layers adds mechanism to prevent duplication of frames.

Access Control

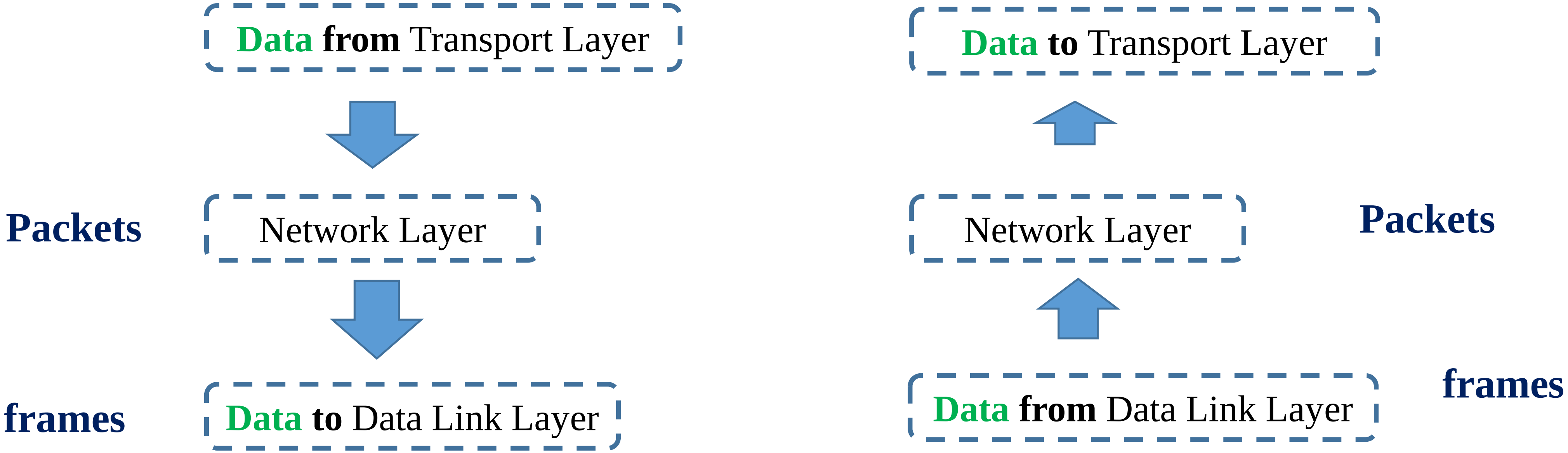
- Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.



Layer 3: The Network Layer:

1. It routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

1. It translates logical network address (IP address) into physical address (48 bit MAC). Concerned with circuit, message or packet switching.
2. Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
3. Connection services are provided including network layer flow control, network layer error control and packet sequence control.
4. Breaks larger packets into small packets.



Data from Transport Layer

Packets

Network Layer

frames

Data to Data Link Layer

Data to Transport Layer

Network Layer

Packets

Data from Data Link Layer

frames

Layer 4: The Transport Layer:

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

1. **Service Point Addressing:**

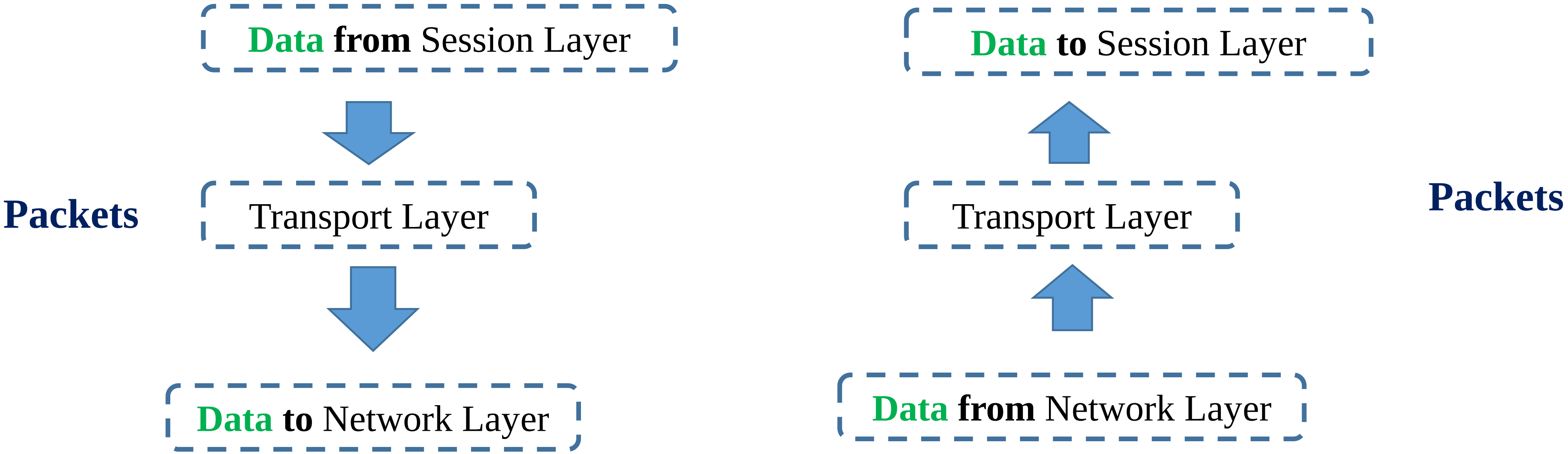
Transport Layer header includes *service point address which is port address*. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.

2. **Segmentation and Reassembling:**

A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message.

1. **Connection Control :** It includes 2 types:
   - *Connectionless Transport Layer*:
     - Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.
   - *Connection Oriented Transport Layer*:
     - Before delivering packets, connection is made with transport layer at the destination machine.
2. **Flow Control:** In this layer, flow control is performed end to end.
3. **Error Control:** Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error.

- Error Correction is done through retransmission.



Data **from** Session Layer

Packets

Transport Layer

Data **to** Network Layer

Data **to** Session Layer

Transport Layer

Packets

Data **from** Network Layer

Layer 5: The Session Layer:

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

1. **Dialog Control:**

   This layer allows two systems to start communication with each other in half-duplex or full- duplex.

2. **Synchronization:**

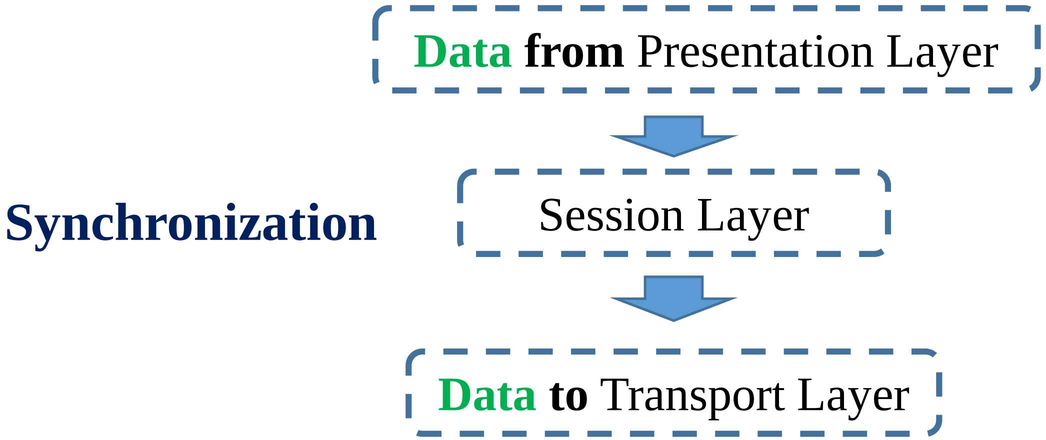
   This layer allows a process to add checkpoints which are considered as synchronization points into stream of data.

Example:

If a system is sending a file of 800 pages, adding checkpoints after every 50 pages is recommended.

This ensures that 50 page unit is successfully received and acknowledged.

This is beneficial at the time of crash as if a crash happens at page number 110; there is no need to retransmit 1 to100 pages.

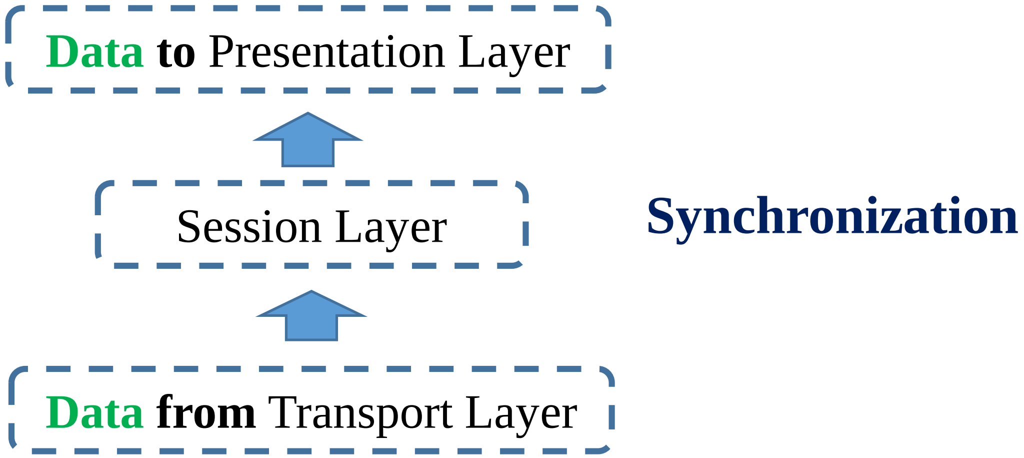


Data from Presentation Layer

Synchronization

Session Layer

Data to Transport Layer



Data to Presentation Layer

Session Layer

Synchronization

Data from Transport Layer

Layer 6 : The Presentation Layer:

1. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It performs Data compression, Data encryption, Data conversion etc.

1. **Translation:**

   Before being transmitted, information in the form of characters and numbers should be changed to bit streams.

   The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods.

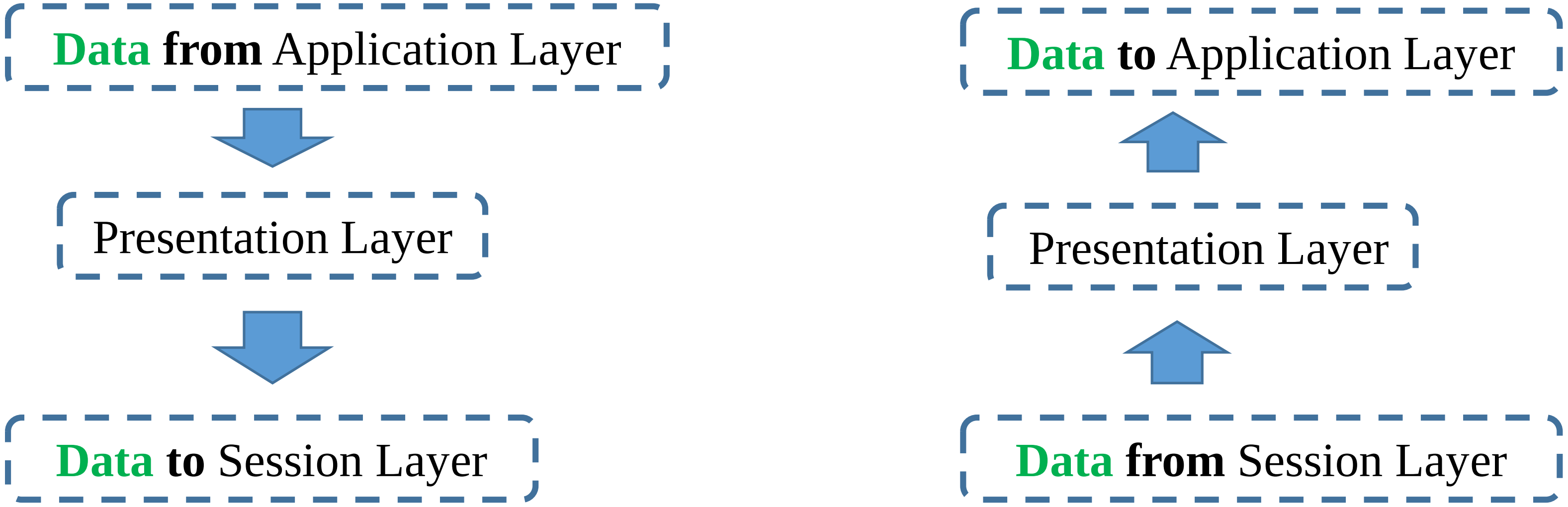
2. **Encryption:**

   It carries out encryption at the transmitter and decryption at the receiver.

3. **Compression:**

   It carries out data compression to reduce the bandwidth of the data to be transmitted.

   The primary role of Data compression is to reduce the number of bits to be transmitted. It is important in transmitting multimedia such as audio, video, text etc.



Data from Application Layer

Presentation Layer

Data to Session Layer

Data to Application Layer

Presentation Layer

Data from Session Layer

Layer 7: The Application Layer:

1. It is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

1. **Mail Services:** This layer provides the basis for E-mail forwarding and storage.

2. **Network Virtual Terminal:**

   It allows a user to log on to a remote host.

   User's computer talks to the software terminal which in turn talks to the host and vice versa.

   Then the remote host believes it is communicating with one of its own terminals and allows user to log on.

3. **Directory Services:**

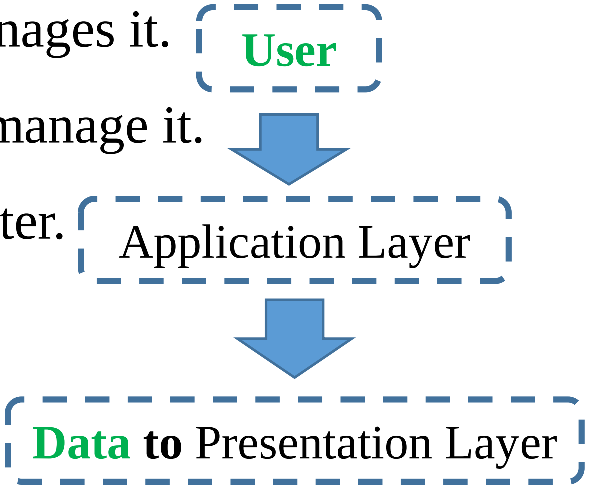
   This layer provides access for global information about various services.

4. **File Transfer, Access and Management (FTAM):**

   It is a standard mechanism to access files and manages it.

   Users can access files in a remote computer and manage it.

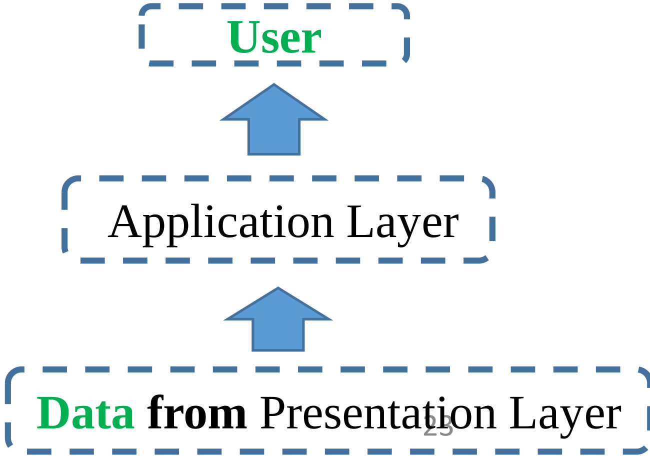
   They can also retrieve files from a remote computer.



User

Application Layer

Data to Presentation Layer



User

Application Layer

Data from Presentation Layer

- Although this model is applicable in IoT, it faces certain challenges, especially when devices are very simple and have limited capabilities and computing.
- A layered approach such as this introduces complexity to the device or software and usually requires more code and memory.
- It also introduces data overhead because every layer requires additional framing and control messages.
- More complexity and data transmitted can mean increased power consumption by devices; again, this might not suit an IoT deployment with simple, battery-powered devices.
- A layered approach does enable more flexibility and scale, however, and also provides the best opportunity for interoperability.

- Some use the full OSI reference model, from physical layer to application layer.
- Others specify only parts of the OSI reference model and leave the remaining aspects of communication up to other technologies.
- This has led to a more simplistic version of the OSI model for IoT that maps more closely to the TCP/IP model.

- The model can be simplified for IoT deployments. Some layers are collapsed here, without losing any functionality.
- This does not mean that one approach is better than the other, particularly because different applications running on top of the communications have different requirements; it simply makes choosing the right option more of a challenge when taking interoperability into account.

- Protocols and communication media, aligning them with the IoT-centric model. Within our focus on communications for data exchange, we look at last-mile communication technologies to the things, or within the fog/edge layers.
- It is important to make a distinction here because the requirements are different and still emerging. The core networks remain the same and are typically service provider or enterprise based (such as with MPLS).
- The main change involves connecting the multitude of things together to allow them to communicate between themselves locally or else bringing them back via some kind of backhaul to a central location.
- Some examples you already are familiar with from the IoT standards overview section; the aim here is to reference the communication elements within them.
- A fundamental concept to understand is that there is no “one size fits all” approach. A deployment in a smart city might have Ethernet and Wi-Fi connections, whereas a deployment to a remote oil field could be cellular or satellite.

- This is extremely important when architecting the system and can dictate architectural and technology decisions.

Example, a gateway might need to be leveraged to provide protocol translation from a legacy system at the edge so that it can be transported through the IoT system by the platform.

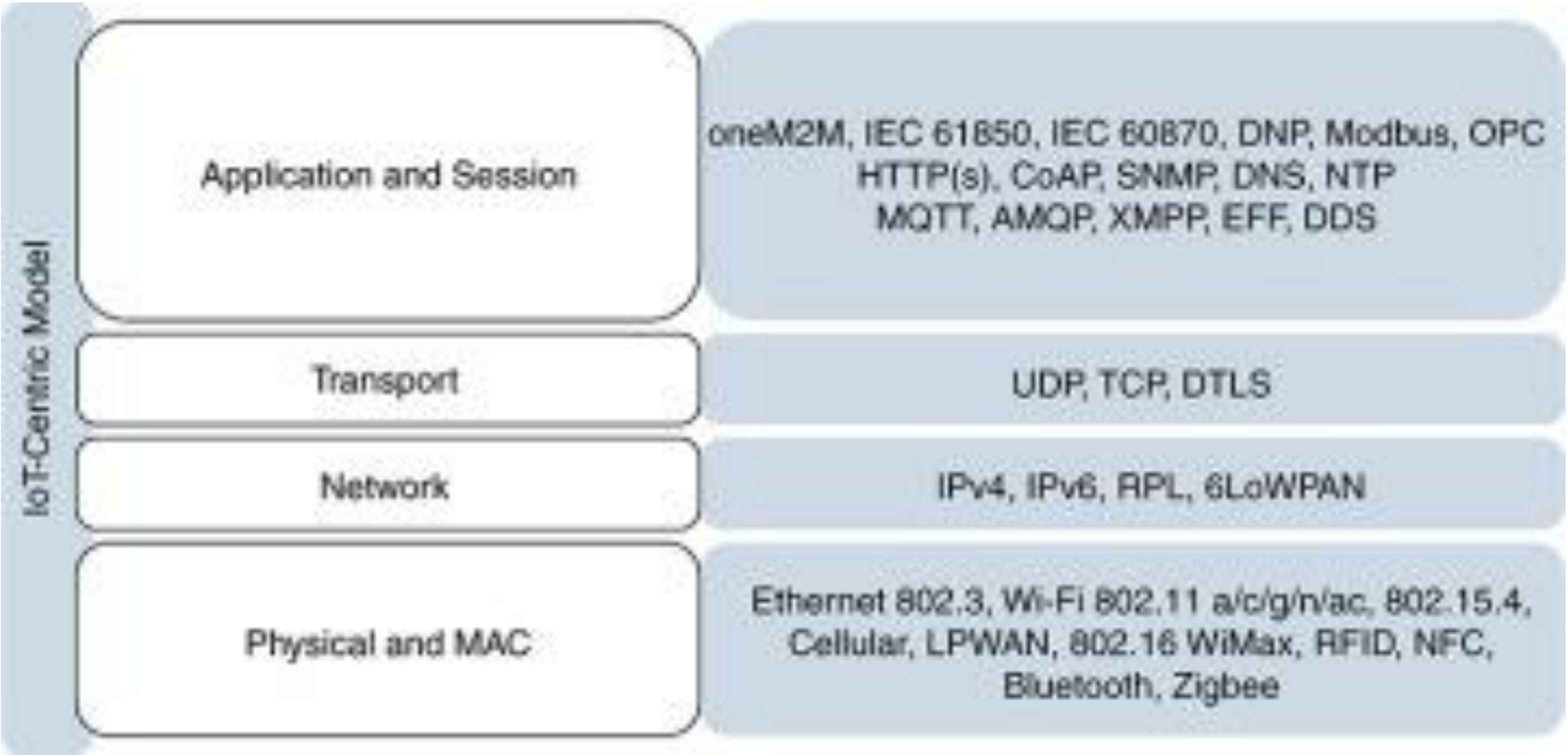
- In another case, a particular function (such as real-time analytics) might have to happen locally because limited bandwidth will not allow a certain amount of data to be transmitted.
- A more powerful endpoint might thus be deployed to do analytics and data normalization at the fog layer.

- From the perspective of the IoT platform, it is important to understand that a wide variety of these protocols need to be addressed as uniformly as possible.
- This can include IP or non-IP, and different protocols are likely to exist at different levels of the IoT hierarchy.
- The IoT platform must provide connectivity interfaces for these protocols at the edge or fog layers, whether natively or via a gateway, and must provide a way to securely transport the data flows to their destinations at any level.
- This applies to both the control and content/data planes.

- This model has four layers to cover the communications stack. Although it covers all the functions required, not all of the protocols fit neatly into one level.

Example, DTLS fits into the transport, application, and session levels. Similarly, 6LoWPAN fits into the network, physical, and MAC levels.

- This model provides a good starting point for organizing thoughts around communication.



IoT-Centric Model

Application and Session	oneM2M, IEC 61850, IEC 60870, DNP, Modbus, OPC HTTP(s), CoAP, SNMP, DNS, NTP MQTT, AMQP, XMPP, EFF, DDS
Transport	UDP, TCP, DTLS
Network	IPv4, IPv6, RPL, 6LoWPAN
Physical and MAC	Ethernet 802.3, Wi-Fi 802.11 a/c/g/n/ac, 802.15.4, Cellular, LPWAN, 802.16 WiMax, RFID, NFC, Bluetooth, Zigbee

- This layer covers how a device is physically connected to a network via wired or wireless mechanisms, as well as how devices are uniquely identified by a MAC address (or potentially another method) for physical addressing.
- Most standards combine the physical and MAC layer protocols; these protocols are essential in establishing communication channels.
- For IoT, considerations when designing at this level include devices that need to operate with a long battery life, require low power consumption, and have less processing capabilities.
- Other points to consider are lower bandwidth availability and the need to scale in terms of connecting and operating many more devices in a single environment.

- In IoT, wired Ethernet 802.3 and Wi-Fi 802.11 a/b/g/n standards are often leveraged, depending on the environment.
- Smart cities and manufacturing plant floors are good examples with dense coverage.
- Other technologies in use include 802.15.4 (802.15.4e, 802.15.4g, WirelessHART, ISA100.11a), cellular (2G, 3G, 4G, CDMA, LTE), Low Power Wide Area Network LPWAN (Long Range Radio LoRa, SigFox, Narrow Band IoT NB-IoT), 802.16 WiMax, RFID, NFC, Bluetooth (including Bluetooth Low Energy BLE), and Zigbee.

- The use of IP not only provides interoperability benefits, but also helps with longevity and future-proofing of solutions.
- With the speed of change of IoT devices and technologies, the physical and data link layers evolve every few years. Using IP provides support for a smooth evolution of technologies, without changing core architectures, affecting the stability of deployments, or introducing new use cases. Even if the endpoints do not support IP, gateways can be deployed at the edge or fog levels to provide connectivity and transport, as well as to support multiple physical and data link layer types.

- Many last-mile communication options can be unreliable and unpredictable, so a new routing protocol was created to address routing for constrained devices such as those in wireless sensor networks.
- The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) routes IPv6 traffic over low-power networks and lossy networks (LLN).
- LLNs are a class of network in which both the devices and their communication mechanisms are constrained.
- LLN devices are typically constrained by processing power, memory, and battery; their communications are characterized by high loss rates, low data rates, and instability. LLNs can scale from a few dozen up to thousands of devices.