**Knowledge and Theory: Networking**

**Part 1 – OSI 7 Model:**

Networking architecture can be divided into seven layers. Each layer provides services to the layer above it and receives services from the layer below it. The seven layers, from top to bottom, are:

**OSI 7 Model**

|  |  |
| --- | --- |
| Level 7 | Application Layer |
| Level 6 | Presentation Layer |
| Level 5 | Session Layer |
| Level 4 | Transport Layer |
| Level 3 | Network Layer |
| Level 2 | Data Link Layer |
| Level 1 | Physical Layer |

**Physical Layer**

The Physical layer is responsible for transmission of digital data [bits](https://www.lifewire.com/definition-of-bit-816250) from the Physical layer of the sending device over the *network communications media* to the Physical layer of the receiving device. Examples of Layer 1 technologies include [Ethernet cables](https://www.lifewire.com/what-is-an-ethernet-cable-817548), [hubs](https://www.lifewire.com/ethernet-and-network-hubs-816358) and cable connectors. Data is transmitted using electric voltages, radio frequencies, etc.

**Data Link Layer**

The Data Link layer gets data from the physical layer, checks for physical transmission errors and packages bits into data "frames". The Data Link layer also manages physical addressing schemes such as [MAC](https://www.lifewire.com/media-access-control-mac-817973) addresses for Ethernet networks, controlling access of any various network devices to the physical medium. Because the Data Link layer is the single most complex layer in the OSI model, it is often divided into two parts, the "Media Access Control" sublayer and the "Logical Link Control" sublayer.

**Network Layer**

The Network layer adds the concept of routing above the Data Link layer. When data arrives at the Network layer, the source and destination addresses contained inside each frame are examined to determine if the data has reached its final destination. If the data has reached the final destination, this Layer 3 formats the data into packets delivered up to the Transport layer. Otherwise, the Network layer updates the destination address and pushes the frame back down to the lower layers.

To support routing, the Network layer maintains logical addresses such as [IP addresses](https://www.lifewire.com/what-is-an-ip-address-2625920) for devices on the network. The Network layer also manages the mapping between these logical addresses and physical addresses. In IP networking, this mapping is accomplished through the [Address Resolution Protocol (ARP)](https://www.lifewire.com/address-resolution-protocol-817941).

**Transport Layer**

The Transport Layer delivers data across network connections. [TCP](https://www.lifewire.com/transmission-control-protocol-and-internet-protocol-816255) is the most common example of a Transport Layer 4 [network protocol.](https://www.lifewire.com/definition-of-protocol-network-817949) Different transport protocols may support a range of optional capabilities including error recovery, flow control, and support for re-transmission.

**Session Layer**

The Session Layer manages the sequence and flow of events that initiate and tear down network connections. At Layer 5, it is built to support multiple types of connections that can be created dynamically and run over individual networks.

**Presentation Layer**

The Presentation layer is the simplest in function of any piece of the OSI model. At Layer 6, it handles syntax processing of message data such as format conversions and encryption / decryption needed to support the Application layer above it.

**Application Layer**

The Application layer supplies network services to end-user applications. Network services are typically protocols that work with user's data. For example, in a Web browser application, the Application layer protocol [HTTP](https://www.lifewire.com/hypertext-transfer-protocol-817944) packages the data needed to send and receive Web page content. This Layer 7 provides data to (and obtains data from) the Presentation layer.

**Question 1 –** Explain what happens, step by step, after you type a URL into a browser.Use as much detail as possible.

1. Browser contacts the DNS (Domain Name System) server to find the IP address of the URL. The DNS maps url addresses to IP Addresses of the host (server) that serves that particular website. The DNS will receive the url of the website and respond with the correct IP address of the host.
2. The browser creates and opens a TCP connection to the web server at port 80.
3. The Browser receives (or fetches) the html code of the page requested from the socket. Browser renders the HTML and displays the page.
4. Browser terminates the connection when window is closed.

**Question 2 -** Compare and contrast the IPv4 and IPv6 protocols.

* IPv4 is an older generation internet protocol for addresses. It is most commonly used today. It contains 32 bits and can be represented such as [198.0.255.0]. It can be represented as 4 bytes (which is 32 bits) and each byte is represented as an integer that can range from 0 – 255 (which is really 28 – 1). Since it has 32 bits, there can be a maximum of 232 unique IPv4 addresses in the world. This is roughly 4.3 billion addresses. Unfortunately, this is not enough to satisfy thr world’s needs.
* IPv6 has 128 bits which can be represented by 6 integers ranging from (0 – 255). There is 2128 unique IPv4 addresses which is more than enough.

**Question 5 -** What are the differences between TCP and UDP? Explain how TCP handles reliable delivery (explain ACK mechanism), flow control (explain TCP sender’s / receiver’s win­dow) and congestion control.

* TCP is reliable and rrdered. Packets will re-send with connection loss to ensure they arrive. It is also heavier and slower than UDP.
* TCP does this with packet headers that include block numbers (that keep track of the order in which these packets should be received), acknowledgements (the sending party continues to send or re-send until it receives an acknowledgement from the receiving party), error management and error handling, timeouts, etc.
* TCP limits the total number of unac­knowledged packets that may be in transit end-to-end. This is to control congestion.
* UDP is unreliable, not ordered lightwight and fast.