# Solutions to Week 8 Data Communication 1

### Question 1

Explain in a few sentences, what are the functions of the **Network (or Internet) Layer and the Data Link Layer** of the TCP/IP model.

Answer:

The **Network or Internet layer** layer adds a header containing the source and destination IP addresses to the data received from the Transport layer. It is responsible for *routing*, which is moving packets (the fundamental unit of data transport on modern computer networks) across the network using the most appropriate paths. It also addresses messages and translates logical addresses (i.e., IP addresses) into physical addresses (i.e., MAC addresses).

The **Data Link layer** uses a Media Access Controller (MAC) to generate the frames that will be transmitted. In addition to framing, the data link layer may also perform mechanisms to detect and recover from transmission errors. For a receiver to detect transmission errors, the sender must add redundant information as an error detection code to the frame sent. When the receiver obtains a frame with an error detection code it recomputes it and verifies whether the received error detection code matches the computed error detection code.

### Question 2

What is the purpose of Address Resolution Protocol (ARP)? What does an ARP request/response packet contain? How does it work in different cases given below:

1. **CASE-1:** The sender is a host and wants to send a packet to another host on the same network.
2. **CASE-2:** The sender is a host and wants to send a packet to another host on another network.
3. **CASE-3:** the sender is a router and received a datagram destined for a host on another network.
4. **CASE-4:** The sender is a router that has received a datagram destined for a host in the same network.

**Answer:**

Address Resolution Protocol (ARP Protocol) is used to find the physical address from the IP address. (An ARP request is a broadcast, and an ARP response is a Unicast.)

**ARP request** is nothing but broadcasting a packet over the network to validate whether we came across destination MAC address or not. ARP request packet contains:

1. The physical address of the sender.
2. The IP address of the sender.
3. The physical address of the receiver is zeros.
4. The IP address of the receiver

(Note, that the ARP packet is encapsulated directly into data link frame.)

**ARP response/reply** is the MAC address response that the source receives from the destination which aids in further communication of the data.

**CASE-1: The sender is a host and wants to send a packet to another host on the same network.**

- Use ARP to find another host's physical address

**CASE-2: The sender is a host and wants to send a packet to another host on another network.**

- Sender looks at its routing table.
- Find the IP address of the next hop (router) for this destination.
- Use ARP to find the router's physical address

**CASE-3:** the sender is a router and received a datagram destined for a host on another network.

- Router check its routing table.
- Find the IP address of the next router.
- Use ARP to find the next router's physical address.

**CASE-4:** The sender is a router that has received a datagram destined for a host in the same network.

- Use ARP to find this host's physical address.

**Question 3**

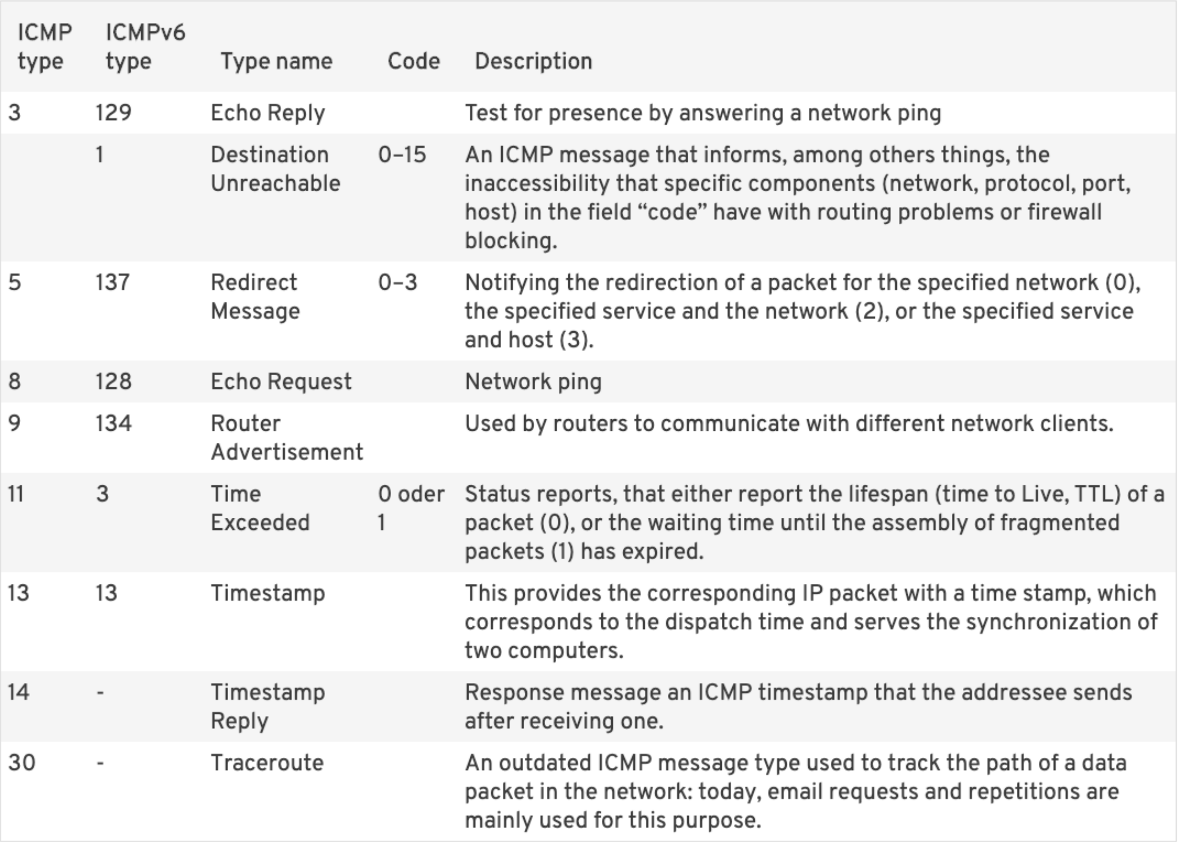
What is the Internet Control Message Protocol (ICMP)? What is ICMP used for?

**Answer:**

**Internet Control Message Protocol (ICMP Protocol) is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.**

A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.

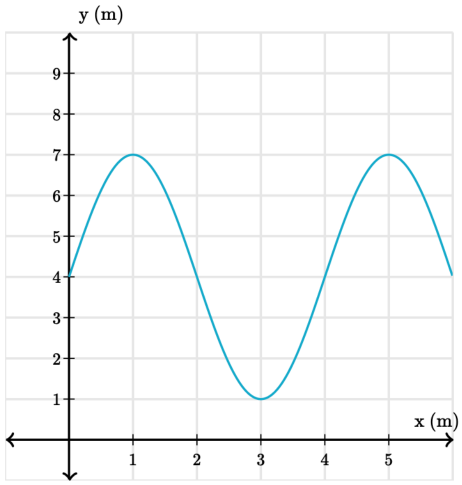
Some of the most important packet types based on the Internet Control Message Protocol are summarised in the following table:



| ICMP type | ICMPv6 type | Type name | Code | Description |
|---|---|---|---|---|
| 3 | 129 | Echo Reply | | Test for presence by answering a network ping |
| | 1 | Destination Unreachable | 0–15 | An ICMP message that informs, among others things, the inaccessibility that specific components (network, protocol, port, host) in the field “code” have with routing problems or firewall blocking. |
| 5 | 137 | Redirect Message | 0–3 | Notifying the redirection of a packet for the specified network (0), the specified service and the network (2), or the specified service and host (3). |
| 8 | 128 | Echo Request | | Network ping |
| 9 | 134 | Router Advertisement | | Used by routers to communicate with different network clients. |
| 11 | 3 | Time Exceeded | 0 oder 1 | Status reports, that either report the lifespan (time to Live, TTL) of a packet (0), or the waiting time until the assembly of fragmented packets (1) has expired. |
| 13 | 13 | Timestamp | | This provides the corresponding IP packet with a time stamp, which corresponds to the dispatch time and serves the synchronization of two computers. |
| 14 | - | Timestamp Reply | | Response message an ICMP timestamp that the addressee sends after receiving one. |
| 30 | - | Traceroute | | An outdated ICMP message type used to track the path of a data packet in the network: today, email requests and repetitions are mainly used for this purpose. |

## Question 4

A transverse wave on a string travels at 20m/s. A graph of the height of the wave along the x-direction at a certain moment is shown below.

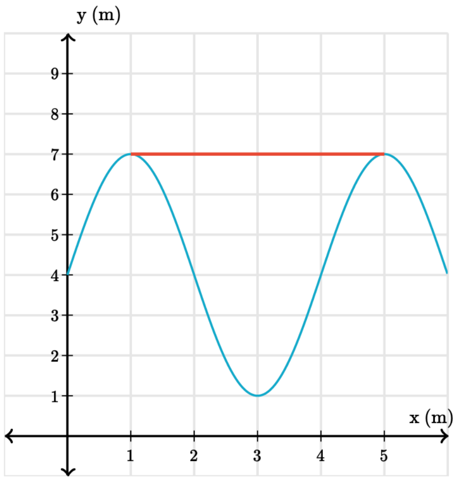


What is the frequency of the wave along the string?

Answer:

The wavelength λ, speed v, frequency f are related through the equation λ = v/f.

We are given v. Let’s also use the graph to determine λ so we can find f.



We can find the wavelength from the graph.

The wavelength λ is 4m. Let’s rearrange the wave equation to solve for frequency and substitute these values: f= v/λ = 20 m/s / 4m = 5Hz.

### Question 5

What are the differences between a MAC address and an IP address?

Explain the use of MAC address and IP address.

Answer:

MAC and IP address both are equally required when a device wants to communicate with another device in a network.

- The full form of MAC address is Media Access Control whereas, the full form of IP address is Internet Protocol address.
- The IP address identifies a connection to a device in a network. On the other hand, Mac address identifies a device participating in a network.
- MAC address is 48 bits (6 bytes) hexadecimal address whereas, IP address has two versions, IPv4 a 32-bit address and IPv6 a 128-bit address.
- MAC address is assigned by the manufacturer of interface hardware. On the other hand, IP address is assigned by the network administrator or Internet Service Provider (ISP).
- Address Resolution Protocol retrieves the MAC address whereas Reverse Address Resolution Protocol (rendered obsolete by BOOTUP/DHCP) retrieves IP address.

### Question 6

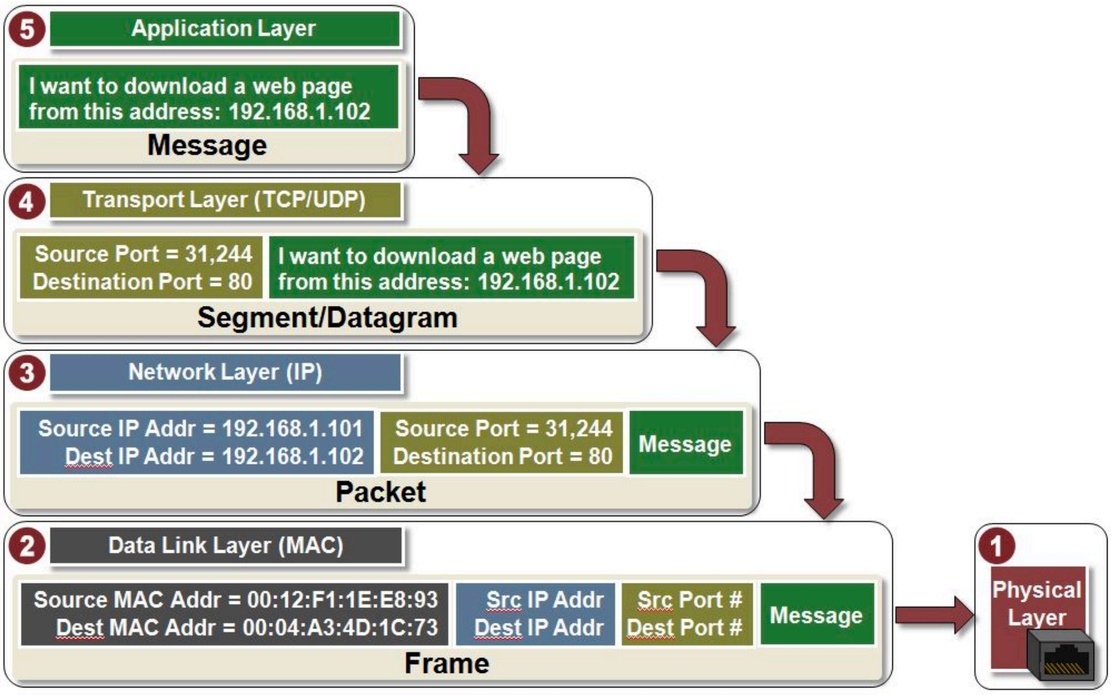
What are TCP/IP Encapsulation and Decapsulation?

Explain in a few sentences, how data is encapsulated at different layers.

Answer:

The term **encapsulation** describes a process of putting headers (and sometimes trailers) around some data. Each layer adds its own header (Data Link protocols also add a trailer) to the data supplied by the higher layer.

Header and trailer added by a layer in the sending computer can be removed only by the peer layer in the receiving computer. For example, header and trailer added by the transport layer in the sending computer can be removed only by the transport layer in the receiving computer.


5
Application Layer
I want to download a web page from this address: 192.168.1.102
Message
4
Transport Layer (TCP/UDP)
Source Port = 31,244
Destination Port = 80
I want to download a web page from this address: 192.168.1.102
Segment/Datagram
3
Network Layer (IP)
Source IP Addr = 192.168.1.101
Dest IP Addr = 192.168.1.102
Source Port = 31,244
Destination Port = 80
Message
Packet
2
Data Link Layer (MAC)
Source MAC Addr = 00:12:F1:1E:E8:93
Dest MAC Addr = 00:04:A3:4D:1C:73
Src IP Addr
Dest IP Addr
Src Port #
Dest Port #
Message
Frame
1
Physical Layer

(Source: https://microchipdeveloper.com/tcpip:tcp-ip-five-layer-model)

| Term | TCP/IP layer | Description |
|---|---|---|
| Data | Application | Upper layers don't use header and trailer with data. But if require, the application that initiates the connection can add header and trailer with data. For example, browsers use HTTP protocol to fetch websites from webservers. HTTP protocol uses a header with data.<br>Since the use of header and trailer in upper layers is application specific, in encapsulation diagram and terms encapsulated data in upper layers is commonly referred as the data. |
| Segment | Transport | Transport layer breaks the received data stream from upper layers into smaller pieces. Next, it creates a header for each data piece. This header contains all necessary information about the piece that the transport layer in remote host needs to reassemble the data stream back from the pieces. Once header is attached, data piece is referred as segment. Once segments are created, they are handed down to the network layer for further processing. |

| Term | TCP/IP layer | Description |
|---|---|---|
| Packet | Network | Network layer creates a header for each received segment from transport layer. This header contains information that is required for addressing and routing such as source software address and destination software address. Once this header is attached, segment is referred as packet. Packets are handed down to the data link layer. In original TCP/IP model the term packet is mentioned as the term datagram. Both terms packet and datagram refer to the same data package. This data package contains a network layer header and an encapsulated segment. |
| Frame | Data Link | Data link layer receives packets from network layer. Unlike transport layer and network layer which only create header, it also creates a trailer with header for each received packet. The header contains information that is required for switching such as source hardware address and destination hardware address. The trailer contains information that is required to detect and drop corrupt data packages in the earliest stage of de-encapsulation. Once header and trailer are attached with packet, it is referred as frame. Frames are passed down to the physical layer. |
| Bits | Physical | Physical layer receives frames from data link layer and converts them a format that the attached media can carry. For example, if the host is connected with a copper wire, the physical layer will convert frames in voltages. And if the host is connected with a wireless network, the physical layer will convert them in radio signals. |

De-encapsulation takes place in receiving computer. In de-encapsulation process, header and trailer attached in encapsulation process are removed.

- **Physical layer** picks encoded signals from media and converts them in frames and hands them over to the data link layer.
- **Data link layer,** first, reads the trailer of frame to confirm that the received frame is in correct shape. It reads rest of the frame only if the frame is in correct shape.

  If frame is fine, it reads the destination hardware address of the frame to determine the fame is intended for it or not. If frame is not intended for it, it will discard that frame immediately.

If frame is intended for it, it will remove the header and the trailer from the frame. Once data link layer's header and trailer are removed from the frame, it becomes packet. Packets are handed over to the network layer.

- **Network layer** checks destination software address in the header of each packet. If packet is not intended for it, network layer will discard that packet immediately. If packet is intended for it, it will remove the header. Once network layer's header is removed, packet will become segment. Segments are handed over to the transport layer.
- **Transport layer** receives segments from network layer. From segment headers it collects all necessary information and based on that information it arranges all segments back in correct order. Next, it removes segment header from all segments and reassembles them in original data stream. Data stream is handed over to the upper layers.
- **Upper layers** format data stream in such format that the target application can understand.