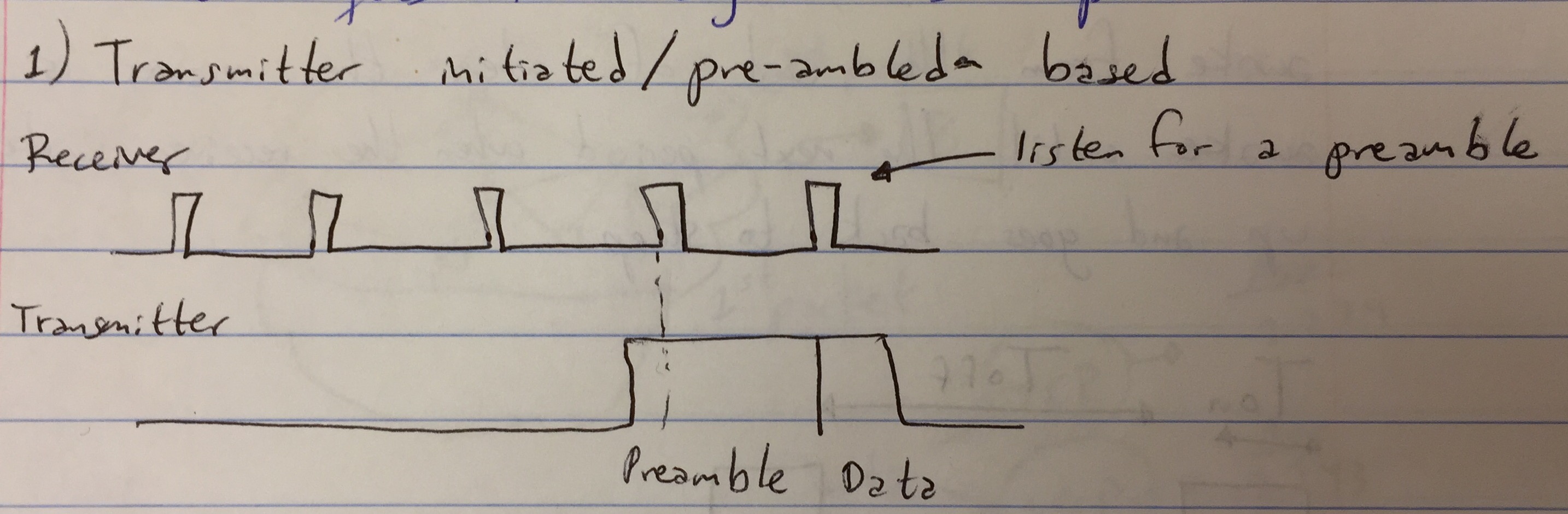
**Asynchronous Sleep Cycling for Low Power Operation**

1) What is the key difference between transmitter initiated (preamble-based) and receiver initiated asynchronous sleep cycling?

The difference is who is checking if data is going to be transmitted. On transmitter initiated, the transmitter sends a preamble and the receiver listens for the preamble. On receiver initiated, the receiver is constantly asking if there is a packet for it. If there is no packet, it goes back to sleep.

2) Transmitter-initiated asynchronous sleep cycling.

****

In the case of the transmitter-initiated asynchronous sleep cycling, the receiver has a predetermined duty cycle where it turns on and off. When the transmitter is going to send data, it sends a preamble that lasts for at least a complete on and off period of the receiver. When the receiver listens the preamble, it changes from low power mode to high power mode to prepare itself to receive the data that will be sent immediately after the preamble is over.

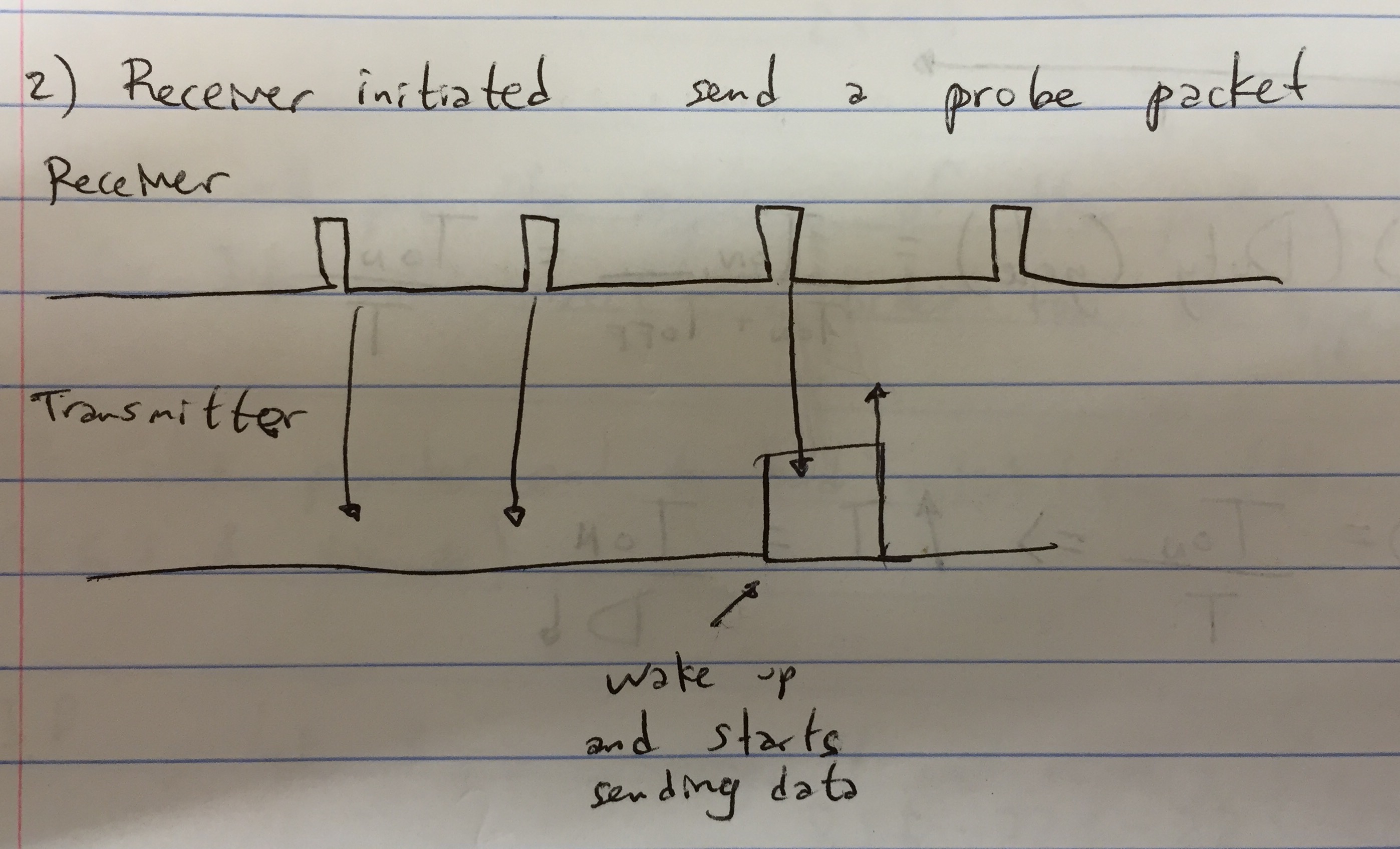
3) As learned from lecture:

D (Duty Cycle) = Ton/T = Ton/(Ton + Toff), where T is defined as the minimum length for preamble from the transmitter to ensure they can communicate.

Therefore, 1% duty cycle is equal to 0.01 in decimal and 1 ms is equal to 10^-3 = 0.001.

T = Ton/D = 0.001/0.01 = 0.1 seconds. Thus, the minimum length for the preamble from the transmitter to ensure they can communicate is 0.1 seconds.

4) Receiver-initiated asynchronous sleep cycling.

****

In the case of the receiver-initiated asynchronous sleep cycling, the receiver has a predetermined duty cycle. When it turns on, it requests the transmitter if there is data available for it. If not, then it goes back to low power mode. If there is data available from the transmitter, it goes to on mode and the transmitters starts sending data.

5) From problem 3:

T = Ton/D = 0.002/0.01 = 0.2 seconds. Thus, the minimum amount of time the transmitter might need to be awake to hear a probe (assuming no packet loss) is 0.2 seconds.

**Network Layer**

7) The phrase “everything over IP and IP over everything” refers to a term in computing used to design every possible way of communicating and transporting the information on a network. IP runs on the physical and link layer of everything using the Internet nowadays. Furthermore, all the devices using the Internet run on IP. The IP is necessary to have an address in every single device.

8) What is the main reason IPv6 was introduced as an upgrade over IPv4?

The reason IPv4 was upgraded to IPv6 was because the Internet was running out of addresses. IPv4 provides more than 4 billion unique addresses. IPv6 uses 128 bits per address, which provides 340 undecillion unique addreses.

9) IP address: 10.120.59.255 = 00001010.01111000.00111011.11111111

mask: 255.255.240.0 = 11111111.11111111.11110000.00000000

If I want to get the network ID, I will have to AND both numbers.

Therefore, it results in 00001010.01111000.00110000.00000000, which is 10.120.48.0.

Network ID = 10.120.48.0

10) Network = 172.19.0.0 and subnet mask = 255.255.255.128

How many subnets?

Since 128 is 1 bits on (10000000), the answer should be 29 = 512 subnets

How many hosts per subnet?

We have 7 bits off on 10000000, so the equation would be 27 – 2 = 126 hosts per subnet

11) The relationship between number of subnets and number of hosts per subnet as the number of bits set to 1 in the subnet mask changes is inversely proportional. As more bits are set to 1 in the subnet mask, the number of subnets increases. However, the number of hosts per subnet decreases.

12) What would be the subnet mask and subnet ID for the following node: 192.168.46.144/25?

Classless Inter-Domain Routing (CIDR) Value = /25 = 255.255.255.128. Therefore, the subnet mask is 255.255.255.128

IP address = 192.168.46.144.

I will have to AND the subnet mask and the IP address,

subnet ID = 192.168.46.128

13) Then answer is option “e.” It is true that there is an upper bound to how many uniquely addresses nodes there can be on the Internet, but that is the reason IPv6 was introduced as an upgrade over IPv4.

**Transport Layer**

14) What does UDP stand for? What is the main functionality?

UDP stands for User Datagram Protocol. It is used primarily for establishing low-latency (almost always active) and loss tolerating (allowing errors) connections between applications on the Internet.

15) There can be 65,535 UDP ports and 65,535 TCP ports because a port number is a 16-bit unsigned integer. Thus, ranging from 0 to 65,535 (2^16).

16) What does TCP stand for? What functionalities does it offer?

TCP stands for Transmission Control Protocol. It offers multiple functionalities. Besides providing port numbers, just like UDP, it provides sequence numbers to enable in order delivery. TCP will put the sequence of the packets back in order. It will correct the order for the application. Furthermore, it proves end-to-end reliability. If a packet is missing, it will request for it. Another functionality TCP provides is abstraction of a connection or session meaning that it organizes the communicated packets into a larger, more coherent entity. These are set up through a series of control message “TCP handshake,” i.e. it requests to start communicating in that precise moment. Finally, TCP provides congestion control. It tries to maximize the bandwidth efficiency by sending out the maximum rate possible, but not too fast when the network is congested.

17) Overall, TCP provides more quality to the user than UDP, but the cost is higher. Therefore, depending on the application when error is acceptable and monetary constraints exist, then UDP will be a good option versus TCP. Furthermore, TCP requires more memory to store the headers of the packets and, therefore, the data transmission is slower because fewer bits of data are stored in the payload, where the content is stored. If memory is another constraint, then UDP will be a better option than TCP as well. On the other hand, if quality is needed for a specific application and it can be afforded, then slower data transmission and extra memory might be accepted. TCP is less cost efficient, but quality is guaranteed.

**Application Layer**

18)

a) SMTP: it stands for Simple Mail Transfer Protocol. SMTP is used when email is delivered from an email client, Outlook Express, to an email server or when email is delivered from one email server to another. SMTP uses port 25. An email client is a desktop application that enables configuring one or more email addresses to receive, read, compose, and send emails through the desktop interface.

b) FTP: it stands for File Transfer Protocol. Most commonly, the files are “uploaded” to a server or “downloaded” to your computer. FTP is the most common way website designers move their website files onto web servers for the world to see.

c) SSH: it stands for Secure SHell. It is a program designed to allow users to log into another computer over a network, to execute commands on that computer and to move files to and from that computer. It effectively replaces telnet, ftp, and the rcp/rsh/remsh programs.

d) Secure copy or SCP is a means of securely transferring computer files between a local host and a remote host or between two remote hosts. It is based on the Secure Shell (SSH) protocol.

e) HTTP: it stands for Hypertext Transfer Protocol. HTTP is an application protocol for distributed, collaborative, and hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text.

f) DNS: it stands for Domain Name Servers. DNS are the Internet’s equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses.

g) RTMP: it stands for Real-Time Messaging Protocol. It was initially a proprietary protocol developed by Macromedia for streaming audio, video, and data over the Internet, between a Flash player and a server. Macromedia is now owned by Adobe, which has released an incomplete version of the specification of the protocol for public use.

h) MQTT: it stands for MQ Telemetry Transport. It is a publish/subscribe, extremely simple and lightweight messaging protocol, designed for constrained devices and low-bandwidth, high-latency, or unreliable networks.

i) XMPP: it stands for Extensible Messaging and Presence Protocol. It is a protocol based on Extensible Markup Language (XML) and intended for instant messaging (IM) and online presence detection. It functions between or among servers, and facilities near-real-time operation.

j) NTP: it stands for Network Time Protocol. It is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use.

19) Standard or typical port numbers?

|  |  |  |
| --- | --- | --- |
|  | Protocol | Port |
| a | SMTP | 25 |
| b | FTP | 989, 990 |
| c | SSH | 22 |
| d | SCP | 22 |
| e | HTTP | 80,81 |
| f | DNS | 53 |
| g | RTMP | 1935 |
| h | MQTT | 1883, 8883 |
| i | XMPP | 5222 |
| j | NTP | 123 |