2018 Network and Communication Examination Solution

1. a. SSL => SSH

    gatehost => gateway

    dilatancy => RTT

    tcppump => tcpdump

    b. i) The extra 28 bytes come from the IP header(20 bytes) and ICMP(8 bytes)

    ii) The 1500 bytes limitation comes from the Maximum Transmission Unit of Ethernet in the data link layer.

    c. i) The line utilization would be $\frac{(65507+28)/(12.5\times10^6)}{15.633+(65507+28)/(12.5\times10^6)} = 0.251 \approx 25.1\%$

    ii) The transfer time is propagation delay + transmission delay:
    $\frac{\text{RTT}}{2} + \frac{L}{R} = 7.8165 + 5.2428 = 13.057$ ms

    d. i) TCP. The connection between webpage and backend is commonly implemented by HTTP, which is based on TCP. The query must send to the backend reliably.

    ii) TCP. UDP won't make the database search faster. In other words, internet connection is not the main limiting factor here. Additionally, the result must be returned reliably as well.

    e. The attacker can set up connection to both ends and pretend to be legitimate. The attacker can clearly see the communication between the frontend and backend. We can use HTTPS protocol so that the attacker will only be able to see the encrypted version of messages.

2. a. i) X => Promiscuous mode

    Y => Monitor mode

    ii) The network might be switches so that packets will only be forwarded to the right destination/ports rather than broadcasted.

    b. i) The broadcast IP is the last IP available in the address space, hence for the first subnet it's $192.168.0.15$ and the second one is $192.168.0.31$, which is just turning the last 4 digits into 1.

    The first usable host is the second available address in the entire address space, thus for the first subnet it is $192.168.0.1$ and for the second one $192.168.0.17$

    The last usable host for the first subnet is $192.168.0.14$ and for the second subnet is $192.168.0.30$

    The network IP is the first available IP in the address space, thus for the first subnet it is $192.168.0.0$ and for the second subnet it is $192.168.0.16$

    The subnet mask for the first subnet (and the second subnet) is $255.255.255.240$

    Calculation is somehow omitted here.

ii) Both the first and the second subnet have 14 available host addresses, so 28 usable hosts in total. **No** IP has been accidentally skipped.

c. The ARP stands for Address Resolution Protocol and is responsible for finding the corresponding MAC address of a host with a given IP address. The router will **1** first send out an ARP reequest to all available host with an IP address, then **2** the host whose IP address matches the given one will send an ARP response to the router with its MAC address. The router will then **3** record/cache the IP/MAC address pair and enable communication with the host. In this case, the first message serves as the ARP request where the router has not yet known the MAC address of the host and cannot communicate with it. The second message will be successfully sent because the router already knows the MAC address after the first message.

d. The wavelength is $378.5 \text{ ft} = 378.5 \cdot 30.48 = 11,536.68 \text{ cm} = 115.3668 \text{ m}$. Hence we can calculate the frequency $f = \frac{c}{\lambda} = \frac{3 \times 10^8}{115.3668} = 2,600,401.5 \text{ Hz} = 2600.402 \text{ KHz}$.

e. Wireless mesh consists of a rich interconnections of hosts and nodes, with many possible routes that a transmission can go through. If one of the host/nodes is down, there are other alternative route that could be used. The lack of net neutrality might affect the service because ISP might be able to block/slow down the connection to the client's server. This mesh topology might be able to help the client by allowing more potential routes in order to provide reliable connections to end users.