2020 Network and Communication Examination Solution

1. a. UDP => TCP

   PAN => LAN

   bait-and-switch => DDoS

   ARP => RTT

   b. i) `ifconfig -a`

   ii) `dig MX example.com`

   iii) Either use the value of 255 minus TTL(Time To Live) field in the `ping shell.example.com` command, or use `traceroute shell.example.com`

   iv) `ssh shell.example.com`

   c. First, we have to use **802.11** protocol to connect to the wireless access point. After connecting to WiFi, we obtain an IP address assgined by the router using **DHCP**, where we first broadcast a `DISCOVER` packet and let the router(also the DHCP serveer) know that the laptop needs to be assigned an IP address. In order to resolve which MAC address corresponds to an IP address, **ARP** is used to determine the correct host. When starting to send packets to the remote server, the **IP**(Internet Protocol) is used and **TCP** is used for reliable transportation of packets (because SMTP is connection-oriented). When resolving for the IP address of the server, the **DNS protocol** is used and hence **UDP** is involved since DNS lookup is based on UDP by default. Sending the email requires **SMTP** to send the mail message to the mail server and receiving the reply involves **IMAP/POP3** to pull off new message from mail server to the local laptop.

   d. In this case, we choose **TCP** for playing these videos. We assume that most of the users will not care about the real-timeness of this application. Since this application does not require real-time data transportation, it is unnecessary to use UDP for faster transmission. TCP will also guarantee reliable connection while UDP might not be able to easily recover from packet loss (which will result in videos being laggy or broken). If we do care about speed, we can use other means to mitigate slow connection such as pre-buffer or use many local CDN.

   e. a) Social engineering

   b) The owner of the TV station can 1️⃣ install a physical gate with password/code only known to the staff working inside, 2️⃣ give every staff a physical verification card/key, or use a biometric scanner, if they want to enter the facility. 3️⃣ They can train their staff to prevent social engineer just like the one in the movie. 4️⃣ The managers at the TV station can invent a clear security policy and try to monitor/log the entrance history of personnels, so that they can acquire evidence once attack happens.

2. a. i) The *DH* number is $g^{ab} \bmod p = 6^{4 \cdot 5} \bmod 41 = 40$

   ii) The ciphertext will be: `dogg`

b. i) The missing IP addresses are $192.172.0.0/16$. The interface 1 will contain all the IP address from $192.168.0.0$ to $192.171.255.255$ since it's preserving the first 14 bits($11000000\ 101010\ *$). The interface 2 will contain the IP address from $192.173.0.0$ to $192.173.255.255$. Between the last address in interface 1 ($192.171.255.255$) and the first address of interface 2 ($192.173.0.0$) is $192.172.0.0$ to $192.172.255.255$, which can be abbreviate to $192.172.0.0/16$.

ii) $0.0.0.0/0$

c. a) i) FDDI : 200, a double ring with each host having four NICs for each line

ii) ring : 100, in a ring each host is connected to its left and right neighbour and hence two NICs per host

iii) line : 98, in a line, every host is connected on both its left and right neighbour except the two end host who only connects to one neighbour, hence a minimum of $48 * 2 + 2 = 98$ NICs is needed.

iv) bus : 50, in a bus, each host is connected to the bus using only one NIC

b) We need to use 8 switches to connect all 50 hosts. We can have one 8-port switch in the middle of the network, with 1 port of it connecting to a host and 7 other ports of it connecting to another 8-port switch. Each outer layer switch can connect up to 7 hosts (since 1 of its port is connecting to the central switch) so add up to $7 * 7 + 1 = 50$ hosts.

d. i) The frequency of the wave will be $f = \frac{3 \cdot 10^8}{0.2244} = 1.337 \cdot 10^9 = 1336.90$ MHz

ii) The total time of travel is $17 \cdot 3600 + 8 \cdot 60 + 58 = 61738$ seconds

Hence it takes $61738.3714 - 61738 = 0.3714$ seconds for the probe to receive the command.

The total number of characters(bytes) of the reset command is therefore
$\frac{56}{8}\ \mathrm{Kbps} \cdot 0.3714\ \mathrm{s} = 2.5998\ \mathrm{KByte} = 2599.8\ \mathrm{Byte} \approx 2600\ \mathrm{Byte}$

Alternatively, if we choose the binary unit then the calculation goes
$\frac{56}{8}\ \mathrm{Kbps} \cdot 0.3714\ \mathrm{s} = 2.5998\ \mathrm{KByte} = 2662.1952\ \mathrm{Byte} \approx 2663\ \mathrm{Byte}$

e. We can use 1️⃣ network monitoring/logging in order to quickly identify which fake news are spreading fast and try to label them as fake news, such as the measure Twitter has taken in the case of fake information posted by Donald Trump. We can also 2️⃣ clearly define the term of use and verify the source of the posted information so that user know the trustworthiness of information they see. We can also 3️⃣ run large-scale public campaign online in order to raise people's awareness of fake news.