**TECHNICAL ASSESSMENT FOR FIXED CONNECYTIVITY UNIT**

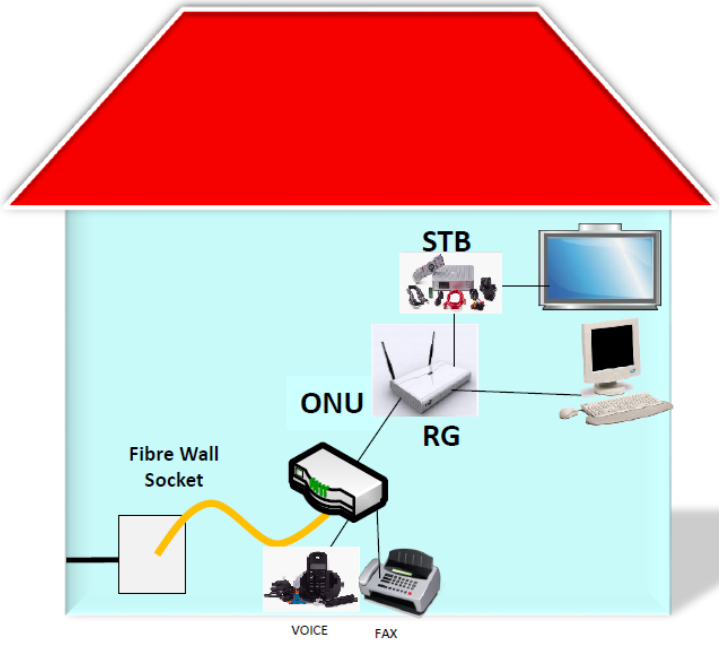
*For Part 2, please install the latest Wireshark program (Stable Release 3.6.6) https://www.wireshark.org/download.html.*

*For Part 3, you will be using Python3 with some basic data science modules, processed and displayed with Jupyter Notebook. Install Anaconda (https://www.anaconda.com/products/individual) to ensure all tools required are available such as pandas module, web driver – chrome or firefox, selenium module and matplolib module).*

*Please upload your answer to a private git repository (i.e. GitLab/GitHub) and share the repository link to mlhadi@tmrnd.com.my, azhari.asrokin@tmrnd.com.my, nabihah@tmrnd.com.my*

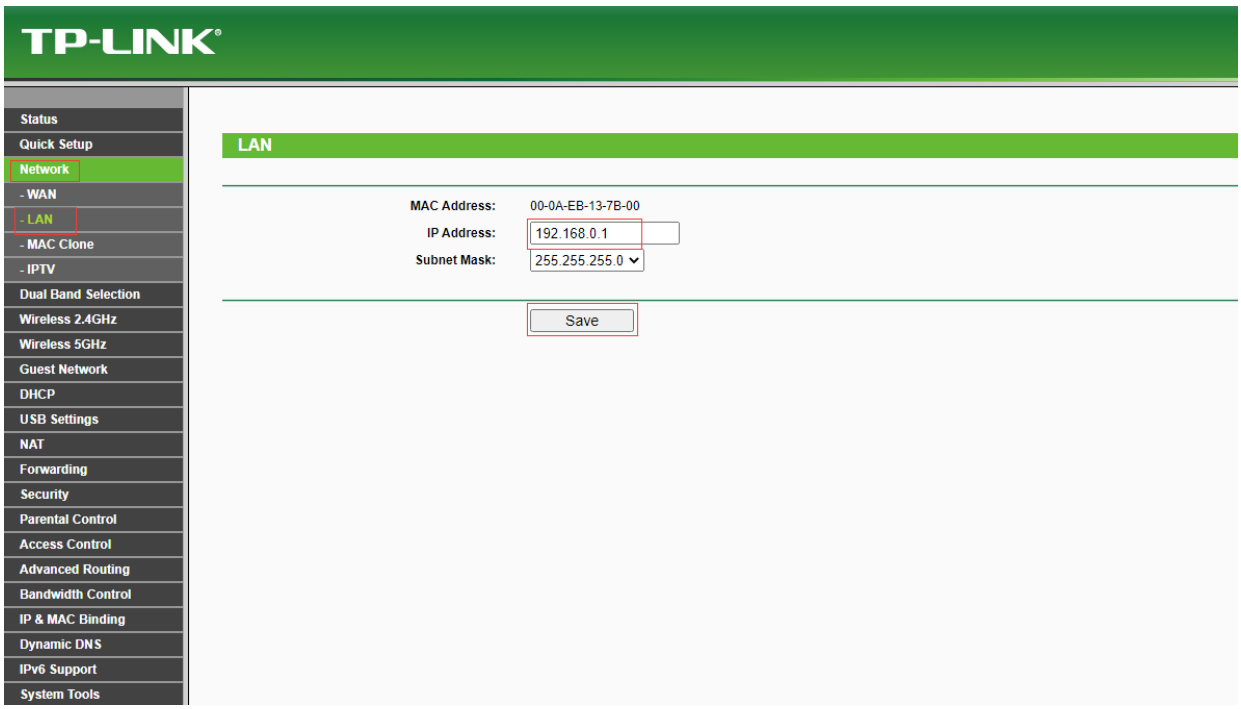
## A. Customer Premise Equipment (CPE)

1. Unifi fiber setup
    - Explain in graphical method the connection of fiber internet in a customer house in Malaysia. Must include Optical Network Unit, Residential Gateway, Setup Box, and DECT phone.




2. Residential Gateway (RG) re-configuration
    - How do you change the following configuration?
        i. IP address of the RG

Log in the web management page




ii. Wifi SSIP name and password

- Using your computer or mobile device, open a web browser. You can use Google Chrome, Microsoft Edge or Mozilla Firefox.
- Log in to the Admin console of your home router.
  Different router manufacturers have different ways of logging in to the Router Admin Console. You may refer to your Router Manual for more details. The most common is http://192.168.1.1.
- On the address bar, type the Router IP address you took note on the previous step then press ENTER.
- Go to Wireless menu option.
- Change the default SSID name in the Wireless Network Name (SSID) field.
  Other router manufacturers follow a similar path to the SSID. Check the website of your router manufacturer or the Router Manual for more details.
- Click Save or Apply to confirm.
  You may need to reboot your router for the changes to take effect.
- Reconnect all your wireless devices using the new WiFi SSID.

## B. NETWORK CONFIGURATION

*Please download the Wireshark file named '**Network.zip**'. The compressed file contains a few activities made by a **User** from a local PC that the candidate needs to explore and find out.*

Based on the file, please answer these questions and if possible, state the lines where the evidence can be found:

1. What is the IP address of the local PC of the user and what is the trigger?
   - ip.src == 192.168.0.104

2. Is it possible to know what is the medium of communication that the user used and how can we know about it?
   - TCP

3. What is the manufacturer's name of :
   - The router connected to the local PC? Destination:
     i. D-LinkIn_9d:ed:f8 (ec:ad:e0:9d:ed:f8)
   - The local PC? Source:
     i. IntelCor_01:30:d8 (3c:9c:0f:01:30:d8)

4. Is there any web browser used by the user and what is the name of the browser and its IP address?
    - Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
    - "8725","79.181134","192.168.0.104","34.107.221.82","HTTP","359","GET /success.txt?ipv4 HTTP/1.1 "

5. Some queries were made in the web browser, can we find out what does the queries are and why?
    - Standard query

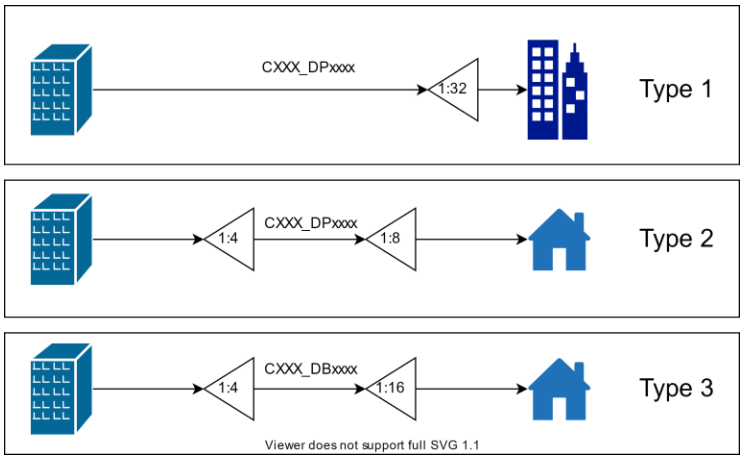
6. Other than the web browser, what other activities can be found occurring during the packet capturing?
    - Web server

7. In your own words, how do you use Wireshark and what are the benefits and the dark sides of using Wireshark?
    - To capture network packet and  monitoring and analysing the packet.

## C. FIBER NETWORK /ANALYTIC

1. You are given a file that contain transmission properties for internet subscribers. You are to identify which subscribers face severe attenuation issues. A severe attenuation is defined as **9** dBm *lower* than the estimated link loss.

   In the given file, you can identify three distinct network configurations, as shown below:




- Type 1 configuration can be identified by repeating digits in the second part of the network identification string, e.g. BGI_C999_DP0001 or BGI_C888_001_DP0001.
- Type 2 configuration can be identified by the last part of the network identification string, e.g. BGI_C001_DP0001, or BGI_C001M_DP001A.
- Type 3 configuration can also be identified by the last part of the network identification string, e.g. BGI_C002_DB0002.

The file may also contain UniFi customers who are on copper transmission (identified with _V in their network identification string, e.g BGI_V001_DPxxxx). You can ignore these customers from your analysis.

The parameters provided in the files are:

1. login_id, customer identification string
2. fdp_id, network identification string
3. tx_power, optical transmit power, given in dBm.
4. rx_power, optical receive power, given in dBm.
5. ranging, distance between transmitter and receiver, given in meters.

Use the following values to estimate the link loss, and find the users with severe attenuation issues as defined above.

| Splitter Ratio | Loss (dBm) |
|---|---|
| 1:2 | 4 |
| 1:4 | 7 |
| 1:8 | 11 |
| 1:16 | 15 |
| 1:32 | 19 |

Use 0.3 dBm/km as the fiber attenuation

Use the Pandas library as your processing and analysis tool.