**ISLAMIC UNIVERSITY IN UGANDA**

FACULTY : SCIENCE

DEPARTMENT : COMPUTER SCIENCE

COURSE : BIT 3

COURSE UNIT : SYSTEM AND NETWORK ADMINISTRATION

LECTURER : DR. KASULE ABDAL

DATE OF SUBMISSION : 23TH MAY 2023

**TASK: ASSIGNMENT 3**

* Describe the various ways and requirements needed to connect a computer to
  + A wired network
  + A mobile network
  + Demonstrate this with a computer (include screen shots in your write up)
* Describe how RADIUS server is used to manage user authentication to a network
* Create three windows 10/11 virtual machines
  + Set it up one as a dhcp server to assign ip addresses to the other two.
  + Hand in all the three virtual machines.

**GROUP MEMBERS:**

|  |  |  |
| --- | --- | --- |
| **NO** | **NAME** | **REG NUMBER** |
| 1 | WATUMWA ISAAC | 220-063011-19529 |
| 2 | BALIKOWA YUSUF | 217-063012-09946 |
| 3 | MUGISHA YASIRI | 220-063011-19629 |
| 4 | SUHAIL MUSA | 220-063011-19313 |
| 5 | ASHRAF HASSAN | 220-063011-19572 |
| 6 | HIGENI ABDUL KARIM | 220-063011-19214 |

**QN1.Describe the various ways and requirements needed to connect a computer to**

**A wired network**

Ethernet Cable

You will need an Ethernet cable, also known as a network cable or LAN cable. It should have the appropriate connectors (usually RJ-45) at both ends.

Network Interface Card (NIC)

A network interface card is required to connect the computer to the network. Most modern computers have built-in NICs. If not, you may need to install a separate NIC into an available expansion slot.

Router or Switch

A router or switch is necessary to connect multiple computers and devices in the network. It acts as a central hub for data transmission.

Internet Service Provider (ISP)

You will need an active internet connection from an ISP to access the internet through the wired network. The ISP will provide you with the necessary credentials and connection details.

**A mobile network**

Wi-Fi Tethering

Enable Wi-Fi tethering on your mobile device and connect your computer to the Wi-Fi hotspot network.

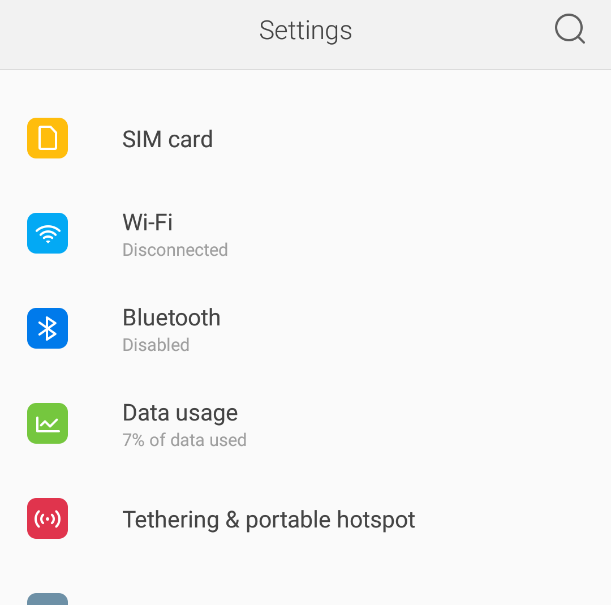
Enter the provided password or passphrase, if prompted.

Once connected, your computer will use the mobile network connection provided by the tethering device.

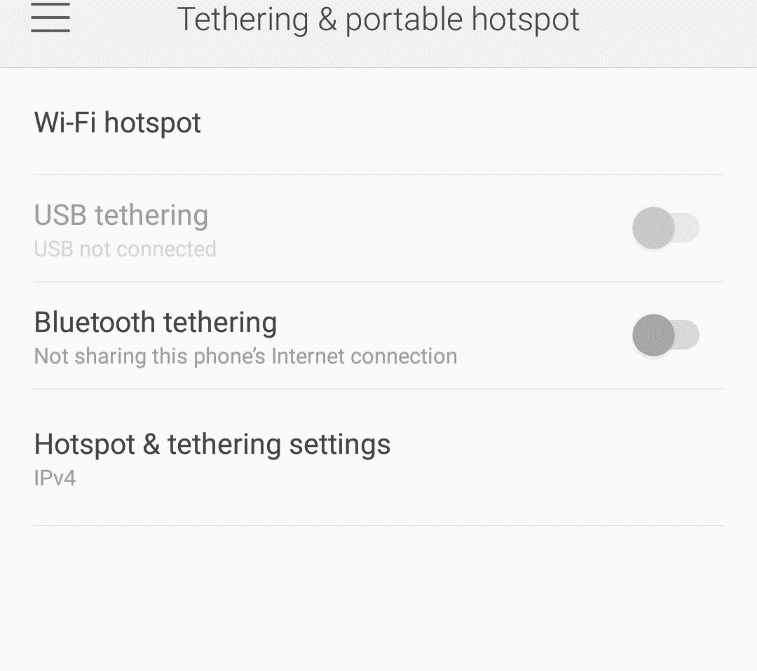
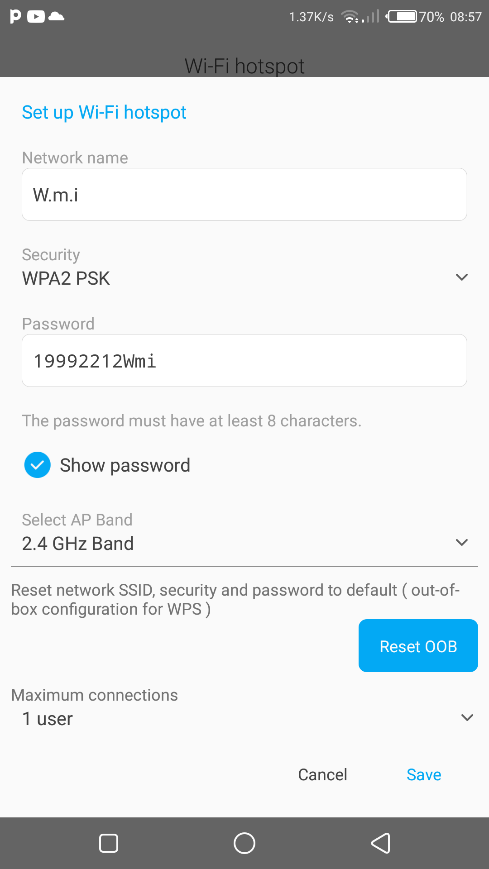
**STEPS**

Ensure that your mobile device supports Wi-Fi tethering (personal hotspot) and that it has an active mobile data plan.

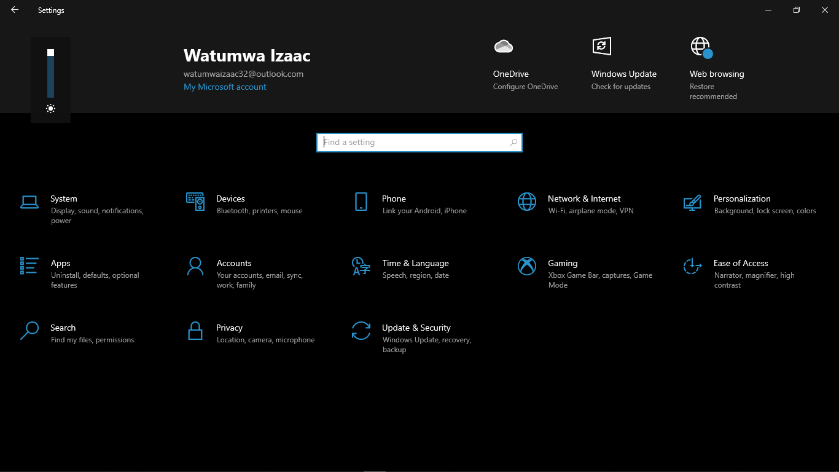
On your mobile device, go to the settings menu and look for the "Personal Hotspot" or "Tethering" option. The exact location and naming may vary depending on the device and operating system.

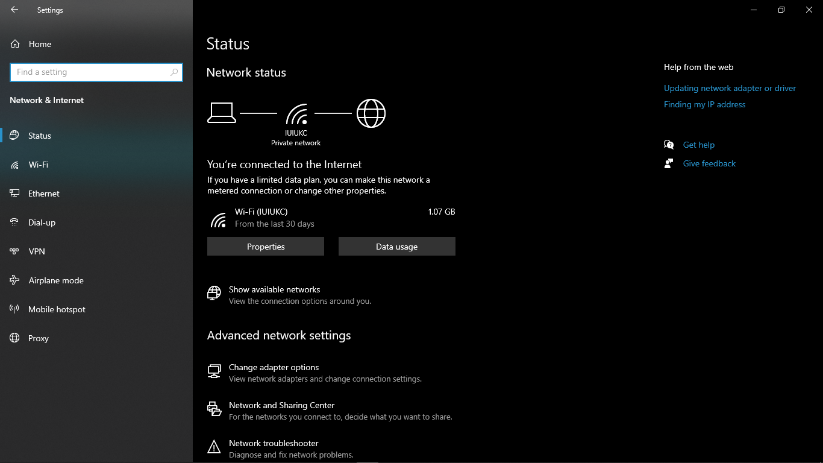


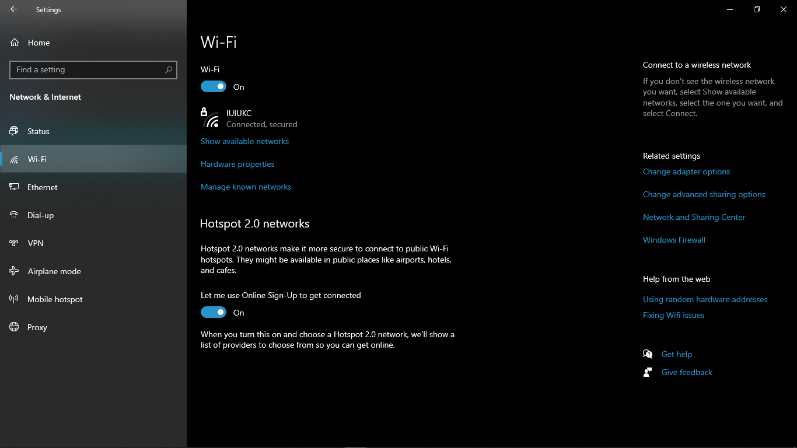
Enable the Wi-Fi hotspot or tethering feature on your mobile device. You may need to set a password or passphrase to secure the hotspot. Take note of this password.

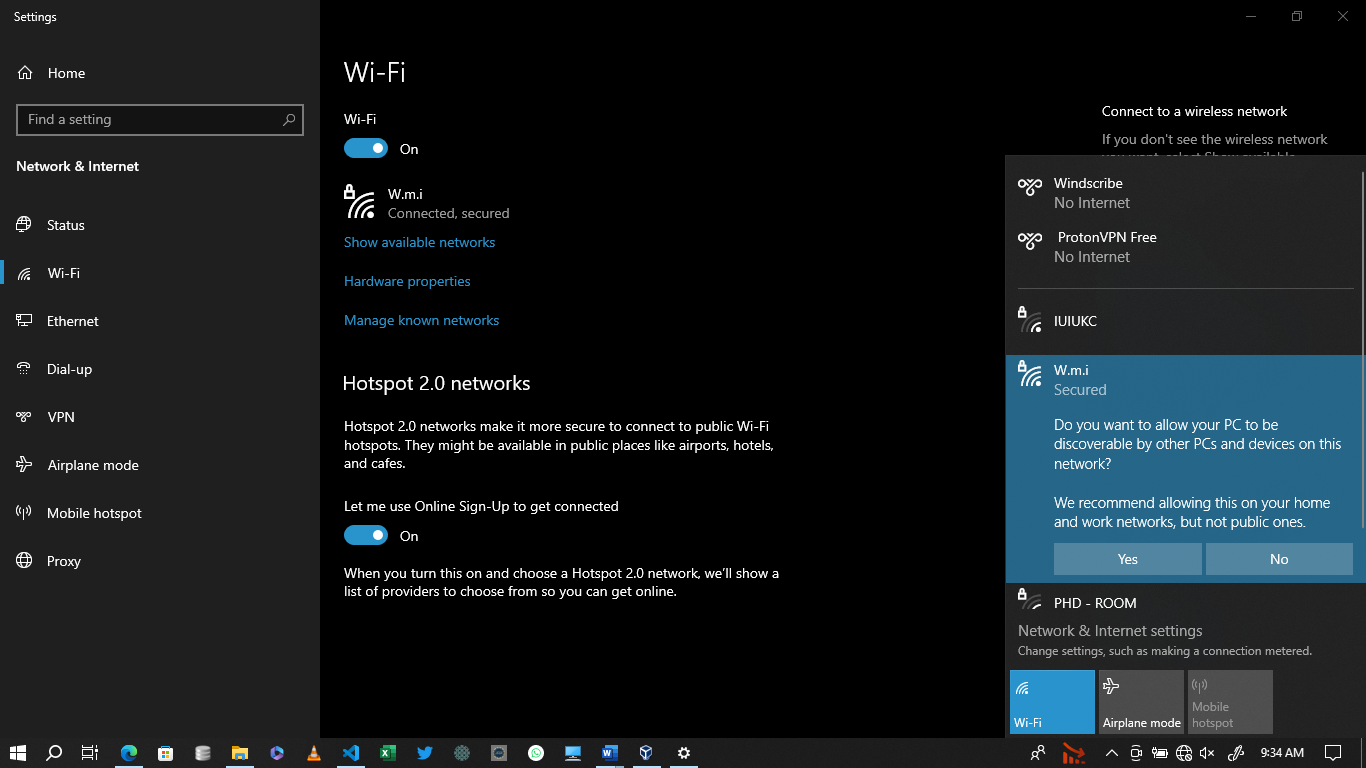
On your PC go to settings and make sure the Wi-Fi capability is turned on. You can usually do this through the network settings or by clicking on the Wi-Fi icon in the taskbar.



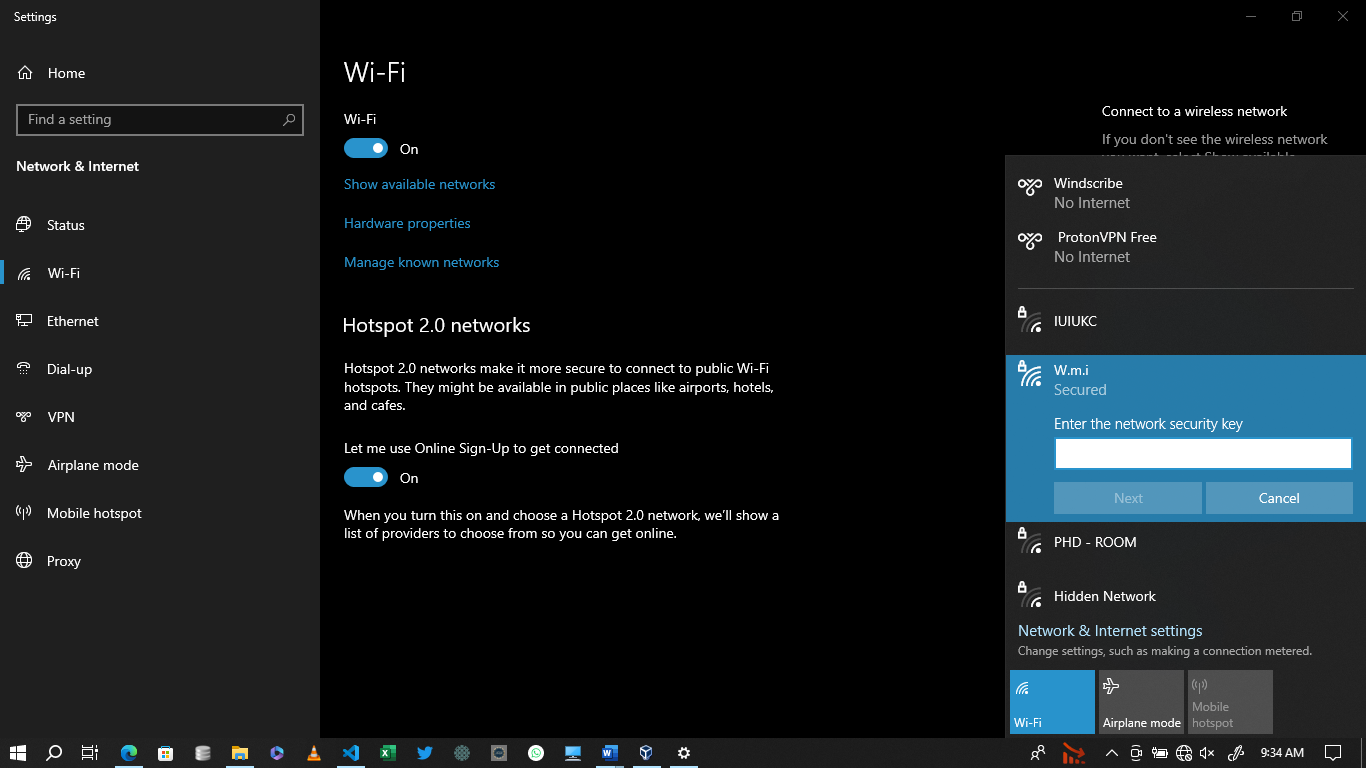




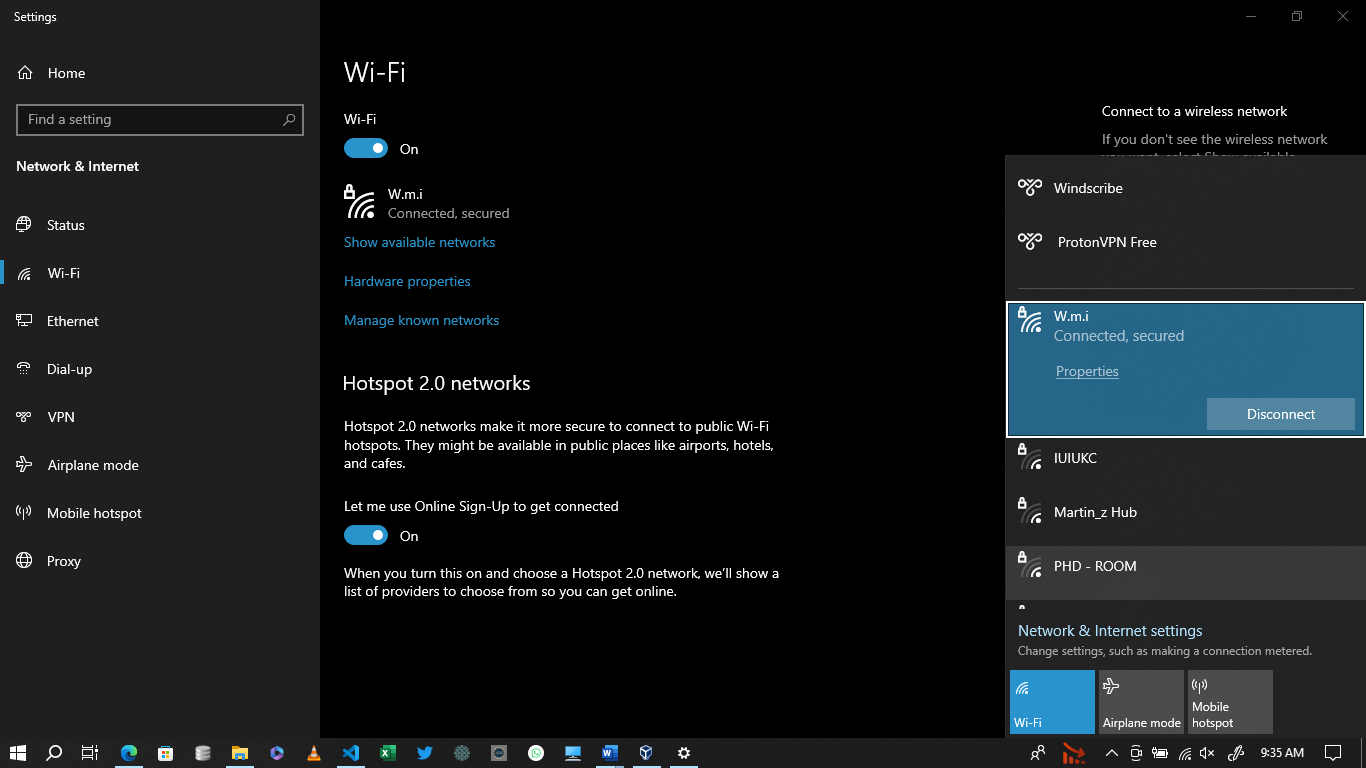
Your PC will scan for available Wi-Fi networks. Locate and select your mobile device's hotspot network from the list of available networks.



If prompted, enter the password or passphrase you set in step 3. This is necessary to establish a secure connection between your PC and the mobile device.



Once connected, your PC will use the mobile network connection provided by the Wi-Fi hotspot. You can verify the connection by checking the network status on your PC or opening a web browser to access the internet.



Top of Form

**Describe how RADIUS server is used to manage user authentication to a network**

RADIUS (Remote Authentication Dial-In User Service) is a client-server protocol that allows remote users to request access to a network resource through a device that communicates with a central RADIUS server. The user submits a username and a password, which are encrypted by the RADIUS server and verified against a database. The RADIUS server then sends an Access-Request message to the device, which grants or denies access to the user.

RADIUS authenticates using two approaches:

Password Authentication Protocol (PAP). The RADIUS client forwards the remote user's user ID and password to the RADIUS authentication server. If the credentials are correct, the server authenticates the user and the RADIUS client enables the remote user to connect to the network.

Challenge Handshake Authentication Protocol (CHAP). Also known as a three-way handshake, CHAP authentication relies on the client and server using an encrypted shared secret. [Compared to PAP](https://www.techtarget.com/searchnetworking/answer/Which-is-most-secure-CHAP-or-PAP), CHAP authentication is considered more secure because it encrypts authentication exchanges and it can be configured to do repeated mid-session authentications.