

# Unit 12 & 13, Assignment 2

## Fault Finding and Solutions

George Hotten

March 7, 2023

## Identifying Faults and Remedies

### Problem #1

**Description** The computer loads up but when opening the web browser, no websites load, and you cannot connect to local network servers.

#### The type of fault

This fault is caused by a lack of a network connection, often caused by unconfigured Wi-Fi, network cabled not plugged in or a lack of a DHCP server on the network. If all the above are correct, a software issue could be causing the issue. For example, a misconfigured firewall.

#### Hardware and software that can be used for troubleshooting

If on a Wi-Fi based network, try using a different device to see if the connection is working. If the connection is working on a different device, perhaps there is an invalid static IP address set for the network on your NIC. You could further try connecting to a different Wi-Fi network on that device to see if that resolves the issue. If it doesn't, it could be a fault with your Wi-Fi adapter.

For all connections, a misconfigured software firewall could be blocking connections to the internet. Using the built-in Windows firewall app settings can be checked to ensure traffic is allowed in and out of your NIC. The Windows Troubleshooter can also identify issues set in Windows that could be blocking a network connection.

#### Sources of technical information and guidance

There are many sources of information you could use for guidance and advice. For example:

- Microsoft's knowledge base for [connection issues](#).
- Online guides from sites such as [Windows Latest](#) and [Aomeitech](#).
- Internal guidelines and procedures for troubleshooting network issues.
- Use OpenAI's [ChatGPT](#).

## Fault remedies

Depending on the issue, there are many ways faults can be remedied. In this example, I will assume that there is no DHCP server on the connected network.

Firstly, log onto your router and locate its DHCP settings and ensure that the DHCP server is enabled. Once the DHCP server is enabled, use the Windows command line to run the following commands: `ipconfig release && ipconfig renew`.

If this does not work, ensure that your computer's firewall allows traffic from ports 67 and 68 to allow traffic from the DHCP server. If all else fails, set a static IP inline with the other devices on your network.

## Comparing tools used to fix the fault

To resolve a lack of a DHCP server, you could use a router's web GUI or, if applicable, the router's command line. For ease of use, I would recommend and personally used the router's web GUI as it is easy to navigate and understand with a low learning curb. It also makes it easier to view and understand data. With a command line, you would need to learn the commands and the layout of the CLI before being able to resolve the error.

For example, with a MicroTik router that is running RouterOS v7, you can either use their GUI via WinBox, or use their CLI. When using the GUI, it is easier to understand as all the possible options are laid out to you.

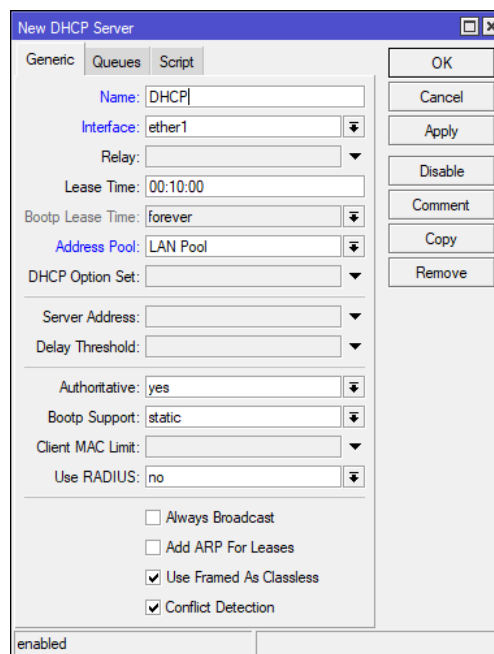


Figure 1: RouterOS v7 via WinBox creating a DHCP server

Compared to the CLI, which requires you to have knowledge of the possible options and of what can be set within those options.

```
MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III  KKK  KKK  RRRRRR   000000   TTT   III  KKK  KKK
MMM MM  MMM III  KKKKK  RRR  RRR  000  000   TTT   III  KKKKK
MMM     MMM  III  KKK  KKK  RRRRRR   000  000   TTT   III  KKK  KKK
MMM     MMM  III  KKK  KKK  RRR  RRR   000000   TTT   III  KKK  KKK

MikroTik RouterOS 7.7 (c) 1999-2023      https://www.mikrotik.com/

Press F1 for help

[george@HNet23RT1] > |
```

Figure 2: RouterOS v7 via SSH

## Problem #2

**Description** A message from the antivirus software has popped up on the screen saying the computer is infected.

### The type of fault

This fault is caused by malware being found within the system. This can happen if a user accesses an infected website or downloads an infected file. The malware can put your data and security at risk as the data could be sent back to the malware's creator. The malware also has the ability to lock files away and destroy your operating system.

### Software that can be used for troubleshooting

There are a broad range of different software solutions you could use to diagnose what type of malware is infecting the system. Different software solutions include Malwarebytes, Avast Anti Virus and Windows Defender. These applications run scans on all your files to find and identify malware that is on your system.

### Sources of technical information and guidance

There are many sources of information you could use for guidance and advice. For example:

- Microsoft's knowledgebase for [removing malware](#).
- Online guides from sites such as [Avast](#) and [AVG](#).
- Internal guidelines and procedures for handling virus infections.
- Use OpenAI's [ChatGPT](#).

## Fault remedies

To fix the fault caused by a virus, I will use Malwarebytes to scan and remove any viruses found. Malwarebytes has real-time protection which can stop any malware from running before it has the chance to do damage to your system. Malwarebytes also completes daily scans checking for malware. If any is found, it is quarantined and deleted from your device.

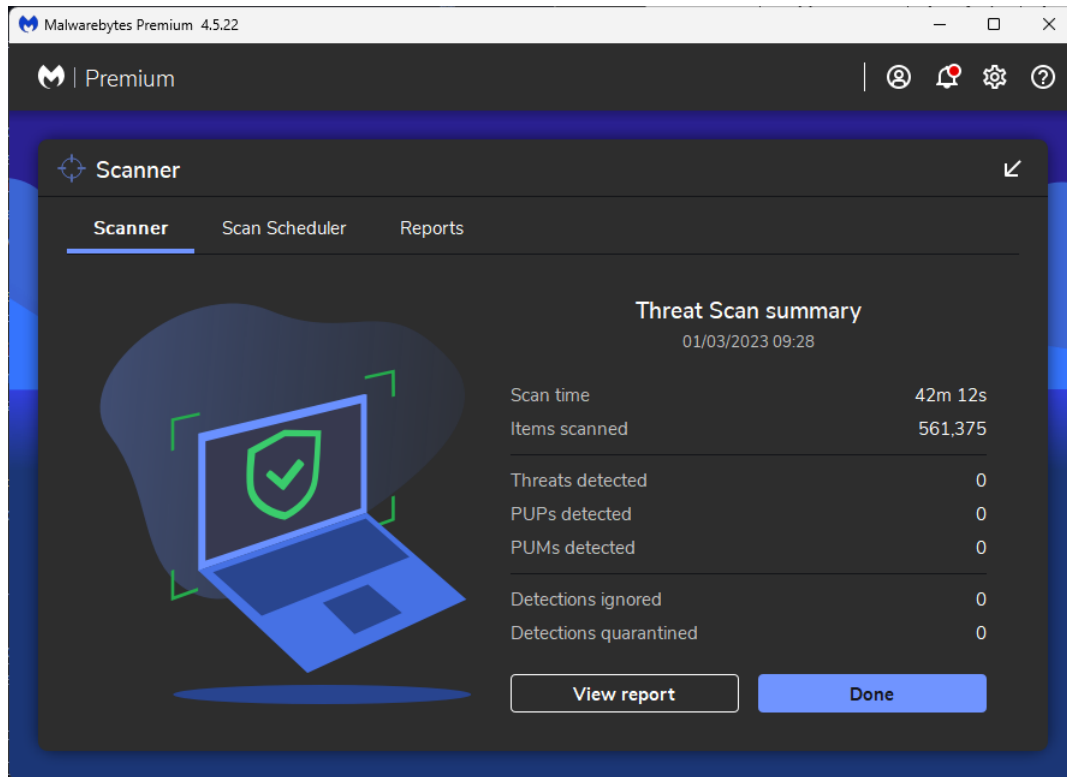


Figure 3: Summary of a completed Malwarebytes scan

## Comparing tools used to fix the fault

I will compare two software tools that can be used to remove a virus. Avast and Malwarebytes. Both tools support real-time protection, scheduled scans and the ability to quarantine malware. However, Malwarebytes focuses more on the detection and removal of malware whilst Avast has a broader range of available tools such as a firewall, password protection and a VPN.

Both antiviruses have a good track record for detecting and removing malware. However, Avast generally performs better at blocking viruses before they get the chance to cause damage whilst Malwarebytes is most suited for removing malware on an already infected system. Therefore, I chose Malwarebytes to remove the identified malware from example system.

## Problem #3

**Description** The computer powers up but 10 short beep codes are heard.

### The type of fault

During boot, motherboards use beep codes to indicate that a fault has occurred and the system may not be able to boot into the operating system. The meaning of the long continuous beep depends on your motherboard as the beep codes are often different per model or manufacture.

### Hardware and software that can be used for troubleshooting

As the meaning of the beep code depends on the motherboard, it would be ideal to review the motherboard's manual that came in the box or by locating the manual on the manufacturer's website. This can be accessed on any internet-enabled device.

### Sources of technical information and guidance

There are many sources of information you could use for guidance and advice. For example:

- Motherboard manuals from [MSI](#) and [Gigabyte](#).
- Internal guidelines and procedures for computers failing to POST - these should contain the beep codes for the motherboards being used.
- Internet sources from [Computer Hope](#) and [Beebom](#).

### Fault remedies

In the problem described there are 10 short beeps heard during power up. To start, you should consult your motherboard manual following the ways listed above. After discovering that this beep code suggests that there is an issue with your CMOS battery, you should check to see if your CMOS battery is properly inserted into the socket. After reseating try turning the computer back on. If the issue persists it may be time to replace your CMOS battery. If a new battery still does not fix the issue, there may be a problem with your motherboard.

### Comparing tools used to fix the fault

When looking for the meaning of beep codes, you could use the paper manual that came with your motherboard, or you could use a digital version found on the manufacturer's website. The advantage of using a digital version over a paper version is that it will always be the most up-to-date version if anything has changed through BIOS updates. However, an advantage over using the paper version is that you have an offline copy in case you are unable to access the internet to help repair the fault.

## Problem #4

**Description** The user is unable to print out documents to the local printer plugged in to the system.

### The type of fault

This fault can be caused by a wide variety of issues. For example, the printer may be misconfigured, you may not have the appropriate drivers installed or there may be an error on the printer (for example, no paper!).

### Hardware and software that can be used for troubleshooting

Starting with hardware, you should ensure that the printer is turned on and is properly connected to your system. Then ensure that there are no errors on the printer, such as no paper or ink. Moving to software, ensure that you download and install the latest drivers from the manufacturer's website. Further ensure that the printer is properly configured with an IP address and subnet mask and that it is recognised within your operating system.

- HP's printer [knowledgebase](#).
- Microsoft's knowledgebase for [printer connection errors](#).
- Internal guidelines and procedures for printing errors.

### Fault remedies

In this example, I will assume the fault was identified as a lack of drivers. To fix the above issue, you should navigate to the manufacturer's webpage and locate the drivers needed for your model of printer. Proceed to then installed the drivers as an administrator and then attempt to print the document. If it still fails, try restarting your computer.

### Comparing tools used to fix the fault

Some manufacturers have a utility that automatically detects and installs the appropriate drivers for the devices you use. However, if the utility wrongly detects a device the wrong drives may be installed which could cause instability or losing the ability to print. The alternate option is download the appropriate drivers directly from the manufacturer's website which ensures that you are downloading the correct driver for your device. However, this would require you to check back to the download site regularly for updates and patches to the driver.

## Judging the Value of Sources

When looking for information online, there is often many articles and posts that come from a wide variety of sources. As some sources are more reliable than others, it is important you verify where any information is coming from before following any instructions or advice given. From the sources I listed above, I shall categorize and rank them in order of how reliable they may be.

### Highest Reliability - Manufacturer's Documentation

Sources from this category are documentation, posts and articles that have been written by the manufacturer of the product you are gathering information on. For example, the Microsoft knowledgebase would be most suitable for gathering information and getting support on the Windows operating system as they are its creators and therefore have the most knowledge about the operating system.

### Moderate Reliability - Internal Guidelines

Sources from this category are documentation that have been written internally using experience resolving previous faults. This documentation would contain what the exact fault was and how it was previously resolved, allowing for any future technicians to resolve the fault. However, care must be taken before following any steps as they may have been specific to certain hardware as, for example, what worked to fix motherboard may not work to fix a different kind of motherboard.

### Low Reliability - Internet Sources

Sources from this category are posts and articles that have been written by a third party individual. These contain steps and instructions on how to fix specific issues, for example providing steps on how to fix a printer that isn't printing. However, the steps provided often lack context and assume the issue is caused by a specific issue when in reality there are a whole range of issues that may be causing the fault. These sources often do not contain any citation and therefore cannot always be trusted.

### Lowest Reliability - AI Generated Responses

Sources from this category are responses to questions that have been generated by an artificial intelligence, such as OpenAI's ChatGPT. Whilst responses often contain more context to the issue, assuming it was provided by the user, there is no source citation and it is impossible to verify if the solution will work without extra research. AI chatbots can also be confidently wrong and will not admit so even if told by the user. This means AI chatbots should be used as a last resort if no other help can be found online, or if the problem is very specific and you are willing to take the risk that the AI is giving you safe instructions to resolve your fault.



## Maintaining Data Integrity and Security

When applying solutions to resolve a fault, it is important that the data on the faulted device remains intact and secure. Therefore, it is important to take all the appropriate steps to ensure there is no risk to data integrity and security.

### Data Backups

When applying solutions to faults, or when a fault occurs, there is a chance of data loss. Because of this it is vital that regular data backups occur of any important data. The importance of the data should dictate how often it is backed up. For example, the most important data to a business could be backed up hourly, whilst less important data can be backed up weekly. You should also consider backing up data before attempting to fix a fault. To ensure data security, the backup should be encrypted to prevent any unauthorized access to the data in case of a cyberattack or a robbery. To future ensure your data is safe, you should keep a copy of your data in an off-site location.

### Recovery Procedures

In the event that data is lost caused by a fault or whilst fixing a fault, data will have to be restored. A plan should be created to ensure the recovery procedure is standardized and effective. This should include restoring the data from the most recent backup and providing a temporary alternate system to be used whilst the backup is being restored. The recovery procedure should be regularly tested to identify any weaknesses and ensure that it is able to quickly and effectively restore data.

### Maintaining Security

When performing repairs, it is essential to ensure that the data held on the system is kept secure. The proper user access rights should be setup to prevent any unauthorized access to sensitive data whilst the system is being repaired. The technician should ensure that the operating system is up-to-date and the most recent virus definitions are installed on your antivirus. This lowers the likeliness of malware infecting the system and potentially stealing data.

### Physical Protection

To ensure the data found on a system is truly secure, it must also be physically protected. This can be done by ensuring that only trusted people have access to the build where the system is stored, and future putting the system behind locked doors ensuring that only people who must access it physically can. This keeps data safe in the event of a robbery as the criminals wouldn't be able to gain access to the physical drive to steal the data.

## Responses to End Users

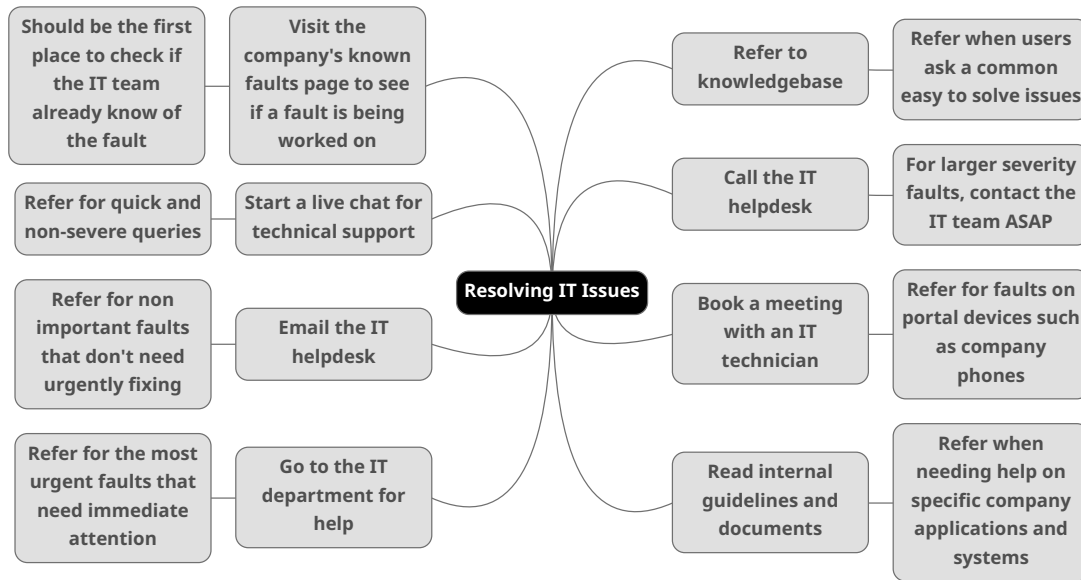


Figure 4: Mind map of ways IT issues can be resolved.

## Moodle Support Discussions

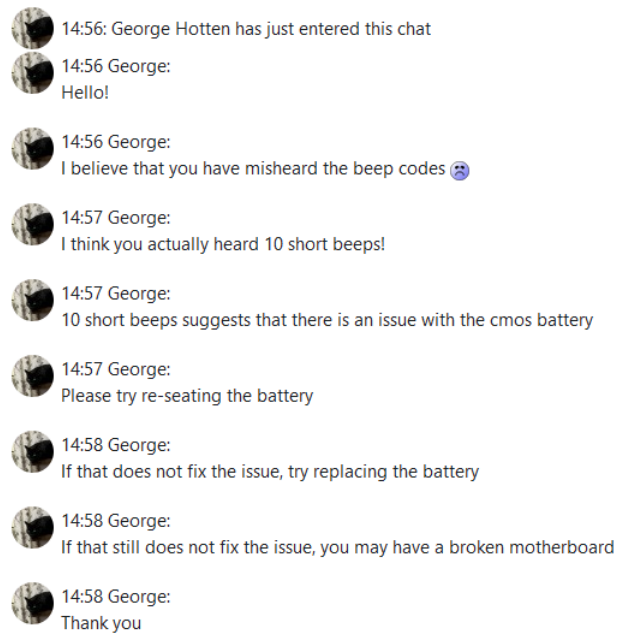
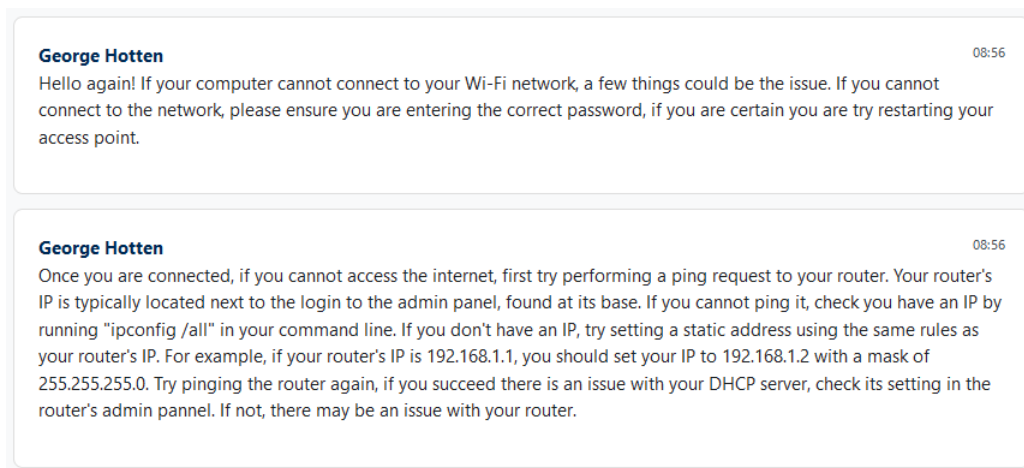
- 
- 14:56: George Hotten has just entered this chat
- 14:56 George:  
Hello!
- 14:56 George:  
I believe that you have misheard the beep codes 😞
- 14:57 George:  
I think you actually heard 10 short beeps!
- 14:57 George:  
10 short beeps suggests that there is an issue with the cmos battery
- 14:57 George:  
Please try re-seating the battery
- 14:58 George:  
If that does not fix the issue, try replacing the battery
- 14:58 George:  
If that still does not fix the issue, you may have a broken motherboard
- 14:58 George:  
Thank you

Figure 5: A PC starts to boot but ten beep codes are given.



**George Hotten** 08:56  
Hello again! If your computer cannot connect to your Wi-Fi network, a few things could be the issue. If you cannot connect to the network, please ensure you are entering the correct password, if you are certain you are try restarting your access point.

**George Hotten** 08:56  
Once you are connected, if you cannot access the internet, first try performing a ping request to your router. Your router's IP is typically located next to the login to the admin panel, found at its base. If you cannot ping it, check you have an IP by running "ipconfig /all" in your command line. If you don't have an IP, try setting a static address using the same rules as your router's IP. For example, if your router's IP is 192.168.1.1, you should set your IP to 192.168.1.2 with a mask of 255.255.255.0. Try pinging the router again, if you succeed there is an issue with your DHCP server, check its setting in the router's admin pannel. If not, there may be an issue with your router.

Figure 6: A PC will not connect to the Wi-Fi network.

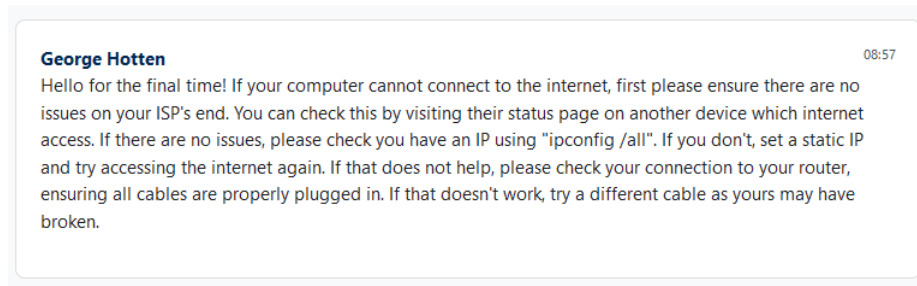
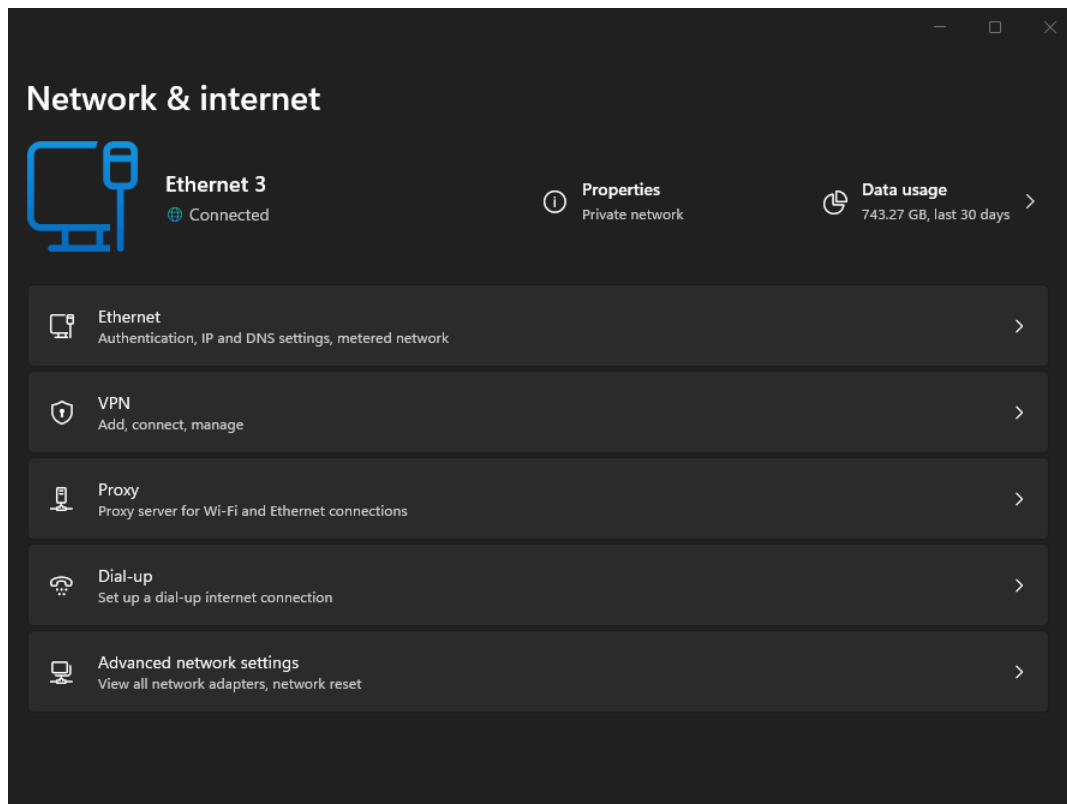


Figure 7: A classroom PC won't connect to the internet. The icon on the lower right of the taskbar shows the Windows "no internet" icon.

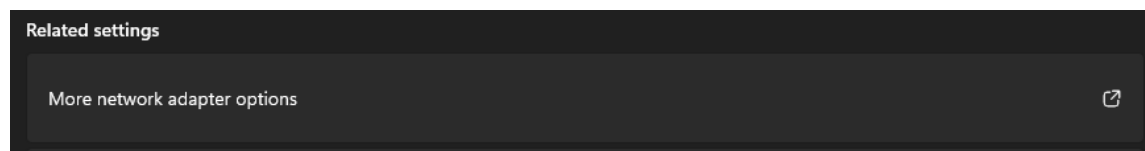
## Additional Support Material *as seen in Teams*

Hello! You have asked me how to set an IP address on your computer when you don't have DHCP! I would love to help!

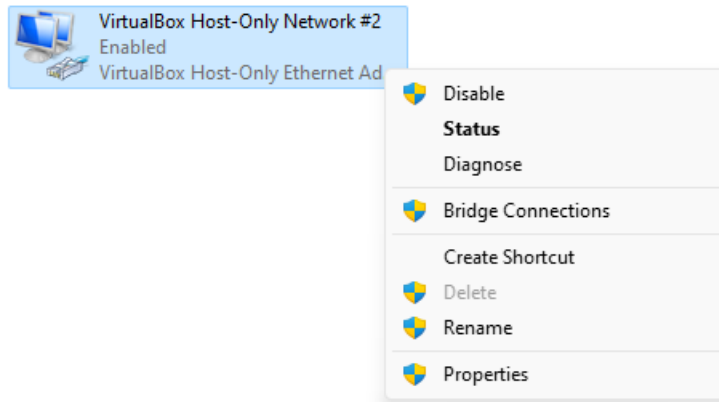
Firstly please right-click the network icon at the bottom right of your computer and enter your Network & internet settings.



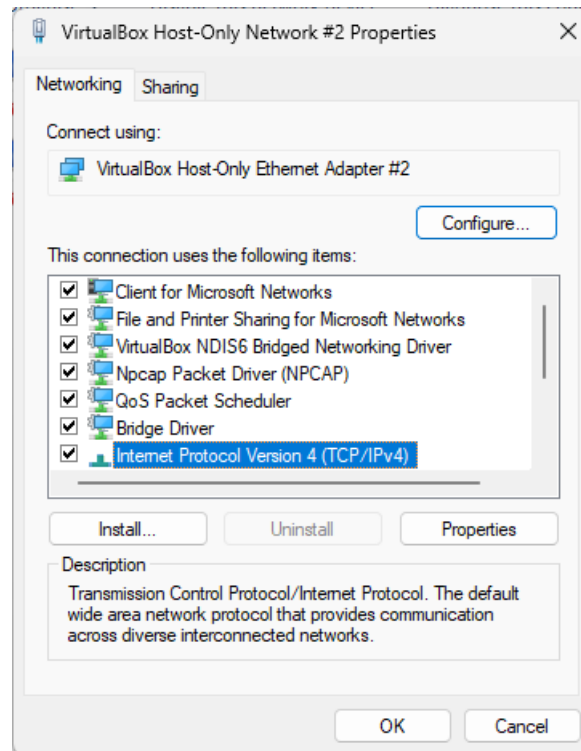
Please now press Advanced network settings, scroll to the bottom of the page and then press More network adapter options.



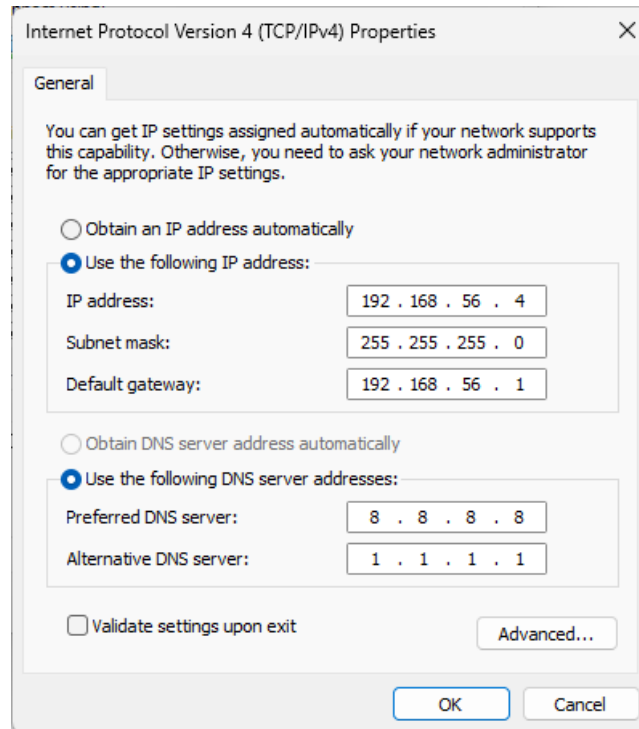
Select your network interface by right-clicking it and pressing Properties.



In the menu that opens, select Internet Protocol Version 4 and select properties.



Finally, select Use the following IP address and enter the appropriate address for your network. Please do the same for your DNS settings.



Finally, press OK, and then OK again, and you now have an IP! You can verify this by opening a command line console and typing the command `ipconfig /all`.

Thanks!