Windows 10 Networking 2018 by Jolie Ballew

Configure IP Settings and Network Connectivity

Connect to the Internet

What are the two kinds of connections?

- Wired connection that uses ethernet connection. This is the easiest way , you can connect it using the router, ethernet extender or ethernet wall port.
- Wireless connection uses wireless hardware.

Network profiles

What are the 3 network profile types?

- Public, Private and Domain. These are pre set configurations that manage security and sharing settings automatically.

What are private networks?

- They are found in homes, in small to mid sized companies.
- Your computer is visible on the network and you can see others' computers too.
- You can access network resources like shared printers.
- Network discovery is tuned on , this what makes your computer discoverable on the network.

What are public networks?

- They are mostly found in public places like hotels, coffee shops ,etc.
- Your computer shouldn't be visible on such a network and the network discovery should be turned off.
- You shouldn't be able to see others' computers either.

What are domain networks?

- These networks are configured for large businesses.
- Resources are available but users need proper permissions to access them.
- Resources you see on the network is determined and managed by the network administrator.

Note:

- In any case that windows does not know what profile to apply it applies the public profile.
- You can change from public to private and vice versa but you cannot change in case of the domain profile types as they are managed and secured by the network administrators and can't be changed by general users.

Configure advanced profile sharing options

How can you change the configuration settings for different profile types?

- By accessing the Advanced Sharing Settings under the Network and Sharing Centre.

Network Connectivity: TCP/IP

What is an IP address?

- A unique string of characters that identifies each computer using the Internet Protocol to communicate over a network.

Extra Notes:

- Internet Protocols: They provide the rules and standards necessary for different devices to communicate with each other on a network. Without these protocols, devices would not be able to understand each other's signals and transmit data effectively.
- TCP/IP is the default Wide Area Network protocol that provides communication across a variety of network types an infrastructures.
- The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data. In simple words, IP finds the destination of the mail and TCP has the work to send and receive the mail

What are the two main functions that an IP address serve?

- It identifies the host /network interface.
- it identifies the host on the network
- Eg: how a house address identifies the house on a street and in a city

What is a MAC or a Physical Address?

- Stands for Media Access Control address.
- It is a unique identifier provided by the manufacturers for identifying individual electronic devices on a network.

Network Connectivity: DHCP/DNS

The IP addresses can be assigned manually or automatically. DHCP is used to assign IP addresses automatically.

What is DHCP?

- Stands for Dynamic Host Configuration Protocol
- DHCP is a network protocol used to dynamically assign IP addresses and network configuration settings to devices on a network
- Eg: When a device (e.g., a computer or smartphone) joins a network, it can send a DHCP request to a DHCP server. The server responds by assigning the device an available IP address and providing other necessary network settings.

What is APIPA?

- It stands for Automatic Private IP addressing.
- When the DHCP server is not available and the static address is also not provided APIPA is a feature in many modern operating systems, such as Windows, that allows a device to automatically assign itself a private IP address.
- It uses a reserved range (169.254.0.0 - 169.254.255.254)

What is DNS?

- DNS stands for the Domain Name System, connecting domain names into IP addresses. This way, browsing the internet becomes easier as people can use words to access various websites, rather than the long IP addresses containing numbers.

Configure Network Adapters

What is a Network Adapter?

- It is located inside a computer and enables the computer to connect to a network.
- There are external adapters too and these connect to USB ports to provide connectivity.
- You can locate all the network adapters from the Device Manager.

Create a VPN

What is a VPN?

- It stands for Virtual Private Network
- It is a technology that provides a secure and encrypted connection over a less secure network, such as the internet. It allows users to access resources and browse the internet with enhanced privacy, security, and anonymity.
- You can create a VPN by navigating to the Settings> Network and Internet> VPN > Add a VPN connection. Enter the following details on the screen
  - VPN provider: Windows built in
  - Connection name: eg: IbisCafe
  - Server name/address: type the address given by the network admin
  - VPN type: Automatic

- Type of sign in info: Username /password
- Enter the username and password
- Click Save
- You can now connect to the new VPN by clicking on connect or simply choose from the network list on the task bar.

Configure Wireless Network Settings

How to connect to a wireless network?

- To connect you choose the network you wish to connect from the network list.

What is the network you want to connect doesn't show up?

- You will need to connect manually, navigate to Network & Internet > Network and Sharing Centre> Set Up a new connection or network > manually connect to the wireless network > choose the wireless adapter > enter the below details(all of which can be obtained from the network admin):
  - Network name
  - Security type
  - Encryption type
  - Security key
- If the network you've connected to is Metered which implies that there are constraints on how much data you can use or transfer while connected to that network, and exceeding those limits might result in additional charges or restrictions.
- To move it to a metered connection simply turn on the toggle under the settings

How do you disable all wireless network activity on your computer?

- Airplane mode is used to disable Wi-Fi, Bluetooth, GPS and cellular

What are hotspots?

- Hotspots are created by devices or equipment that have internet connectivity and the capability to broadcast a Wi-Fi signal, allowing other devices to connect to the internet through them.

What helps you to manage the consumption of data?

- Data usage allows you set data usage limits for the networks your using

How do you troubleshoot network connectivity?

- First check if you are connected to a network
- Next check if the network adapter has been installed or it has been disabled

- Go to the Network and Sharing center and if you don't see any connection, perhaps the Wi-Fi adapter is disabled, click on change adapter settings to investigate, right click to enable the adapter.

What do you do if you are able to access the internet but not the resources on the network?

- In this case perhaps the network is configured public instead of private. Go to the settings and change the network profile.

What do you do if the issue is still unresolved?

- Run the network trouble shooter
- To easily access this setting right click on the network icon from the task bar > trouble shoot problems.
- You might also have a connectivity issue if you have a static IP assigned when you should have a IP assigned automatically by the DHCP server. To check if the DHCP has got disabled navigate to change adapter settings > you notice that the network is available but it says "Not connected". In this case, right click and choose properties. Select IPV4 and choose properties, make sure the radio button is on Obtain IP address automatically.

Configure and Maintain Network Security and Preferences

Configure a Windows Defender Firewall

What ensures safety while using different networks?

- Windows Defender Firewall is a fundamental component of Windows security, helping to safeguard your computer from network threats and unauthorized access. While it provides basic network protection, some users may opt to complement it with additional security measures, such as third-party firewall solutions or antivirus software, for more comprehensive protection.
- On accessing the firewall if you notice everything is green , then the network is healthy

How do you troubleshoot of the firewall is turned off?

- It may be because of a third part firewall installed on your computer or a malware infiltrated the system.
- click on turn Windows firewall on/off from the left pane and make the selections

How do you change the settings so allow remote users?

- Get to the main firewall screen and click on Allow an app or feature through Windows Defender Firewall, choose what feature or app you would want to allow on private/private or both

Note: To block all incoming traffic on firewall, select all the checkboxes under the Turn on Firewall in customize settings

Manage windows firewall with advanced security

How do you manage firewall rules to allow or block an app ?

- By choosing block the connection under inbound and outbound rules in advanced settings

Create a program rule

What are the different rules that you can create?

- **Program rules** are based on specific programs or applications installed on your computer. These rules allow or block network traffic for individual applications.
- **Port rules** are rules that are based on network ports.
- **Predefined rules** are rules that come preconfigured with the firewall software.
- **Custom rules** are rules that you create manually based on your specific requirements.

What are the steps to create a Program Rule?

- Let's take blocking IE as an example
- Navigate to Windows Defender Firewall> Advanced settings> Outbound rules> Right Click New rule> Choose Program Rule
- Enter the IE program path
- Select Block the connection under Action
- Select all checkboxes if you want the rule to apply on all profile types
- Give a name for the rule and finish.
- If you go back to IE , you'll observe that the connection has failed

Create a connection security rule

What is a Connection Security Rule and what are the different types?

- A Connection Security Rule is a type of firewall rule that is used to define security settings for network connections.
- Navigate to Windows Defender Firewall> Advanced settings>Connection Security Rules> Right Click inside the empty pane to create a new rule
  The different types are:
  - **Isolation:** Restrict connections based on credentials , often used to keep the internal network healthy. Eg: Domain membership, compliance policies, computer status or health.
  - **Public Connection Security Rule:** Defines security policies for connections to public networks, such as the internet, to enhance protection against threats.

- **Authentication Exemption:** A rule to state what connection types should be excluded from authentication. Eg: A single IP, Subnets,
- **Server-to-Server :** Secures communication between servers by enforcing encryption and authentication for data integrity.
- **Tunnel :** A rule to authenticate connections between two computers when data needs to pass through an intermediate and untrusted network
- **Custom :** Offers highly customizable security settings, allowing you to define specific security requirements based on your network's needs.

How do you create a Connection Security Rule?

- Let's create an Authentication Exemption rule that creates an exemption based on their IP addresses
- Navigate to Windows Defender Firewall> Advanced settings>Connection Security Rules >Authentication Exemption
- Click Add to add the IP address range
- Finish by clicking next
- Name the rule

Networking Troubleshooting Basics

Use ping to troubleshoot network connectivity

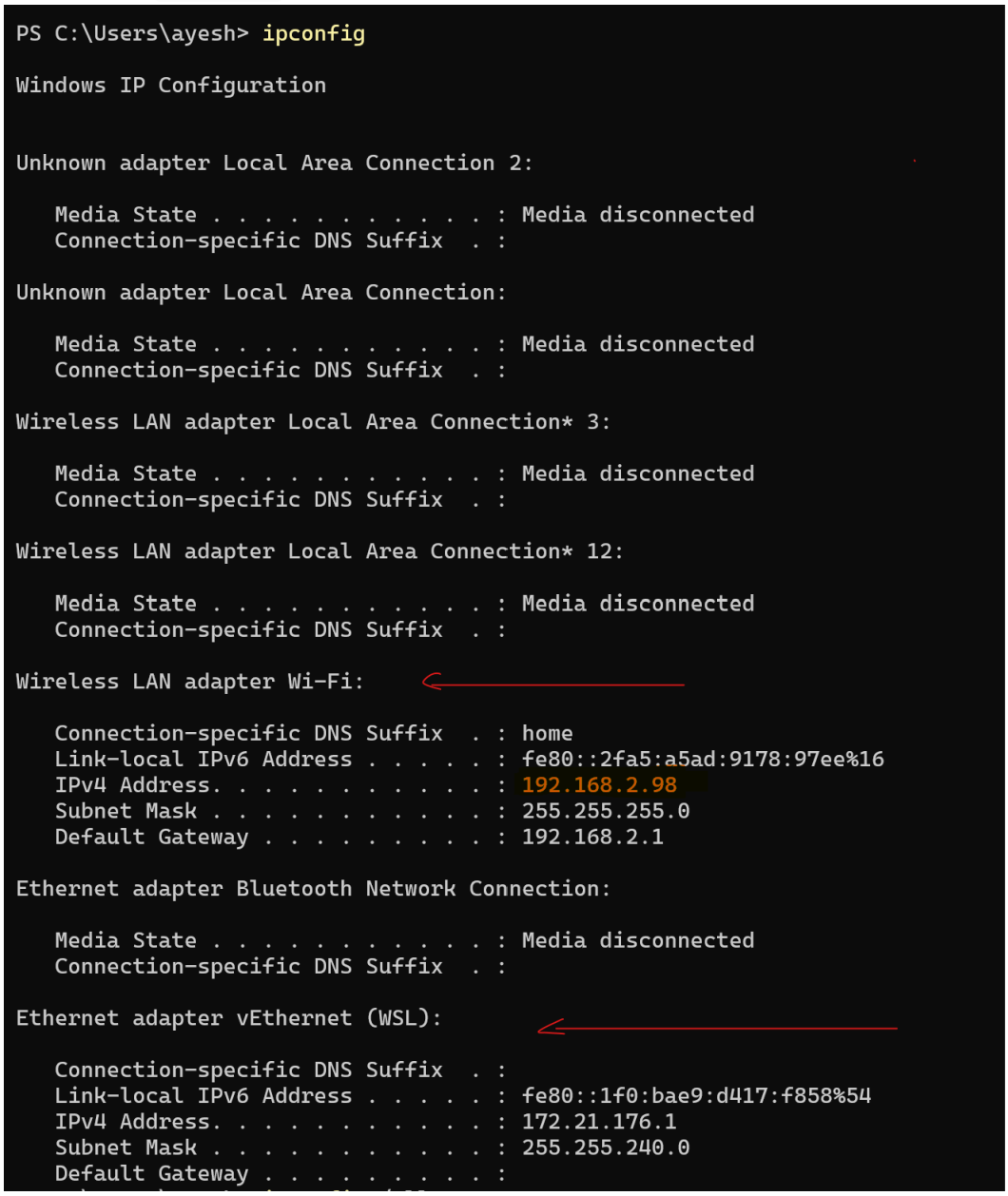
- The command line tool ping is used to troubleshoot connectivity , name resolution and reachability.
- You can run the ping command from command prompt or Windows Powershell
- First verify if your TCP/IP stack is working properly by typing> **ping 127.0.0.1**
- This is the loopback address validates that your network adapter is configured properly
- If you do not have a successful ping and get errors resolve by performing troubleshooting mentioned above
- You can also test it by typing> **test - connection 127.0.0.1***
- You can ping the host by typing> **ping** (IP address of the problematic remote host)
- If you get a ping timed out message then it may be due to the network congestion issue
- In the above case add a wait and now the command becomes> ping (IP address) -w 5000

Use ipconfig to troubleshoot network connectivity

What is `ipconfig`?

- The `ipconfig` command is used to display information about the network configuration and refresh DHCP and DNS Settings.
  When do you use ipconfig command?

- The `ipconfig` is used when we encounter problems with the computer's IP configuration or network connectivity.
  How to use the command?
- To use the `ipconfig` command we will need to open Command Prompt or PowerShell



What is the first step to perform when you have problems with your IP?

- The first step to do this is to release the current IP Address with the `Ipconfig /release` command . This means that we will inform the DHCP server that we don't want to use the assigned IP Address any longer.
- After you have released the IP Address you will need to request a new one from the DHCP Server. We can do this with the `Ipconfig /renew` command
- The changes apply only to the active adapter.
- You could ignore errors with multiple other adapters.
- This resolved most problems with conflicting IP addresses.

Can you release a static IP address? What needs to be done in this case?

- No, Static IP addresses cannot be released/renewed. IP addresses cannot be released from any disconnected media either.
- To troubleshoot enable the DHCP by going to the Network and Internet> Right Click on the Wi-Fi and choose properties > TCP/IPV4> properties> Choose Obtain an IP address automatically.
- To confirm you can type the command `Ipconfig /all` and observe that DHCP is enabled.

How do you troubleshoot when a network adapter isn't available ?

- First check if the network adapter is available by typing `ipconfig`.
- In this case the adapter is disabled and needs to be enabled.
- Navigate to Network connections from Network and Internet , right click and choose enabled.

Use `tracert` to troubleshoot network connectivity

When is `tracert` used?

- You use the `tracert` (short for "traceroute") command when you want to diagnose and analyze the path that network packets take from your computer to a destination host or server on the internet.
- This displays the routing and timing information between a host and a network destination.
- The command works by tracing the data as it passes from router to router and each one it passes through is referred to as a hop. By evaluating the hops, you can point out where the problem occurs.
- Not that you won't use `tracert` to resolve problems with routers that are out of your control, like those on the internet. If you know that one of the problematic routers is yours then you can go ahead and take the next steps to resolve.

Use `pathping` to troubleshoot network connectivity

When is `pathping` used?

- Combines functionality of `ping` and `tracert` with additional calculated information , such as packet loss at a given network hop.
- It helps you to find the location of a packet loss in a route between you and a host (server, router, website etc).
- Where a `ping` command can only test the network connection between the source (your computer) and the destination, `pathping` will test the connection to each hop between it. When you run a `pathping` , it will first trace the route to the destination and then performs a ping to each node in between it.

```
PS C:\Users\ayesh> pathping www.linkedin.com

Tracing route to l-0005.l-msedge.net [13.107.42.14]
over a maximum of 30 hops:
  0  host.docker.internal [192.168.2.98]
  1  mynetwork.home [192.168.2.1]
  2  otwaon1093w_coreloop.net.bell.ca [142.124.41.149]
  3     *        *        *
Computing statistics for 50 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           host.docker.internal [192.168.2.98]
                                 0/ 100 =  0%   |
  1    8ms     0/ 100 =  0%     0/ 100 =  0%  mynetwork.home [192.168.2.1]
                                 0/ 100 =  0%   |
  2    9ms     0/ 100 =  0%     0/ 100 =  0%  otwaon1093w_coreloop.net.bell.ca [142.124.41.149]

Trace complete.
```

- Depending on the number of hops between you and the destination it can take a couple of minutes before the results are calculated.
- First, the command will trace the router, showing your every node on the route. This alone is already really useful information, you can immediately see where the problem occurs