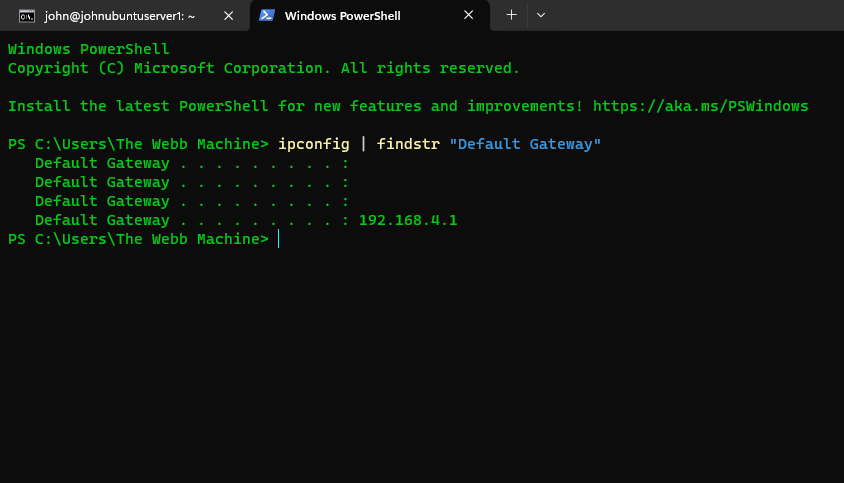
**Understanding Default Gateways and Routes**

* **Default Gateway:** Your default gateway is the IP address of the router on your network that handles traffic destined for addresses outside of your local network. Think of it as the door out of your house to the rest of the world. When your computer wants to send data to a device on the internet, it'll send it to the default gateway.
* **Default Route:** The default route tells your computer where to send all traffic when it doesn't have a more specific route. This usually points to your default gateway.

**How To Find Your Default Gateway and Default Route:**

**1. Windows**

* Open a Command Prompt (**Start** > type **cmd** > press **Enter**)
* Type the following commands and press Enter: **ipconfig | findstr “Default Gateway”**



**ipconfig (Windows)**

Purpose: The "ipconfig" command serves as a foundational tool in Windows network configuration. Its primary function is to provide detailed information about the TCP/IP network configuration of the system. This includes essential details such as IP addresses, subnet masks, and the default gateway.

Output: When executed without any additional parameters, "ipconfig" provides an extensive output, revealing comprehensive information about network adapters and their associated settings. This data is invaluable for understanding the current network setup of the system.

**| (The Pipe Symbol)**

Purpose: In the realm of command-line interfaces, the pipe symbol "|" holds significant importance. It serves as a mechanism for redirecting the output of one command to serve as the input for another command, enabling seamless data flow between different commands.

Function in this context: When used in conjunction with "ipconfig", the pipe symbol facilitates the transfer of the entire output generated by the "ipconfig" command and channels it into the input of another command, in this case, "findstr".

**findstr (Windows)**

Purpose: "findstr" stands as a powerful text search utility within the Windows command-line environment. It specializes in scanning lines of text to identify specific patterns or strings as specified by the user.

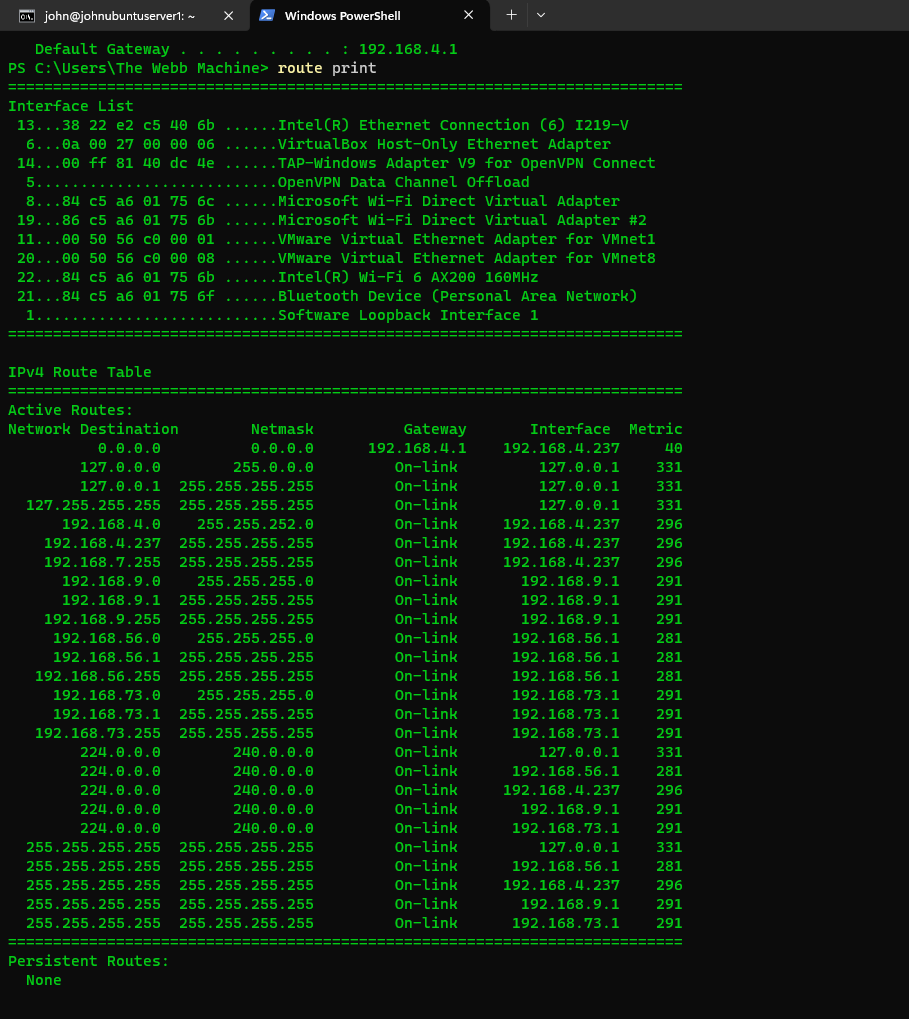
Function in this context: In the context of network analysis, "findstr" is employed to filter the output produced by "ipconfig". By searching for lines containing the text "Default Gateway", it effectively isolates and extracts the relevant information regarding the default gateway configuration from the extensive output of "ipconfig".

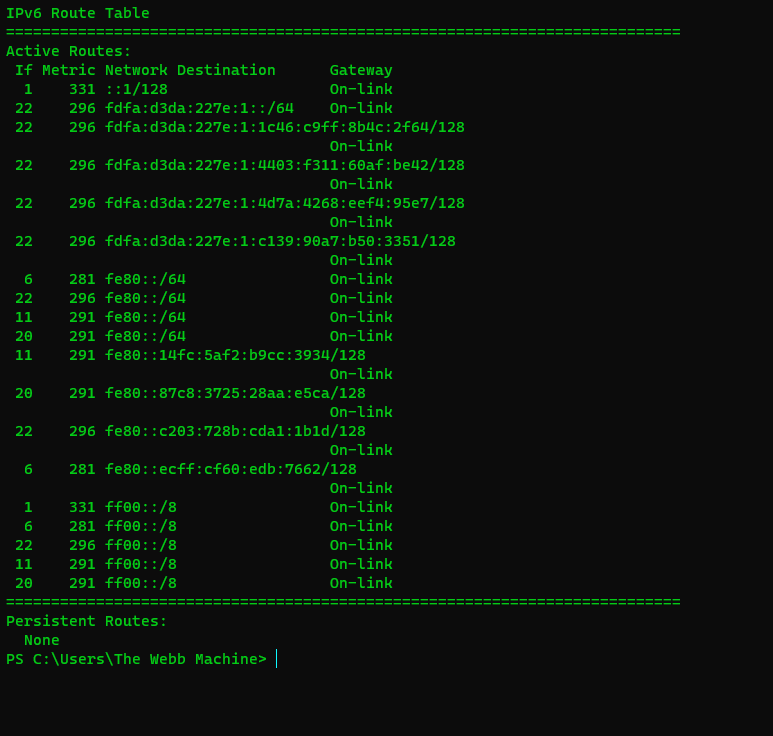
**Overall Effect**

The combination of "ipconfig | findstr "Default Gateway" acts as a precision tool in the arsenal of a cybersecurity analyst. By leveraging this command sequence, analysts can efficiently extract crucial network configuration details, such as the default gateway information, from the overwhelming amount of data provided by "ipconfig". This focused approach enhances visibility and facilitates rapid analysis, which is essential for identifying and addressing potential security vulnerabilities within network infrastructures.

2. Viewing Routing Details

To generate a comprehensive routing table, providing information on how network packets were forwarding discovering the default gateway I entered the following command : **route print**





The "**route print**" command is a network utility used to display the current routing table of your system. The routing table contains information about the paths your data packets can take to reach different networks.

3. **Interpreting and Analyzing**   
Here's a breakdown of the interface list data and IPv4 Route Table data provided in the first image of the route print results.

**Interface List**

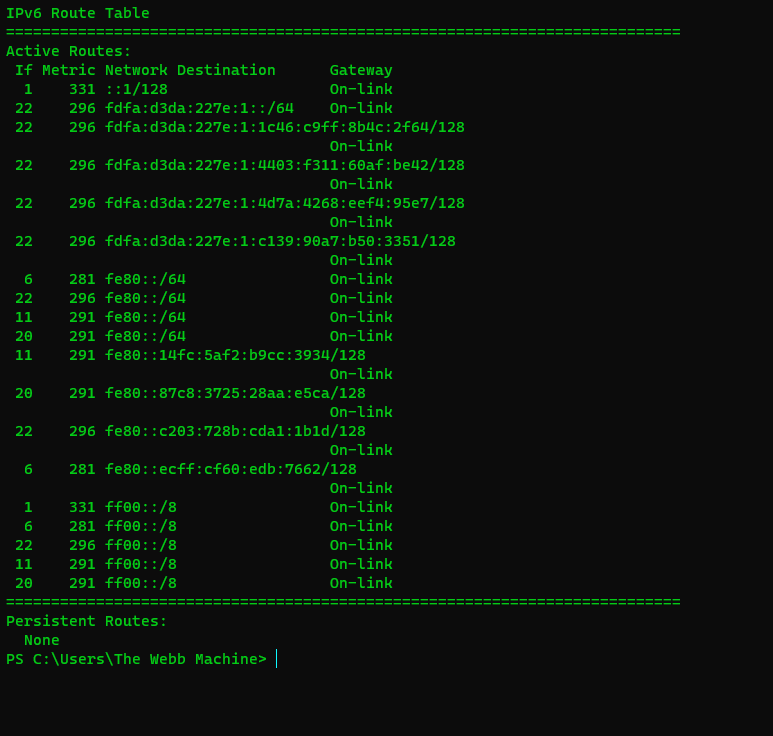
* **Interface List Header:** Indicates that this section provides information about your system's network interfaces.
* **Numbers (13, 6, 14, etc.):** Unique identifiers assigned to each network interface.
* **Physical Addresses (38 22 e2 c5 40 6b, etc.):** Also known as MAC addresses, these are hardware-level addresses that uniquely identify each network adapter.
* **Descriptions:**
  + **Intel(R) Ethernet Connection (6) I219-V:** Your primary wired Ethernet connection.
  + **VirtualBox Host-Only Ethernet Adapter:** A virtual network adapter used by VirtualBox for communication between virtual machines and the host system.
  + **TAP-Windows Adapter V9...:** A virtual network adapter used by VPN software like OpenVPN.
  + **Microsoft Wi-Fi Direct Virtual Adapters:** Virtual adapters that enable Wi-Fi Direct connections for screen mirroring and other features.
  + **VMware Virtual Ethernet Adapters...:** Virtual adapters used by VMware for communication between virtual machines and the host system.
  + **Intel(R) Wi-Fi 6 AX200 160MHZ:** Your wireless network card.
  + **Bluetooth Device (Personal Area Network):** Your Bluetooth adapter

**IPv4 Route Table**

* **Headers (Network Destination, Netmask, Gateway, Interface, Metric):** Define the columns of information in the routing table.
* **Active Routes Header:** Indicates that these are the network routes your system currently uses to send data.
* **List of Routes:** Each row represents a route, example:
  + **Network Destination:** 192.168.4.0
  + **Netmask:** 255.255.252.0
  + **Gateway:** On-link
  + **Interface:** 192.168.4.237
  + **Metric:** 296

**Interpretation:** This route means that any traffic destined for a device with an IP address in the range of 192.168.4.0 – 192.168.7.255 will be sent directly out of the network interface with IP address 192.168.4.237. "On-link" indicates that the destination network is directly connected to this interface.

* **0.0.0.0 / 0.0.0.0 Route:** This is the **default route**. Traffic for any destination not matched by a more specific route will be sent to the gateway configured here (192.168.4.1)



**Table Structure**

* **Headers:**
  + **Network Destination:** The IPv6 network address that the route applies to.
  + **Netmask:** This isn't shown explicitly, but all entries have a /128 netmask. This means each route is for a single IPv6 address.
  + **Gateway:** The next-hop router to send packets for that destination
  + **Interface:** The network interface used to send the packets.
  + **Metric:** The cost of the route. Lower metrics mean a route is preferred.

**Key Observations**

* **Predominantly Link-Local Routes:** Most addresses start with "fe80," indicating they're link-local addresses. These are valid only within your local network segment.
* **On-link Gateways:** Most entries have an "On-link" gateway. This means the destination address is directly reachable on the local network – no router is needed. Your computer would use neighbor discovery mechanisms (similar to ARP in IPv4) to find the target's MAC address.
* **Multiple Routes for Single Addresses:** You'll notice some addresses have multiple routes with different interfaces and metrics. This provides some redundancy in case one interface fails.