**Network Traffic Monitoring on Windows Platform**

Network Traffic monitoring is the method of studying the incoming and outgoing traffic on a computer network via specialized hardware and/or software.

The benefit of network traffic monitoring is the ability to track down network problems and use the information to guarantee bandwidth and quality of service for business applications.

At the Basic level in netwrork traffic monitoring we generally collect and view the upload & download statistics , but on advanced level many more details can be viewed.

There are multiple ways to monitor Network traffic on Windows starting from using bare method of windows command prompt without installing any additional 3rd party software , to advanced Open source network monitor tools available on line.

# Method 1 : Using Network shell (netsh) -

Network shell (netsh) is a command-line utility that allows you to configure and display the status of various network communications server roles and components after they are installed on computers running Windows Server.

Network traces that are collected using the netsh commands built in to Windows are of the extension "ETL".

netsh trace start persistent=yes capture=yes tracefile=filename

netsh trace stop

Refference : <https://learn.microsoft.com/en-us/windows-server/networking/technologies/netsh/netsh>

# Method 2 : Using Microsoft own tool “Network Monitor 3.4” -

# Microsoft Network Monitor 3.4, is a tool for capturing network traffic.

# Refference : <https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/collect-data-using-network-monitor>

# Download : <https://www.microsoft.com/en-in/download/details.aspx?id=4865>

# Method 3 : Using psutil module in Python to create Custom Netwrok monitor Tools -

# psutil (python system and process utilities) is a cross-platform library for retrieving information on running processes and system utilization (CPU, memory, disks, network, sensors) in Python. It is useful mainly for system monitoring, profiling, limiting process resources and the management of running processes.

Refference : <https://psutil.readthedocs.io/en/latest/index.html>

<https://thepythoncode.com/article/make-a-network-usage-monitor-in-python>

Above link has three python scripts for monitoring network traffic in following custom ways.

1. [Total Network Usage](https://thepythoncode.com/article/make-a-network-usage-monitor-in-python#total-network-usage)
2. [Network Usage per Network Interface](https://thepythoncode.com/article/make-a-network-usage-monitor-in-python#network-usage-per-nic)
3. [Network Usage per Process](https://thepythoncode.com/article/make-a-network-usage-monitor-in-python#network-usage-per-process)

# Method 4 : Using Advanced 3rd party applications “Wireshark” –

# Wireshark is a powerful network protocol analyzer that lets you capture and analyze network traffic in real time.

# And its FREE.

# Refference : <https://www.wireshark.org/docs/wsug_html_chunked/>