**IP Change Detection and System Shutdown**

This project provides a PowerShell script to monitor changes in the IP address of **physical Ethernet interfaces** and shut down the system if a change is detected. Ideal for enterprise environments to prevent users from connecting unauthorized networks (e.g., using a modem).

**Features**

* Disables Wi-Fi and virtual adapters (VMware, VirtualBox, Hyper-V, etc.)
* Only monitors **physical Ethernet interfaces**
* Ignores VPN or loopback interfaces
* Stores one IP snapshot per day
* Compares the current IP against the daily initial snapshot
* If changes are found → system shutdown
* VPN IP changes are **ignored**
* Compatible with Group Policy for centralized deployment

**Files**

* check\_ip\_change\_and\_shutdown.ps1: PowerShell script
* check\_ip\_and\_shutdown.bat: Batch file for running script via Task Scheduler
* README.md: Documentation

**Deployment Instructions**

**Step 1: Create Folder and Copy Files via Group Policy**

To deploy the script across your organization:

1. **Open Group Policy Management** (gpmc.msc)
2. Create or edit an existing GPO linked to your target OU.
3. Go to:

User Configuration / Preferences / Windows Settings / Files

1. Right-click → New → File
   * **Action:** Create
   * **Source file:** Path to your .ps1 or .bat file on a shared location
   * **Destination file:** C:\ProgramData\Check\_IP\check\_ip\_change\_and\_shutdown.ps1
2. Repeat for each script file (.ps1, .bat).

**Step 2: Set Folder Permissions (Optional)**

* Ensure that C:\ProgramData\Check\_IP\ is **readable and executable** by all users.

**Step 3: Configure Task Scheduler**

1. Create a scheduled task (with highest privileges) to run:
   * **Action:** Run program

Program: powershell.exe

Arguments: -File "C:\ProgramData\Check\_IP\check\_ip\_change\_and\_shutdown.ps1"

* + OR if PowerShell is blocked:

Program: C:\ProgramData\Check\_IP\check\_ip\_and\_shutdown.bat

1. **Trigger:** At user logon or periodic schedule (e.g., every 5 minutes)

**Notes**

* The script creates and stores IP snapshots in:

C:\ProgramData\IPMonitor\

* A new file is created daily and used as the baseline for that day.
* VPN connections are ignored by **interface type**, so even manually named VPNs are excluded.