Date – 22/09/2025 Configuring a Second Internet Service Provider (ISP) on your UDM Pro

You can enhance your network's reliability and performance by adding a second ISP to your UniFi Dream Machine Pro (UDM Pro). This can be configured for either failover (switching to the second ISP when the primary one fails) or load balancing (distributing traffic across both ISPs).

1. Adding a Second ISP and Configuring WAN2

To add a second ISP, you will utilize the secondary WAN port on your UDM Pro. This is typically the SFP+ port labeled "WAN 2".

Configuration Steps:

1. **Physical Connection:** Connect your second modem or internet source to the WAN 2 port on your UDM Pro.
2. **Access the UDM Pro Interface:** Log in to your UDM Pro's network controller.
3. **Navigate to Internet Settings:** Go to `Settings` > `Internet`.
4. **Select the Secondary WAN Port:** You will see your primary WAN connection. The second WAN port should also be listed. Click on it to configure it.
5. **Choose Your Connection Type:** You can configure your WAN2 connection in one of the following ways, depending on the service provided by your ISP:
    - **DHCP:** If your ISP automatically assigns an IP address, select "DHCP". This is the most common setup for residential and small business connections.
    - **PPPoE (Point-to-Point Protocol over Ethernet):** If your ISP requires a username and password to connect (common for DSL), select "PPPoE" and enter the credentials they provided.
    - **Static IP:** If your ISP has assigned you a fixed IP address, select "Static IP". You will need to enter the IP address, subnet mask, gateway, and DNS server information provided by your ISP.

2. Setting Up Failover or Load Balancing

Once your second ISP is configured, you can choose how the UDM Pro utilizes both connections.

- **Failover:** This is the default and most straightforward setup. If your primary internet connection goes down, the UDM Pro will automatically switch all traffic to the secondary WAN connection. When the primary connection is restored, it will switch back.
- **Load Balancing:** The UDM Pro also supports load balancing, which allows you to use both internet connections simultaneously. This feature, sometimes referred to as "Distributed" mode, lets you balance the traffic between the two WAN ports based on a specified ratio. For instance, you could set a 50/50 split or another ratio depending on the speeds of your two

connections. Keep in mind that load balancing functionality and its specific implementation might vary with different firmware versions of the UDM Pro.

To configure Failover or Load Balancing:

1. In the `Settings` > `Internet` section, you will find the option to configure how the dual WAN setup behaves.
2. You can select "Failover" to ensure uninterrupted internet access or choose "Distributed" for load balancing.

3. Configuring a Static IP in UDM Pro

If your ISP provides a static IP address, you will need to configure it manually in the WAN settings.

Steps for Static IP Configuration:

1. Navigate to `Settings` > `Internet` and select the appropriate WAN port.
2. In the IPv4 Connection settings, choose "Static IP".
3. Enter the following information provided by your ISP:
    - **IP Address:** Your unique static IP address.
    - **Subnet Mask:** Defines the range of your network.
    - **Gateway:** The IP address of your ISP's router.
    - **DNS Servers:** The IP addresses of the DNS servers you wish to use (you can use your ISP's DNS or a public one like Google's 8.8.8.8).
4. Apply the changes to save your configuration.

4. Finding Your Static IP Address

If you have a static IP address from your ISP, they will typically provide this information to you directly.

- **Check your welcome email or documentation:** Your ISP usually includes your static IP details in the initial setup information.
- **Contact your ISP's support:** They can provide you with your static IP address and other necessary configuration details.
- **Log in to your ISP's customer portal:** Some ISPs provide this information in the account management section of their website.
- **Check your router's WAN settings:** If you have an existing router from your ISP, you can often find the static IP information in its web interface, usually under a "WAN" or "Internet" status page.

Securing Your Laptop at the Hardware Level

1. How to Set a BIOS/UEFI Password

Setting a BIOS or UEFI (the modern equivalent of BIOS) password provides a fundamental layer of security for your laptop, preventing unauthorized access to the system's core settings and even booting into the operating system.

General Steps to Set a BIOS/UEFI Password:

1. **Enter the BIOS/UEFI Setup:**
    - Restart your laptop.
    - As it boots up, press the designated key to enter the BIOS/UEFI setup. Common keys include `F1`, `F2`, `F10`, `Delete`, or `Esc`. The correct key is usually displayed on the screen during startup.
2. **Navigate to the Security Section:** Use the arrow keys to find a "Security" or "Password" tab in the BIOS/UEFI menu.
3. **Set the Administrator/Supervisor Password:**
    - Look for an option like "Set Supervisor Password" or "Set Administrator Password." An administrator password allows full access to all BIOS/UEFI settings.
    - Enter a strong password and confirm it.
4. **Set the User Password (Optional):**
    - You may also have the option to set a "User Password" or "Power-on Password." This password will be required every time the laptop is turned on.
5. **Save and Exit:**
    - Navigate to the "Exit" tab and select "Exit Saving Changes" or a similar option. You can often press the `F10` key to save and exit.

Important Note: The exact steps can vary between laptop manufacturers and models. Refer to your laptop's manual or the manufacturer's website for specific instructions.

2. How an Administrator Sets the Password

The process for an administrator to set the BIOS password is the same as described above. The key distinction is the type of password being set:

- **Supervisor/Administrator Password:** This is the master password for the BIOS/UEFI. It allows the administrator to change any setting within the BIOS/UEFI.
- **User Password:** This password only allows the user to boot the computer but restricts access to most BIOS/UEFI settings. An administrator with the supervisor password can change or remove the user password.

Controlling Website Access

How to Block Websites Using the Hosts File

The hosts file is a plain text file in an operating system that maps hostnames to IP addresses. By editing this file, you can redirect a website's domain name to a non-existent or loopback IP address, effectively blocking access to it from your computer.

Windows:

1. **Open Notepad as Administrator:**
    - Search for "Notepad" in the Start Menu, right-click on it, and select "Run as administrator."
2. **Open the Hosts File:**
    - In Notepad, go to `File` > Open.
    - Navigate to `C:\Windows\System32\drivers\etc`.
    - Change the file type from "Text Documents (*.txt)" to "All Files (*.*)".
    - Select the "hosts" file and click "Open."
3. **Block a Website:**
    - At the end of the file, add a new line.
    - Type `127.0.0.1`, press the `Tab` key, and then type the website address you want to block (e.g., `www.example.com`).
    - For comprehensive blocking, you might want to add entries for both the `www` and non-`www` versions (e.g., `127.0.0.1 example.com`).
4. **Save the File:** Go to `File` > `Save`.

macOS and Linux:

1. **Open the Terminal:**
    - On macOS, you can find the Terminal in `Applications` > `Utilities`.
    - On Linux, it's usually in your applications menu or can be opened with a keyboard shortcut like `Ctrl+Alt+T`.
2. **Open the Hosts File:**
    - Type the following command and press Enter: `sudo nano /etc/hosts`
    - Enter your administrator password when prompted.
3. **Block a Website:**
    - Use the arrow keys to move to the end of the file and add a new line.
    - Type `127.0.0.1`, press the `Tab` key, and then the website address (e.g., `www.example.com`).
4. **Save the File:**
    - Press `Ctrl+O` to write the changes, and then `Ctrl+X` to exit the editor.

Detailed Guide to Using BitLocker

BitLocker is a full-volume encryption feature included in certain versions of Windows that helps protect your data from unauthorized access if your device is lost or stolen.

1. What is BitLocker and System Requirements

BitLocker encrypts entire drives, making the data unreadable without the correct password, PIN, or recovery key.

System Requirements:

- **Windows Version:** BitLocker is available on Windows Pro, Enterprise, and Education editions. It is not available on Windows Home editions.
- **Trusted Platform Module (TPM):** For the highest level of security, your computer should have a TPM chip (version 1.2 or later). The TPM is a microchip that provides hardware-based security functions. Most modern laptops have one. If you don't have a TPM, you can still use BitLocker with a startup key on a USB drive or a password, but this requires a change in Group Policy settings.
- **BIOS/UEFI:** The computer's BIOS or UEFI must be compatible with the TPM.

2. How to Turn on BitLocker for Your Operating System Drive

1. **Open BitLocker Management:**
    - Click the Start button, type "Manage BitLocker," and press Enter.
2. **Turn on BitLocker:**
    - In the BitLocker Drive Encryption control panel, you will see your drives listed. For your operating system drive (usually C:), click "Turn on BitLocker."
3. **Choose How to Unlock Your Drive at Startup:**
    - If you have a TPM, you'll be prompted to choose an unlock method. You can typically choose to have the drive unlock automatically at startup or require a PIN or a startup key (a file on a USB drive) for added security.
4. **Back Up Your Recovery Key:** This is a crucial step. The recovery key is a 48-digit number that allows you to access your encrypted drive if you forget your password or PIN, or if BitLocker detects a security risk. You will be given options to:
    - Save it to your Microsoft account.
    - Save it to a file (on a separate, unencrypted drive or USB).
    - Print the recovery key.

      It is highly recommended to save your recovery key in a safe place that is separate from the encrypted computer.
5. **Choose How Much of Your Drive to Encrypt:**
    - **Encrypt used disk space only:** This is faster and ideal for new PCs.

- **Encrypt entire drive:** This is more secure for PCs that have been in use, as it encrypts all data, including deleted files that might still be recoverable.

6. **Choose Encryption Mode:**
    - **New encryption mode (XTS-AES):** Best for fixed drives on the same computer.
    - **Compatible mode (AES-CBC):** Better for removable drives that you might use on older versions of Windows.
7. **Run BitLocker System Check:** It's recommended to check the box to run a system check to ensure everything is working correctly before encryption begins.
8. **Restart and Encrypt:** Your computer will restart, and the encryption process will begin. This can take some time, depending on the size of your drive, but you can continue to use your computer while it's in progress.

3. How to Enable BitLocker for Fixed and Removable Data Drives (BitLocker To Go)

The process for encrypting other internal hard drives or external drives (like USB flash drives) is similar to encrypting the OS drive, but it's called **BitLocker To Go** for removable drives.

1. **Connect the Drive:** Plug in the USB drive or ensure the internal drive is recognized by Windows.
2. **Open BitLocker Management:** Go to the "Manage BitLocker" control panel.
3. **Turn on BitLocker:** Find the drive you want to encrypt under "Fixed data drives" or "Removable data drives - BitLocker To Go" and click "Turn on BitLocker."
4. **Choose How to Unlock the Drive:**
    - You will be prompted to set a password to unlock the drive each time you connect it. You can also use a smart card.
5. **Back Up Your Recovery Key:** As with the OS drive, you must back up your recovery key.
6. **Encrypt the Drive:** Choose your encryption options and start the encryption process.

4. Managing BitLocker

In the "Manage BitLocker" control panel for an encrypted drive, you have several options:

- **Back up your recovery key:** If you lose your initial backup, you can create a new one.
- **Change password/PIN:** You can update your unlock credentials.
- **Remove password:** You can remove the password requirement for unlocking a drive.
- **Turn off BitLocker:** This will decrypt the drive. This process can take a significant amount of time.
- **Suspend protection:** You can temporarily suspend BitLocker protection if you need to make system changes like updating the BIOS.

5. Checking BitLocker Status and Recovering an Encrypted Drive

To check the status:

- **Control Panel:** The "Manage BitLocker" window will show the encryption status of each drive (e.g., "BitLocker on," "BitLocker encrypting," "BitLocker off").
- **File Explorer:** An encrypted and locked drive will have a gray lock icon. An unlocked drive will have a gold unlocked icon.
- **Command Prompt:** You can use the command `manage-bde -status` in an administrative Command Prompt to get detailed status information.