Date – 23/09/2025 Comprehensive Guide to Advanced Laptop and Network Configuration

Section 1: How to Set Up a Second Router or Network in UDM Pro

The Ubiquiti UniFi Dream Machine Pro (UDM Pro) is a powerful, all-in-one networking device. One of its key features is the ability to create multiple, distinct networks, effectively acting as a "router-on-a-stick." This is useful for segmenting traffic for security and performance reasons, such as creating a separate network for guests, IoT devices, or a home office. This guide will walk you through creating a new network (LAN) and assigning it to a specific port, to which you could connect a secondary switch or router (in access point mode).

Prerequisites:

- A fully set up and operational UDM Pro.
- Access to the UniFi Network Controller (via `unifi.ui.com` or the local IP address).
- An Ethernet cable.
- A secondary device to connect (e.g., a switch, another Wi-Fi router configured in AP mode).

Step-by-Step Instructions:

Step 1: Access Your UDM Pro Dashboard

1. Open a web browser and navigate to your UDM Pro's dashboard.
2. Log in with your Ubiquiti account credentials or your local admin credentials.

Step 2: Create a New Virtual Network (LAN)

1. Once logged in, navigate to the **Settings** section (usually a gear icon).
2. In the Settings menu, select **Networks**.
3. Click on **Add New Network** or "Create New Network".
4. **Name your network:** Give it a descriptive name, such as "IoT Network," "Guest LAN," or "OfficeNet."
5. **Configure the Gateway IP/Subnet:** This is the core of your new network. You need to define an IP address range that does not overlap with your existing primary network.
    - For example, if your main network is `192.168.1.1/24`, you could set this new network to `192.168.2.1/24`. This makes the UDM Pro's address on this network `192.168.2.1` and allows for IP addresses from `192.168.2.2` to `192.168.2.254`.
6. **Advanced Configuration:** You can expand the "Advanced" or "Manual" settings to configure more options.
    - **Network Type:** Ensure it is set to "Standard" or "Corporate".
    - **VLAN ID:** Assign a unique VLAN ID to this network (e.g., 2, 10, 20). This tags all traffic from this network, allowing switches and access points to differentiate it. Let's use VLAN 20 for this example.

    - **DHCP Server:** Ensure the DHCP Server is enabled. This will automatically assign IP addresses to devices that connect to this new network. You can adjust the DHCP range if needed.
7. Click **Add Network** or "Save" to create the new virtual network.

Step 3: Assign the New Network to a Physical Port
Now you must tell the UDM Pro which of its physical switch ports should belong to this new network.

1. Navigate to the **UniFi Devices** section (an icon of a UDM Pro) and click on your UDM Pro in the list.
2. A properties panel will slide out. Select the **Ports** tab.
3. You will see a visual representation of the UDM Pro's front panel. Click on the port you want to use for your second network (e.g., Port 3).
4. In the port's configuration menu, find the **Port Profile** or "Native VLAN/Network" setting.
5. By default, it is likely set to your primary LAN. Click the dropdown menu and select the new network you just created (e.g., "IoT Network").
6. Click **Apply Changes**. The port will now exclusively handle traffic for your new network.

Step 4: Connect Your Secondary Device

1. Take an Ethernet cable and plug one end into the port you just configured on the UDM Pro (e.g., Port 3).
2. Plug the other end into the WAN/Internet port of your second router (if using it as an access point) or the uplink port of a switch.
    - **Important:** If you are using a secondary consumer router, you must configure it to operate in "Access Point (AP) Mode" or "Bridge Mode." This disables its own routing and DHCP functions, preventing conflicts with the UDM Pro, which is now managing the network.
3. Any device that now connects to this secondary switch or AP-mode router will be part of the isolated network you created, receiving an IP address from the `192.168.2.x` range.

Step 5 (Optional): Create Firewall Rules
For true network segmentation, you need to create firewall rules to control traffic between your new network and your primary network.

1. Navigate to **Settings > Security > Firewall Rules**.
2. You can create rules to block the new network from accessing your main network. For example, create a "LAN In" rule with the action "Drop," source as your new network's IP range, and destination as your main network's IP range.

By following these steps, you have successfully used the powerful features of the UDM Pro to create and isolate a second network, enhancing your network's security and organization.

Page 2: Securing Your Laptop at the Hardware Level

Section 2: How to Set a BIOS/UEFI Password on a Laptop

A BIOS (Basic Input/Output System) or UEFI (Unified Extensible Firmware Interface) password is a critical layer of security that functions before your operating system (like Windows or macOS) even starts to load. Setting this password can prevent unauthorized users from changing boot settings, booting from an external device (like a USB drive to bypass the OS login), or altering critical hardware settings.

Types of BIOS/UEFI Passwords:

- **Supervisor/Administrator Password:** This is the master password. It grants full access to all BIOS/UEFI settings. If this is set, no changes can be made without it.
- **User/System Password:** This password is required to boot the computer itself. The system will halt and ask for this password immediately upon startup. It provides a lower level of access to the BIOS settings than the supervisor password.

General Procedure (Applicable to Most Brands):

Step 1: Enter the BIOS/UEFI Setup Utility

1. **Shut down your laptop completely.** A restart is not always sufficient.
2. **Power on your laptop** and immediately start pressing the designated key to enter the setup utility. This key must be pressed within the first few seconds of startup. Common keys include:
    - **Dell:** F2 or F12
    - **HP:** Esc or F10
    - **Lenovo:** F1, F2, or the dedicated "Novo" button
    - **ASUS:** F2 or Del
    - **Acer:** F2 or Del
    - **Microsoft Surface:** Press and hold the Volume-Up button, then press and release the Power button.
3. You will know you are successful when you see a text-based or graphical interface that looks very different from your normal operating system.

Step 2: Navigate to the Security Section

1. The BIOS/UEFI interface is typically navigated with the arrow keys, with Enter to select and Esc to go back. Some modern UEFI interfaces support mouse input.
2. Look for a tab or menu item labeled **Security**. Use the arrow keys to navigate to it.

Step 3: Set the Desired Password(s)

1. Inside the Security tab, you will find options like:
   - `Set Supervisor Password`
   - `Set Administrator Password`
   - `Set User Password`
   - `Password on Boot`
2. **To set the Administrator/Supervisor Password:**
   - Select the `Set Supervisor Password` option and press Enter.
   - A dialog box will appear asking you to `Enter New Password`. Type your chosen password carefully. Note that you may not see characters as you type.
   - Press Enter.
   - You will be asked to `Confirm New Password`. Re-type the exact same password and press Enter.
   - A confirmation message will usually appear stating the password has been set.
3. **To set the User Password (for boot-up):**
   - Follow the same procedure as above, but select the `Set User Password` option.
   - After setting a User Password, you might need to enable the `Password on Boot` or a similar option to ensure the laptop asks for it every time it starts.

Step 4: Save Changes and Exit

1. This is a critical step. Your changes will be lost if you do not save them properly.
2. Navigate to the **Exit** tab.
3. Select the option that says **Exit Saving Changes** or **Save Changes and Reset**. A common hotkey for this is **F10**.
4. A confirmation dialog will appear. Select **Yes** or **[Y]** and press Enter.
5. Your laptop will now restart.

Step 5: Test the Password

- If you set a User or Power-On password, the laptop should immediately halt on the next boot and prompt you for it.
- To test the Supervisor password, restart the laptop again, re-enter the BIOS/UEFI setup, and try to access a setting. It should now prompt for the password before allowing any changes.

CRITICAL WARNING:
If you forget your BIOS/UEFI password, it is extremely difficult to reset. Unlike an operating system password, there is no simple "Forgot Password" link. Resetting it may involve physically opening the laptop to disconnect the CMOS battery or shorting motherboard jumpers, and on many modern

laptops, it may require professional service from the manufacturer. **Store your BIOS password in a secure location.**

Page 3: Integrating Your Laptop with Cloud-Based Identity

Section 3: How to Set Up (Join) Microsoft Entra ID on a Laptop

Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) is Microsoft's cloud-based identity and access management service. Joining your laptop to Entra ID allows you to sign in to your device using your work or school account (e.g., your Microsoft 365 credentials). This provides seamless single sign-on (SSO) to cloud apps and allows your organization to manage the device and apply security policies.

Prerequisites:

- **Windows Edition:** You must be running Windows 10/11 Pro, Enterprise, or Education. Windows Home editions do not support Entra ID Join.
- **Permissions:** You must have the necessary permissions within your organization's Entra ID tenant to join devices.
- **Internet Connection:** An active internet connection is required during the setup process.
- **Your Entra ID Credentials:** You will need your work or school email address and password.

Step-by-Step Instructions:

Method 1: During the Initial Windows Setup (Out-of-Box Experience - OOBE)
This is the recommended method for new devices.

1. Proceed through the initial Windows setup screens (selecting region, keyboard layout, etc.).
2. When you reach the screen that asks, "How would you like to set up this device?", select **Set up for work or school**.
3. On the "Let's set things up for your work or school" screen, enter your work or school email address (your Entra ID credential).
4. You will be redirected to your organization's sign-in page. Enter your password. You may also be required to complete a multi-factor authentication (MFA) prompt (e.g., via the Microsoft Authenticator app).
5. After successful authentication, Windows will continue the setup process, registering the device with Entra ID and applying any policies from your organization (via a service like Microsoft Intune).
6. Once setup is complete, you will be at the Windows desktop, and your device will be fully joined to Entra ID.

Method 2: On an Already-Configured Windows Laptop
If your laptop is already set up with a local account, you can join it to Entra ID through the Settings app.

1. Open the **Settings** app (Windows key + I).
2. Go to **Accounts**.
3. In the left-hand menu, select **Access work or school**.
4. At the top of this screen, click the **Connect** button.
5. A new window will pop up. At the bottom of this window, click the link that says **Join this device to Azure Active Directory** (this text may vary slightly but will reference Azure AD or Entra ID).
6. You will be prompted to enter your work or school email address. Enter it and click **Next**.
7. You will be taken to your organization's sign-in page. Enter your password and complete any MFA requirements.
8. You may see a screen confirming you are connecting to the correct organization. Click **Join**.
9. After a few moments, you will see a confirmation screen saying, "You're all set!". Click **Done**.
10. **Restart your laptop.** This is a crucial step.
11. After restarting, on the Windows login screen, click **Other user** in the bottom-left corner.
12. You can now sign in using your work or school email address and password. Your Entra ID account will be created as a new user profile on the laptop.

How to Verify the Entra ID Join Status

You can confirm that your device is successfully joined.

1. **Via Settings:** Go back to **Settings > Accounts > Access work or school**. You should now see a connection listed that says "Connected to [Your Organization's Name] Azure AD."
2. **Via Command Prompt:**
   - Open Command Prompt as an administrator.
   - Type the command `dsregcmd /status` and press Enter.
   - Look for the `AzureAdJoined` parameter in the "Device State" section. It should say **YES**.

By joining your device to Entra ID, you have integrated it into your organization's security and management ecosystem, streamlining access and enhancing compliance.

Page 4: Managing User Access on Your Laptop

Section 4: How to Create a New User Account on a Laptop

Creating separate user accounts is a fundamental aspect of computer security and organization. It allows multiple people to use the same device while keeping their files, settings, and applications separate. It is also a best practice for security, as daily tasks should be performed on a "Standard User" account rather than an "Administrator" account to limit potential damage from malware.

This guide covers creating a local user account on both Windows and macOS. A local account is one that exists only on that specific device and is not tied to a Microsoft or Apple cloud account.

Part A: Creating a New Local User in Windows 11

Method 1: Using the Settings App (For users without a Microsoft account)

1. Open the **Settings** app (Windows key + I).
2. Navigate to the **Accounts** section.
3. Select **Family & other users**.
4. In the "Other users" section, click the **Add account** button.
5. A Microsoft sign-in window will appear. **Do not enter an email address.** Instead, click the link that says **I don't have this person's sign-in information**.
6. On the next screen, click the link that says **Add a user without a Microsoft account**.
7. Now you can create the local account:
   - **Who's going to use this PC?:** Enter a username for the new account (e.g., "Guest," "John").
   - **Make it secure:** Enter a password for the account, then enter it again to confirm.
   - **In case you forget your password:** You will be required to set up three security questions. Choose a question from each dropdown menu and provide an answer.
8. Click **Next**. The new local account will now appear under "Other users."

Step 1.1: Change the Account Type (Optional)

By default, new accounts are created as **Standard Users**, which is recommended for security. If you need this user to have administrative privileges (to install software and change system settings), you must change their account type.

1. Back in the **Family & other users** settings page, click on the new account you just created.
2. Click the **Change account type** button.
3. In the dropdown menu, change the selection from "Standard User" to **Administrator**.
4. Click **OK**.

Method 2: Using the `netplwiz` Command

This is a more traditional and direct method.

1. Press **Windows key + R** to open the Run dialog box.
2. Type `netplwiz` and press Enter.
3. The "User Accounts" window will open. Click the **Add...** button.

4. At the bottom of the new window, click the link **Sign in without a Microsoft account (not recommended)**.
5. On the next screen, click the **Local account** button.
6. Enter a username, password, and a password hint. Click **Next**.
7. Click **Finish**. The user is now created. To make them an administrator, select the new user in the `netplwiz` window, click **Properties > Group Membership**, and select **Administrator**.

Page 5: Managing User Access (macOS) and Finalizing Your Setup

Part B: Creating a New User in macOS

1. Click the **Apple menu** in the top-left corner of the screen.
2. Select **System Settings** (on newer macOS versions) or **System Preferences** (on older versions).
3. In the System Settings window, scroll down and click on **Users & Groups**.
4. Click the **Add Account...** or **Add User...** button.
    - You will be prompted to enter your current user's password to unlock the ability to make changes. This is a security measure.
5. A new sheet will appear where you can configure the new account.
    - **New Account:** Choose the type of account you want to create from the dropdown menu:
        - **Administrator:** Can add and manage other users, install apps, and change system-wide settings.
        - **Standard:** Can install apps and change their own settings, but cannot change system settings or other users' information. This is the safest option for most users.
        - **Sharing Only:** Can only access shared files remotely, cannot log in to the computer locally.
    - **Full Name:** Enter the user's full name (e.g., "Jane Doe").
    - **Account Name:** macOS will automatically suggest a short account name (e.g., "janedoe"). You can change this, but it must be all lowercase and have no spaces. This will be the name of their home folder.
    - **Password:** Enter a password for the new user.
    - **Verify:** Re-enter the password to confirm it.
    - **Password Hint:** Add an optional hint to help the user remember their password if they forget it.
6. Click the **Create User** button.
7. The new user will now appear in the list on the left. They can now log in by choosing their name from the login screen or via the Fast User Switching menu in the menu bar.