UDM Pro Network Configuration & Expansion

1. How to connect two routers to UDM Pro and enable bridge mode

This is a common point of confusion. You do not connect two *routers* to the UDM Pro for internet; you connect two **modems**. The goal is to have the UDM Pro be the single, authoritative router for your entire network. To achieve this, the devices from your Internet Service Provider (ISP), like Hathway, must be configured to stop acting as routers.

This is done by enabling **Bridge Mode**.

The Process:

- **Step 1: Enable Bridge Mode on ISP Devices:** Before anything else, you must log into the admin panels of both of your Hathway routers and find the setting for "Bridge Mode," "IP Passthrough," or "Modem Mode." Enabling this turns off their routing, firewall, and DHCP functions, making them simple modems that pass the internet connection directly through. If you cannot find this setting, you must call Hathway support and ask them to do it for you remotely.
- **Step 2: Connect to UDM Pro WAN Ports:** The UDM Pro has two internet ports (WAN ports).
    - Connect the first Hathway modem to **WAN1** (the standard RJ45 Ethernet port, usually Port 9).
    - Connect the second Hathway modem to **WAN2** (the SFP+ port, usually Port 10). To do this, you will need an **SFP+ to RJ45 Adapter** (e.g., the Ubiquiti U-ACC-CM-RJ45-1G), which allows a standard Ethernet cable to plug into the SFP+ port.

2. How to set up load balancing with two routers in UDM Pro

Once you have two active internet connections plugged into the WAN1 and WAN2 ports, you can configure the UDM Pro to share the network traffic across both. This is called Load Balancing. It increases your total internet capacity but does not combine the speeds for a single download.

The Process:

- **Step 1: Navigate to Internet Settings:** In your UniFi Network Controller, go to **Settings > Internet**.
- **Step 2: Configure the Secondary WAN Port:** You should see both WAN ports listed. Select your secondary port (WAN2).
- **Step 3: Enable Load Balancing:** In the settings for WAN2, you will find the **Load Balancing** configuration.
    - Choose the **Distributed** option. This tells the UDM Pro to actively use both connections at the same time.

    - Set the distribution ratio. For two identical 300 Mbps connections, you would set this to **50%**, ensuring traffic is split evenly between them.
    - The "Failover" option is different; it only uses the second connection if the first one fails. For increasing capacity, you must use "Distributed."
- **Step 4: Apply Changes:** The UDM Pro will provision and begin balancing the traffic from your employees across both internet lines.

3. How to extend Wi-Fi using two old routers with the same SSID

This is the correct way to expand your Wi-Fi coverage using non-UniFi hardware. The principle is the same as above: the UDM Pro is the only router. Your old routers must be converted into simple Wi-Fi Access Points.

The Process:

- **Step 1: Isolate and Configure:** Disconnect the old router from everything except power. Connect a laptop directly to one of its LAN ports.
- **Step 2: Enable Access Point (AP) Mode:** Log into the old router's admin panel. Find the **Operation Mode** setting and change it from "Router" to **"Access Point Mode"** (or AP Mode). This turns off its routing and DHCP functions.
- **Step 3: Configure Wi-Fi:** In the wireless settings, set the **SSID (Network Name)** and **Password** to be *exactly the same* as your main UniFi network.
- **Step 4: Set a Different Channel:** To prevent interference, manually set the 5 GHz Wi-Fi channel to be different from your other UniFi APs. If one AP is on channel 36, set this one to 48.
- **Step 5: Connect to the UDM Pro:** Run an Ethernet cable from a **LAN port** on your UDM Pro to a **LAN port** on the old router. **Do not use the WAN/Internet port** on the old router. Repeat this process for the second old router, ensuring it also uses a unique Wi-Fi channel.

Page 2: Windows, Microsoft Accounts & UniFi Settings

This section addresses issues related to connecting a Windows device to a corporate environment and explains specific UniFi features.

4. Why Entra ID does not appear when adding a work/school account

The primary reason is the **version of Windows** you are using.

- **Windows Home Editions:** These versions are designed for consumers and lack the necessary networking and security components for full corporate integration. When you go to "Access work or school," you get a simplified dialog box that only allows you to add an account for accessing apps like Office 365 and OneDrive.

- **Windows Pro/Enterprise/Education Editions:** These versions include the full feature set. The "Access work or school" dialog box shows **Alternate actions**, including **"Join this device to Microsoft Entra ID"** and "Join this device to a local Active Directory domain."

Therefore, if you are running Windows 11 Home, the option to join Entra ID will not appear because the operating system does not support it.

5. Why device management could not be enabled with Microsoft Basic account

The term "Microsoft Basic account" typically refers to a personal Microsoft account (e.g., @outlook.com, @gmail.com, @hotmail.com). **Device Management (MDM - Mobile Device Management)** is a feature for **organizations** to manage security policies on devices that access their data.

A personal account has no "organization" behind it. There are no policies to apply and no management server (like Microsoft Intune) to enroll with. The feature is fundamentally incompatible with a personal account, as there is no entity to perform the management.

6. & 7. Why a basic account cannot connect a work ID / Why company Microsoft ID cannot be added to laptop login

These are two sides of the same issue, and the reason is almost always **Organizational Security Policy**. Your company's IT department uses a service like Microsoft Intune to set strict rules about what kinds of devices can connect to their network. The error "Device management could not be enabled" is a direct result of one of these policies blocking your device.

Common blocking policies include:

- **Device Platform Restrictions:** The most common reason. The policy is configured to **only allow Windows Pro or Enterprise editions** to enroll. Your Windows Home laptop is identified and automatically blocked.
- **Enrollment Restrictions:** The policy may be set to block all personally owned devices, only allowing corporate-owned hardware to join.
- **Device Limit:** Your user account may have already reached the maximum number of devices it is allowed to register (e.g., 5 devices).
- **Conditional Access Policies:** These are advanced rules that might require a device to be "compliant" (e.g., have BitLocker encryption enabled, which is a Pro feature) before it is allowed to connect.

The solution is not something you can fix. You must **contact your IT administrator**, as only they can check the Intune logs and tell you which policy is blocking your device. The most common resolution is for you to **upgrade your PC from Windows Home to Pro**.

8. What is “Load Configuration” in UniFi device settings

"Load Configuration" is a time-saving utility in the UniFi Controller. It allows you to **copy the entire configuration from one UniFi device and apply it to another identical device.**

For example, if you have two U6-LR access points and you have perfectly tuned the first one (manually setting channels, transmit power, etc.), you can simply select the second U6-LR, choose "Load Configuration," and select the first AP as the source. It will instantly copy all the radio settings, saving you from having to configure the second device manually.

9. What is a SIEM server in UniFi integrations

SIEM stands for **Security Information and Event Management**. A SIEM server is a centralized logging and security analysis system used by IT and security professionals.

- **Function:** It collects, aggregates, and analyzes log data from hundreds or thousands of devices across a network (firewalls, servers, switches, APs, etc.).
- **Purpose:** By having all logs in one place, a SIEM can detect security threats and suspicious patterns that would be impossible to see by looking at individual devices. It is used for threat detection, generating alerts (e.g., "Warning: 100 failed login attempts from this IP address in 5 minutes!"), and creating compliance reports for audits.
- **UniFi Integration:** The UniFi integration allows your UDM Pro to automatically send all its system, traffic, and security logs (like firewall blocks and threat detections) directly to your company's SIEM server for real-time analysis.

Page 3: ISP Routers & The Importance of Bridge Mode

This section explains the common issues with ISP-provided hardware and the critical role of Bridge Mode.

10. Why Hathway router does not show bridge mode

The reason you cannot find a "Bridge Mode" option in the admin panel of your Hathway-provided RL Tech router is because **Hathway has deliberately disabled or hidden it in the device's firmware.** This is a common practice among ISPs for several reasons:

- **Simplified Support:** Their support team only has to learn and troubleshoot one standard configuration. Supporting complex setups with customer-owned routers is more difficult and costly for them.
- **Network Control:** It allows them to maintain a greater degree of control over the device that is terminating their network connection.

- **Feature Lock-in:** Sometimes, ISPs offer add-on services (like Wi-Fi extenders or parental controls) that rely on their router's proprietary software. Disabling their router would disable these services.

Solution: Although the button is not visible to you, the feature almost always exists. The only way to enable it is to **call Hathway's technical support**, specifically ask for "Level 2" or business support, and state that you need your device put into Bridge Mode for your business firewall. They can push the configuration change remotely.

11. What happens if bridge mode is not enabled

If you connect a second router (like your UDM Pro) to your ISP router without enabling Bridge Mode, you create a network condition called **Double NAT (Network Address Translation)**. This is a problematic and incorrect network configuration.

Imagine your office building has two security desks: one at the main entrance (the ISP router) and a second one right behind it (the UDM Pro). A visitor (internet traffic) has to check in at the first desk, get a temporary pass, and then immediately check in at the second desk to get another pass. This causes confusion, delays, and communication breakdowns.

Specific Technical Problems Caused by Double NAT:

- **DHCP Conflicts:** Two devices are trying to be the "boss" of assigning IP addresses, leading to IP address conflicts and devices being unable to connect.
- **Firewall Conflicts:** Two separate firewalls are filtering traffic. The ISP firewall may block traffic that you have explicitly allowed on your UDM Pro, making rules hard to manage.
- **Performance Degradation:** The extra processing step adds latency (ping) to all your traffic.
- **Application & Service Failures:** Many services that rely on direct, two-way communication will fail. This includes:
    - **VPNs** (both connecting into and out of the office)
    - **Online Gaming** (especially hosting a game)
    - **VoIP and Video Conferencing** (can lead to one-way audio or call drops)
    - **Port Forwarding** (will not work without complex, dual configurations)
    - **Remote Desktop** and other remote access services.

12. Why internet still works fine without bridge mode on UDM Pro

This is the most deceptive part of a Double NAT setup. For many basic activities, the internet will **appear** to work fine, which leads people to believe their setup is correct.

The Reason:
Simple, outbound web traffic—like browsing websites, streaming video (Netflix, YouTube), or checking email—is very resilient. Your computer sends a request out, and the server sends a response back to

that specific request. This type of communication can usually navigate a Double NAT setup without any noticeable issues for the end-user. The two "security desks" can handle this simple in-and-out traffic, albeit inefficiently.

The Hidden Problems:
The failures do not appear during simple consumption of content. The problems start the moment you need **complex or unsolicited incoming communication**. As listed in the previous point, any service that requires the outside world to initiate a connection to your network (like a remote employee connecting to your office via VPN) will be blocked by the first firewall (the ISP router) and will likely fail.

In a business environment where reliability, performance, and services like VPN are critical, **Double NAT is unacceptable**. The network may "work" for browsing, but it is fundamentally broken, unstable, and will cause hard-to-diagnose problems that will frustrate employees and impact productivity. Enabling Bridge Mode is the only correct solution.
56.5s