# Understanding Your Network and UniFi Console

### Explanation of WAN IP Obtained from Upstream Router (DHCP)

When your UniFi Dream Machine Pro (UDM Pro) is connected to an upstream router (like the one from your Internet Service Provider - ISP), it typically obtains a WAN (Wide Area Network) IP address through a process called DHCP (Dynamic Host Configuration Protocol).[1][2]

- **What is a WAN IP?** The WAN IP is the unique address assigned to your network that allows it to communicate with the internet. Think of it as your network's public mailing address.
- **How DHCP Works:** Instead of manually configuring the IP address, subnet mask, gateway, and DNS servers, DHCP automates this process.[1] Your UDM Pro sends out a request to the upstream router, which then assigns it an available IP address from its pool.[3][4] This makes network setup significantly easier.[1] The UDM Pro will automatically obtain an IP address from your ISP.[1]

In your UDM Pro's settings, you can configure the WAN port to use DHCP.[1] This is the default and most common setup for home and small business networks.[5]

### Why the UniFi Console Website Might Be Disabled and How to Reach It

There are several reasons why you might not be able to reach your UniFi OS console website:

- **Network Configuration Issues:** If your computer is not on the same network as the UniFi console, you won't be able to access it directly via its IP address.
- **Incorrect IP Address:** You might be typing the wrong IP address for the console.
- **Firewall Rules:** A firewall on your computer or network could be blocking access to the console's web interface.
- **Console is Offline or Unresponsive:** The UniFi console itself might be offline or have encountered an issue.

### How to Reach the UniFi OS Console Site:

1. **Direct Connection via IP Address:** The most common way to access your UniFi console is by typing its IP address into a web browser.[6] You can find the IP address on the console's LCD screen or by using a network scanning tool like the WiFiman mobile app.[6] For UniFi Cloud Gateways, you can often just navigate to `unifi/` in your browser.[6]
2. **UniFi Site Manager:** If you have a UI (Ubiquiti) account and have enabled remote access, you can manage your console from anywhere through the UniFi Site Manager at `unifi.ui.com`.[7] The web interface is designed to establish a direct connection to your console when you're on the same local network.[7]
3. **Mobile App:** The UniFi Network mobile app (available for iOS and Android) allows you to set up and manage your console.[6]

4. **SSH and Debug Console (Advanced):** For troubleshooting or advanced management, you can access the console's command-line interface.
    a. **Debug Console:** This is the recommended method for directly connecting to a UniFi device and can be enabled in the UniFi Network settings.[8][9][10]
    b. **SSH (Secure Shell):** If the UniFi OS is down, you can use SSH. This is an advanced method and should be used with caution as incorrect commands can disrupt your network.[8] SSH is disabled by default on UniFi Consoles and needs to be enabled in the settings.[8]

## Working with Your HikVision Camera

### How to Connect HikVision DS-2DE2A404IW-DE3 Camera to HDMI

The HikVision DS-2DE2A404IW-DE3 is an IP network camera and, based on its specifications, it does **not** have a direct HDMI output.[11] This type of camera is designed to transmit video data over a network.

To view the camera's feed on a screen with an HDMI input (like a TV or monitor), you would typically use one of the following methods:

- **Network Video Recorder (NVR):** Connect the camera to a HikVision NVR via an Ethernet cable. The NVR then connects to a monitor via an HDMI cable, allowing you to view and record footage from multiple cameras.
- **Computer with HikVision Software:** You can view the camera's live feed on a computer using HikVision's software (like iVMS-4200) or through a web browser by navigating to the camera's IP address.[12] You could then connect your computer to an HDMI display.
- **Third-Party Decoder:** A network video decoder is a device that can receive video streams from IP cameras and output them to an HDMI or other video interface.

### How to Reset a HikVision Camera

Resetting your HikVision camera can be useful if you've forgotten the password or need to restore it to its factory settings.[13][14] There are a few ways to do this:

- **Hardware Reset Button:** This is often the most straightforward method.[15][16]
- **Web Browser:** You can perform a factory reset through the camera's web interface.[13]
- **SADP Tool:** This software can be used to reset the password, but a full factory reset is typically done via the hardware button or web interface.[17][18]

**How to Perform a Hardware Reset on a HikVision Camera**

The specific location of the reset button can vary by camera model, but it is often found near the SD card slot.[15][19] For the DS-2DE2A404IW-DE3, the reset button is located near the memory card slot.[20]

Here are the general steps for a hardware reset:[12][13][15][16][19]

1. **Power Off the Camera:** Disconnect the power supply.[16] If the camera is powered by PoE (Power over Ethernet), unplug the network cable.[16]
2. **Press and Hold the Reset Button:** Use a small tool like a paperclip to press and hold the reset button.[16]
3. **Power On the Camera:** While still holding the reset button, reconnect the power.[13][15]
4. **Continue Holding:** Keep the reset button pressed for about 10-20 seconds.[13][15] You might see the camera's indicator lights flash.[16]
5. **Release the Button:** After the recommended time, release the reset button.[13][16] The camera will then restart with its factory default settings.[19]

After a reset, the camera will be in an "inactive" state, and you will need to use the SADP tool or a web browser to set a new password and reconfigure its network settings.[15][19]

**What is the SADP Tool in HikVision Cameras?**

SADP (Search Active Devices Protocol) is a free software utility provided by Hikvision.[21][22] Its primary function is to scan your local network to find connected Hikvision devices like IP cameras and DVRs/NVRs.[17][23]

Key uses of the SADP tool include:[17][21][24]

- **Device Discovery:** It finds Hikvision devices on your network, even if they are on a different IP subnet.[17]
- **Device Activation:** When you first connect a new Hikvision camera, it will be inactive. You use the SADP tool to activate it by setting an admin password.[24][25]
- **Network Parameter Configuration:** You can easily view and change the IP address, subnet mask, gateway, and other network settings of your devices.[21][23]
- **Password Resetting:** If you forget your device's password and it doesn't have a physical reset button, you can use the SADP tool's "Forgot Password" feature.[17][18] This involves exporting a file or QR code to send to Hikvision support for a reset file.[17][18]
- **Firmware Information:** It allows you to see the current firmware version of your devices.[21]

### What is "Reset IPC" in HikVision IP Cameras?

"IPC" stands for "IP Camera." So, "Reset IPC" simply means resetting the IP camera to its factory default settings. This is the same process as described in the hardware and software reset sections above. The goal is to erase all custom configurations, including the password, IP address, and any other settings you may have changed, and return the camera to its original state.

### How to Reset the Password on a HikVision DS-2DE2A404IW-DE3

If you have forgotten the password for your HikVision DS-2DE2A404IW-DE3, you have a few options:

1. **Hardware Reset:** As detailed above, performing a hardware reset will erase the password along with all other settings, allowing you to set a new one.[14][25]
2. **SADP Tool "Forgot Password" Feature:** This is useful if you cannot physically access the camera's reset button.[17][18]
    a. Open the SADP tool and select your camera from the list.
    b. Click the "Forgot Password" link.[18]
    c. You will be prompted to export a file or a QR code.[18]
    d. You then send this file or code to your supplier or Hikvision technical support.[17]
    e. They will provide you with a reset file that you can import using the SADP tool to reset the password.[17]
    f. It's important to keep the device powered on throughout this entire process.[17]

### What is a GUID File in HikVision Devices?

A GUID (Globally Unique Identifier) file in the context of Hikvision devices is related to the password reset process. When you use the "Forgot Password" feature in some versions of Hikvision's software or on the device's web interface, you may be prompted to export a GUID file. This file contains unique information about your device. You then send this GUID file to Hikvision support or your distributor. They use this file to generate a unique key file that you can then import back into the device to securely reset your password. This method adds a layer of security to the password reset process, ensuring that only the authorized user can reset the password.

## Advanced Networking with UDM Pro

### How to Check the IP Address on Your Phone

Knowing your phone's IP address can be useful for various networking tasks. Here's how to find it on both Android and iOS devices:

- **On an iPhone or iPad:**[26][27][28]
    - Open the **Settings** app.
    - Tap on **Wi-Fi**.

    - Tap the "i" icon next to the Wi-Fi network you are connected to.[26]
    - Your IP address will be listed under the "IPv4 Address" section.[28]
- **On an Android Phone (steps may vary slightly by manufacturer):**[26][27][28][29][30]
    - Open the **Settings** app.
    - Go to **Connections** or **Network & Internet**, then tap on **Wi-Fi**.[27][28]
    - Tap on the name of the Wi-Fi network you are connected to, or the gear icon next to it.[28][30]
    - You may need to tap on "Advanced" or "View more".[27][28]
    - Your IP address will be displayed.[29]

**How to Connect the UDM Pro with an Additional Router**

You can connect a second router to your UDM Pro to extend your network's reach or create a separate network segment.[31][32][33][34] The most common and recommended way to do this is to configure the second router as an "Access Point" (AP).[33] This ensures that the UDM Pro remains the primary router managing your network, which helps to avoid issues like Double NAT.[3]

**How to Connect Two Routers in the Same Network and Use Them Together**

Here is the general process for connecting a second router to your main UDM Pro network:

1. **Identify Your Routers:** Your UDM Pro will be your **main router**, and the additional router will be the **secondary router**.[3]
2. **Physical Connection:** Use an Ethernet cable to connect a **LAN port** on your UDM Pro to a **LAN port** on the secondary router.[3][35] **Do not** use the WAN/Internet port on the secondary router for this type of setup.[3][36]
3. **Configure the Secondary Router:** This is the most critical part. You will need to change some settings on the secondary router before connecting it to the UDM Pro.[31][32][35][36]

**How to Split People into Two Routers to Balance Internet Speed with UDM Pro**

While you can't truly "split people" in a way that perfectly balances internet speed with a simple two-router setup, you can strategically place the routers and assign devices to them to improve overall network performance.

The idea is to have the UDM Pro and the second router (acting as an access point) in different locations to provide better Wi-Fi coverage throughout your space. Devices will then connect to the router with the strongest signal.

For more advanced load balancing, you would typically use features built into high-end routers or dedicated load-balancing hardware. The UDM Pro itself has dual WAN capabilities for load balancing between two different internet connections, not for balancing users between two internal routers.[1][37]

**How to Configure Router 2 (Turn off DHCP, Set Static IP, Wi-Fi Setup)**

To properly integrate a second router into your UDM Pro network without causing conflicts, you need to configure it as a "dumb" access point. This involves:

1. **Accessing Router 2's Admin Panel:** Before connecting it to the UDM Pro, connect a computer directly to the second router via an Ethernet cable.[35] Log in to its web interface using its default IP address (e.g., 192.168.1.1 or 192.168.0.1).[32]
2. **Turn Off DHCP:** This is the most important step. Your UDM Pro is already handling DHCP for your network. Running a second DHCP server will cause IP address conflicts.[3][35][36] Find the DHCP server settings on the second router and disable it.[3][36]
3. **Set a Static IP Address:** You need to assign the second router a static IP address that is within the same subnet as your UDM Pro's LAN, but outside of the UDM Pro's DHCP range.[31][36]
    a. For example, if your UDM Pro's IP is 192.168.1.1 and its DHCP range is 192.168.1.100 to 192.168.1.200, you could set the second router's IP to 192.168.1.2.[3][36]
    b. This ensures you can still access the second router's admin panel later if needed.[35]
4. **Wi-Fi Setup:**
    a. **SSID (Network Name):** You can either set the Wi-Fi name and password to be the **same** as your UDM Pro's Wi-Fi network to create a seamless roaming experience, or you can give it a **different** name to easily distinguish between the two access points.[31]
    b. **Wireless Channel:** To minimize interference, set the Wi-Fi channel on the second router to be different from the channel used by your UDM Pro (and any other nearby Wi-Fi networks).[36] For example, on the 2.4 GHz band, use channels 1, 6, or 11 as they don't overlap.

**Step-by-Step Setup of Router 2 in the Same Network**

Here is a consolidated, step-by-step guide:

1. **Prepare Router 2:**
    a. It's a good idea to perform a factory reset on the second router to start with a clean slate.[34]
    b. Connect a computer to one of the LAN ports of Router 2.[35]
2. **Log in to Router 2:**
    a. Open a web browser and enter the default IP address of Router 2.
    b. Log in with the default username and password.
3. **Configure Router 2's Settings:**
    a. **Disable DHCP:** Locate the LAN or DHCP settings and turn off the DHCP server.[3][36]
    b. **Set Static LAN IP:** Change the router's LAN IP address to an available static IP on your UDM Pro's network (e.g., if your UDM Pro is 10.0.1.1, set Router 2 to 10.0.1.2).[3][36] Make sure this IP is outside the DHCP pool of the UDM Pro.[31]

    c. **Configure Wi-Fi:** Set the SSID (Wi-Fi name) and password.[31] For best performance, choose a different Wi-Fi channel than your main router.[36]
    d. **Save and Reboot:** Save your changes. The router will likely reboot.[3]
4. **Connect the Routers:**
    a. Connect an Ethernet cable from a **LAN port** on your UDM Pro to a **LAN port** on Router 2.[3][35]
5. **Test the Connection:**
    a. Connect a device to Router 2's Wi-Fi network or one of its LAN ports.
    b. You should be able to access the internet. Your device should get an IP address from the UDM Pro.

**Whether Blocking Rules in UDM Pro Also Apply to a Second Router**

Yes, if you have configured the second router correctly as an access point (with DHCP turned off), then all traffic from devices connected to the second router will still pass through the UDM Pro. This means that any blocking rules, firewall rules, traffic management, and other security features you have set up on the UDM Pro will be applied to all devices on your network, regardless of whether they are connected to the UDM Pro directly or through the second router.

The UDM Pro acts as the central gateway and "brain" of your network. The second router, in this configuration, is simply extending the network and does not perform any routing or filtering of its own. It just passes all the data to the UDM Pro to be processed. The UDM will prevent DHCP traffic from passing from the WAN side, which helps avoid conflicts with an upstream router, and a similar principle of centralized control applies to its LAN-side security features.