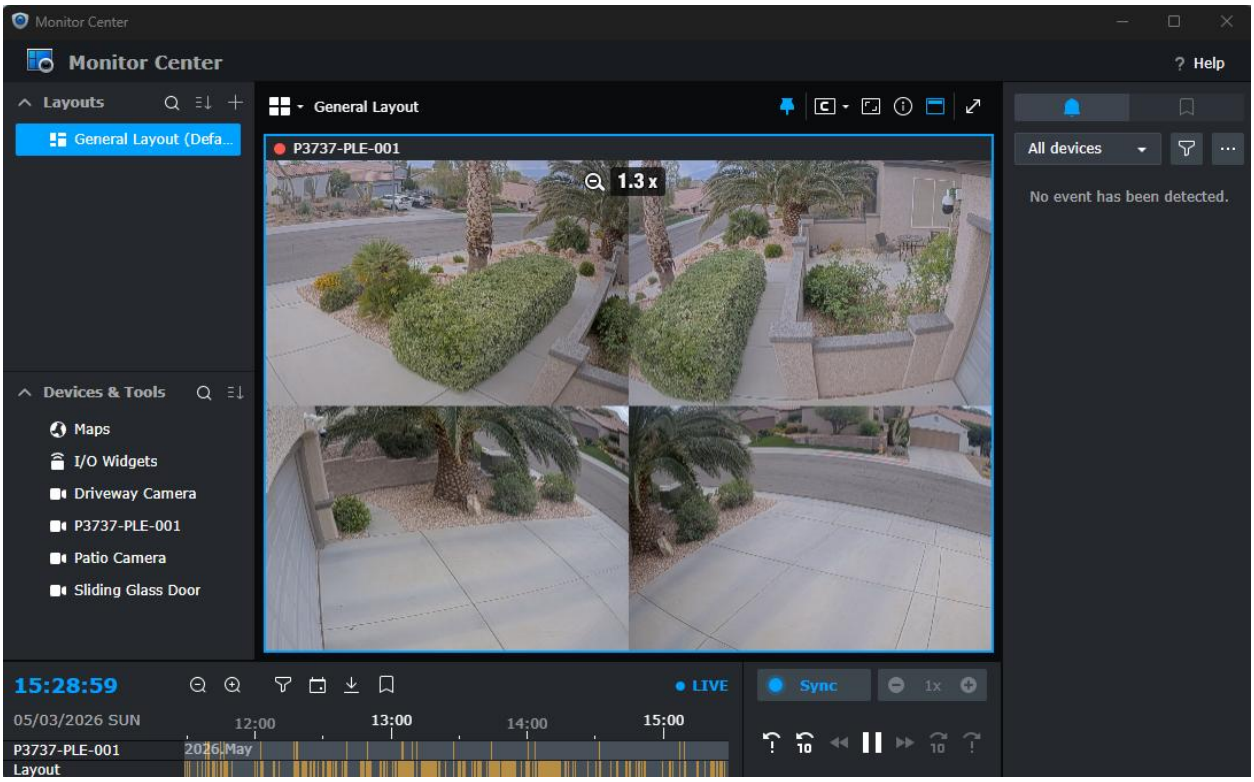
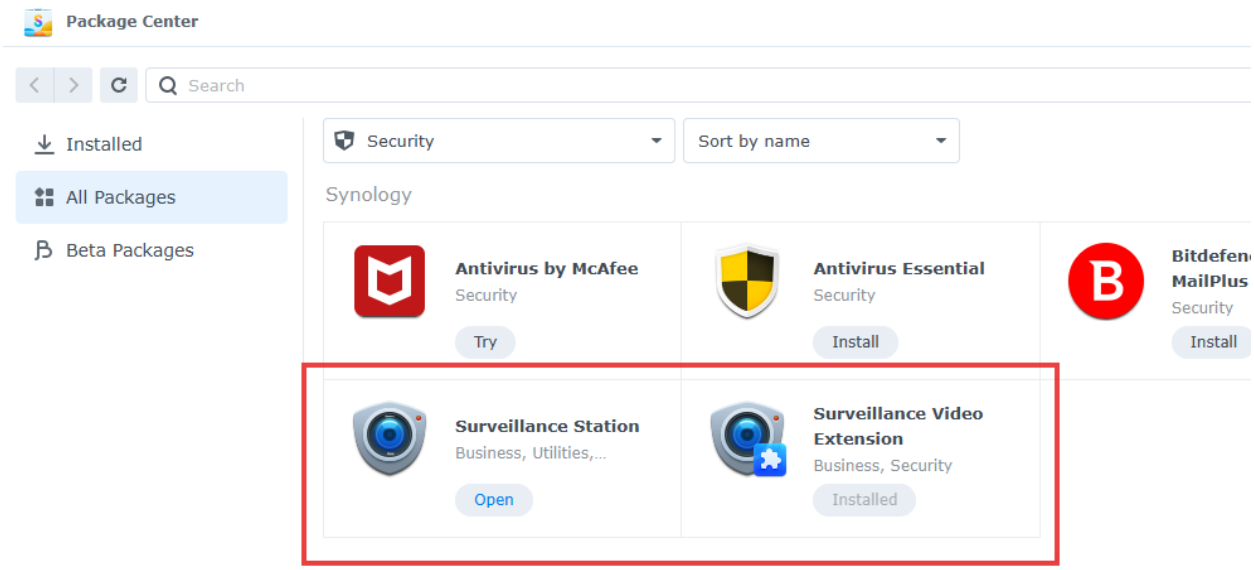
Video Surveillance



Contents

Video Surveillance Recording

The Synology NAS has an optional product that can be installed ("Surveillance Station") that is very nice and allows you to record audio/video data from IP cameras on your network. This section describes the non-obvious things that are required set this up. You will need to install the two packages shown below onto your NAS. Note that this comes with 2 camera licenses – you will need to purchase more if needed.



PoE (Power over Ethernet)

Cameras require both power and an ethernet/signal connection. Using a PoE switch allows you to route both the power and ethernet through a standard ethernet cable – making the installation much cleaner. I chose to use the following PoE+ switch available on Amazon for $273.

You don't need special cables, normal CAT5/6 ethernet cables work fine.

PoE comes in 3 varieties: PoE (15W/channel), PoE+ (30W/channel), and PoE++ (60-100W/channel.)

You can also plug non-PoE devices into it AS LONG AS your switch (this one does) supports the 802.3 AF/AT protocol (check the manual/label) which allow devices to negotiate whether they need power or not. Cheaper switches may not have this and will damage non-POE devices because they always supply power.

Camera Reviews

Click on the following links to see my comments about various cameras.

Reolink RLC-823S2 IP Camera

Axis P3737-RLE IP Camera

Camera Configuration

You might think that you can then just plug cameras into your network and detect them with Surveillance Station. This is what I thought and I wasted hours before I realized that the cameras need to be configured **BEFORE** you can connect them to Surveillance Station.

This is typically done by downloading a configuration app from your camera vendor. The examples below use the Reolink Client (available here) since my first camera was a Reolink 5MP Security PoE IP Camera model RLC-510A available on Amazon for $55.

Adding New Cameras to Reolink App Confusion

The Reolink App allows you to add a new camera using either its: UID, IP address, or Link.

IMPORTANT – IP address ONLY works if the app is running on the same network as the camera!

Use the camera UID to add the camera to the app the first time – this will work even if the app and camera are on different local networks as long as they are bridged by a router that supports plug and play of course.

The Reolink camera UID is located on the serial number sticker of the camera.

This drove me crazy and I wasted about 4 hours setting up my 2nd camera because I forgot about this and tried to use the IP address which constantly failed on a separate network. But I could see the 1st camera working just fine. I even tried updating the PC routing table but this didn't fix it either.

Using a laptop with the Reolink app and connecting directly to the camera network then using IP addresses also work fine, but is more involved.

Adding New Cameras to Surveillance Station Confusion

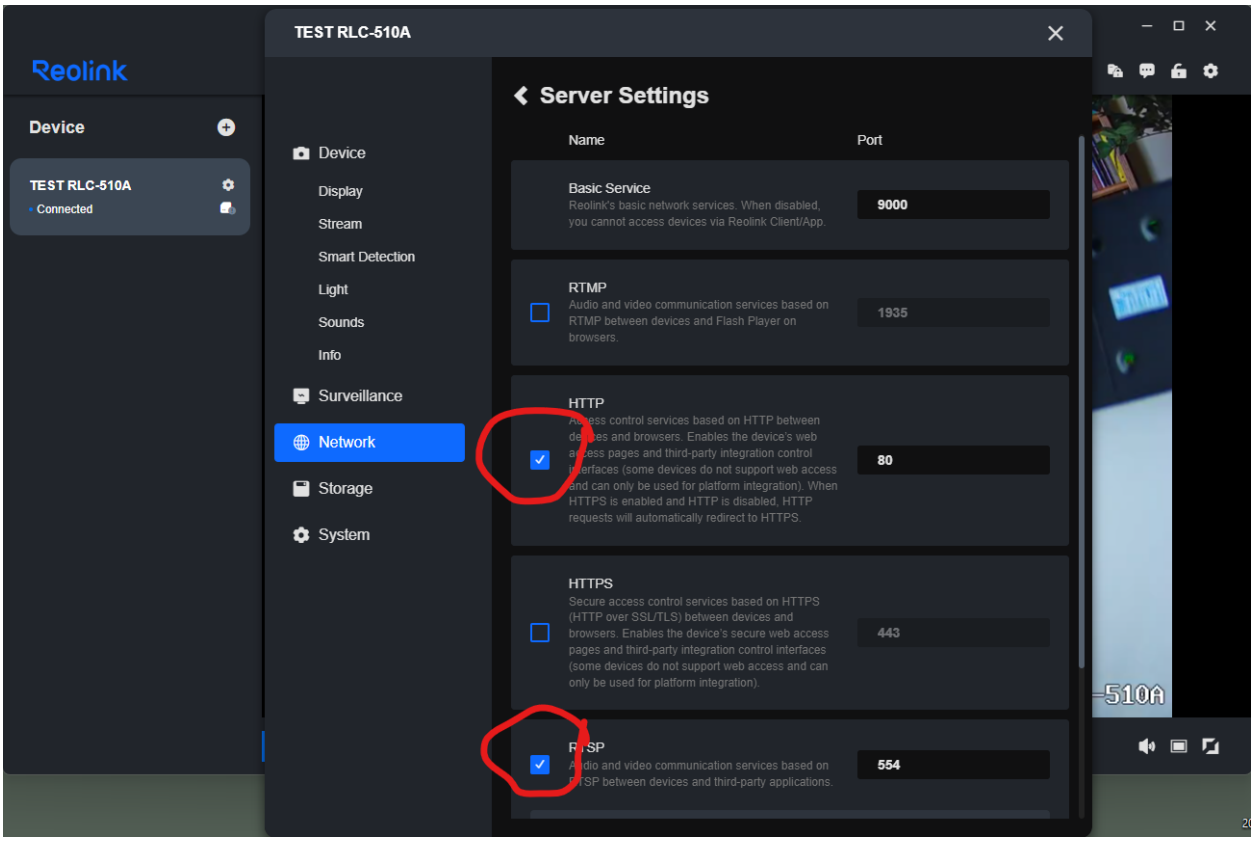
Surveillance Station needs an IP address to connect to the camera so you will need to setup your cameras on the router with DHCP reservations for their MAC addresses so that the cameras will always have the same IP address.

Camera Port Confusion

Another confusing aspect of IP Cameras is that they support multiple TCP ports – typically one port to configure the camera (9000 for the RLC-510A), and then other ports to allow your application to read the camera data (typically 80 for HTTP, or 443 for HTTPS.)

Your app (Surveillance Station in this case) typically does NOT know how to connect to the configuration port and expects the camera to be properly setup to communicate before you start using it with the app.

What was annoying for me at first that I assumed the camera enabled some ports by default, but it does NOT! You have to manually enable appropriate server protocol in the camera configuration app as shown below (Surveillance Station requires HTTP and RTSP, other apps may have different requirements.) Failure to do this will result in hours of frustration chasing down bogus error messages later when trying to 'activate' the camera.

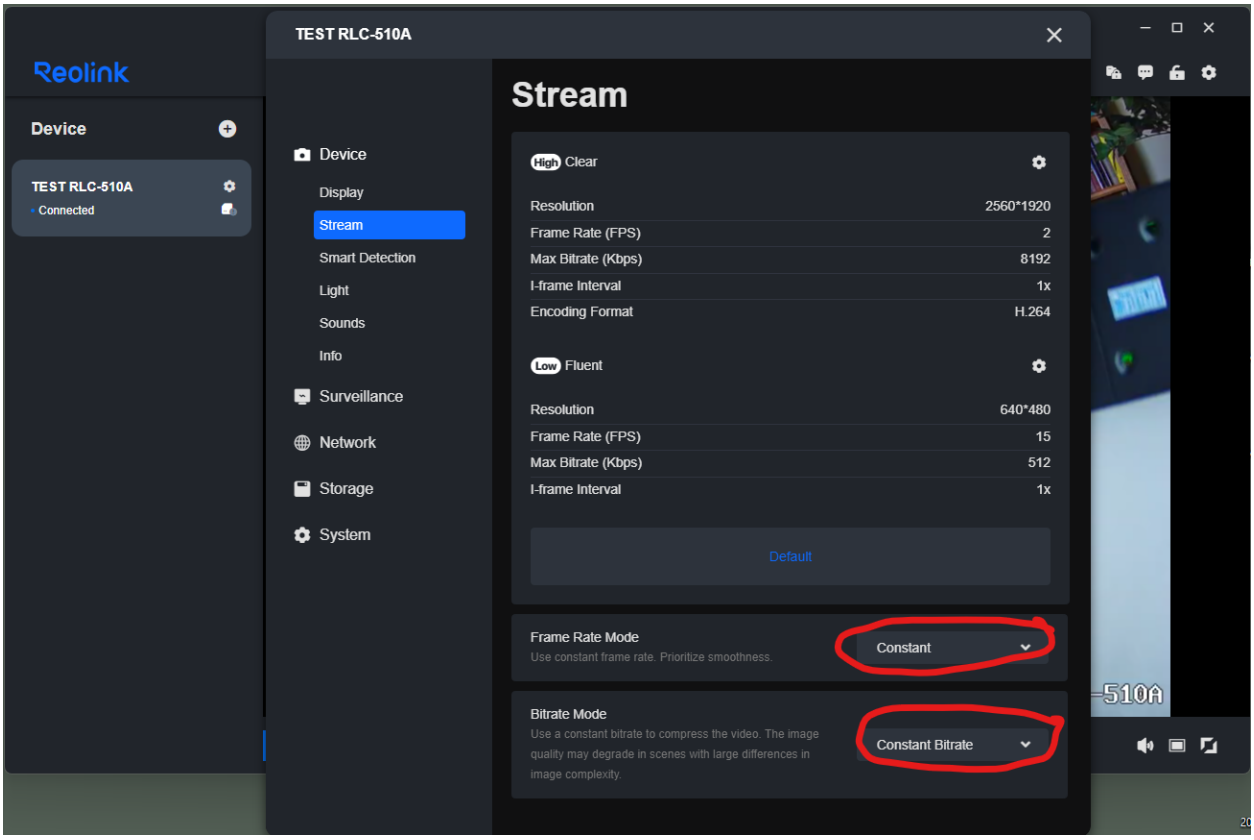


Stream Configuration

Another confusing aspect is that the Stream configuration must be the same on the camera as on the app (Surveillance Station.)

An example of this confusion is that the RCL-510A camera supports BOTH ‘Constant’ and ‘Variable’ frame/bit rates – HOWEVER Surveillance Station ONLY supports ‘Constant’ frame/bit rates SO you need to make sure the camera is configured for ‘Constant’ otherwise the connection will fail.

This is just one example – you need to make sure ALL of the camera configuration matches the app settings.



Other Camera Configuration Settings

Most of the other settings are pretty self-evident.

Once you have the camera configured you add it to Surveillance Station and it should work as expected.

Using a Separate LAN for Cameras

Ideally you want your cameras on their own ethernet LAN so that the high rate of camera traffic will not interfere with your normal LAN activity.

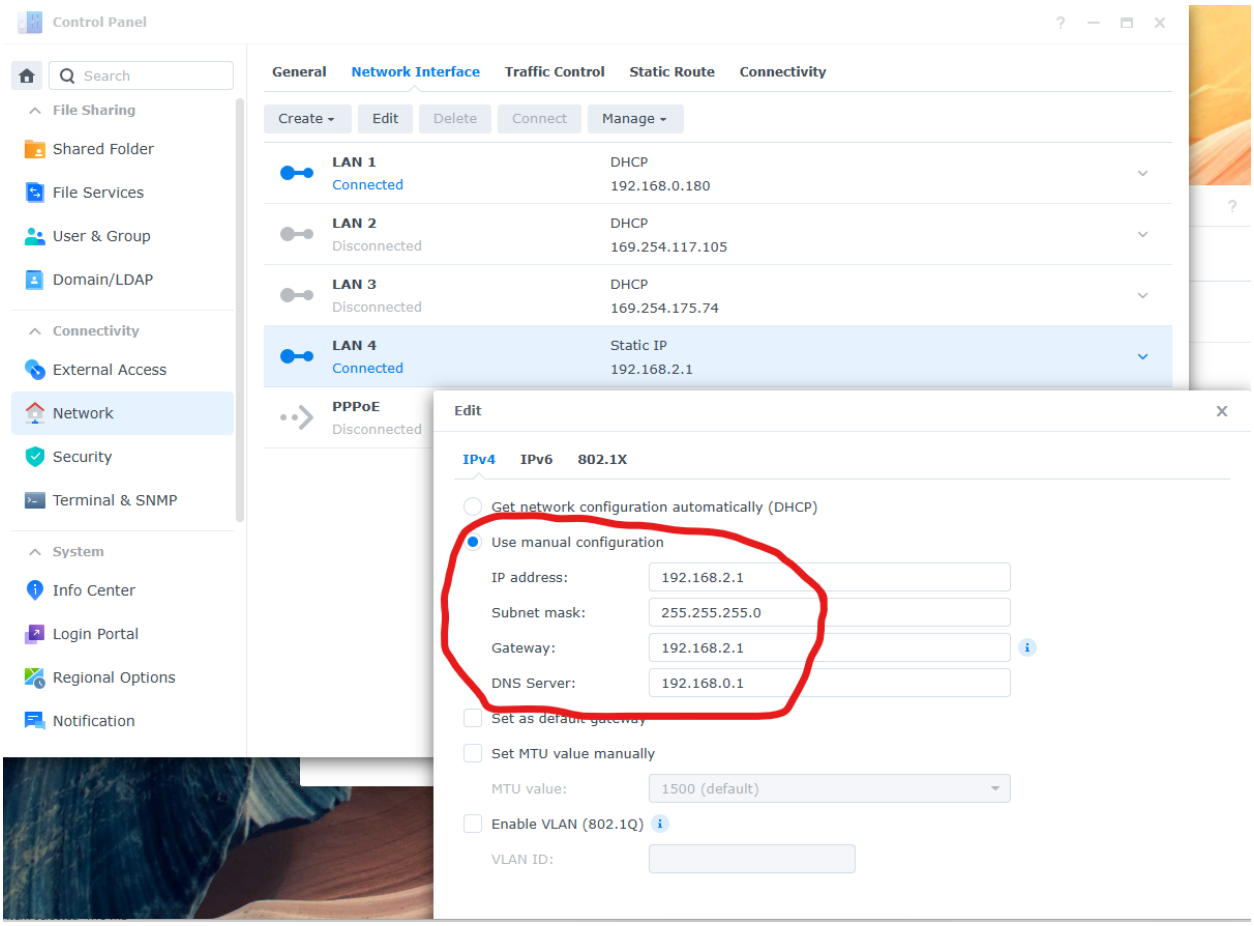
However, there are several considerations that need to be thought through when doing this.

- DHCP Server – it is highly recommended to use DHCP (rather than static IP) so that each camera MAC address has a 'fixed' IP address. Your choices are as follows:
    - Synology NAS supports a built-in DHCP server which works nicely.
        - However, there is no 'clean' Synology NAS support for routing packets between the two networks. So, if you need packet routing (and I would recommend it as it makes configuration MUCH easier) you would need to also add a router – which would have its own DHCP server negating the benefit of using the NAS DHCP.
        - If, on the other hand, you don't need packet routing, then this is the way to go. This would be the way to setup a completely isolated camera network, which would be more secure but a maintenance nightmare.
    - Use a separate router and enable it's DHCP server.
        - This would be my RECOMMENDED way to go as it is MUCH simpler to maintain.

LAN Configuration

On my DSM there are 4 ethernet ports and I randomly chose to connect the cameras to port 4.

Setup the ethernet configuration to use a new network (different from the main LAN 1) as follows:



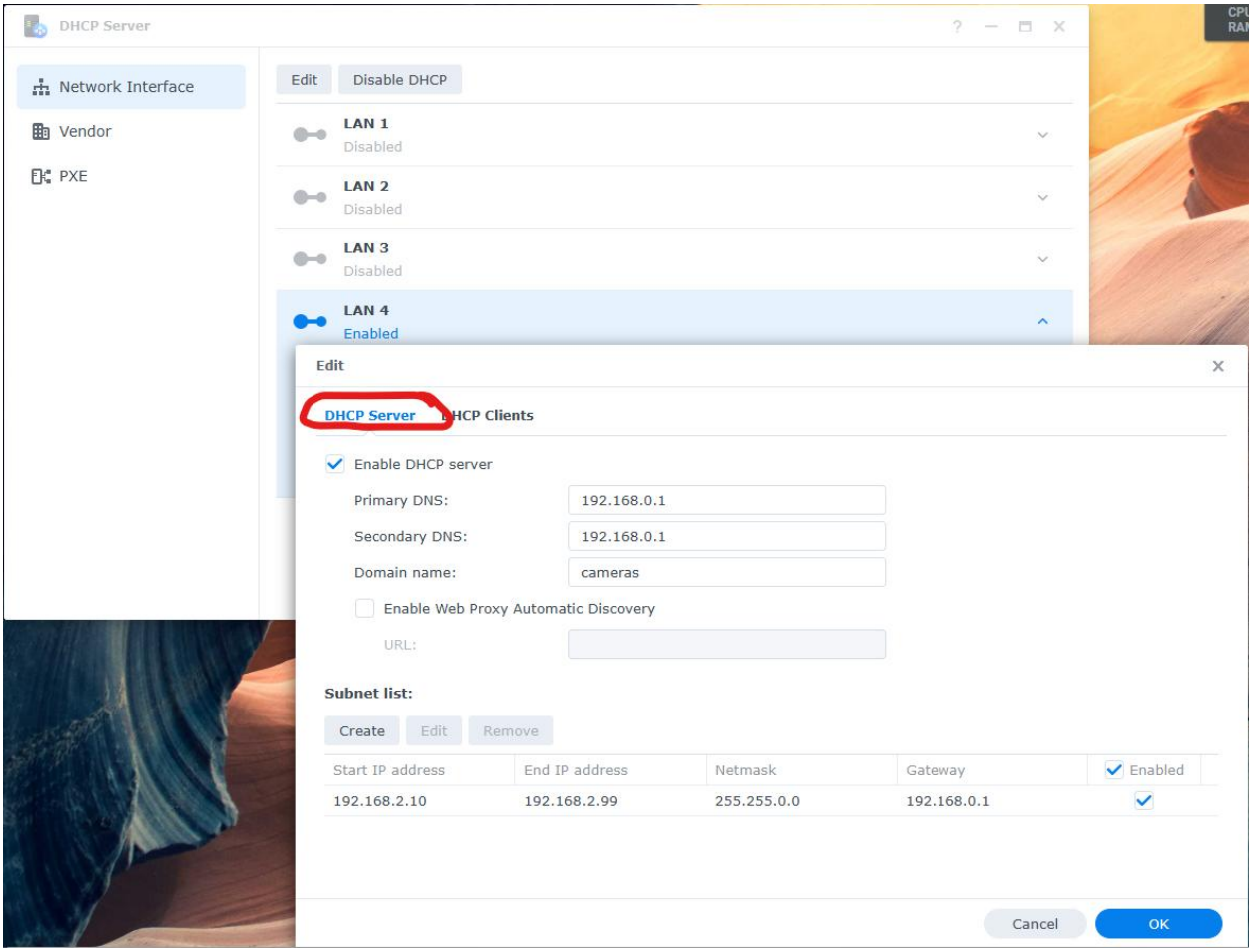
Physically connect your POE switch to the LAN 4 port.

NAS DHCP Server Configuration

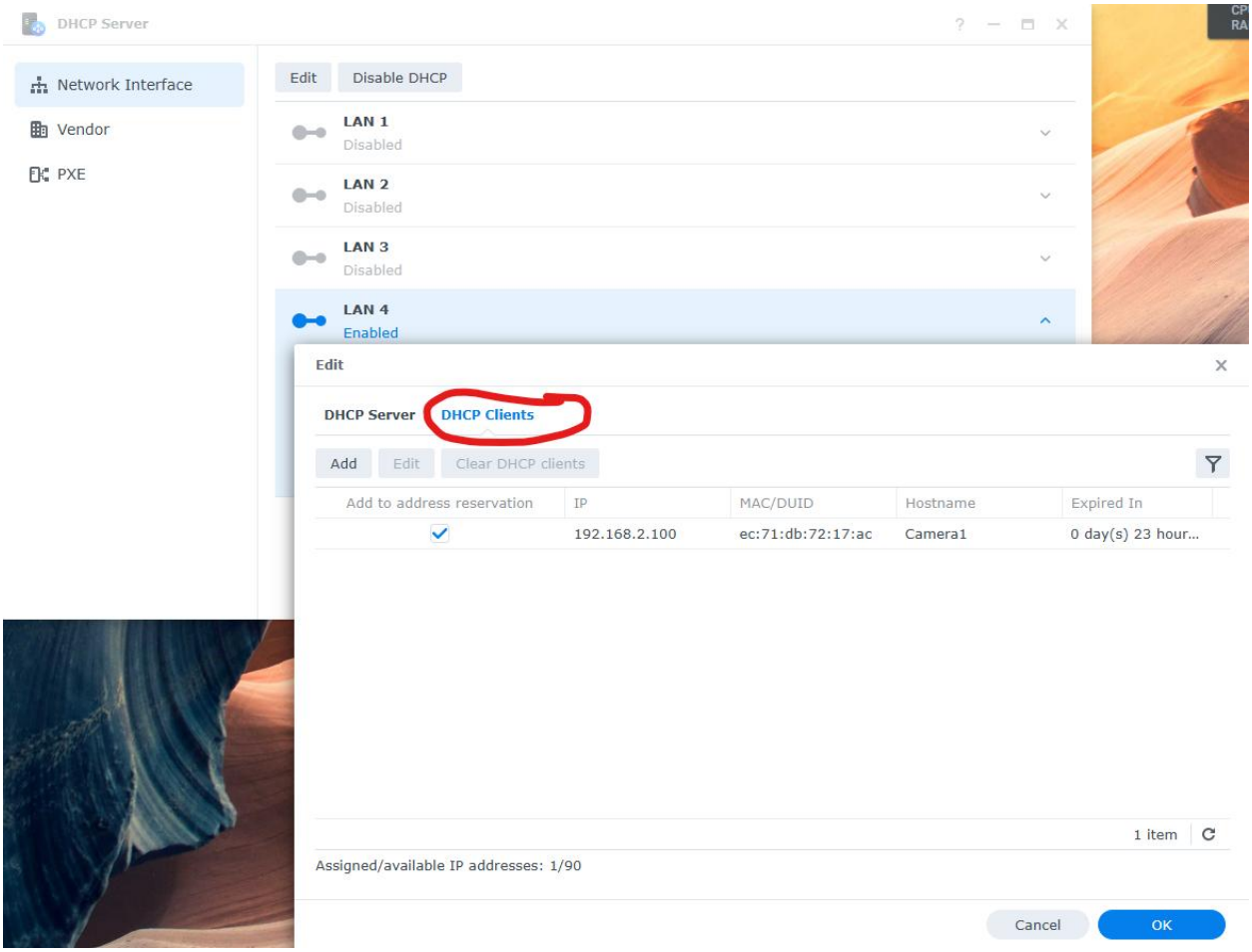
Install the ‘DHCP Server’ app (if not already installed.) Alternatively, you could configure each camera with static IP addresses on another network, but it is much cleaner to do it this way with a DHCP server.

Configure it, using the ‘DHCP Server’ tab, to automatically assign the lower ranges (if you need this hooking up laptops etc.) using the ‘Create’ button.

Make sure to check the ‘Enable DHCP server’ checkbox so that DHCP is enabled on this LAN, and assign your primary LAN DNS settings here manually (although you shouldn’t really need these for the cameras.)



Then switch to the ‘DHCP Clients’ tab and use the ‘Add’ button to add static IP reservations for each of your camera MAC addresses.



If you plug in a camera without setting a reservation, it will show up on this screen and you can use the MAC address displayed to create a reservation.

Note that ‘greyed out’ entries in this screen are NOT active. This is very helpful to tell if a device is present or not.

Router Configuration

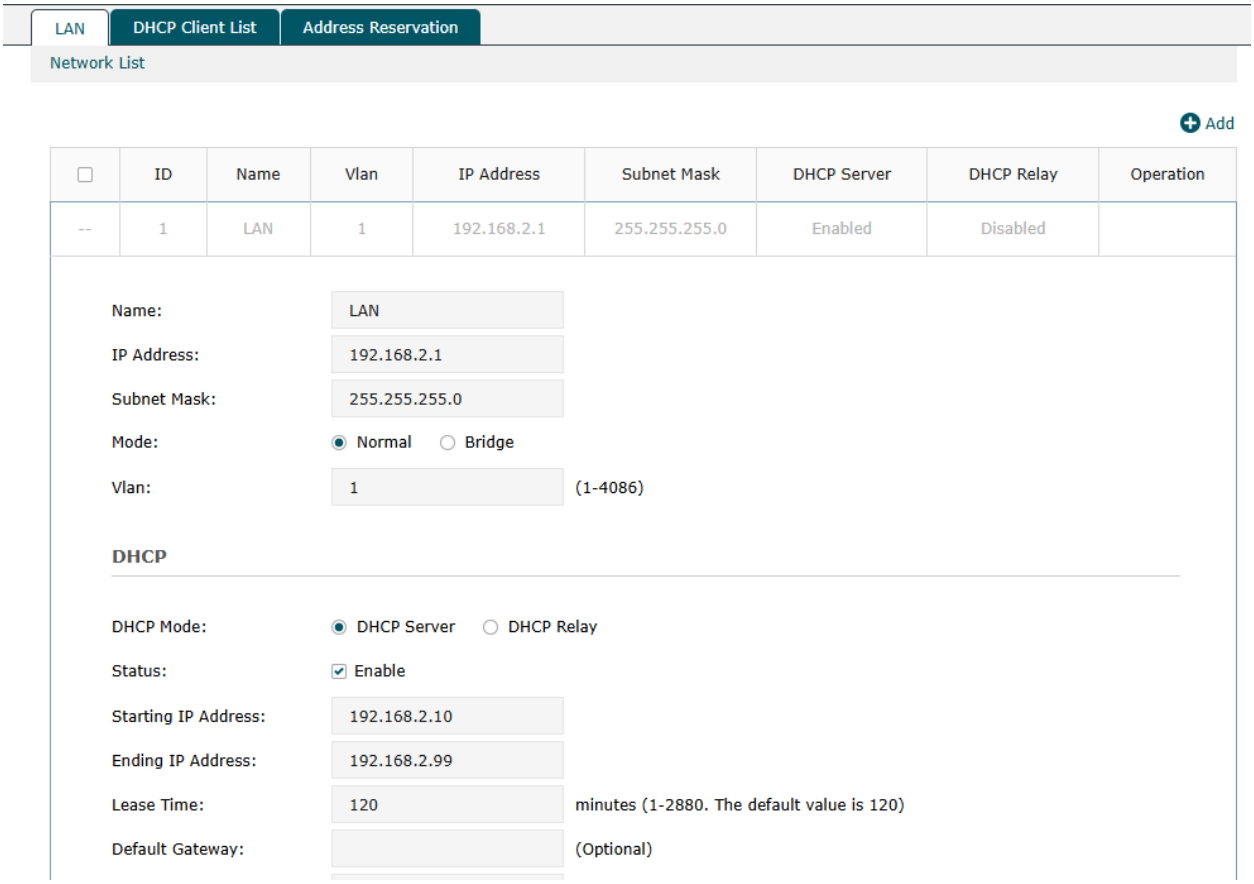
Physically connect your router between your home network (WAN) and your camera network (LAN.)

The following describe how to configure the TP-Link ER605 router but should be similar for other routers as well. There are several other common setups (Time Server, etc.) that are not described here because they are so common it is assumed you know how to set them up. Only the core setup items that could be confusing are described here.

You will initially need to do this configuration with a laptop connected to one of the router LAN ports. Once it is configured, you can then remote in to the router IP address using any web browser.

Configure LAN

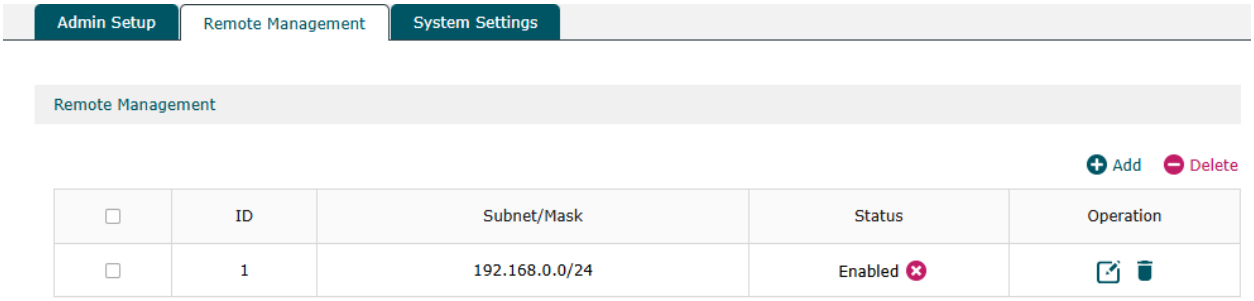
Setup you LAN as appropriate. Set the 'Ending IP Address' to something below where you are going to assign cameras (192.168.2.10 - 192.168.2.99) – I assigned cameras starting at 192.168.2.100.



Setup your camera 'Address Reservation's on the tab above with that name.

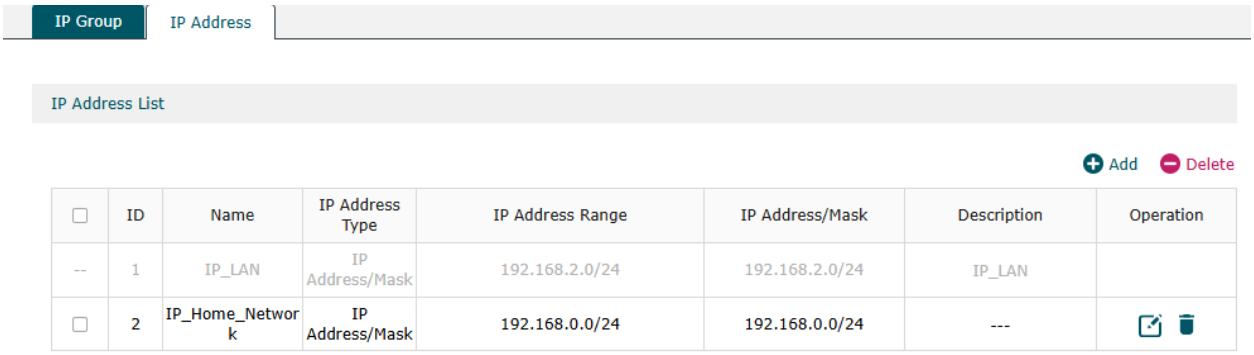
Remote Management

Enable remote management so you can use a computer on your home network to update the router configuration (otherwise you will need to attach a laptop to one of the router LAN ports to configure it.)

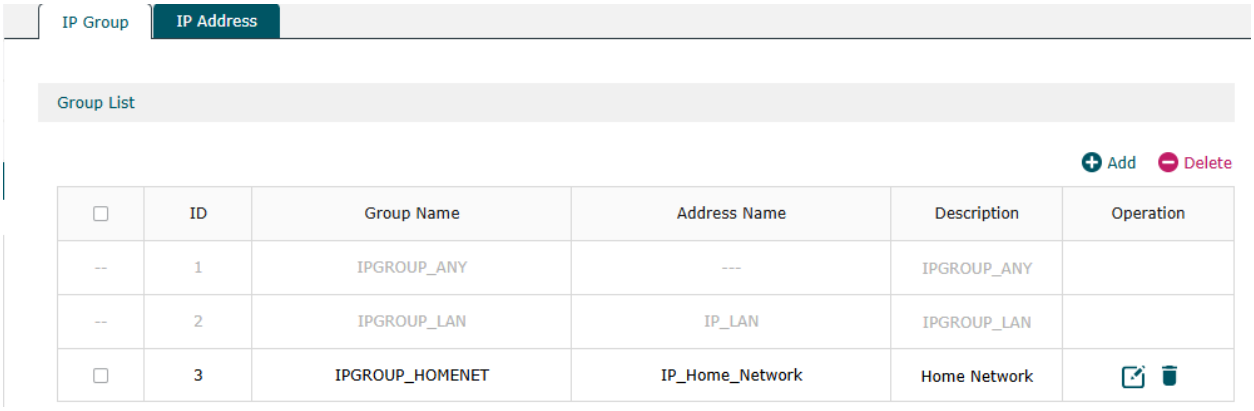


Create an IP Group entry for your Home Network (WAN)

First create and IP Address entry:

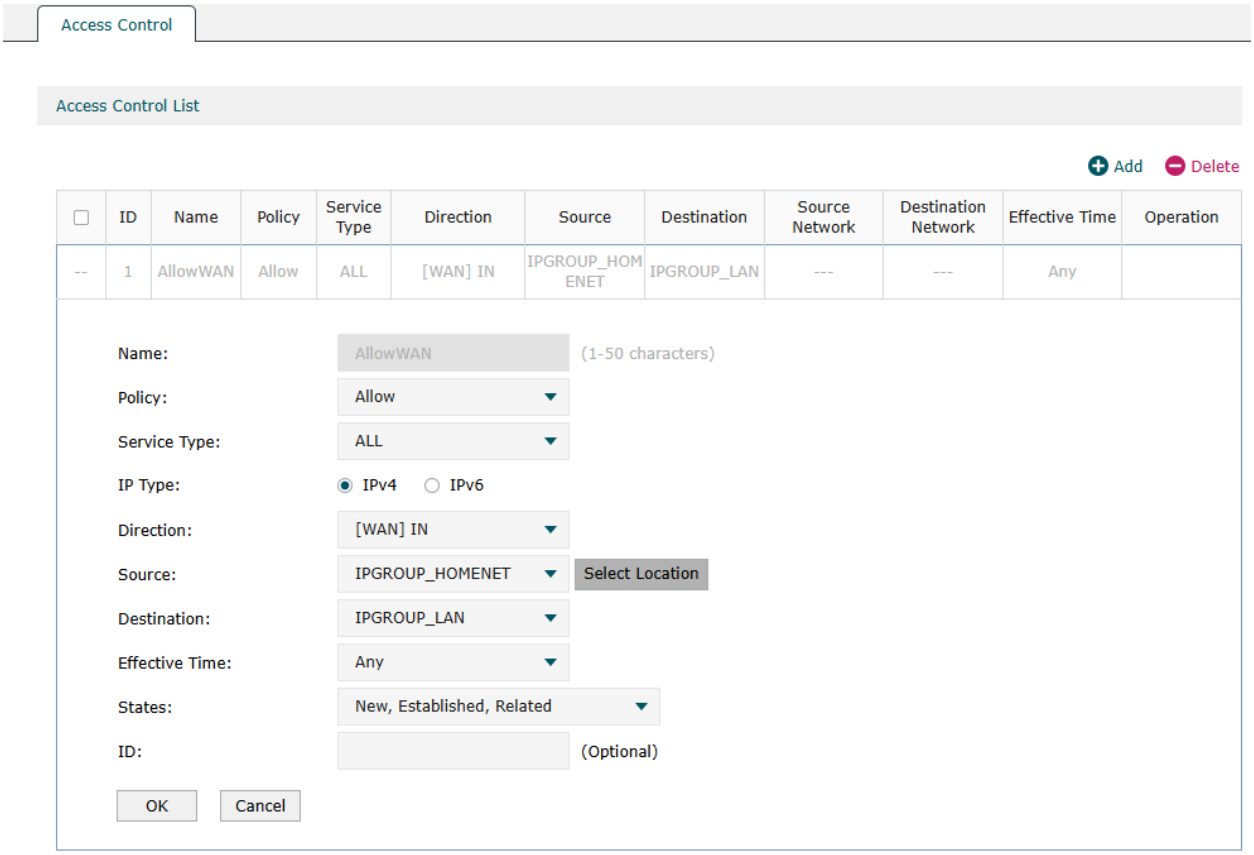


Then the IP Group entry:



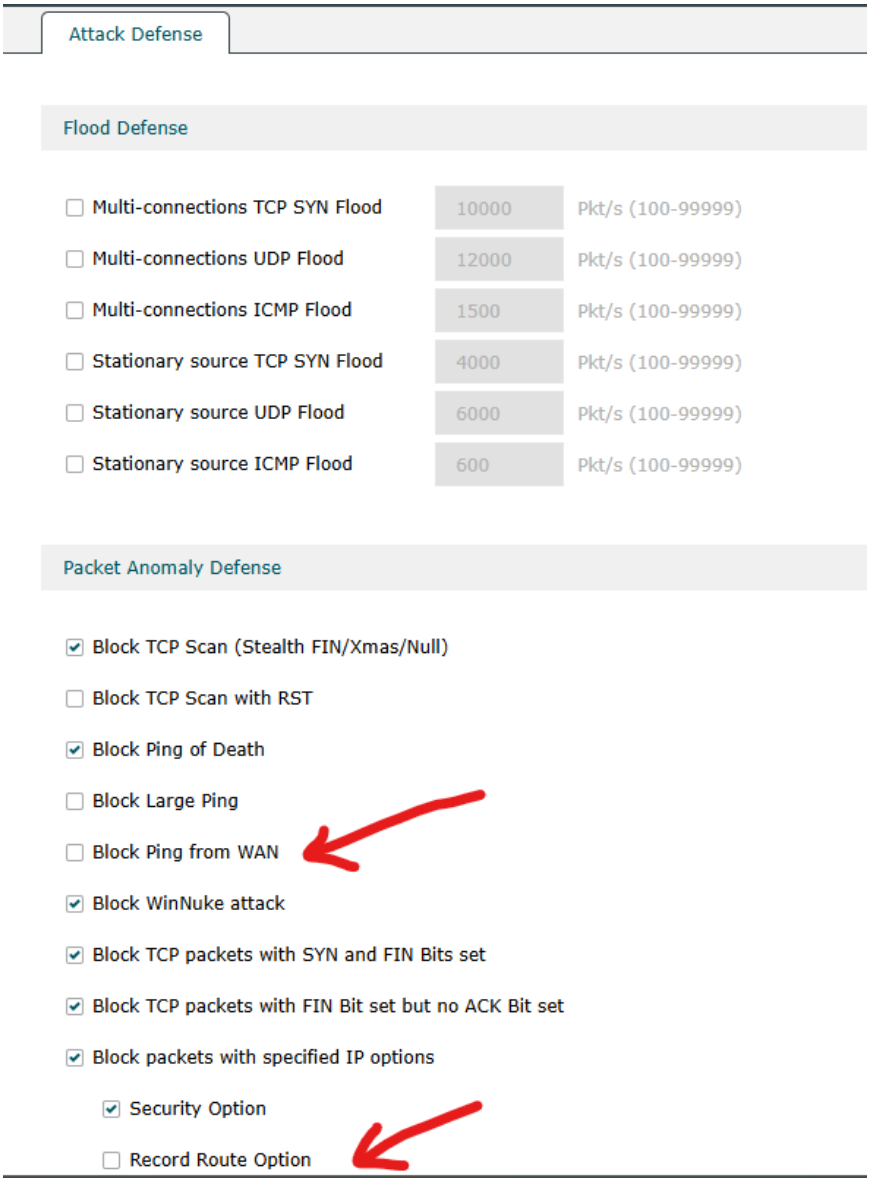
Create Access Control Rule to Allow WAN Traffic

This is necessary to be able to access the LAN network from the WAN – otherwise all in-bound traffic is blocked by the router. You can be more specific if you have security concerns, the rule below allows ALL traffic originating from my WAN network ONLY (no internet traffic) to come through.



Un-Block Firewall Rules you Need

If you need to use ‘Ping’ or ‘Tracert’ from the WAN you will want to un-check the following.



Update Your PC Routing Table

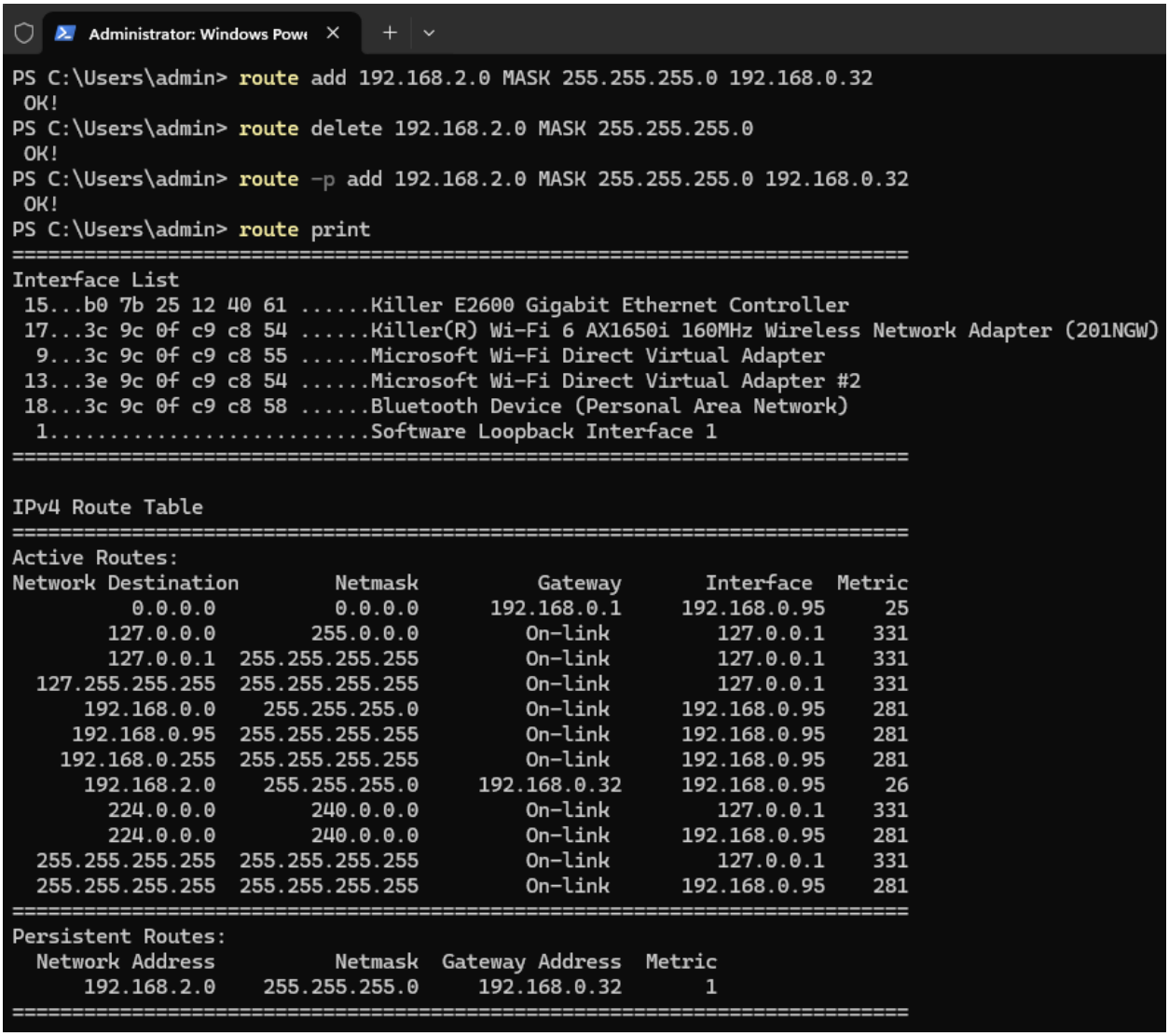
Once you have the router configured, you still need to update your PC routing table to tell it 'where' your Camera Network can be reached through the router. Failure to perform this step results in your attempts to access your Camera Network being routed out to the Internet (default resolution) which, of course, will never work.

This can only be done through the 'Admin' terminal (WindowsKey-X, Terminal-Admin.) The following lines show how to add a route to the Camera Network (192.168.2.0) through the Router (192.168.0.32).

1st line – add a temporary route (gone at power down.)

2nd line – remove the temporary route.

3rd line – add a permanent route (persists through power down.)

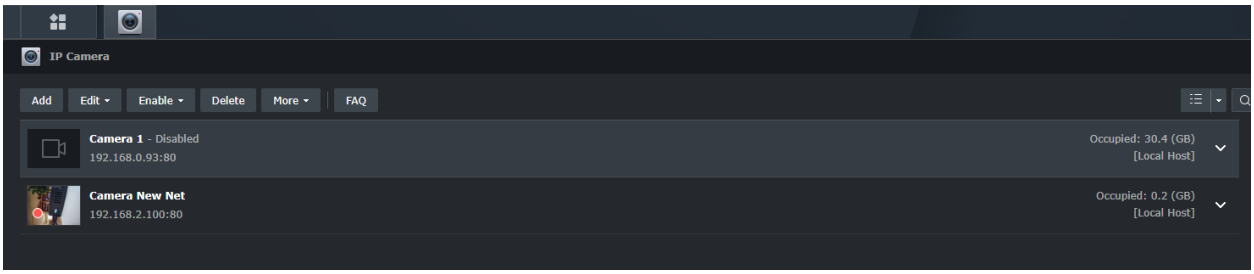


Surveillance Station

Adding a Camera to Surveillance Station

Once you have the camera with its reserved IP, you can proceed normally and add it in ‘Surveillance Station’ using the IP assigned here.

Shown below is the same camera, that I used to have on LAN 1, which is now connected on LAN 4.

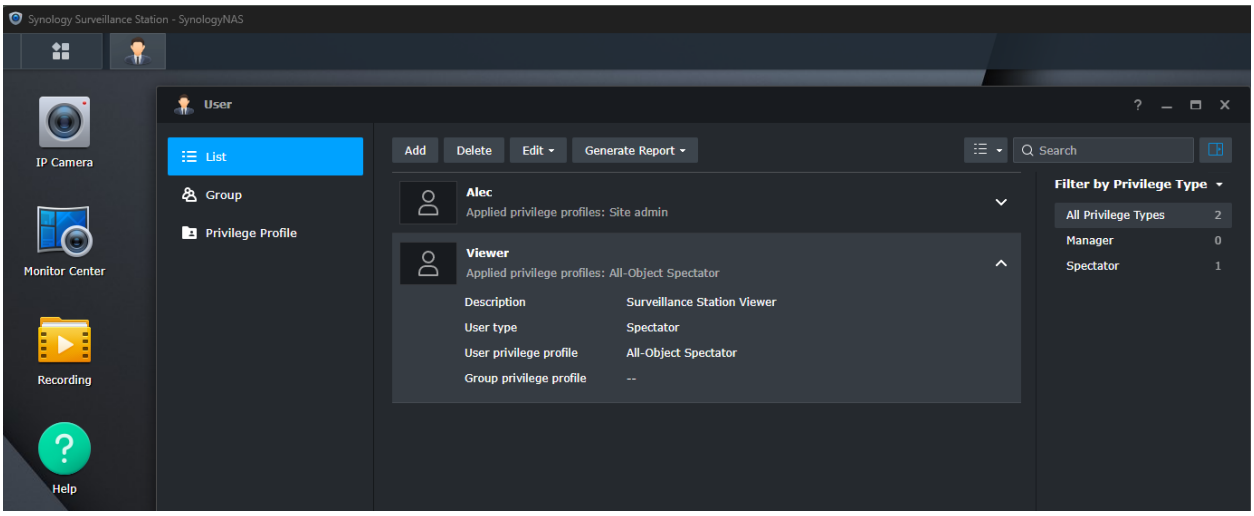


If you have a camera unit with multiple cameras inside you can setup multiple Surveillance Station cameras (all using the same IP address) with each one configured for a different video stream. Some cameras may also allow you to setup a single Surveillance Station camera using a video stream that groups all of the individual cameras together.

Access Privileges for Surveillance Station

To access Surveillance Station, your user account either has to have ‘admin’ privileges, OR you have to ‘grant’ the privileges to a non-admin user. You generally don’t want to use admin privileges for security reasons – but you could.

In the example below, the NAS user ‘Viewer’ has been assigned ‘Spectator’ rights which allows them to ‘look’ at videos but not change anything. You can safely use this user to look at videos without any security risk.



The user ‘Alec’ has been assigned ‘Site Admin’ rights which allows them to add/remove cameras and change configuration values. This set of rights is useful for every day management, however there are several things that even the ‘Site Admin’ can’t do – like add/remove licenses.

To get access to ALL of the features you must log in with a NAS user account that has full ‘admin’ rights.

Accessing Video on a Tablet

You can access your video on a tablet using an app called ‘DS cam’ which you can download. Here is an example of where having the ‘Viewer’ user is directly applicable since you might not trust this 3rd party app and not want to give it ‘admin’ rights when you login.