Networking for Lasershows, BEYOND, and Entertainment

Introduction

A somehow “brief” overview of networking for laser shows and the entertainment industry. As well as understanding how BEYOND (and QS) Utilize your PC and your network to achieve a show. And finally how to tune your system to best handle those specific needs of our protocols and entertainment technology in general. Buckle up and have a coffee ready.

This guide assumes a completely unmanaged network, one where all your switches are unmanaged and there is no “network engineer” on site to make it all pretty and clean, and instead that you are just trying to make your shows more reliable utilizing basic networking equipment. Because of this we may skip over some things for sake of simplicity.

For a bit of context to why this document needs to be made in the first place:

//It is both a great benefit and a known risk that we allow our users to utilize their own hardware with our software, letting them pick their own PC’s and control needs. This is in stark contrast to most show production control manufacturers who sell “processing units” or “consoles” or “media servers” to run their software on. This usually will cost a lot more for the end user but allows quality control in significant ways. By allowing users to choose their own PC’s and equipment, we must then program to the lowest common denominator of pc and setup. As you can imagine, it’s impossible to test every single computer combination, windows update, weird security software etc. on your pc. This can lead to issues on unique PC setups like yours. Thus, this document better informs the users on what to use and how to figure out why their specific setup may be having issues, and what changes they can make to have more reliable lasershows with their setup. //

The Basics of Networking

Luckily you won’t need to become a real network, or IT engineer to do lasers, however you do need to understand a few important things to know and will deal with when working not only in the laser industry but in the live entertainment industry as a whole.

Basically, in a show environment you need to create a network where all devices on the network can communicate with each other, but not outside. This setup is known as a LAN or Local area network. When a local area network gets connected to other networks, its known as a WAN or Wide area network. Technically the internet is a WAN and all the devices in your home if not connected to the internet is a LAN.

For shows we are typically building a LAN between every device on our network we want to communicate with each other and keeping every other device off. You may have also heard of VLAN’s or Virtual Local

Area Networks. Which is where multiple networks are all connected using the same networking equipment and cables, but virtually separated from each other using software on the networking equipment. This show LAN can be expanded to be a WAN connected to the internet for sure, but this is less common in shows and often if people need internet they utilize a secondary WAN just for internet connected to either the Wi-Fi on the device or on another adapter.

Every device on the network needs some sort of identifier for the rest of the devices to know who's who on the network, this identifier is known as an "ip address", or an IP. These are basically ID's that are set for each device so the network can communicate between them.

IP Addresses are set in either two ways, automatically, or manually. We call automatic IP assignment "DHCP" or "Dynamic Host Configuration Protocol". And we call manually set IP addresses "Static IP's".

- Auto IP (sometimes referred to as APIPA or Automatic Private IP Addressing) where every device elects it's own IP address after checking with the other devices in the network that the elected IP address is still available. Auto IP uses IP addresses in the range 169.254.0.1 to 169.254.255.254
- DHCP is where some sort of master looks for devices and gives them ip addresses automatically. This is how your home router gives IP's to things in your house like your phone, laptop, and TV. This is a simple solution and can get devices up and running quickly. But the downside is that every time the network is established, the ip address are likely to change which can cause other issues.
    - Its interesting to note that most devices in "auto ip" or "DHCP" first search of a DHCP server, and if they cant find one, revert to the Auto IP system. This is why device in Auto IP can take a few seconds to connect.
- Static IP is where a human goes to each device and determines what ip addresses each device will have, they will remember this address and will use that device whether it works with the current network or not.

When setting an IP address of a device you will see 3 things:

- IP Address
- Subnet Mask
- Gateway

You will also see options for DNS but this is only really relevant for WAN's.

In most show environments you will only need to worry about two of these numbers, the IP address and the subnet mask. We know what the IP is, but what is the subnet mask? A subnet mask is how you define how broad of a view of the network you want your device to have. This can be wildly complicated but our purpose we will make it simple.

Both IP Addresses and Subnet Masks are comprised of 4 0-255 values in the IPV4 standard, and look something like this:

- 192.168.1.101
- 255.255.255.0

This is a very common setup for a home network. You can imagine this really as 4 tiers of numbers where they are like

1. Universe
    1. Galaxy
        1. Solar System
            1. Planet

So if you wanted devices to to all be in the same solar system, you would put them into the same universe, galaxy, and solar system.

- 192.168.1.101
- 192.168.1.102
- 192.168.1.103

The purpose of a network mask is to identify how “wide” your network is. Generally, this is seen in this format:

- 255.255.255.0

This value identifies that only the last value in your IP addresses matters within your network, If you had multiple solar systems, then your network would need a mask of

- 255.255.0.0

This would enable your network to occupy both the “solar system” and the “planets”.

The mask itself is designed to tell your device how far and wide it should be listening to, or broadcasting to. You can think of the mask value as an increasing and decreasing values of possible IP addresses. A super narrow mask might be something like 255.255.255.240, where there are only 14 possible devices, and a mask of 255.0.0.0 would mean there could be 16,777,214 possible devices. As you can imagine, if a device was doing a “broadcast” protocol, that is a huge difference.

For most people, and most show production environments, its usually safe and easy to just keep things as tight as possible by utilizing a narrower mask.

You may encounter an “IP Schedule” This is where a network engineer has designated devices to be within different groups in a show environment and may look something like this:

1. Lighting 10.1.1.xxx
2. Audio 10.1.2.xxx
3. Video 10.1.3.xxx
4. Lasers 10.1.4.xxx

In this case all your devices for lasers should have addresses that start with 10.1.4.1 and count from there. Often people will start important devices at 10, and sub devices at 101.

Why should you use 10.x.x.x as a prefix? This is because standards boards have designated 10.x.x.x as a “private” network. 10.x.x.x also is within the standard for the art-net protocol, which often leads lots of users to use 10.x.x.x in other disciplines.

Art-net also allows use for 2.x.x.x however, this is classified as a “public” IP address and actually used within addresses all over the internet, and if you connect your local network to the internet you may run

into issues, so we recommend 10.x.x.x as a good starting point, or utilizing the ubiquitous 192.168.1.x prefix as this is also designated as IP addresses for “private” networks.

With this schedule, controllers could be configured to be something like

1. Lighting Network
    1. Consoles
        1. 10.1.1.11/255.255.255.0
        2. 10.1.1.12/255.255.255.0
    2. Artnet Nodes
        1. 10.1.1.101/255.255.255.0
        2. 10.1.1.102/255.255.255.0
        3. 10.1.1.103/255.255.255.0
        4. …… >
2. Lasers
    1. Laser Computers
        1. 10.1.4.11/255.255.255.0
        2. 10.1.4.12/255.255.255.0
    2. Laser Projectors
        1. 10.1.4.101/255.255.255.0
        2. 10.1.4.102/255.255.255.0
        3. 10.1.4.103/255.255.255.0
        4. …… >

In this example network setup, the lighting consoles can communicate with their Artnet nodes, and laser computers can talk to the laser projectors, all within the same wiring infrastructure. This separates them really only in “visibility” and as far as a unmanaged switch is concerned, the data is still first come first serve.

If you wanted every device to be able to talk to the other, allowing for lighting consoles and lasers to talk, for instance, you would want to set the mask on every device to

- 255.255.0.0

This allows the device to see both 10.1.1.x devices and 10.1.4.x devices. Just keep in mind our lesson from masks before, this will widen your network overall, and create a lot more traffic if using “broadcast” protocols.

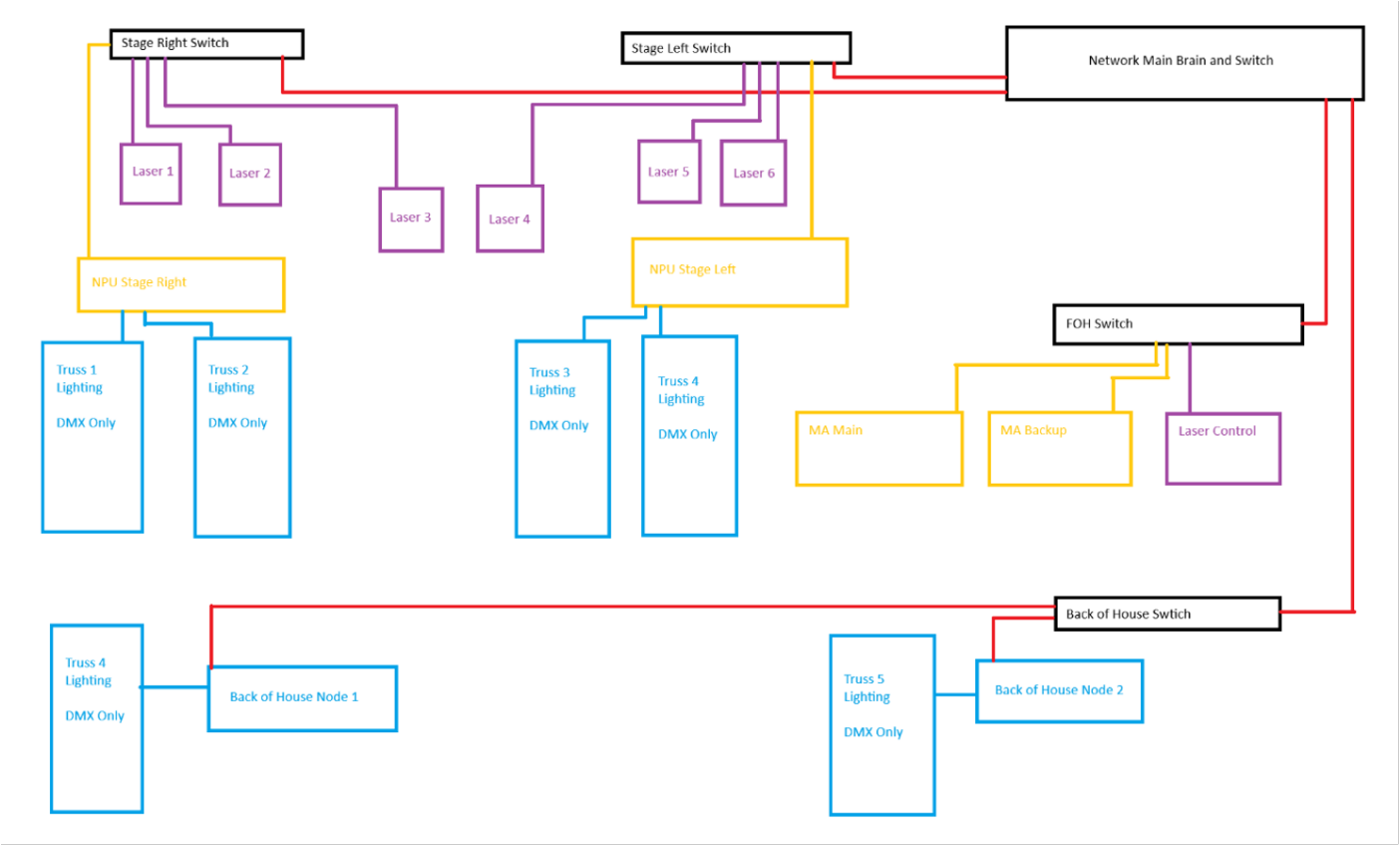
Now if you are after something simpler, then you can leave everything on DHCP/ Auto IP, and if all you have connected to your pc is laser projectors through an “Unmanaged” switch, everything should work fine In this case, your devices will discuss amongst themselves what IP addresses they should be, and set them. And if you want to talk to anyone else (like lighting), you should use a separate ethernet port on your computer.

We ignored “Gateway” previously, but gateways are basically where your device should contact first, this can assist managed networks to help your data navigate the network the way they want it to. In highly managed networks, you will need to set the gateway, and that will be the IP address of the device managing the data. This could be a “router” in some scenarios, or other devices that manage networks.

In a lot of show environments, you won’t need to assign a gateway, but if a gateway is specified for a specific network setup, you will NEED to add the gateway address, or your device won’t be able to connect and communicate.

Basic IP Schedule Example and network layout

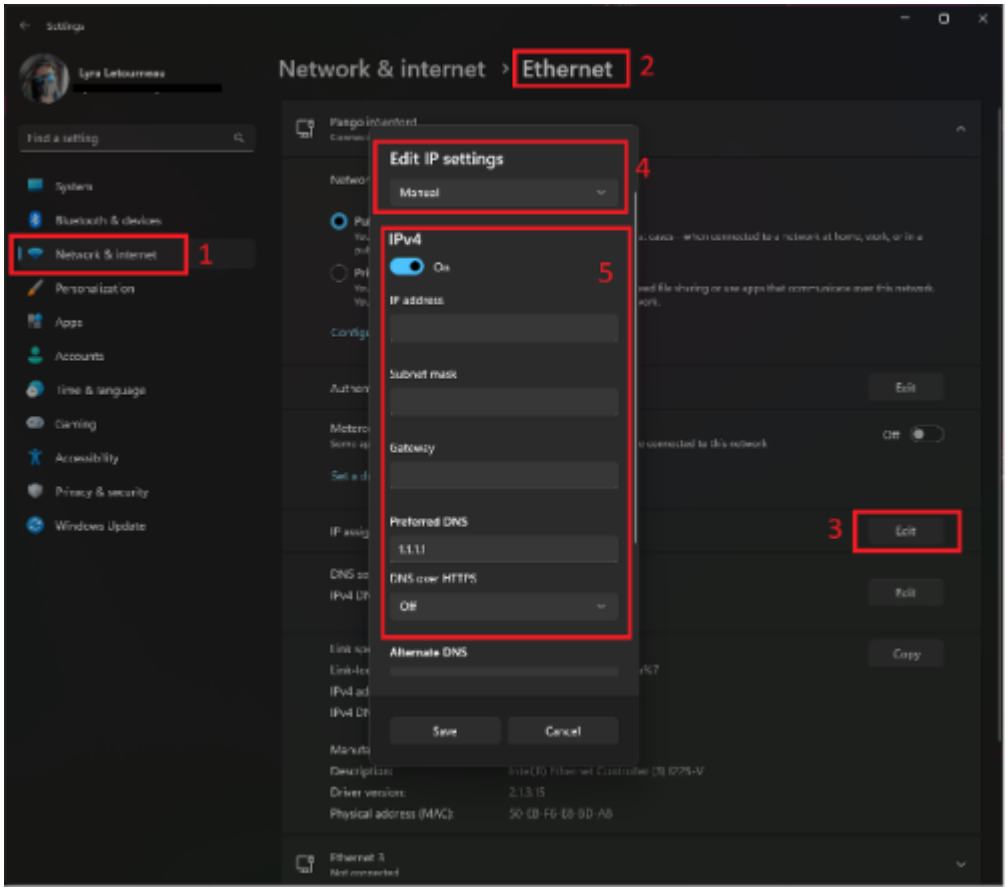
Device	Location	IP Address	Subnet Mask
Grand MA FOH Main	FOH	10.1.2.11	255.255.0.0
Grand MA FOH Backup	FOH	10.1.2.12	255.255.0.0
NPU Stage Left 1	Stage Left	10.1.2.101	255.255.0.0
NPU Stage Left 2	Stage Left	10.1.2.102	255.255.0.0
NPU Stage Right 1	Stage Right	10.1.2.103	255.255.0.0
NPU Stage Right 2	Stage Right	10.1.2.104	255.255.0.0
Back of House Node 1	Spot Tower 1	10.1.2.201	255.255.0.0
Back of House Node 2	Spot Tower 2	10.1.2.202	255.255.0.0
Laser Control PC	FOH	10.1.3.11	255.255.0.0
Laser 20W SR 1	Stage Right	10.1.3.101	255.255.0.0
Laser 20W SR 2	Stage Right	10.1.3.102	255.255.0.0
Laser 10W DSE 1	Downstage Center	10.1.3.103	255.255.0.0
Laser 10W DSE 2	Downstage Center	10.1.3.104	255.255.0.0
Laser 20W SL 1	Stage Right	10.1.3.105	255.255.0.0
Laser 20W SL 2	Stage Right	10.1.3.106	255.255.0.0



Setting IP’s on your devices.

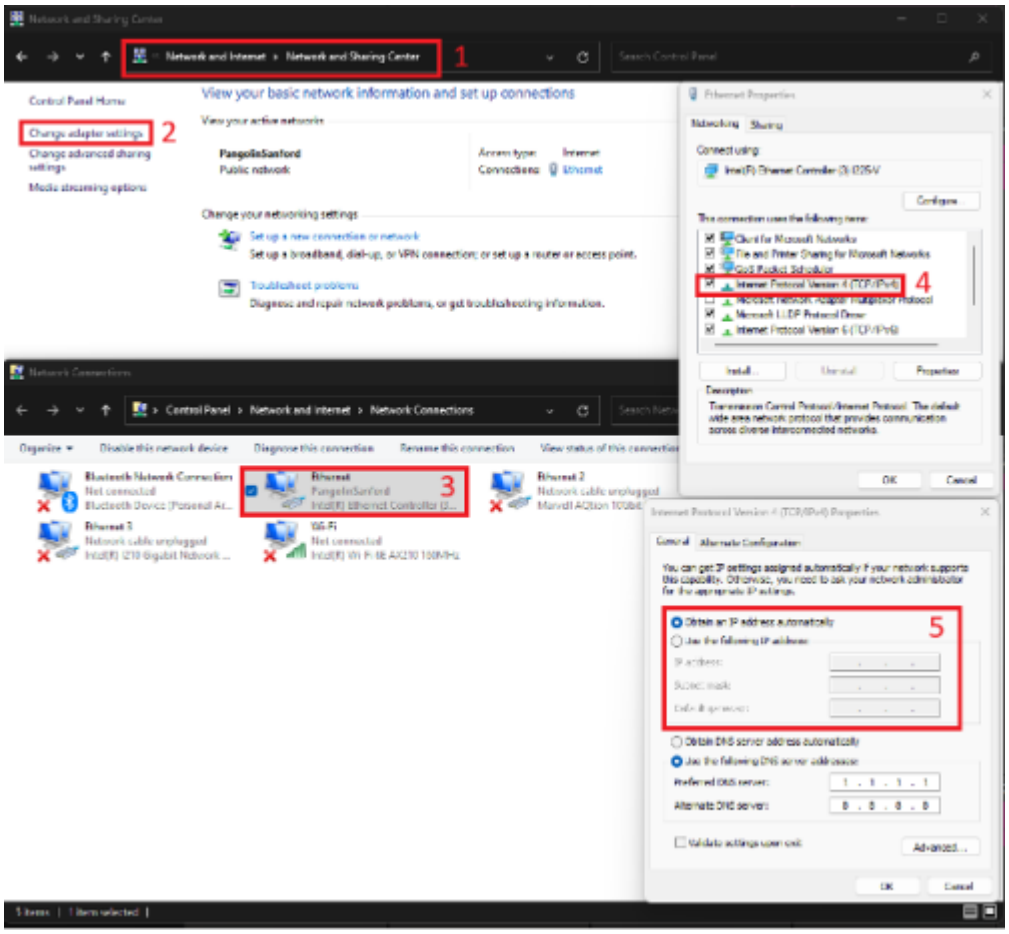
On windows there are two main ways to set your ethernet devices IP, first, and simply in the main windows settings:

1. Go to Network and Internet Settings
2. Select “ethernet”
3. “Edit” IP Assignment
4. Select Manual
5. Enter IP Settings



Or in your control panel

1. Go to the “Network and Sharing Center” (You can search for this in the search bar of Windows
2. Go to “Change adapter Settings”
3. Right click and go to “Properties” on the ethernet adapter you would like to change, All available adapters will be seen in this list, X’s marked next to disconnected adapters.
4. Double click on “Internet Protocol Version 4”
5. Select “use following IP Address” and enter in your IP.



On FB4

Go to the “Network Setup” Dropdown while within a mode that uses network (Like BEYOND Mode). Turn auto IP off until you have a red x. Then enter in the address in the fields below for IP, Mask and gateway. This can also be done in FB4 Settings window.



Types of Data (Packets)

There are also two main types of data that is sent on these networks, TCP and UDP. When data is sent from one device to another, it is sent in small chunks. These chunks of data are called “packets” these

packets can be either TCP or UDP. They are chosen mainly for the biggest difference between them. TCP has guaranteed delivery, while UDP does not.

TCP packets are sent from a host device to a client device first by sending the packet, then once the client device receives the packet, it acknowledges the arrival of the packet to the host device, if the host does not receiver an acknowledgement in time, the host retransmits the packet to the client device and the process starts again. As well, the client device can check the integrity of the data using a checksum.

UDP packets are sent from a host device to a client, and there is no guarantee the packet will actually arrive at the client side.

These differences is why downloading files can sometimes be slow but always deliver a fully functioning file, but sometimes in games people can jitter around and “lag”, one is TCP and the other is UDP.

There are other significant differences between these two packet protocols, but for our purpose in lasers and entertainment, this is the main difference.

How do different network protocols use networking?

If you have setup your IPs correctly, your wiring is good, and the networking equipment can keep up, everything will basically just work.. However.. as you can imagine, that is much easier said than done.

There are a couple caveats. You will often find protocols that are “Broadcast, Multicast, or unicast” These three options basically mean whether the protocol will be sent out to every single Ip, to multiple specific Ip’s, or one individual Ip. Broadcast usually allows data to get to where it needs to go, but is very wasteful and inefficient, that’s where multi and unicast come into play, allowing the user to decide specific Ip’s and devices to transmit the data to. Most protocols decide the option for you as part of the protocol, while others give you the option. This is part of why people may choose one protocol over another.

BEYOND’s laser Protocol

Now that we know how networks work and how to set them up, lets talk about the peculiarities of our laser control protocol we use in BEYOND and why it leaves us with some unique challenges.

There main problem we are concerned with when it comes to the laser protocol over network is speed and timing.

So lets talk about speed, and how fast. When we think about our lasers, we need to consider how fast they actually are going. In extreme cases, if you had 60kpps scanners, frames with 200 points, you are talking 300 frames a second! Multiply that by tens of lasers all needing to be perfectly synced with each other, now you’re talking a lot of data that needs to be perfectly synced.

Synchronization is also very important, every single laser in your rig needs to be perfectly timed as well, as if they are all slightly off, you may not necessarily “see” it, but you will “feel” it.

To achieve this synchronization, first, all FB4's on the network sync with the PC and each other to have the exact same "clock time" with each other. On the BEYOND side, the software calculates every lasers next frame, caches these frames, and when they are all finished they are given a "display time" for a few milliseconds in the future and sent off down your network port, to your switches and to each laser. Over the next couple milliseconds every laser controller in the rig receives their frame, and waits for that "display time" to come to output. When that time comes, they all display the frame they got for that moment in time.

This is how BEYOND keeps every single laser in time with each other, enabling smooth output and things like distributed scanning. The controllers just get a heartbeat signal that keeps all their clocks matched up and things are synced.

When networks are slow, or data is getting damaged by overloaded switches, or bad cables, the TPC process can be slowed down immensely, causing tons of rebroadcasted frames, and frames will "miss" their "display time" and you get "lag" or no output. Often, waiting for a rebroadcasted frame can take tens of milliseconds, which lead to extremely late frames.

So, wait, are you using TCP or UDP for BEYOND?

Historically, we have utilized TCP for its delivery guarantee, and while there were a few builds that did make it to the public in early 5.0 days to try and utilize UDP we did revert back to TCP and BEYOND has used TCP for the majority of its life. This has many benefits and drawbacks as you see from the next section of this document. This choice is not final however, and we have continued to do testing and experimentation with UDP instead. And it may very well make it into future versions if deemed more reliable. For the average user. Of course, if the rest of your network is solid, it wont really matter, but those nuances are for when things go wrong.

Why fames get "delayed"

Now most users who have done laser shows will have seen the "purple fb4" notification and may even have heard this means "frame delay". Now that you know everything from this document from above hopefully you can see how things can get delayed and you get the purple notification.

Two types of frame delay:

- CPU (Computer) induced delay.
- Network induced delay.

First lets discuss CPU. When BEYOND calculates all the frames for all the projectors in your setup, it live calculates everything, and the process looks something like this:

Cue Frame> Cue effects> Cue Timing> Live FX> Routing> Projection Zone reshape> Projector settings application> Packaging> Delivery

BEYOND does repeat similar frames, and does some optimization, however when lots of effects, different routings, (or the real challenge), offsetting effects are introduced, this drastically increases the calculation time for output. This leads to your computer not being able to actually calculate every single

frame before the cycle time expires and BEYOND needs to start over. This cycle time is important for speed and timing and safety reasons like the previous chapter describes.

CPU induced delay will often appear in real life in dropout or lag in order of zones. Where the first few lasers in your setup may be running fine but you may not even get any output out of your last few lasers, where it degrades more and more between each end. This is an example of very obvious CPU delay.

Secondly, network induced delay. This is when data makes it out of BEYOND, but doesn't make it to the laser controllers before the "display time" they are expecting the frame by. This could mean it failed the TCp-IP check, it could mean it never received anything, or it could mean it was receiving the data when the time elapsed. Either way the data didn't make it in time, and the fame it was expecting (or if it got it late) has expired. Of course, frames need to expire for the speed and timing and safety concerns from before.

Network induced delay is a little more complicated because it can be many factors at play, but lets talk about the general steps data has to make it through, and the common reasons that part can cause issues.

- Network adapter on your PC (or USB ethernet device)
    - Network port is just too slow (USB 2.0 devices, or 100mbps only devices)
    - Network port is busy with other data (like other software, VPN's, other protocols etc.)
    - Network port is trying to be energy efficient and becomes slow
    - Network port is tuned to prioritize UDP packets (usually this is for keeping your online games from lagging)
    - Network port is trying to encrypt the data, or send it to the wrong place first (VPN's, security software, unneeded gateways etc.)
    - Network adapter is underpowered for 100m run (this is becoming more common with network adapters, especially USB 3.2 devices utilizing the ASIX AX88179A Chip, as this chip that cannot meet the distance specifications and issues appear after 10 meters of cable length)
    - Network adapter is set to the wrong speed.
- Cables in your setup (especially the home run)
    - Cables that are damaged may still connect but run at slower speeds.
    - Cables that are too long will degrade data and cause increased rebroadcasts of data, (general top rating is 100 Meters, best to use less than that if you can, and if you need more use switches or fiber.)
    - Cables with bad shielding may degrade performance when run next to high voltage power, or other noise inducing electronics.
    - Connectors making bad connections (corroded terminals and connectors, or that don't lock due to missing clip)
- Network Switches
    - Switches may have management and are trying and absolutely failing to move data where it needs to go fast enough.
    - Switches may not have the "packets per second" throughput needed to handle the very high number of frames, high FPS and high projector count setups nay need.
    - Switches may have high performance ports and lower performance ports, and homerun line to the PC may be connected to a lower performance port.
    - Switches with management may block data or prioritize other data delaying laser data.

There are even more particular situations that can be introduced but this is a good list of the most common issues.

How do you determine if it's CPU or Network? Utilize the updated in 5.2 FB4 Data Transmission monitor located under System>Monitoring> FB4 Data Transmission Monitor, under the "Overview/ NetStat" Tab. If you are having issues, icons will appear in the top rows next to your projectors. Use the Key below to determine what kind of issue is happening.



Buying and Setting up your PC for success

When purchasing a PC, you should consider how big of laser shows you will be doing, will you be doing multiple protocols at once? Do you intend to use video output? Do you love 40 lasers from one pc and offset effects every single one? Well, you will need a powerful enough pc to achieve this, our processing requirements are closer to video than to lighting so treat it that way. Get a modern high-performance pc.

Rough specs to choose:

- i7 or i9 intel CPU, Modern
- 16GB of ram is fine for most laser shows, 32 GB of ram if you intend to run multimedia.
- Get some sort of GPU, just make it a discrete GPU not integrated, Nvidia 3060 class (or generational equivalent) is fine, just to offload the GUI to the VGA. Some things in BEYOND may be calculated on the GPU in the future, so best to be prepared.
- Get an NVME based Hard drive, they are fast and more durable than spinning drives, or even run beyond on portable SSD's so the install can travel with you to any pc, but that's another topic for another day.
- Intel based Networking port.

- Lots of USB IO, lots of our accessories we use are USB, you will need the ports.
- Touchscreen is always nice.

When purchasing a PC, you should look for PC's with Intel based network ports, these seem to be the best setup to handle our protocol out of the box, Realtek is fine as well, but the one to be worried about is "Killer" ports. These ports are set up for gaming and seem to prioritize every single data packet before ours. Unfortunately, most gaming computers which people use for show production these days come with killer ports. If you have a Killer port, do yourself a favor and get a USB ethernet device using intel or Realtek chips/ drivers. And a completely fresh install of windows will help as well to rid the killer software running the ports.

Killer port issues may become irrelevant if in the future we switch to UDP communication.

Often you can find Intel or Realtek chips not on "gaming" computers, but "workstation" PC's, high performance computers targeted at creative professionals, they generally are better setup for our needs.

The first thing you should do for a show computer is install windows from scratch, this computer is not your personal gaming computer anymore, it's a dedicated show computer and a completely fresh instillation of windows allows you to get rid of any bloat and give you a good baseline to start with.

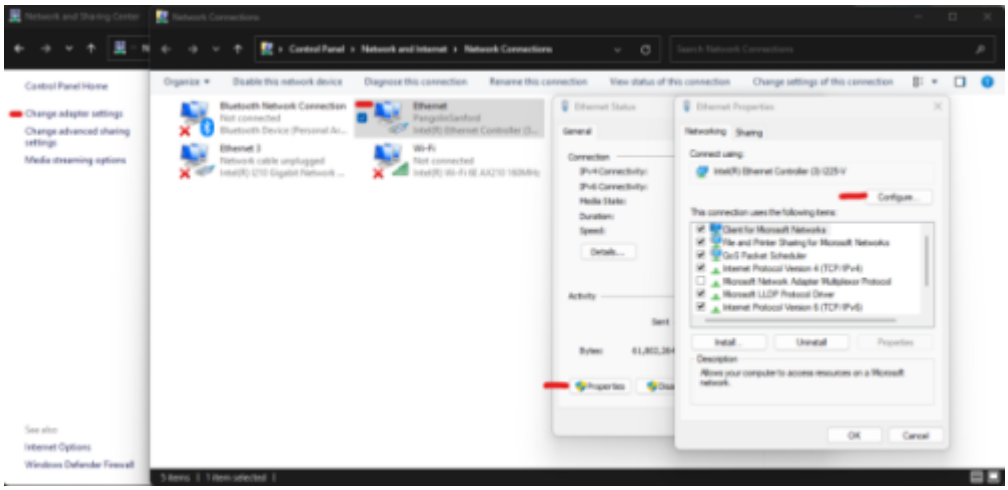
Use as little security as possible. This may seem counterintuitive, however the less things interacting with your network the better. Just use your show computer as a show computer and utilize internet for work and you should be fine. Turn off firewalls, don't use 3rd party security software etc. Windows defender on its own usually is fine and you don't need to turn that off. BEYOND when first started, will run a small app that will disable the firewall functions that inhibit BEYOND data, so you probably won't have to worry about firewall.

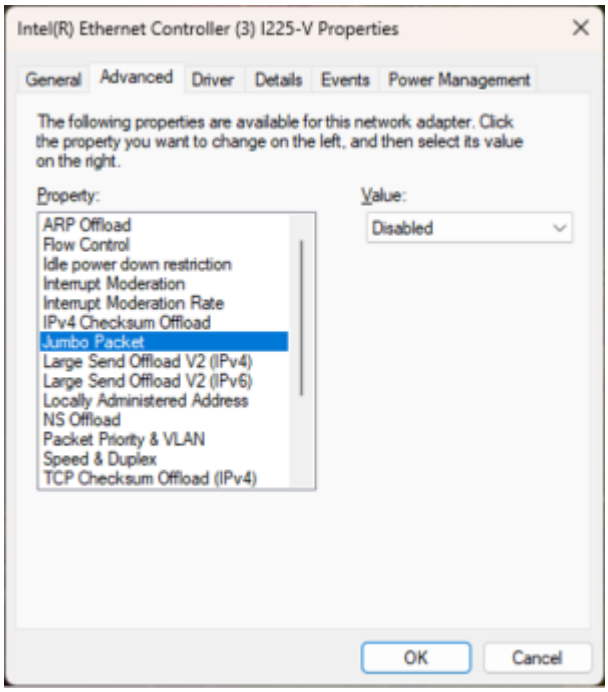
Disable Windows Updates, if you are on windows pro versions, you can do this through the UI pretty easily, however if you are on a Home version, you need to disable windows update through the "Services.msc" application. Here is a good guide on Toms Guide

If using a laptop, disable all power saving options. There are a lot of them, go through as many places as you can to disable all power savings options, sometimes they exist in the bios of your laptop and there are a few inside of windows itself. Here is a basic guide on the Microsoft forum.

If using multiple protocols in your rig, separate them onto different network ports and networks overall. Utilize USB ethernet devices, or if on a desktop install add in cards that give you more ports, this allows you to also ensure they are intel based.

Sometimes, you may need to do driver-based adjustments, including disabling "Jumbo Frames", "Energy Efficient Ethernet" and other driver level features. Found in this chain:





Some extra steps you can take:

- Uninstall everything you don’t need from the windows install.
- Turn off all windows telemetry.

These can be achieved utilizing .bat files you can find online but proceed with caution and do your own research on that, you can very much install viruses or completely ruin your install/ break your driver if done incorrectly so I will not be providing documentation, or bat files. If this seems like something you want to do, research it.

Choosing network gear for success

As a laser technician and not a networking engineer, there are probably two choices you should consider when purchasing networking equipment.

- High performance Unmanaged Networking equipment

If you don't want to break the bank, your best choice is to grab high performance unmanaged networking equipment, unfortunately these are few and far between as generally those who need high performance, like to play around and create unique settings, but for most show production technicians, they just want to plug it in and for it to work. It can be tempting to purchase low grade and consumer level networking gear for home networks like cheaper TP-Link, or Netgear for example. Especially because "FB4 only has 100mbps on it anyway!!". but instead, you should purchase something like Cisco's small business unmanaged series.

These devices are not that much higher price, but have the CPU built in to handle the amount of data, and low latency requirements of our industry. You can find similar products from other industry brands like Mikrotik, Netgear, TP-link, Zyxel and more.

Show Production Specific Networking Equipment

If you have more money to spend, and are looking to do some V-Lans, and make things a bit easier for yourself, then there are several companies who build and sell switches designed to do this. Some of the more popular ones are:

1. Luminex
2. ProPlex
3. Swisson
4. Pathport

Their products aren't cheap but do provide enterprise quality networking equipment while making it plug and play and easy for most show production professionals to set up and use quickly and easily. They also usually include pre-sets for common industry protocols to ensure the data is most efficiently transmitted.

Fast and high-performance switches are important because not all "1gbps" ports are created equal. As discussed before, our protocol is actually very sensitive due to speed, timing, and safety. Fast networking equipment not just from a port speed level but an actual "packets per second" level is very important to allow the data to fly through the networking gear without issue. And when the network gets saturated with multiple protocols and tons of devices, this is extremely important.

Cabling, it may all seem the same, but we recommend getting cat6a category networking cable. It has a lot more speed in case things break, and they all come with solid plastic cores that improve strength and durability.

You can buy very nice expensive "production" ready networking cable if you want, and it will be more reliable, but you can buy cheaper cables, and get the reliability out of purchasing cat6a instead of cat5e.

Summary

If you have been doing lasers for years and never had an issue with auto ip, great! Congratulations! But

I’m glad you still went through and read this whole document to familiarize yourself with how networking works, and how we utilize it to create our beautiful laser displays. You did read the whole thing, right? And not just skip to the summary hoping there was a tl;dr? well sorry but you will need to read the whole thing.

Creating a strong, reliable, and capable network can be very complex when you start to dig into it. And if all you are doing is plugging in 10 lasers to one unmanaged switch and plugging your pc into that using auto Ip, it will probably always work, but simple is never the name of the game in production.

By following all these steps, following best practices, etc. you minimize the risk of your network failing you on a show and gives you a better result overall when doing your shows. Hopefully to the point where you will never experience any issues.

Appendix Situations:

- If you have found yourself with a laptop with a killer ethernet port, you will need to not only utilize a USB ethernet device to not use the killer port, you will also need to format your windows computer to remove all piece of the software, as it will try and manage other non-killer ports you attach to your pc.
    - It is possible to massage killer ports into functioning fine, but to be honest its not worth the trouble and its just easier and cheaper to purchase a separate device.
    - If BEYOND stream changes to UDP, Killer ports will actually become the best ports to use, so it’s not necessarily a bad thing, but important to understand.
- USB 3.2 Gen1 USB to ethernet adaptors. It seems a large number of these devices are utilizing a chip from ASIX named AX88179A. These adaptors are causing issues due to the devices’ inability to be stable at cable lengths over 10M.
    - If you already have one of these devices or are experiencing issues with your USB to ethernet device, use a switch and a short cable at FOH before your homerun to stage, this should clean things up.
    - Or just buy a non USB 3.2 specific ethernet adaptor.

Just tell me what to buy!

Here is a link to our amazon store to what we use internally, and you may find useful. These products are not “Guaranteed” to work every time, but we wouldn’t put something on this store that gave us issues.

LINK

From:
http://wiki.pangolin.com/ - **Complete Help Docs**

Permanent link:
http://wiki.pangolin.com/doku.php?id=beyond:system_and_networks&rev=1698334441

Last update: **2023/10/26 17:34**