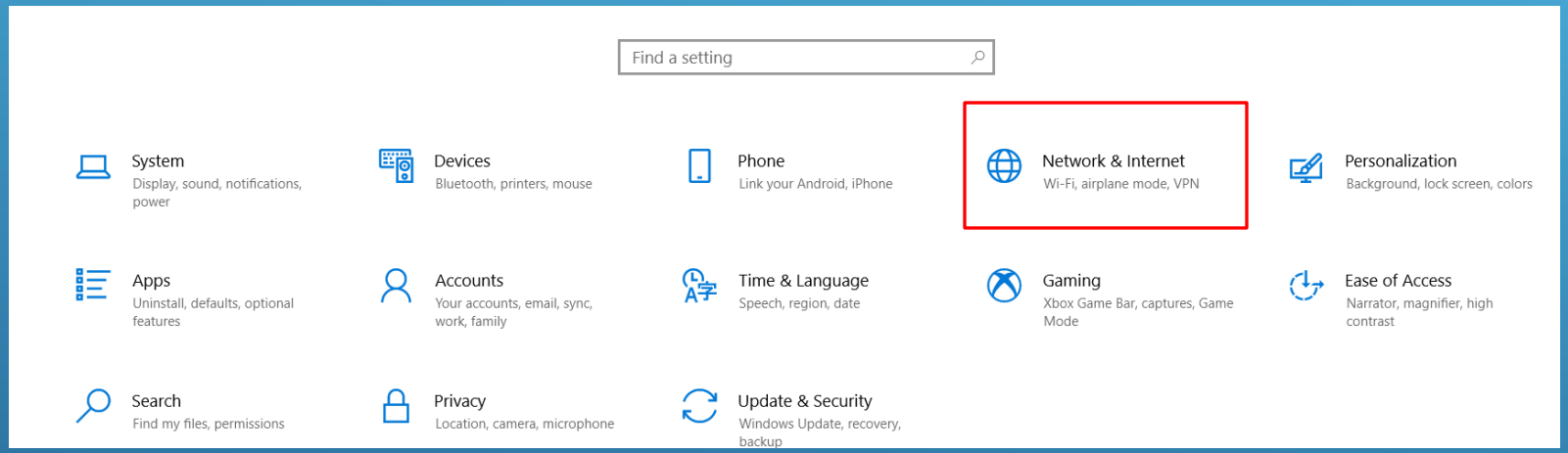
Vigitron Technical Series

Accessing and Programming Your Network

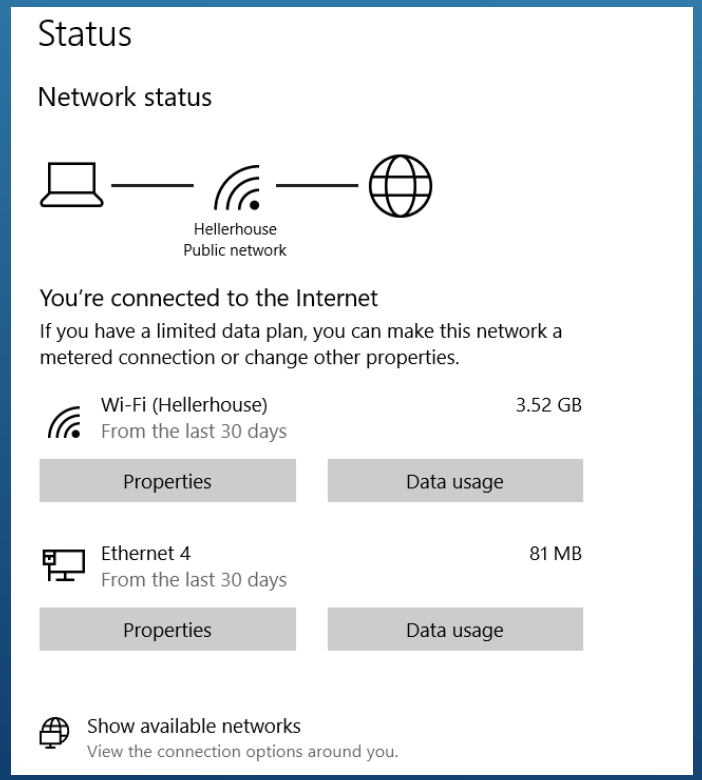
VIGITRON

Setting up your Computer

Setting Up Your Computer :



Window Settings



Shows all your connected networks

You can maintain different network connections such as direct network connection and wifi however you will only be able to access one network at a time

Change you computer settings

Ethernet

Ethernet 3
Not connected

Ethernet 2
Not connected

Unidentified network
No Internet

Select Change adaptor options

Related settings

Change adapter options

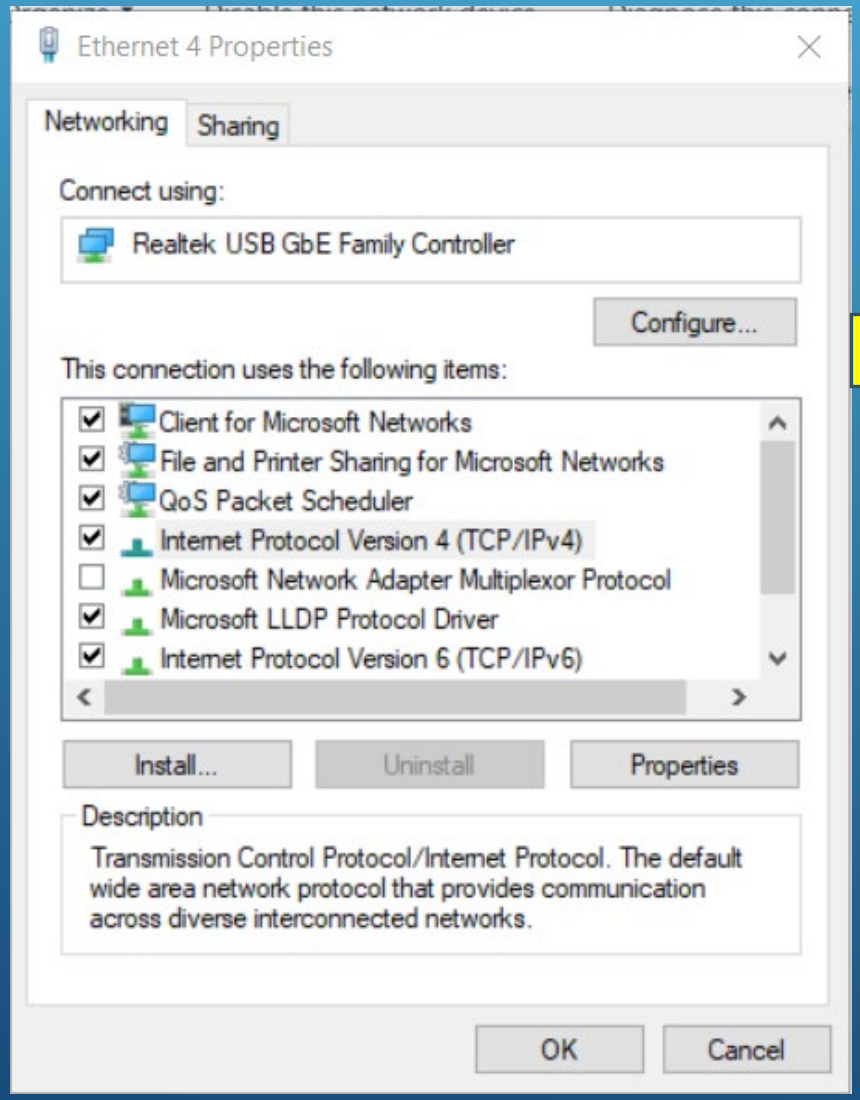
Change advanced sharing options

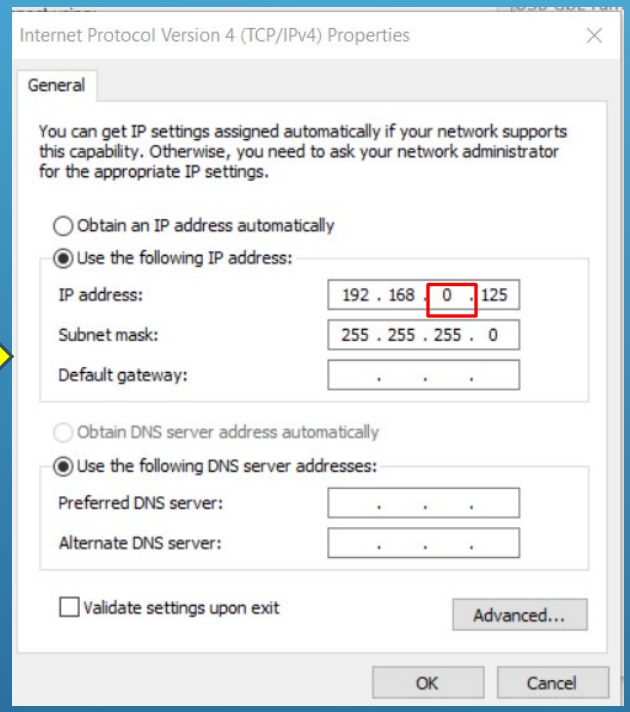
Network and Sharing Center

Windows Firewall

Your active network connections will appear
Select your network and right click and select properties

Change you computer settings





Make certain your computer is on the same network as the switch or the connected device

You cannot have the same address within a network on more than one device
The last 3 digitals are the most important

Select Internet Protocol 4 (TCP/IPv4) to enter new IP address and subnet if needed.

IPv4 uses 32 bit addressing while IPv6 uses 128 providing almost unlimited address numbers and higher security. However it is more complex. As such its use is limited to highly secure network and in some cases mobile

In General you will encounter Class A or Class C networks

Independent networks will generally use Class C
Networks where the security network is integrated into the larger corporate network will use Class B

IP Class	Address Range	Maximum number of networks
Class A	1-126	126 (2^7-2)
Class B	128-191	16384
Class C	192-223	2097152
Class D	224-239	Reserve for multitasking
Class E	240-254	Reserved for Research and development

Used for a large number of hosts- up to 16 million

Most used by corporations due to security

Used for smaller local area networks

127.0.0.0.0 is a special IP address called a loopback address. It is used for the local host such as your host computer an enables the host to transmit and receive data. This allows the connected device to transmit and receive its own data packets.

Determine your Network

In order to access your network switch or any other connected device your computer must be on the same network.

It can be possible for your switch and connected devices to be on different networks

Addressing is based on 1 and 0 – or base 2 and can be 8,16 or 24 bits. – so the highest number is 256 which includes all connected devices

192.168.1.100

Network | Host

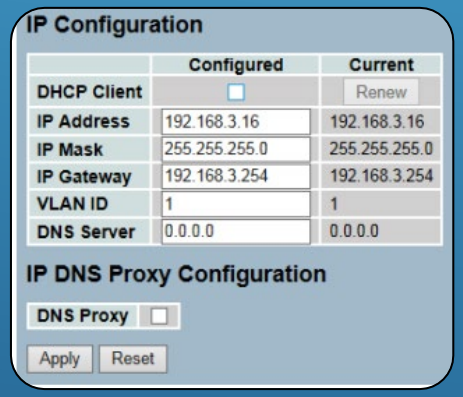
192.168.0.100

Network | Host

Similar Addresses but completely different networks: The key is the third series of numbers

Same Subnet

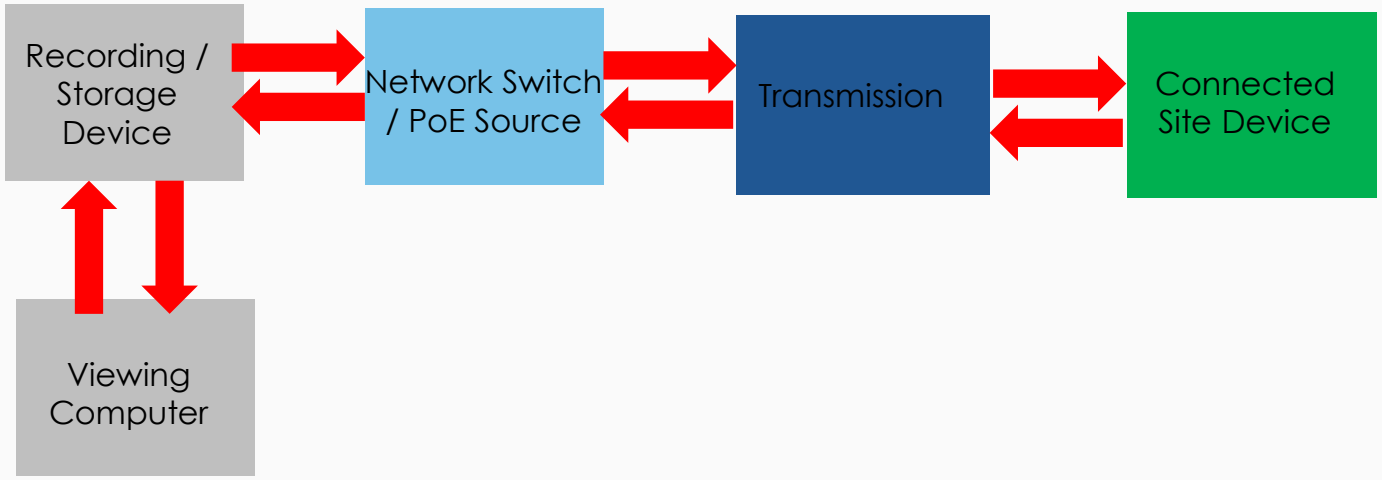
All Addressable components should be on the same subnet with conflicting IP addresses.



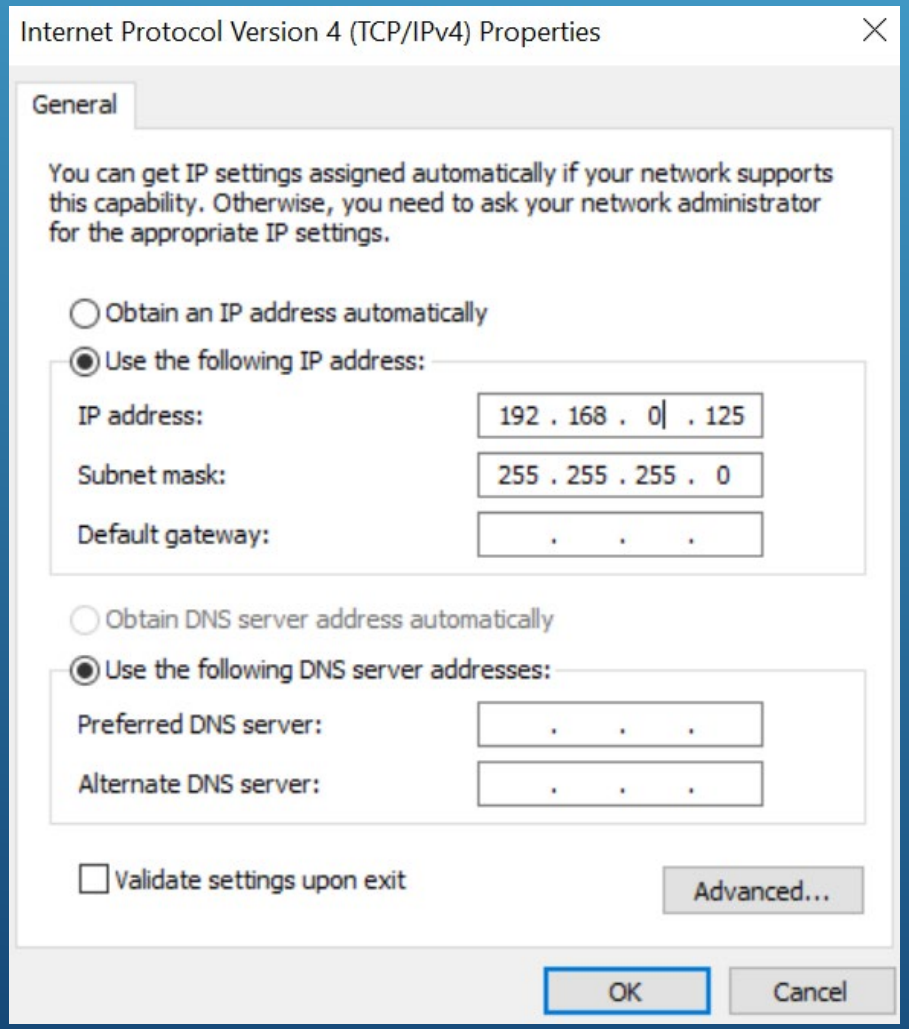
192.168. 3. 16 XXX

All address should be on the same subnet

All connected devices should have different addresses



Addressing your Computer – Defining the parts



A **subnet Mask** defines the range of IP addresses that can be used – the range is the same 0-255 as the address divided into the same format. – The length of the subnet is important

Default is 255.255.255.0 = 24 bits
255.255.0.0=16 bits
255.255.255.255=32 bits

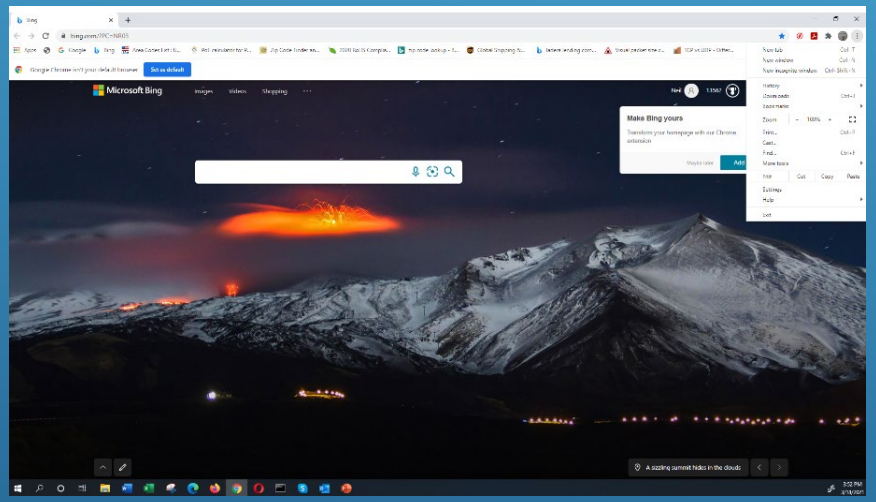
Think of each section as 8 bits 2*8

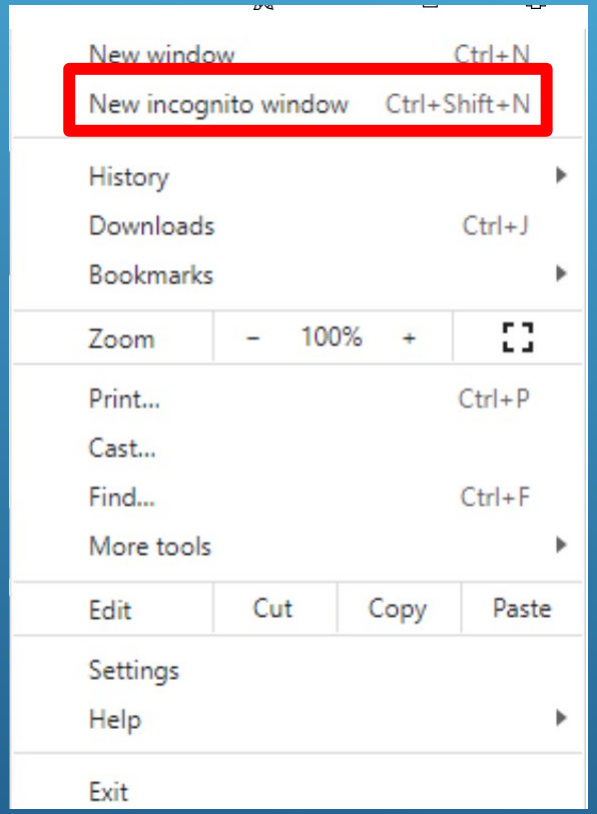
A default gateway is used from the client to other networks outside of its own network – It is generally used for Internet applications. As security networks are internal – it is not generally used

A DNS or Doman Name System – coverts website names into addresses – when access a website you enter the name and not the address As security networks are internal – it is not generally used

I Can’t Log In

I changed the switches (Cameras) IP address and cannot log in.





Various web browsers especially Chroma can retain previous pages preventing log in with IP address

2. Defining Network Operating Problems and Solutions

- Webrowers

Do not use webrower standard modes

Standard modes maintain Browser History/Cookies/ and Temporary Internet Files. All of these can prevent you from access the your network web based devices, naming switches

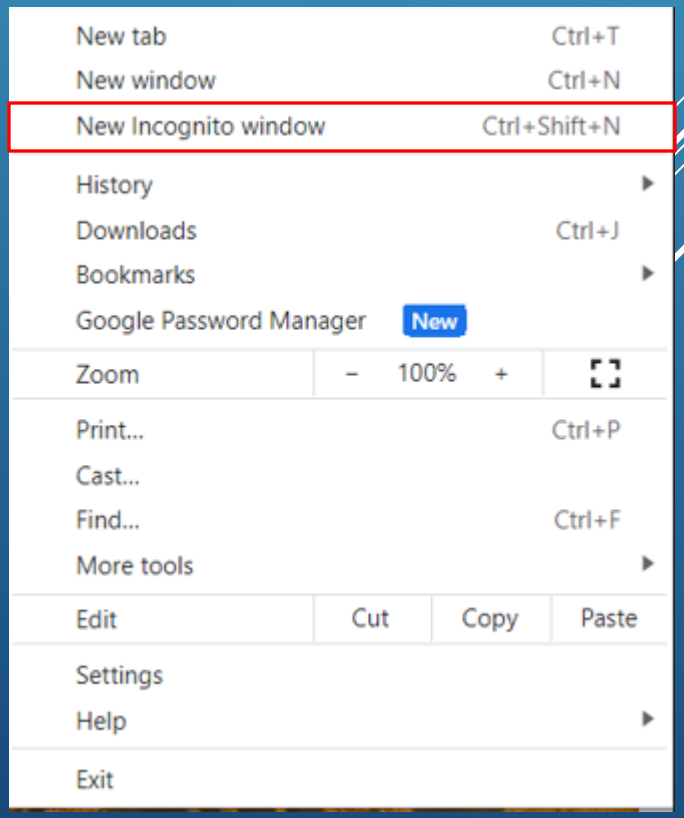
Accessing you Browser's Private Mode

Browser	Mouse	Keyboard
Chrome	Settings (top right) & New Incognito Window	Ctrl + Shift + N
Edge	Settings (top right) > New InPrivate Window	Ctrl + Shift + P
Firefox	Settings (top right) > New Private Window	Ctrl + Shift + P
Brave	Settings (top right) > New Incognito Window	Ctrl + Shift + N
Safari	Settings (top right) > Private mode	Shift + Command + N

Method one: Keyboard

The following Example is Google:

Method Two:



3. Switch Port Setup and Problems

IP Configuration

Mode	Router	
DNS Server 0	No DNS server	
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	☐	

Not Recommended to use DNS due to security reasons – Security networks are enclosed networks

DNS (Domain Name System) Proxy server is found between client an individual server to protect the clients IP addresses

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
☐	1	☐	0		192.168.0.150	24		
Delete	0	☐	0					

Related to DNS

Add Interface

VLAN 1 Must be maintained

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
Delete				0

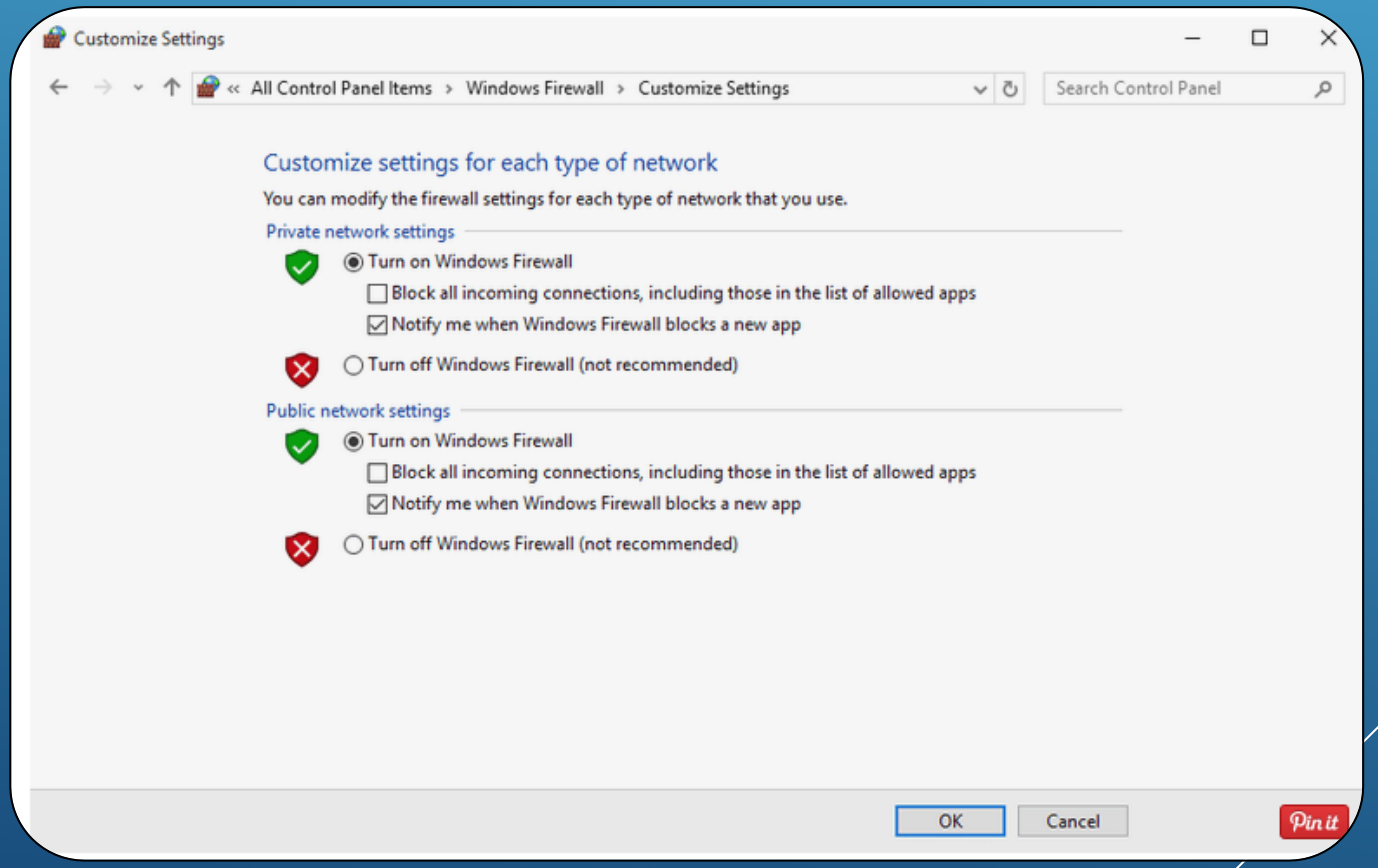
Add Route

Save Reset

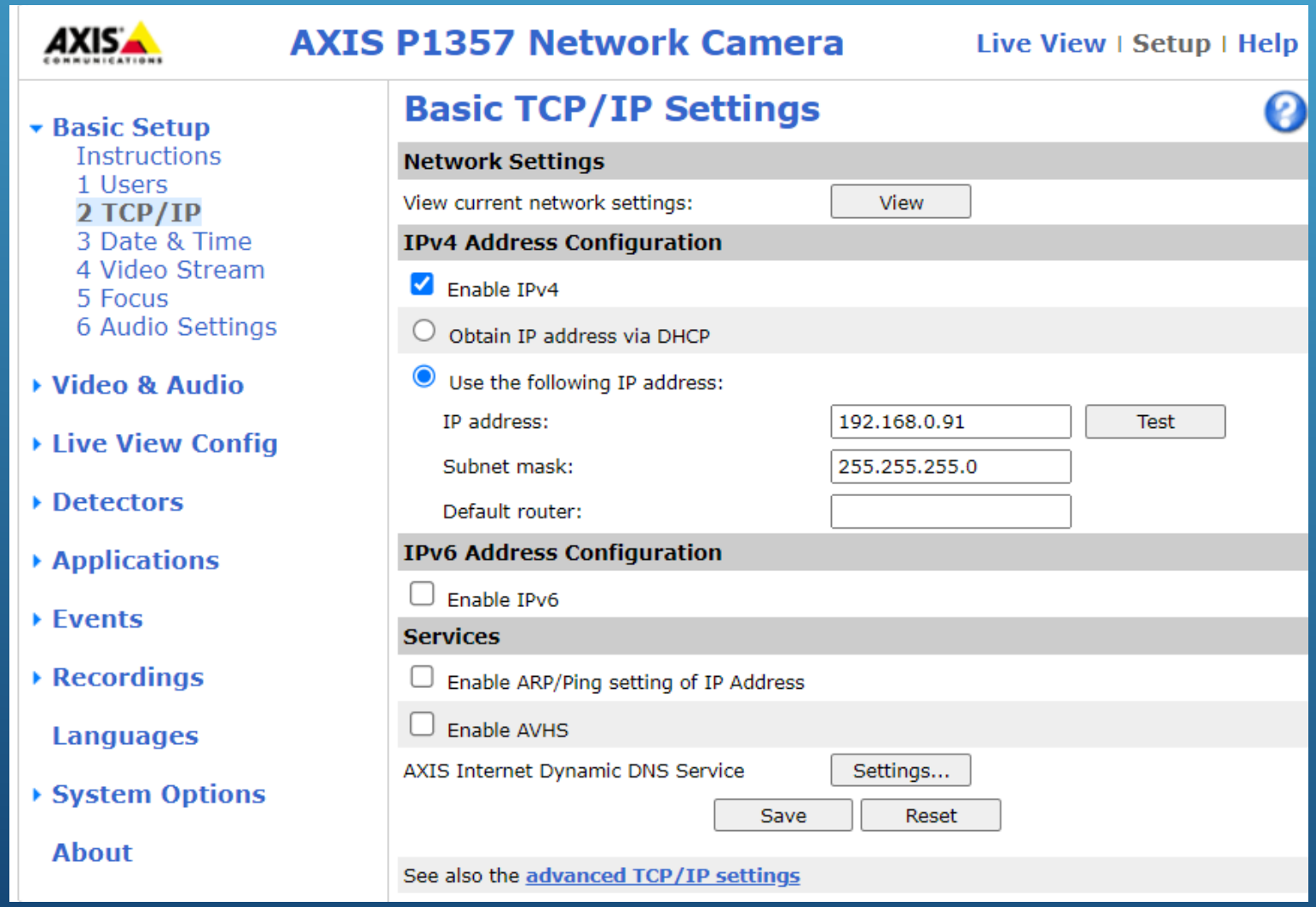
IP Route defines a static IP address connection (Layer 3 Lite) – *Next Hop is a IPv6 link based on the Gateway*

Firewalls

If you are using firewalls, you may have to turn them off.



Camera and other connected devices have their own individual network integration



Testing The Connection

ICMP
What does it tell you---if you have a connection
What doesn't tell you
a. Packet size handling
b. Quality of connected device transmission

ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Internet Control Message Protocol
Ping Length is packet size- limited to non jumbo frames
Ping count- number of pings transmitted
Ping interval – duration between pings

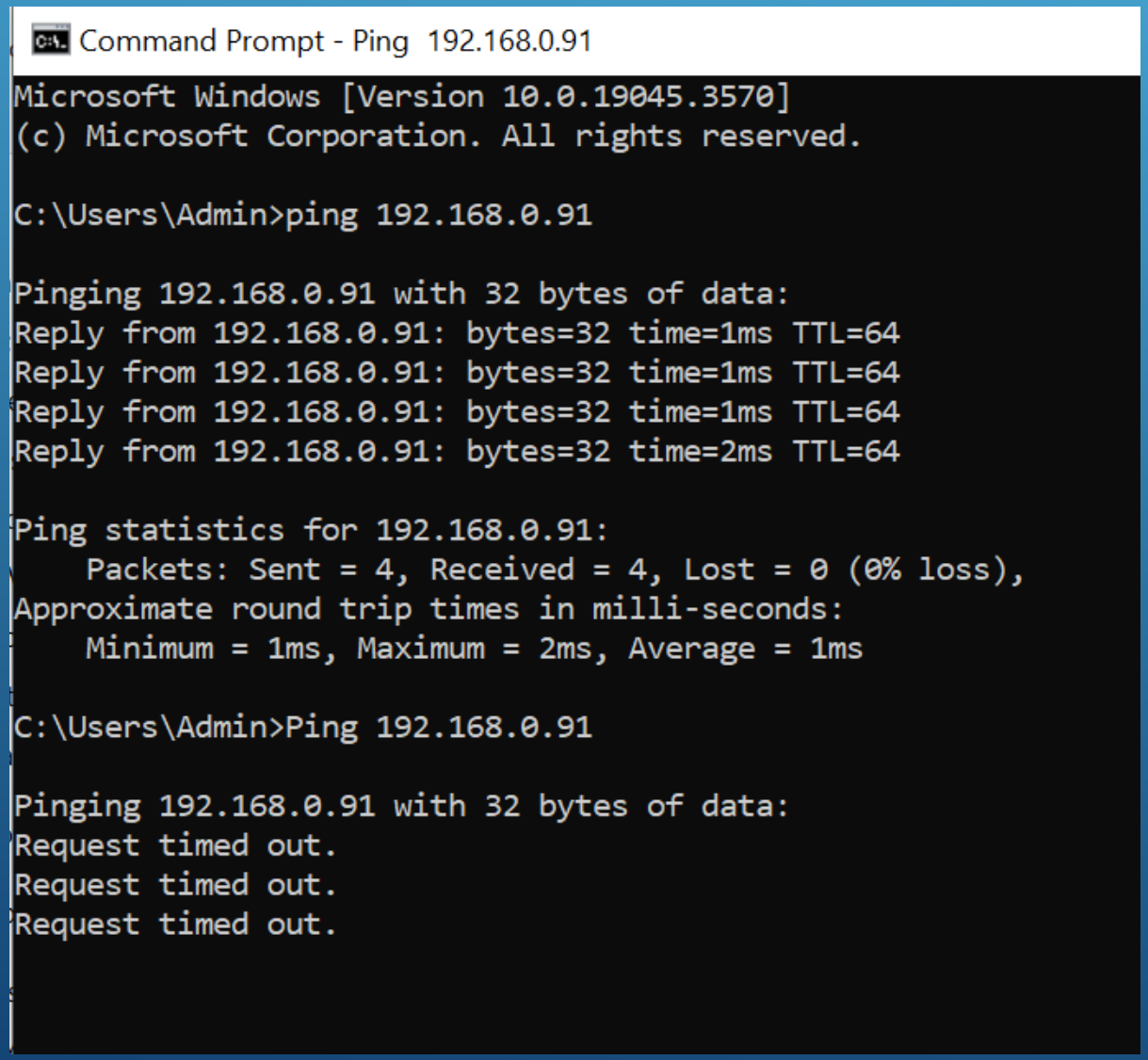
ICMP Ping Output

PING server 192.168.0.91, 56 bytes of data.
64 bytes from 192.168.0.91: icmp_seq=0, time=100ms
64 bytes from 192.168.0.91: icmp_seq=1, time=0ms
64 bytes from 192.168.0.91: icmp_seq=2, time=0ms
64 bytes from 192.168.0.91: icmp_seq=3, time=0ms
64 bytes from 192.168.0.91: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

PING server 192.168.0.91, 1452 bytes of data.
1460 bytes from 192.168.0.91: icmp_seq=0, time=40ms
1460 bytes from 192.168.0.91: icmp_seq=1, time=0ms
1460 bytes from 192.168.0.91: icmp_seq=2, time=0ms
1460 bytes from 192.168.0.91: icmp_seq=3, time=0ms
1460 bytes from 192.168.0.91: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

Sequence number- will increase by one
Time – duration for the reach the connect device and come back to the source

Alternative Ping Method using a computer



Traceroute- tells you how the data travels from source to destination
What does Traceroute mean—Latency – why does my connection time out

Traceroute

IP Address	0.0.0.0
Max TTL	30
Wait Time	5

TTL- Time to Live: Duration until transmission is no longer valid- 0=packet is turned off

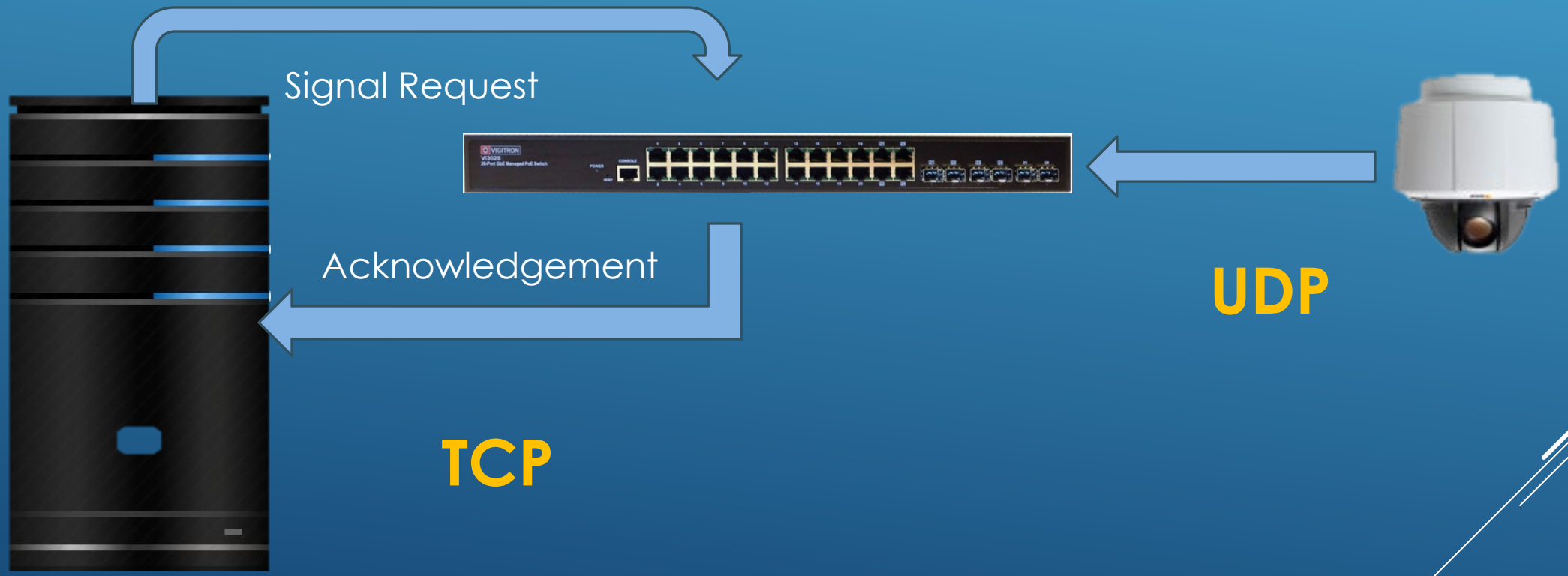
Time between packet transmission

Traceroute Output

traceroute to 192.168.0.91 (192.168.0.91), 30 hops max, 56 byte packets
1 192.168.0.91 70.580 ms 100.241 ms 36.964 ms
Traceroute complete

Hop=the number of hops from the port to the connected device and back – 3 packs are sent and each time is displayed.- Applies to TCP not UDP

Security Network Communication Path

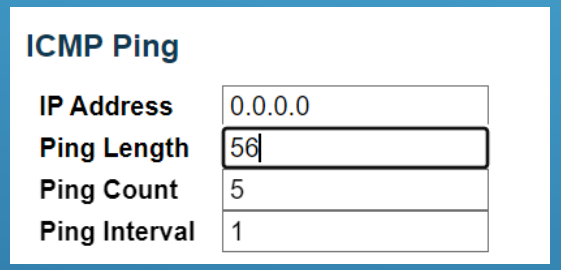


Differences between Ping and TraceRoute

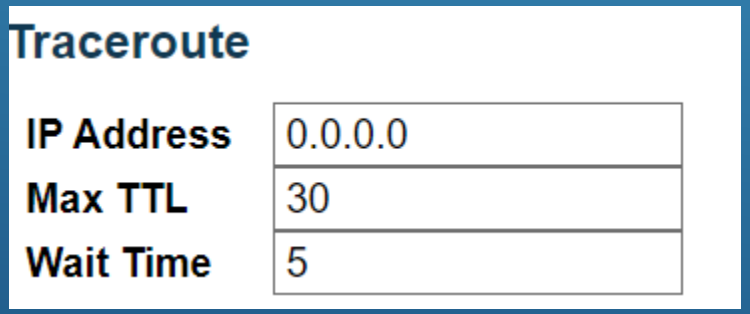
Do I have a **connection?**

Why is this important: You need to see if the switch port is actually connected to the remote device.

Cameras are usually UDP Communications which are one way



What is my connection path and how long does it take me to get there- **Latency issues**



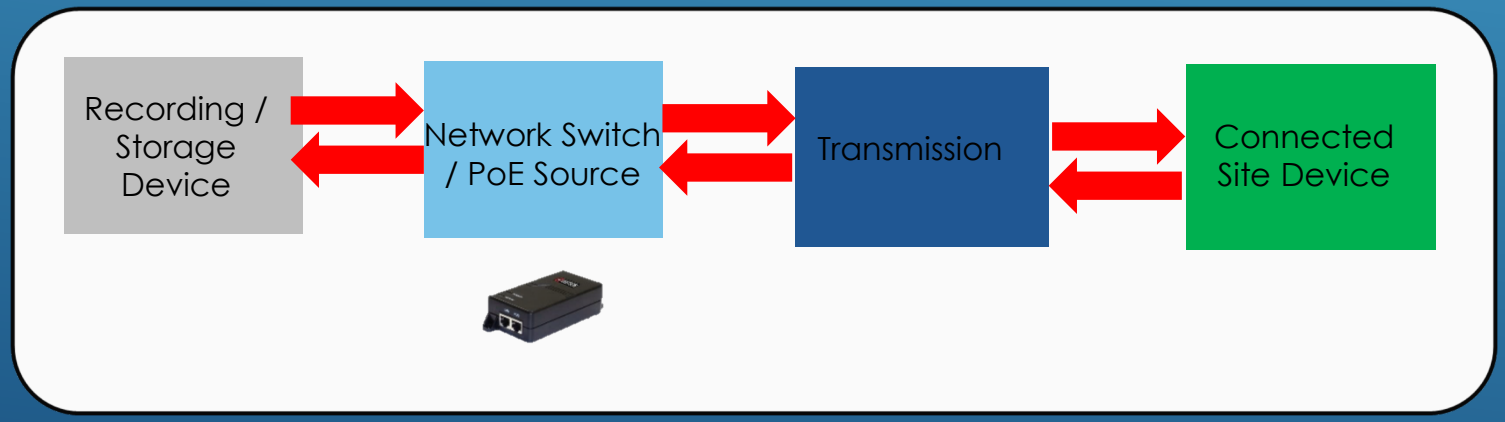
Why is this important: Communications from network switches to servers/NVR are TCP. These communications are bidirectional and require the sender receive an acknowledgement (ACK) from the remote device. The maximum time is **500ms**, but is set by the server software. The software also determines the number of retransmission.

The key is Latency.

Problem: Some of cameras are going offline intermittently

Probable Cause: The camera is probably surging due to activation of accessory functions such as day/night, auto back focus, etc. requesting power beyond the ability of the switch to provide it.

Probable Repair: Provide more PoE power at the source

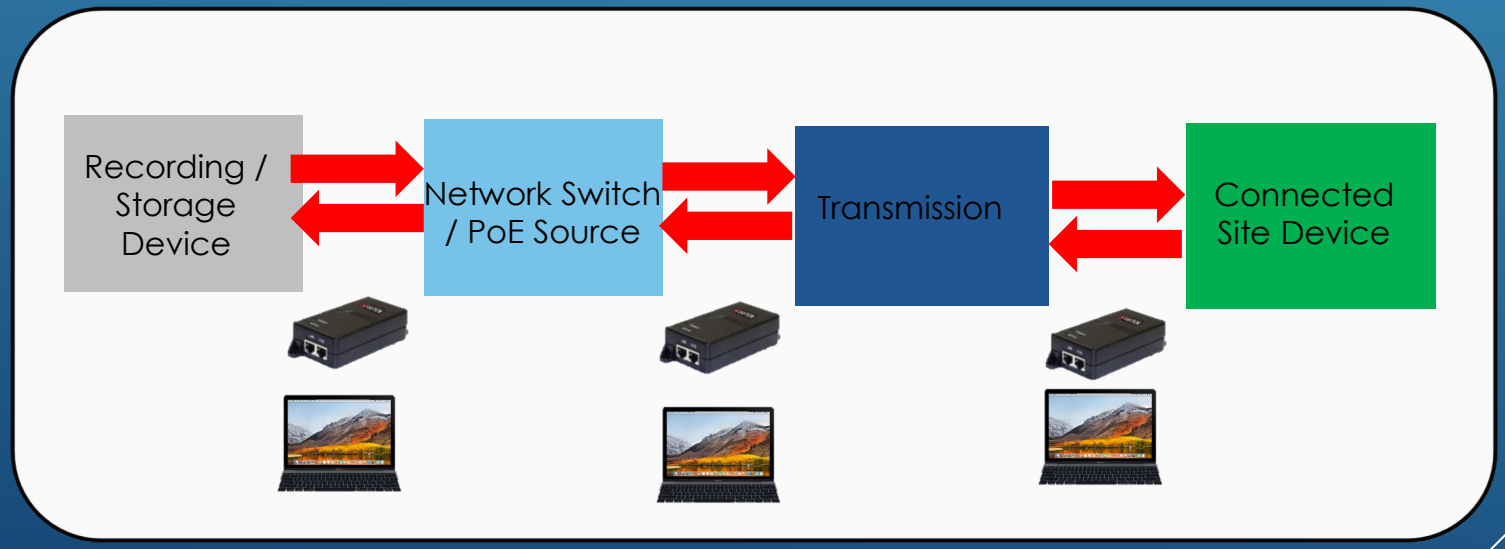


Isolate the Failure Point

Make certain your laptop is properly addressed.

Make certain the PSE (power supply) meets the requirements of the power device.

Most IP cameras will allow you directly view camera video, others will require you to download a driver.

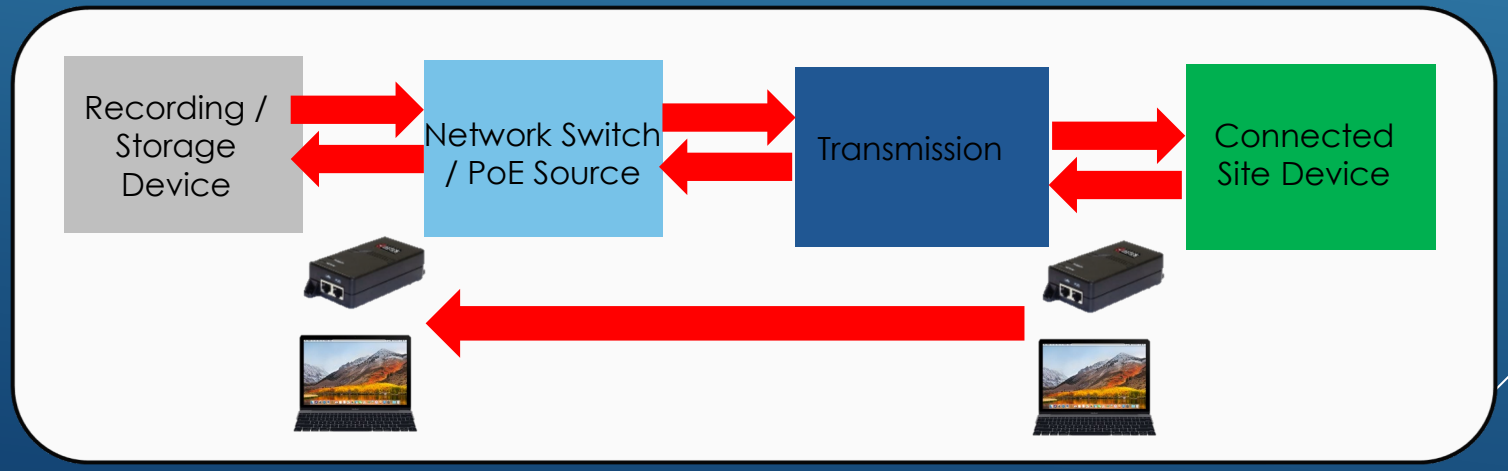


Troubleshooting: Detail Check

Using the laptop/PSE combination, access the connected device starting at the closest point to that device. The PSE will provide the PoE power.

At each point confirm to you can access the connected device, first by issuing a ping and next if the connected device is a video camera, confirm you can see the video.

At the point where you can no longer see the connect device will determine where the problem is.



Enterprise Switch Unique Programming Features

Easy to Read Ports Status

Link down but PoE Present

Link up and PoE Present

No PoE- Indicates Bandwidth

Differences between Ping and TraceRoute

Do I have a **connection?**

ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Why is this important: You need to see if the switch port is actually connected to the remote device.

Cameras are usually UDP Communications which are one way

What is my connection path and how long does it take me to get there- **Latency issues**

Traceroute

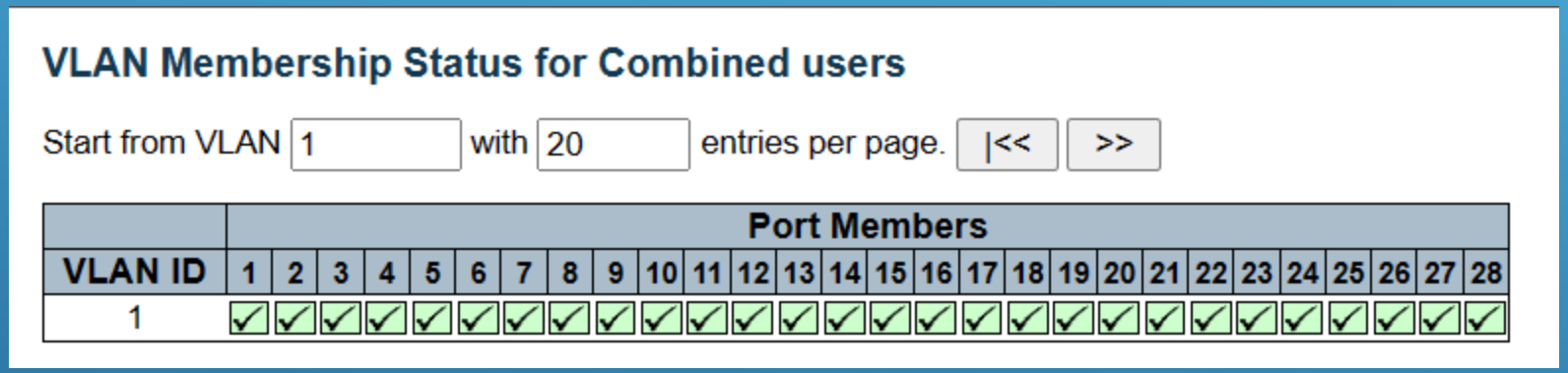
IP Address	0.0.0.0
Max TTL	30
Wait Time	5

Why is this important: Communications from network switches to servers/NVR are TCP. These communications are bidirectional and require the sender receive an acknowledgement (ACK) from the remote device. The maximum time is **500ms**, but is set by the server software. The software also determines the number of retransmission.

The key is Latency.

Programming Switch VLAN

VLAN RULES



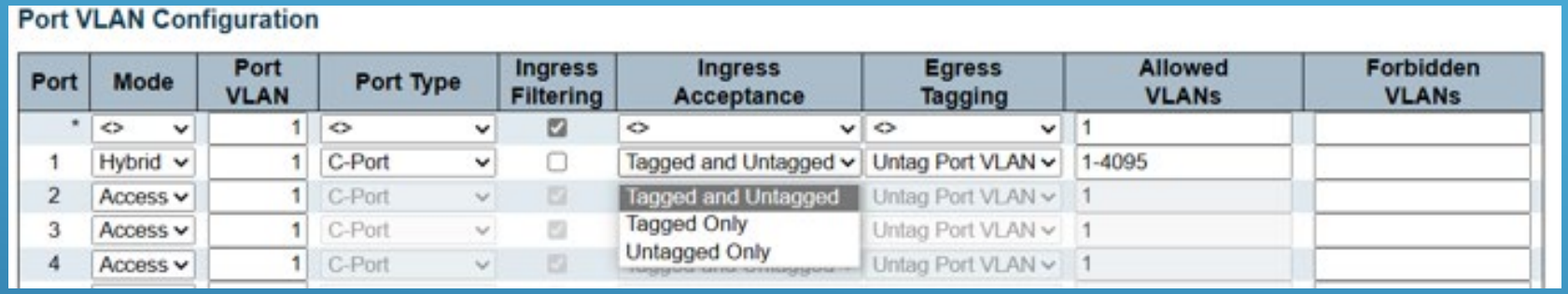
VLAN Membership Status for Combined users

Start from VLAN 1 with 20 entries per page. |<< >>

	Port Members																										
VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

To maintain access your connections must always be part of a VLAN

There must always be a VLAN 1



Tagging:

Network switch tagging is a technique used to separate network traffic into different virtual networks. It is used to improve network performance, security, and manageability. In a tagged VLAN, each frame is assigned a VLAN ID that identifies the VLAN to which it belongs. This allows multiple VLANs to share the same physical switch port. Tagged ports are also known as trunk ports

An untagged VLAN is a VLAN that does not have a VLAN ID assigned to it. When a frame is sent from an untagged port, the switch adds the default VLAN ID to the frame. This is also known as an access port

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Access:

Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics: Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1

Accepts untagged and C-tagged frames
Discards all frames not classified to the Access VLAN- (meaning frames assigned to ports in the VLAN)
On egress all frames are transmitted untagged

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	

Trunk:

Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: By default, a trunk port is member of all VLANs (1-4095)

The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs

Frames classified to a VLAN that the port is not a member of are discarded

By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress

Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-4095	

Hybrid:

Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware

Ingress filtering can be controlled

Ingress acceptance of frames and configuration of egress tagging can be configured independently

Port Types :

Entrance Exit

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
2	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Access	1	Unaware	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	S-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	S-Custom-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Unaware-the port is transmitted without any type- it can be assigned to any VLAN port

C-Port – If no port type is indicated upon engress (exit)
Most Common –assigned to a specific VLAN

S-Port- Only Frames with this tagged are handled others are dropped

S-Custom Port- S Port + information on the frame size with regards to standard or Jumbo Frames

VLAN Set Up-Example

VLAN Membership Configuration

Refresh | << | >>

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	VLAN Name	Port Members 1	2	3	4	5	6	7	8	9A	10A	9B	10B
☐	1	Security	☑	☑	☑	☑	☐	☐	☐	☐	☑	☑	☑	☑
☐	2	Client	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑

Add New VLAN

Apply Reset

VLAN Membership Configuration

Refresh | << | >>

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	VLAN Name	Port Members 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
☐	1	Security	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑
☐	2	Client	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Add New VLAN

Apply Reset

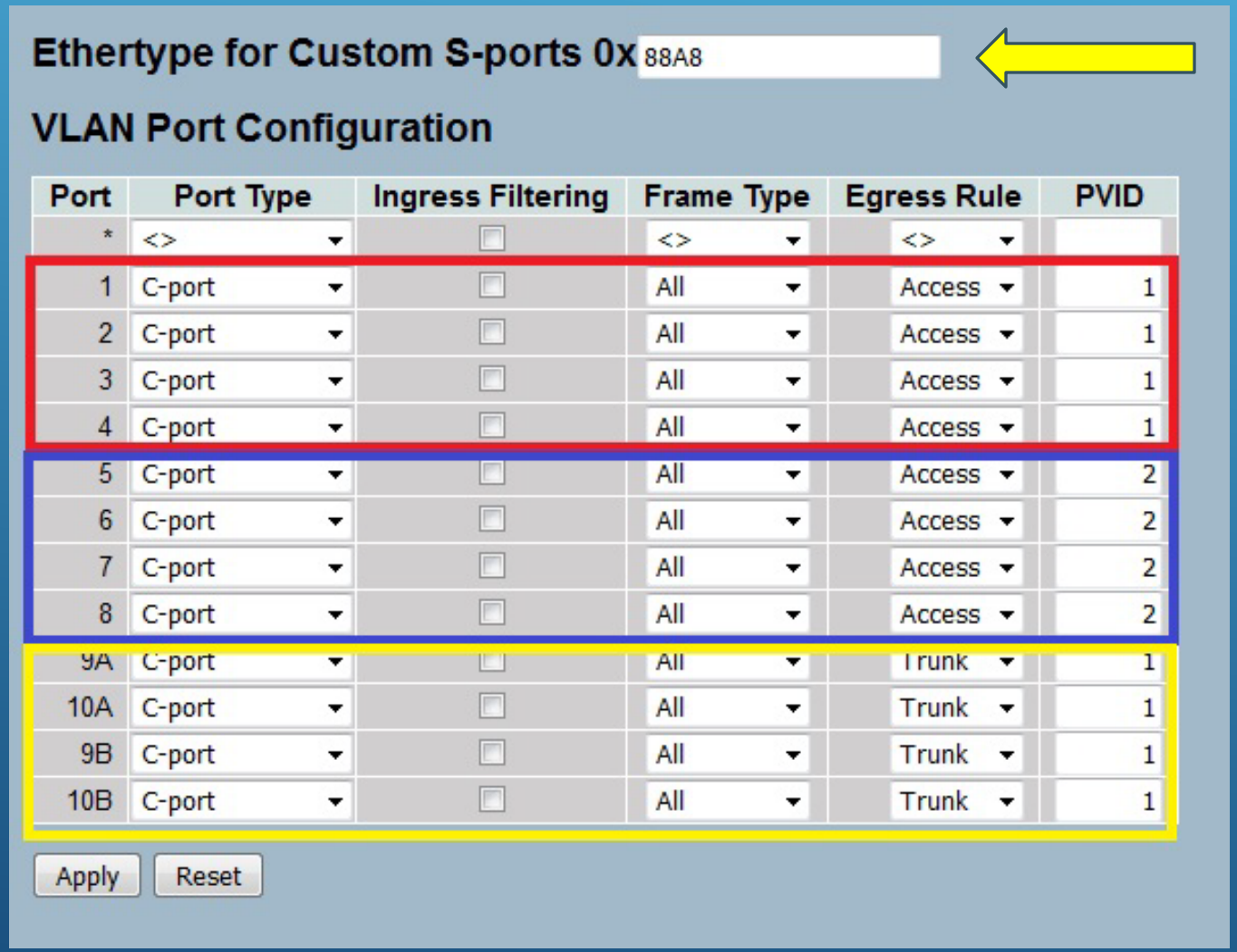
VLAN Set Up-Example

Access:

Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics: Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1

C-Port – If no port type is indicated upon engress (exit)

Most Common –assigned to a specific VLAN



Service VLAN tag identifier (S-Tag) on Q-in-Q tunnel it embeddes 802.1Q used with routers allowing a single VLAN to support multiple VLANs

Trunk:

Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: By default, a trunk port is member of all VLANs (1-4095)

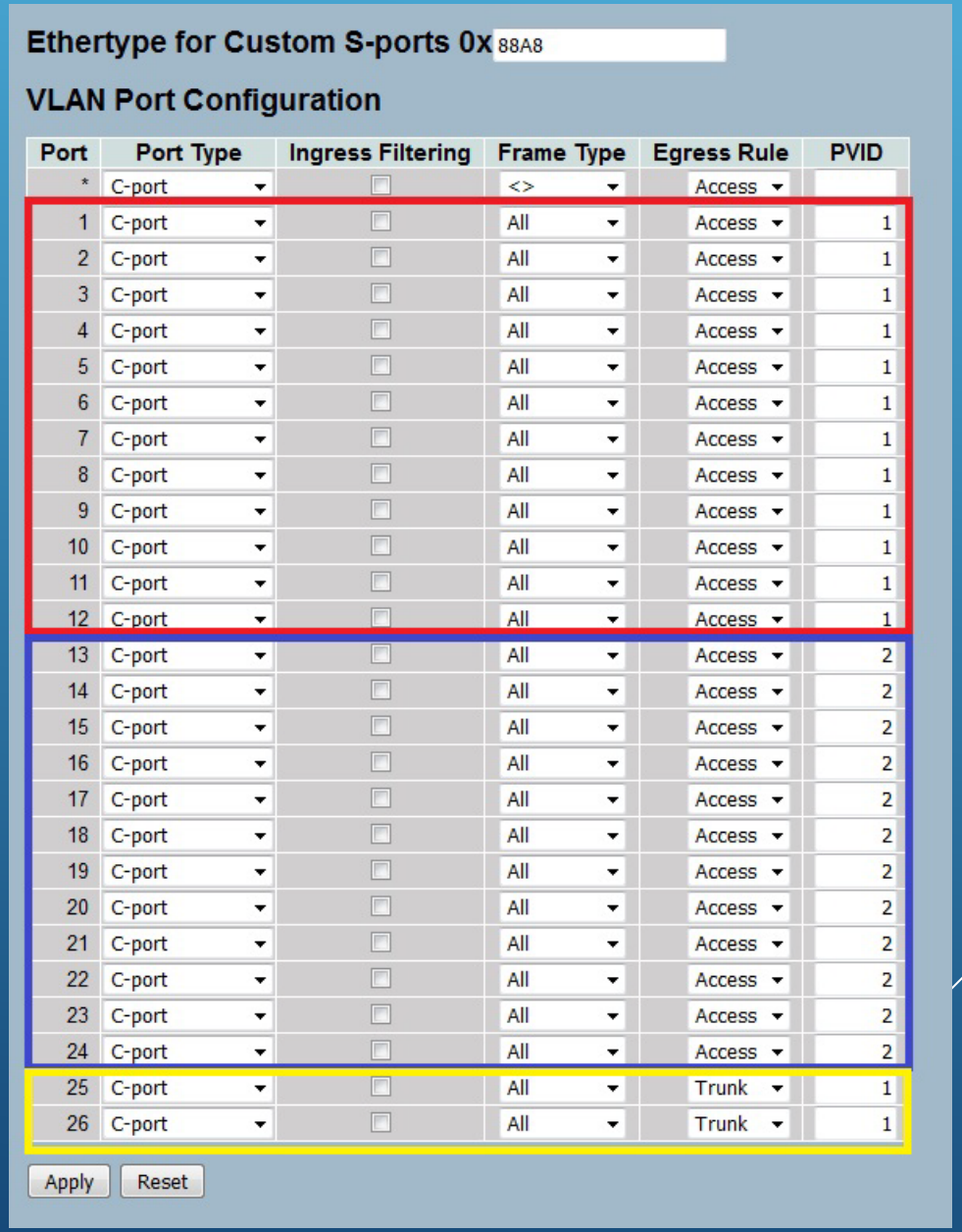
The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs

What is a PVID

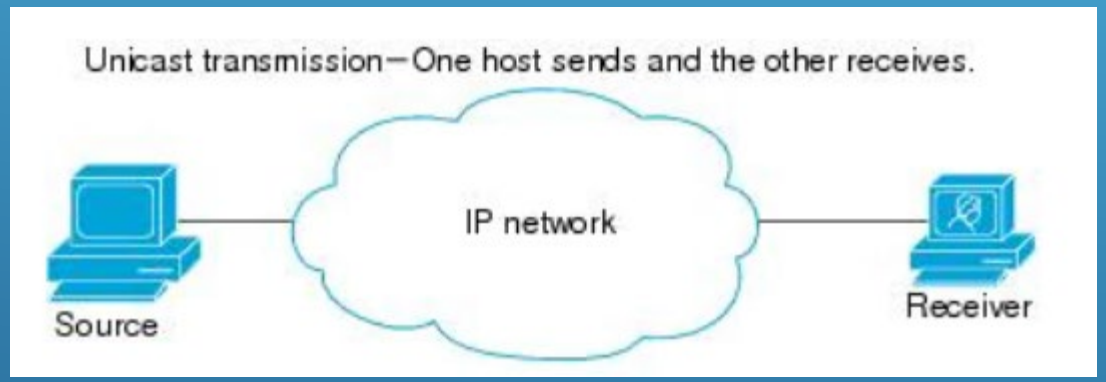
PVID is a private VLAN

PVID help to separate traffic on different ports and allow different VLANs to be use the same trunking – where this occurs one VLAN is considered as the primary and the other secondary. All PVIDs share the same primary VLAN

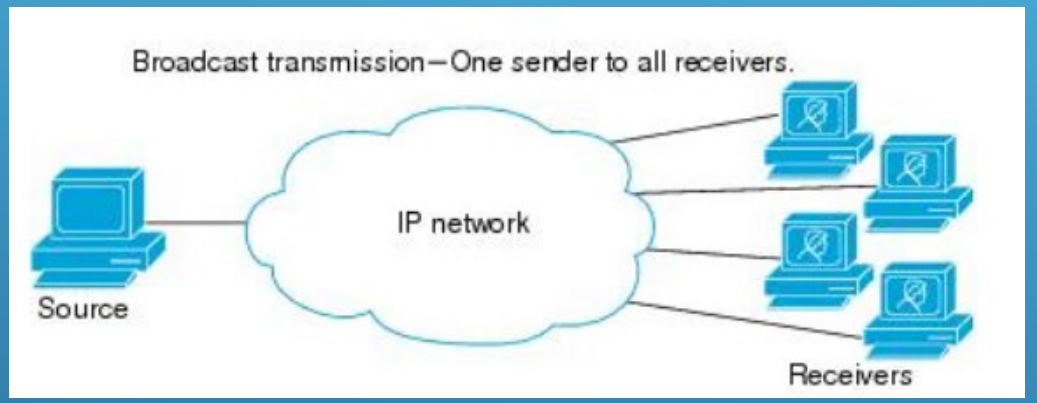
PVID will generally be used when you are **Trunking** which is used to aggregating (combining) multiple physical network links into a single port.



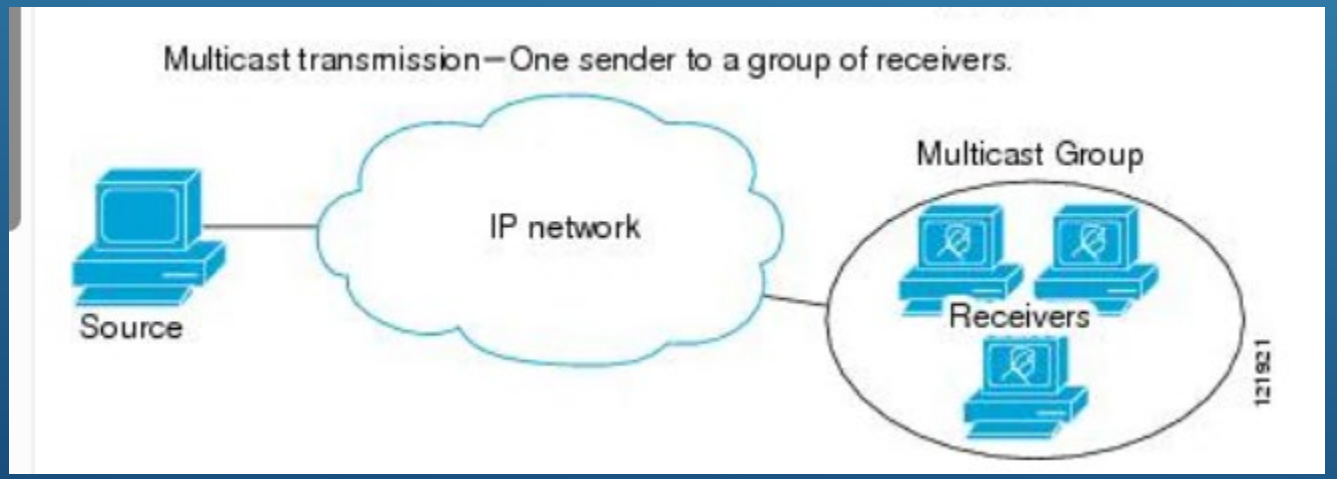
IGMP – Multicasting- Internet Group Management



Source sends to one client- both are identified with by their individual IP address



Broadcast – every connected device can receive source information

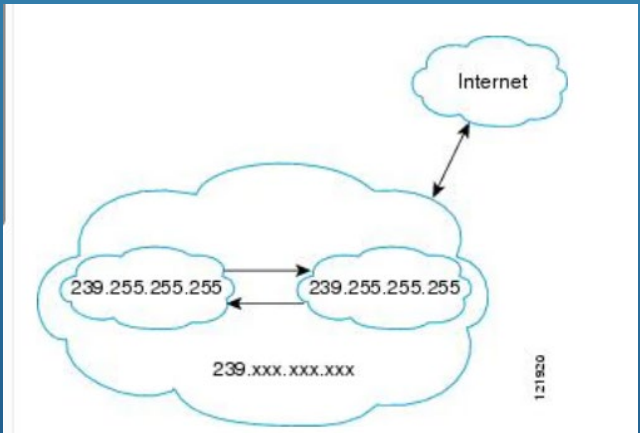


Source sends only to clients who are requesting it

Programming IGMP- Multicasting

Global Configuration	
Snooping Enabled	☐
Unregistered IPMCv4 Flooding Enabled	☑
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	☐
Proxy Enabled	☐

Flooding Enable:
Monitors flooding only when IGMP is active
Range of address – assigned for source –specific multicasting /8=IV4P, /32 =IPv6
Used to reduce traffic to avoid forwarding unnecessary messages to the router side
Use to restrict traffic via a proxy



Range of addresses

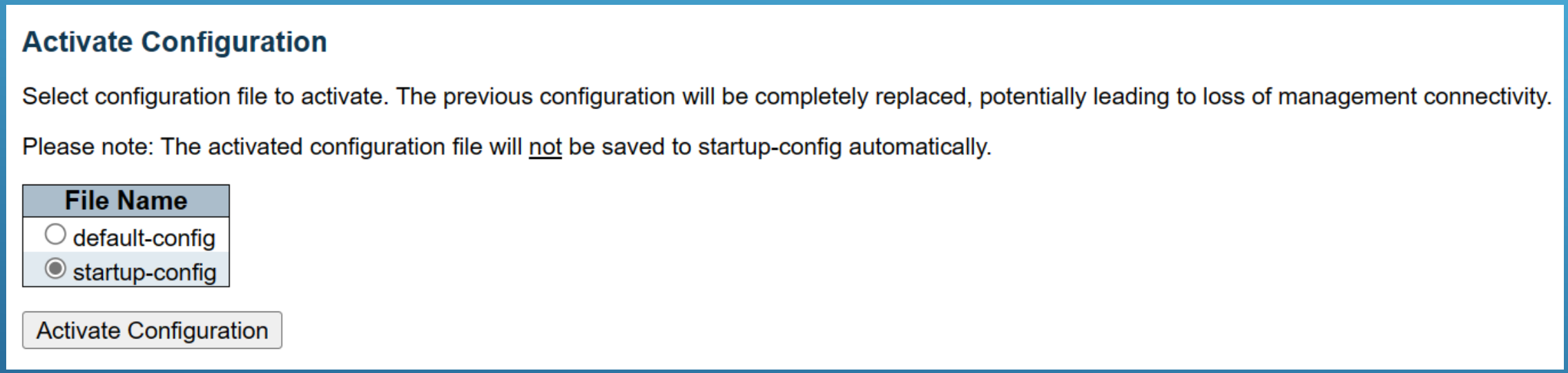
Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited

Router Port- defines the port

Fast Leave-used to remove group when a leave message is received without receiving a last member message – only use when connect to a specific port

Throttling – defines the number multicast ports

Saving your Programming



One of the most overlooked but important programing operations is the need to save your switch programming.

After you have finished programming your switch check to see if you need to save your total program.

If this is not performed and power is lost, switch programming will revert back to default