ZyPer4K Network Requirements & Security Considerations

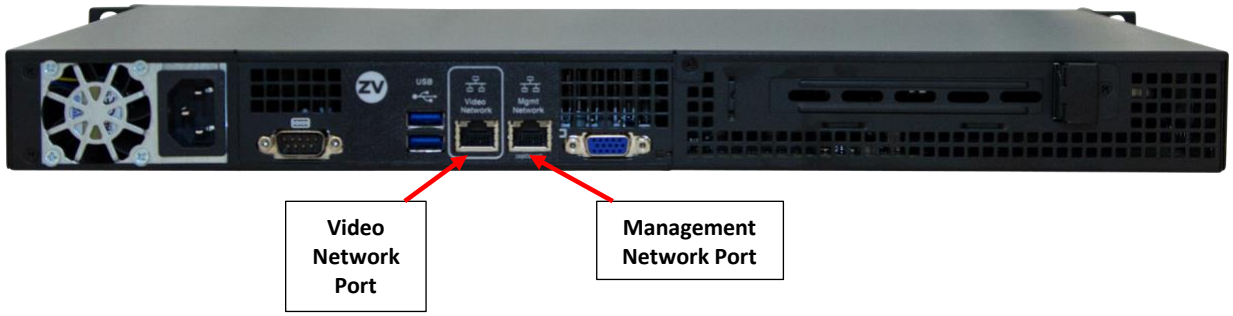
ZeeVee, Inc.
295 Foster Street, Suite 200
Littleton, MA 01460 USA
July 23, 2024

Table of Contents

ZyPer Management Platform Hardware

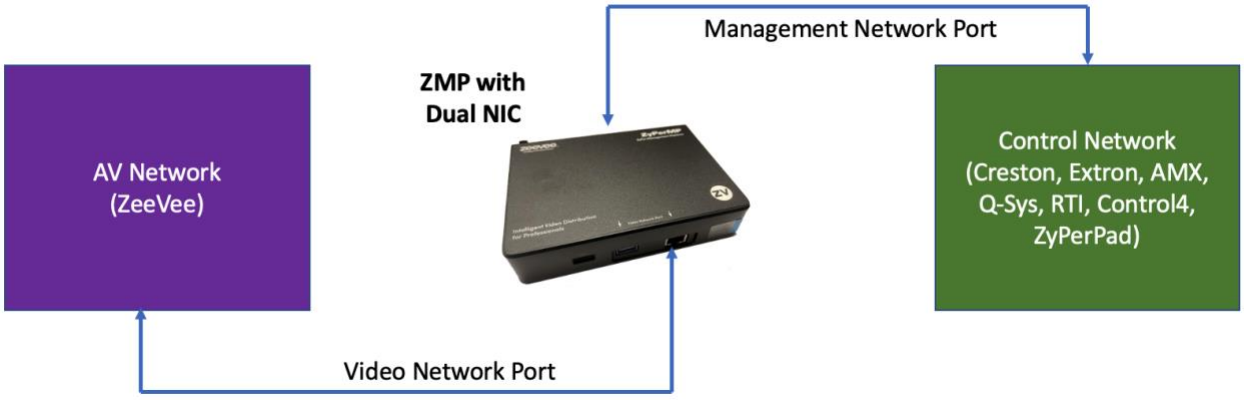
The ZyPer Management Platform (ZMP) is available from ZeeVee in two different hardware options. NUC and Rack Mount Server. Both versions have two network interfaces. It is important that the port labeled “Video Network” is connected to the LAN containing the ZyPer4K encoder/decoder endpoints. The port labeled “Management Network” is available to separate the Video AV Network from a corporate or Control Network.

Rack Mount ProServer ZMP



NUC ZMP

Example ZMP Connections



Important Crestron Note

The Crestron **CP4N Series-4 Controller** has a special LAN port labeled “Control Subnet”. This port should never be connected to the ZeeVee AV network. (The LAN with ZeeVee encoders and decoders). This “Control Subnet” can be on the same network port as the ZeeVee ZyPer Management Platform “Management Network”.

Using the “Control Subnet” on the Video Network will cause catastrophic failures to the system.

Basic elements of ZyPer4K communication

ZyPer4K uses layer 2 / layer 3 IPV4 protocols

IP Address allocation

IP Addresses for the ZyPer4K units can be allocated using any of the following mechanisms:

1. DHCP – If a DHCP server is located on the network the ZyPer4K can be configured to obtain an IP address from this source.
2. Static – The ZyPer4K units can always be configured manually with a Static IP address.
3. Link-Local – The ZyPer4K will automatically assign a Link-Local address in the 169.254.x.x range if neither DHCP or Static address selection is used.

Note: When the ZyPer4K is equipped with an optional Icron USB or Dante Transmitter module, the USB/Dante module itself will have a unique IP Address. This address is always acquired via DHCP or Link-Local mechanism. It is important that a DHCP server has a pool of addresses large enough to account for these USB/Dante IP Addresses as well as the ZyPer4K IP Address. The USB module cannot be assigned a Static address. The Dante Transmitter can be assigned a Static address via Dante Controller.

Important Note: If the Icron USB module is installed, the ZyPer4K itself should not be given a Static IP address. In this case the ZyPer4K should use a DHCP or Link-Local address.

Ports

The following Ports are used by the ZyPer4K and the ZyPer Management Platform

ZyPer Management Platform

ZMP (GUI): TCP ports 80, 8001 and 8080
Telnet: TCP port 23
SSH: TCP port 22
FTP: (default) TCP ports 20 and 21
FTP: (passive) TCP ports 21 and some ports >1023

Between ZyPer Management Platform and ZyPer4K Units

General communications: UDP port 6969 and 6970
RS232: UDP ports 10001 to 10004
USB: UDP port 6137 (Note USB support is optional except on XS units)

Video and Audio (multicast)

The focus of ZyPer4K is transporting high resolution video and audio data across 10 Gb Ethernet networks. A typical video data stream consumes three to nine gigabits per second, depending on its resolution format. In order to manage this bandwidth, the basis of ZyPer4K's AV transmission protocol is multicasting. This way, these high data rate streams are only sent through ports across links where they are needed. Some of the most serious considerations for network deployment – especially in multi- switch environments – are around ensuring that the network is setup to handle this properly. Bandwidth management is a key design consideration. Any significant loss of data (due to oversubscription or other reason) will result in visible on-screen problems. Ensuring that high data rate streams are routed *only* where they are needed is critical.

Control: IR, RS-232 (unicast with some optional multicast and broadcast)

ZyPer4K carries various low-speed control communications as well. These signals are typically triggered by a user-facing control system and are used to control things like turning on and off a display. Infrared signals and RS-232 signals are included here. These packets are typically sparse, and data rates are in kilobits per second. The data packets are always unicast between the ZyPer Management Platform and ZyPer4K endpoints. Sometimes the communication is directly between endpoints.

Discovery (Broadcast)

ZyPer4K runs its own auto-discovery mechanism. It relies on broadcast communication between all endpoints and the ZyPer Management Platform.

Note: Supporting multicast content delivery over multiple VLANs requires an experienced network engineer to configure the switches/network. The information above is provided for information purposes only. ZeeVee can only provide very limited support in configuring such a network. The implementation is almost entirely left to the end customer.

Discovery (Multicast)

As noted above, the default method of discovery is broadcast. The system however can be configured to use multicast for discovery. This allows the server to discover ZyPer4K endpoints using multicast across subnets when multicast routing is enabled. When in multicast mode there must be an IGMP querier running – usually that would be the multicast router querier.

The API command to enable multicast discovery is:
set server discoverMode all multicast

Important Note: Multicast discovery is only supported on ZyPer4K-XS/XR and Wallplate units. It is not supported on the ZyPer4K Classic units. (White boxes)

Note: Supporting multicast content delivery over multiple VLANs requires an experienced network engineer to configure the switches/network. The information above is provided for information purposes only. ZeeVee can only provide very limited support in configuring such a network. The implementation is almost entirely left to the end customer.

The 1 Gb utility port

The ZyPer4K units include built-in Ethernet switching capability, in order to provide 1 Gb connectivity that can be piped through the 10 Gb link.

USB 2.0

Some ZyPer4K products include the capability to distribute and switch USB traffic across the 10 Gb Ethernet network. In general, this USB functionality is compatible with any type of USB device. However, the consumption of Ethernet bandwidth by the USB devices must be considered in the system design.

Switch selection and network topology

ZyPer4K is compatible with any 10 Gb Ethernet switch that has Layer 2/3 "non-blocking" switching capabilities. Support for multicast, IGMPv2 with IGMP snooping and IGMPv2 fast-leave is required.

When IGMPv2 fast-leave is configured; when the device receives a leave message, it immediately stops forwarding to that port.

Most switches' default behavior is to broadcast packets. Watch out for this and make sure to enable IGMP Snooping before trying to use ZyPer4K.

Important Notes:

1. If using switching/L2 network with IGMP snooping
    a. Cannot have a multicast router anywhere in the network
    b. If more than one switch, cannot have proxy querier running
    c. If using Netgear, then more than one switch is fine since it does not require a proxy querier
    d. If using Cisco, then can only have one switch since it requires a proxy querier to be running

2. If using multicast routing with PIM/Sparse-mode
    a. Each switch must be acting as a router, separate subnets/VLANS.
    b. Each switch needs to be a Rendezvous Point in order to ensure shortest-path routing.
    c. Devices will not be discovered automatically unless broadcast forwarding is enabled between subnets for the devices.
        i. Or, manually add devices using the API

Note: ZyPer4K devices support IGMPv2 but are compatible with IGMPv3 networks. (Routers)

Regarding trunk ports

QSFP ports can usually be configured as single 40 Gb trunk port or as four independent 10 Gb ports. If you intend to use the port as a high bandwidth link to another switch, be sure to configure it as a 40 Gb trunk port. Otherwise, you're just adding extra 10 Gb ports to your switch, and if you connect them all to the same switch, you made a loop, and 3 ports will get shut down, leaving you with only 10 Gb between the switches.

Regarding "stackable switches"

A stackable switch works with other stackable switches to present themselves as one cohesive "single switch." The entire system can be easily configured from a single IP address. This type of system is compatible with ZyPer4K, but note that bandwidth must still be managed. Typically, a system of stackable switches is *not* fully non-blocking, meaning that there will be bottlenecks (often 40 Gb links between switches with 24, 48, or more 10 Gb ports). Bandwidth demands of the ZyPer4K system must be compared against the user requirements (how much video must be routed over the stacking ports to meet the user requirements) and all this must be considered in the design of the system's connectivity.

Regarding "leaf-spine"

Leaf-spine comes into play when number of endpoints surpasses the size of a single switch. ZyPer4K devices connect to leaf switches and leaf switches connect to spine switches. Leafs mesh into spines meaning that every leaf is connected to every spine. This is compatible with ZyPer4K but like for Stackable switches, bandwidth has to be managed where the limiting factor will be the trunk bandwidth between leaves and spines.

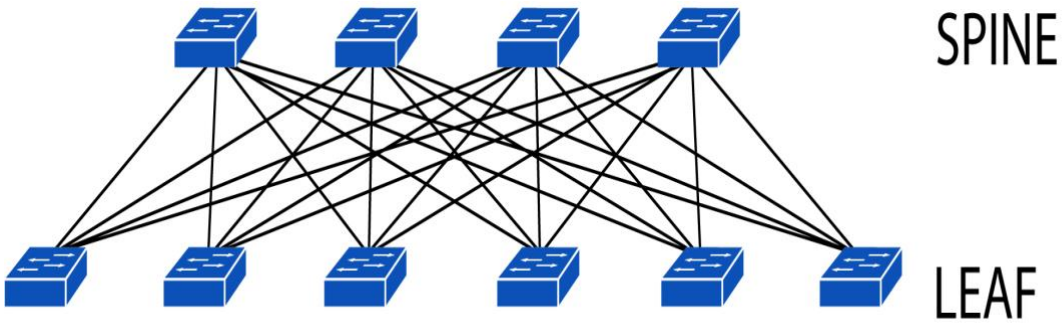


Figure: Illustration of leaf-spine topology

Multi Subnet Networks (Port Forwarding)

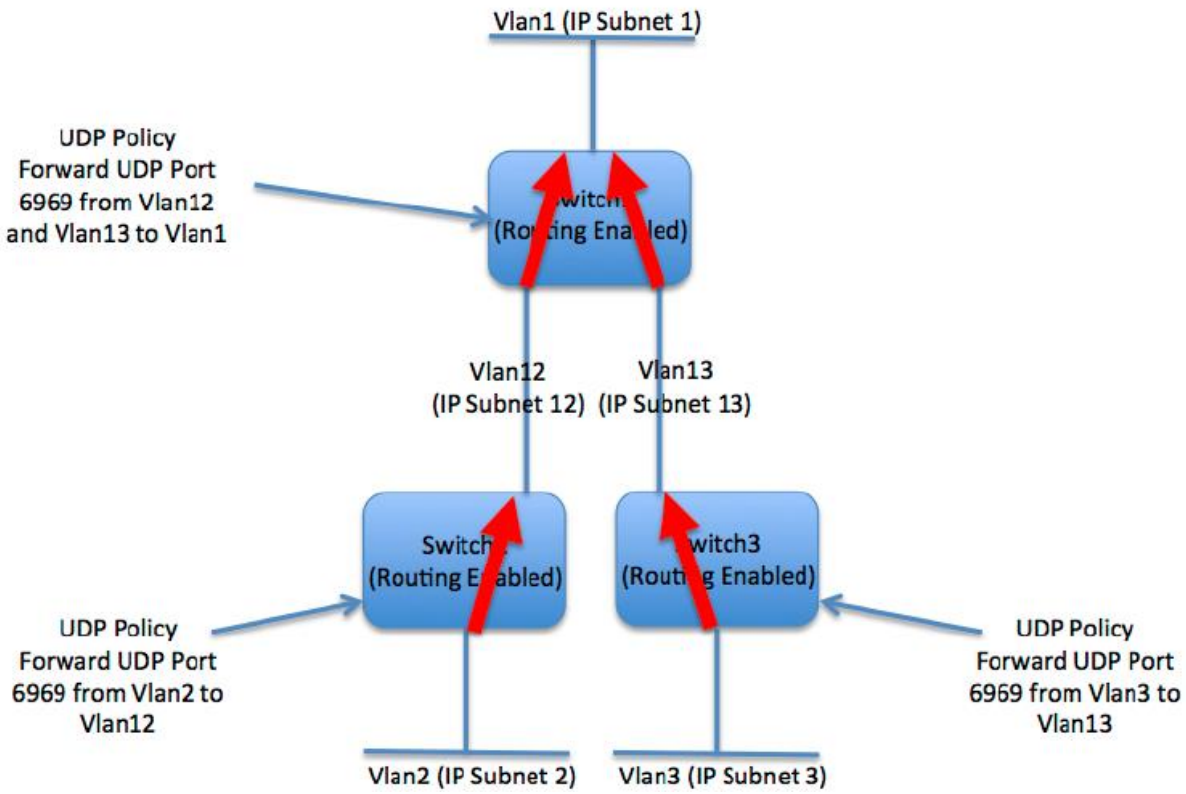
It is strongly recommended that the ZyPer4K system be deployed on a single dedicated video network. This allows the endpoint discovery system to easily find and identify encoders and decoders in the system. It is possible however to deploy the ZyPer4K on a multi subnet network. In this case steps must be taken to ensure that the devices can all be discovered and managed by the ZyPer Management Platform (ZMP).

Note: The instructions below involve advanced network configuration and management concepts. A qualified network engineer should be involved in making these configuration updates and the network switch provider may need to be consulted to ensure support of needed features.

The ZyPer4K encoders announce themselves to the ZyPerMP management platform using a UDP allnets broadcast packet (destination 255.255.255.255). These announcement packets will typically not pass through a network router since they are an IP broadcast. Therefore, in order for the ZyPer Management Platform to successfully discover the ZyPer4K devices, they are required to be in the same broadcast domain (or VLAN).

In order to allow the ZeeVee Management Platform to discover the ZyPer4K encoders and decoders we utilize a feature called UDP port forwarding on the switches. In a standard configuration the routing switches will not forward an IP broadcast packet received on one VLAN to other VLANs. UDP port forwarding will be configured on the switches in order to forward specific UDP broadcast packets received from the VLANs where the encoders and decoders are placed to the VLAN where the ZMP is located. Once this is done, the ZMP is able to successfully discover and manage the encoder and decoder devices. ZyPer4K Encoders and Decoders send UDP packets on port 6969 in order to advertise themselves to the ZMP. By creating UDP port forwarding polices on the routing switches, we can arrange for those packets to be delivered to the ZMP to allow it to discover and manage them.

The diagram in the figure below shows how the UDP policies are configured to forward the advertisement packets to the ZyPer Management Platform on VLAN1.



Special Note: ZyPer4K endpoints that contain USB need to also have UDP port 6137 forwarded from the ZMP to all endpoint VLANs.

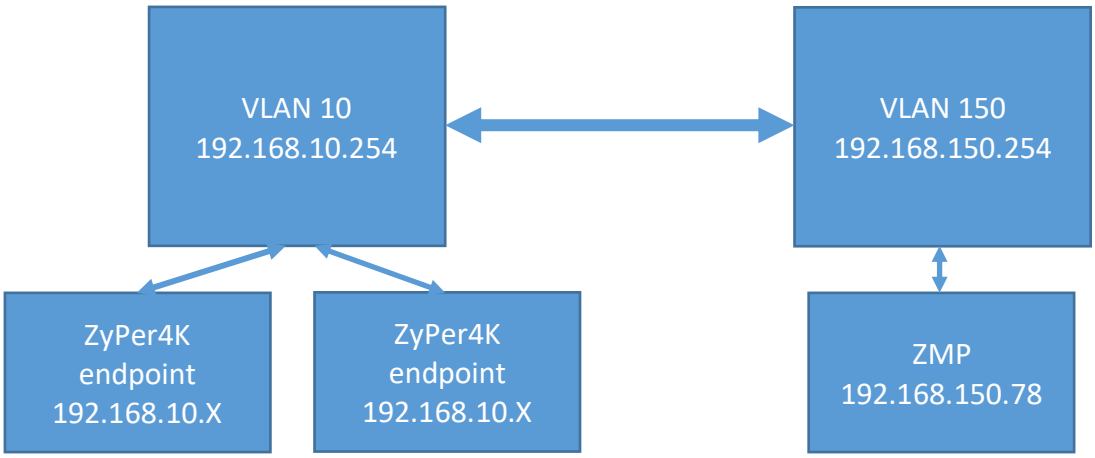
Multi Subnet Networks (Manual Device Additions)

It is strongly recommended that the ZyPer4K system be deployed on a single dedicated video network. This allows the endpoint discovery system to easily find and identify encoders and decoders in the system. It is possible however to deploy the ZyPer4K on a multi subnet network. In this case steps must be taken to ensure that the devices can all be discovered and managed by the ZyPer Management Platform (ZMP).

Note: The instructions below involve advanced network configuration and management concepts. A qualified network engineer should be involved in making these configuration updates and the network switch provider may need to be consulted to ensure support of needed features.

It is possible to manually tell the ZyPer Management Platform the IP Address of ZyPer4K devices that are located on a different VLAN/Subnet than the ZMP itself.

The example below is a case with two different VLANs/Subnets.



The ZyPer4K Endpoints are located on VLAN 10 and the 192.168.10.X subnet.
The ZyPer Management Platform is on VLAN 150 and the 192.168.150.X subnet.

The ZMP will automatically discover any ZyPer4K endpoints located on VLAN 150. The ZMP will NOT automatically discover any ZyPer4K endpoints located on VLAN 10. However, given the proper circumstances, the ZyPer4K endpoints on VLAN 10 can be manually added to the ZMP for control.
For this to work, the network MUST be configured to route traffic between VLAN 10 and VLAN 150. How to configure the network to allow routing between VLANs is beyond the scope this document and should be done by a qualified network engineer. A simple test to confirm routing is that a device in VLAN 10 can ping a device in VLAN 150.

The ZyPer4K endpoints need to have a known IP Address. The IP Address should either be assigned by a DHCP server or assigned statically.

Once this is done, the user needs to log into the ZMP Command Line Interface (CLI). Example: telnet 192.168.150.78 based on the drawing above.

The ZMP configuration is shown below:

```
Zyper$ show server config
server(192.168.150.78);
  server.gen; autoEdidMode=enabled, redundancy=enabled
  server.ipServerAddress; mode=dhcp, address=192.168.150.78
  server.ipManagementAddress; mode=static, address=192.168.20.2
  server.ntpServer; address=129.6.15.28
  server.telnetAccess; mode=enabled
  server.encoderDefault.edid; audio=allowCompressed
  server.dataTunnelMode; telnet=telnetHandshakeMode
  server.logging; level=3
  server.isaac; address=192.168, subsystemId=Wallyworld
Success
```

Now use the “add device” command to manually add the ZyPer4K endpoints.

```
Zyper$ add device ipAddress 192.168.10.81
Success
```

In the above example, the IP Address of a ZyPer4K endpoint located in VLAN 10 is 192.168.10.81

ZyPer4K endpoints need to be added one at a time.

You can get a listing of all “user added” devices with the “show device userAdded” command.

```
Zyper$ show device userAdded
device(d8:80:39:eb:1c:ee);
  device.gen; model=Zyper4K, type=encoder, name=London, state=Up,
uptime=0d:18h:32m:36s, lastChangeId=55
  device.ip; address=192.168.10.79
device(d8:80:39:59:f1:ff);
  device.gen; model=Zyper4K, type=decoder, name=Right, state=Up,
uptime=0d:18h:32m:36s, lastChangeId=52
  device.ip; address=192.168.10.81
device(d8:80:39:59:af:be);
```

```
  device.gen; model=Zyper4K, type=decoder, name=Left, state=Up,
uptime=0d:18h:30m:5s, lastChangeId=56
  device.ip; address=192.168.10.82
device(d8:80:39:5a:69:a9);
  device.gen; model=Zyper4K, type=encoder, name=Laptop, state=Up,
uptime=0d:18h:32m:36s, lastChangeId=70
  device.ip; address=192.168.10.96
Success
```

Note that when using the “add device” command it is no longer required to perform port forwarding on port 6969. This is automatically handled by the ZyPer Management Platform.

Note that for ZyPer4K endpoints to stream audio/video between VLAN 10 and VLAN 20 the network must be configured to pass multicast traffic between the VLANs. That is another topic beyond the scope of this document.

Multicast management

In order to minimize overall bandwidth consumption, ZyPer4K relies on multicast routing for distributing audio and video data. The basic idea is to *only* send AV data through switch ports where it is needed. **IGMP Snooping must be enabled**. As few as two video streams at 4K can oversubscribe a 10 Gb link, so getting multicast right is critical.

***Important note**: the switch must be configured to drop any packets from a multicast stream with no subscribers. Some switches could treat such packets as broadcast and impact the bandwidth and performance of the entire network.*

Multicast source addresses

The ZyPer Management Platform is responsible for assigning multicast source addresses to transmitters. Each transmitter will be assigned three or four source addresses. Separate source addresses are used for:

- Video, including the embedded audio from an input video source
- Scaled video, including the embedded audio from an input video source
  - Note: This feature provides video/audio for Multiview windows
- Audio that has been extracted from the input video source stream

- Audio brought into the transmitter via I2S (*e.g.*, analog audio input)

ZyPer4K encoders must be assigned multicast addresses in the range of 224.1.1.1 to 238.255.255.255. You can assign a specific range to not conflict with other multicast devices on the network.

Note that addresses 224.1.1.253 and 224.1.1.254 are reserved.

Multicast addresses for each encoder can be assigned manually by the user. This can be accomplished all at once with a single command:

Set All API command example:
set device encoders sendIpMcastRange 224.1.2.1 224.1.3.255

Note: This feature/command is enabled in API version 1.4 and above.

The above command will set all 3-4 multicast addresses for every encoder

- Video, including the embedded audio from an input video source
- Scaled Video, including the embedded audio from an input video source
  - Note: This feature provides video/audio for Multiview windows and is only supported with ZyPer4K units with HDMI 2.0 capability
- Audio that has been extracted from the input video source stream (Downmix audio)
- Audio brought into the transmitter via I2S (*e.g.*, analog audio input)

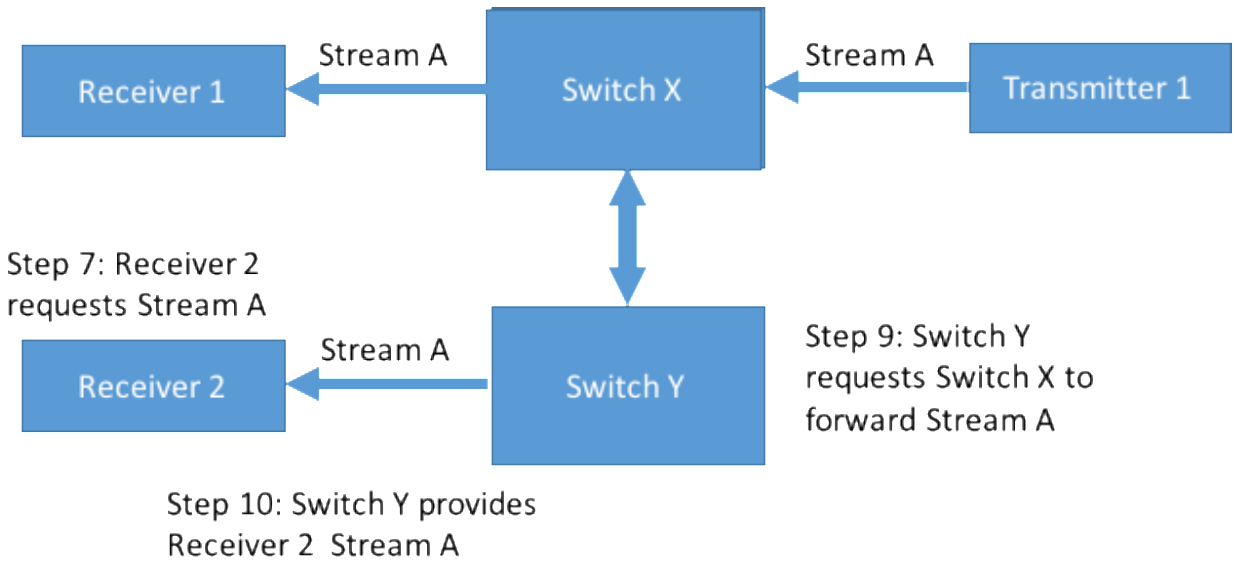
Multicast routing management

In a single switch environment, IGMP suffices to enable the switch to understand which traffic must be routed to which ports. In a ZyPer4K system, the switch will only transmit video to those ports where a ZyPer4K receiver has requested a particular stream. In a multi-switch environment, higher-level protocols must be employed so that “switch X” can understand which streams are demanded by receivers connected to “switch Y.” If this is not carefully managed, trunk links can easily be oversubscribed by multiple (dozens or more) streams of 8 Gb video.

The basic communication flow is:

1. Switch X is connected to switch Y via a 40 Gb trunk link. No video traffic is currently passing between them.

2. Transmitter 1 is connected directly to switch X, and sending stream A into that switch.
3. Switch X needs to notify switch Y that stream A exists. Stream A still does not traverse the trunk link.
4. Receiver 1 is also connected directly to switch X, and makes an IGMP request to switch X for stream A.
5. Switch X begins routing stream A to receiver 1, who displays the video signal. Still there is NO video traffic across the trunk port between switches.
6. ZyPer4K receiver 2 is connected directly to switch Y.
7. ZyPer4K receiver 2 requests stream A by issuing an IGMP request to switch Y (which receiver 1 is connected to directly).
8. Switch Y realizes that it does not have access to stream A, but switch X has notified switch Y about stream A.
9. Switch Y sends a request to switch X to provide stream A across the trunk link.
10. Switch X complies, begins routing stream A across the trunk link to Switch Y, and switch Y begins providing stream A to receiver 2.
11. Later, if receiver 2 releases his IGMP subscription to stream A (and no other receivers on switch Y have requested stream A), then stream A should be removed from the trunk link.



The implementation of these higher-level protocols is vendor specific. One example of such a protocol is Protocol Independent Multicast (PIM), implemented by Extreme Networks and others.

Multicast Management Warnings

It is critical that the Network does not contain a multicast router. The presence of a multicast router will cause fatal errors to the ZyPer4K multicast delivery system.

The Network should also not contain an IGMP Querier as this will also cause fatal errors to occur with the ZyPer4k multicast delivery system. Note that in a single Switch solution IGMP Query can be enabled on the Switch without causing any issues. (Netgear has a special implementation that works with IGMP Query enabled) Note: There are exceptions to this rule. Please contact ZeeVee support team if using Cisco or Juniper switches.

Multicast TTL (Hop Limit)

The TTL (Time to Live) value for video and audio streams is 32.

Network performance issues

Bandwidth management

The ZyPer4K video system has no tolerance for link oversubscription. Lost packets translate to lost pixels on screen. Video data is transmitted via UDP, so there is no retransmission (since retransmitted packets would be too late anyway). There is intelligence built into mask small errors (by filling in surrounding or previous pixels, *etc.*), but any significant loss of data will result in significant image problems on screen.

The easiest solution is to design a fully non-blocking network. This is relatively straightforward for smaller systems, with affordable “top of rack” switches ranging to around 100 non-blocking ports. Beyond that size, blade-based systems of non-blocking switches exist, but can be expensive. A spine and leaf architecture may be more affordable and may fit more neatly in the physical layout of the network.

To design a cost-efficient system, the video routing use cases must be carefully considered and weighed against bandwidth availability.

The following table gives a summary of how much data a ZyPer4K video stream consumes. The data rate does scale up and down with video format (resolution, frame rate, *etc*). It is critical that the network is designed to handle the worst-case routing scenario demanded by the use cases. Special attention must be paid to the bottlenecks – the 40 Gb trunk ports between 10 Gb switches.

Resolution	Frame Rate	Bit Depth	Chroma	Ethernet bandwidth consumed (Gbps)	Notes
1280x720	60p	8-bit	4:4:4	1.6	
1920x1080	60p	8-bit	4:4:4	3.2	
1920x1080	60p	8-bit	4:2:2	2.2	
3840x2160	30p	8-bit	4:4:4	6.4	
3840x2160	60p	8-bit	4:4:4	8.7	Compressed from 12 Gbps
Multiview Window	30p	8-bit	4:4:4	9.5	Maximum bandwidth at Decoder for all streams in multiview

The ZyPer4K 1 Gb port

ZyPer4K products include a 1 Gb “utility port” whose traffic is piped back through the main 10 Gb AV port of the endpoint. The ZyPer4K units include an Ethernet switch built in, which is how this traffic is connected back to the 10 Gb network. A few notes on this port:

- This port is disabled by default and must be enabled via the ZMP if it is to be used.
- The 1 Gb port does not support jumbo packets.
- There is no VLAN or priority assigned to the 1 Gb port.
- ZyPer4K does not implement any form of STP or loop protection. The 1 Gb port must ***never*** be looped back to the same switch as the 10 Gb port.

Because there is no priority assigned to this port, keep in mind that traffic from this port may trigger an oversubscription condition and cause video failures. This can be especially bad through trunk links. Consider a 48-port 10 Gb switch with a single 40 Gb uplink. Potentially 48 ZyPer4K endpoints could be connected, each with some Ethernet device on the 1 Gb port. If all of these devices were to maximize their bandwidth consumption (1 Gb each), that would be 48 Gb consumed without a single video link in place. Use of the 1 Gb port must be very carefully considered in complex multi-switch Ethernet networks.

USB switching

ZyPer4K products that include USB switching accomplish this over Ethernet through the use USB controller chipset. This chipset uses broadcast, multicast, and unicast communication to create the feature set. As long as the rules for handling ZyPer4K AV traffic are adhered to, then USB will work. There are no special additional rules for USB. However, do consider that USB traffic will also eat into system bandwidth. Complex Ethernet devices (webcams, data storage devices) can consume hundreds of megabits per second. When a point to point link is established between two USB endpoints, the Ethernet communication is unicast.

Typical USB Bandwidth

USB devices have instantaneous and operating bandwidths. For example, High Speed devices have an instantaneous bandwidth of 480Mb/s. However, real world throughput of an individual device is never the full transfer rate. USB devices connected to a PC, must share the available USB bandwidth. Each device does not have an instantaneous bandwidth of 480Mb/s. The typical operating bandwidth of several USB devices are shown in the table below to demonstrate the different bandwidths that might be encountered.

Device	Typical USB Bandwidth Required
Mouse	< 100 Kb/s
Keyboard	17 Kb/s
Flash Drive	80 Mb/s
Low Resolution / High Compression Web Camera	80 Mb/s
DVD or CD Writer	80 Mb/s
Interactive White Board	100 Kb/s
Hard Disk	336 Mb/s maximum

Bandwidth Use Summary

The ZyPer4K can transmit AV data from multiple sources simultaneously over the 10 Gb Ethernet port. These sources include: HDMI (Video and Audio), 1 Gb Utility port, USB 2.0 port, Analog audio, RS-232 port, IR port. Maximum bandwidth of each port is shown below:

ZyPer4K Port	Maximum Bandwidth
Primary AV input (HDMI, DisplayPort, HDSDI, Analog)	12 Gbits/sec (3840x2160, 4:4:4 @ 60 Hz) (will be compressed to approximately 8.7 Gbits/sec maximum)
1 Gb Ethernet	1 Gbit/sec
USB 2.0	480 Mbits/sec
Analog Audio	2.3 Mbits/sec (48k x 24 bits x 2 channels)
RS-232	115 Kbits/sec
IR	60 Kbits/sec

Security

The ZyPer4K system with companion management platform implement several different security related features.

In an AV over IP system, you can provide a level of security by keeping the video traffic private from the main network. This can be done as simply as adding a new

VLAN for the AV equipment. Many customers create a dedicated AV network that is physically disconnected from the main network. The available Enterprise class management platform provides for two independent network interfaces to more easily separate the AV network from the corporate network.

Customers with highly secure networks will run vulnerability scans on all network devices. One of the tools that can be used is Nessus from Tenable. Please contact ZeeVee for a detailed analysis of Nessus scans of the ZyPer Management Platform.

Encryption between endpoints

All AV traffic between ZyPer4K encoders and decoders uses an Advanced Encryption Standard (AES-128). This level of encryption is sufficient to protect U.S. Government classified information up to the SECRET level. AV traffic encrypted with AES-128 includes Audio, Video, RS-232, USB and IR communications.

High-bandwidth Digital Content Protection

High-bandwidth Digital Content Protection (HDCP) is a form of digital copy protection developed to prevent copying of digital, audio & video content as it travels across connections. The system is meant to stop HDCP-encrypted content from being played on unauthorized devices or devices which have been modified to copy HDCP content. Before sending data, a transmitting device checks that the receiver is authorized to receive it. If so, the transmitter encrypts the data to prevent eavesdropping as it flows to the receiver.

ZyPer4K units support High-bandwidth Digital Content Protection (HDCP 2.2) from end to end. This feature cannot be disabled and provides a 100% assurance of HDCP compliance.

Management Platform

Direct from ZeeVee, the Control System has a basic level of security. Access to the management platform either via the ZMP GUI (via JSON) or the API (via Telnet or SSH) is password protected to prevent unauthorized access.

Note that starting with release 2.1 of the API, Telnet access to the management platform can be disabled. See the Management Platform User Guide for details.

USB Ports

The ZyPer4K USB ports can be filtered to disable unauthorized access.
Filter options include:

- None – Allows any USB compatible device to interface over ZyPer4K
- HID – Allows only Human Interface Devices (Mouse/Keyboard)
- Storage – Allows any USB compatible device except Mass Storage

1Gb Ethernet utility port

The 1Gb Ethernet utility port found on the ZyPer4K encoders and decoders provides a convenient means of accessing the network. For security reasons these ports can be disabled via the API. (Disabled by Default)

The API command is as follows:

set device <device:mac|name> utilityPort enabled|disabled

Port Based Access Control

The ZyPer4K family of products support 802.1X MAC-address Authentication or MAC Address Authentication Bypass (MAB)

802.1X MAC-address Authentication Bypass is an authentication mechanism that lets devices authenticate to the network using their MAC address as an identifier

- A list of authorized MAC addresses of device's NICs is maintained on the RADIUS server for MAB purpose
- MAB can be configured on a per-port basis on the switch
- When a device tries to connect, the switch sends the MAC address of each client to the authentication server
- The RADIUS server checks the MAC address of the client NIC against the list of authorized addresses
- The RADIUS server returns the access policy and VLAN assignment to the switch for each client

Practically speaking, you just have to enter the list of your ZyPer4K TX and RX devices MAC addresses into the RADIUS server and enable on the network.

MAC Address Authentication or MAB is supported by all the major switch vendors including Arista, Cisco, Dell, Extreme, HP, Netgear and Commscope/Ruckus.

10Gb Security

The fact that ZyPer4K is on a 10Gb network and uncompressed video traffic is always greater than 1Gb provides a level of security to “remote data theft”. External (Internet) access to any 10Gb AV over IP system will be conducted using a link with 1Gb or much less bandwidth. For example: it is a physical impossibility to steal uncompressed AV traffic with a bandwidth of 6.5Gb/sec via a 1Gb/sec link.

Appendix 1: Recommended Switches

The following 10Gbit switches are recommended for use with the ZyPer4K. Please note this is not an all-inclusive list. There are many other switches available that will function with the ZyPer4K.

Manufacturer	Model #	Number of Ports		Notes
		Copper	Fiber	
Netgear	ProSafe XS708T	8	2 (shared)	Disable Multicast Storm Control
Netgear	ProSafe XS712T	12	2 (shared)	Smart Switch
Netgear	ProSafe XS716T	16	2 (shared)	Smart Switch
Netgear	M4300-8x8F	8	8	Fully Managed Switch
Netgear	M4300-12x12F	12	12	Fully Managed Switch
Netgear	M4300-16X	16	0	Fully Managed Switch
Netgear	M4300-24X	24	4 (shared)	Fully Managed Switch
Netgear	M4300-24XF	2 (shared)	24	Fully Managed Switch
Netgear	M4300-24x24F	24	24	Fully Managed Switch
Netgear	M4300-48X	48	4 (shared)	Fully Managed Switch
Netgear	M4300-48XF	2 (shared)	48	Fully Managed Switch
Netgear	M4300-96X	96	96	96 Max Ports. Configurable as mix of Copper/Fiber.
Netgear	M4500-48XF8C	0	48	Included 8 100Gb uplink ports for connection to spine switch
Netgear	M4500-32C	0	32	32-port 100G fiber spine switch
Netgear	M4350-24X4V	24	4	24-port PoE+ with 4x25Gb fiber uplink ports
Netgear	M4350-36x4V	36	4	36-port PoE+ with 4x25Gb fiber uplink ports
Netgear	M4350-24X8F8V	24	8	24-port PoE+ with 8 fiber ports and 8x25G uplink ports
Netgear	M4350-40X4C	40	4	40-port PoE++ with 4x100G uplink ports
Netgear	M4350-32F8V		40	32-port fiber switch with 8x25G fiber uplink ports
Extreme	X670-G2-48x-4q	0	48	4x 40Gb QSFP+ ports
Extreme	X690-48x-2q-4c	0	48	2x 40Gb QSFP+ ports
Extreme	X690-48t-2q-4c	48	0	2x 40Gb QSFP+ ports
Arista	720XP-48TXH-2C-S	48		48 PoE+ ports with 2x100G and 4x25G uplink ports
Arista	CCS-755-CH	240	240	Linecard based (PoE+ or SFP+)
Arista	CCS-758-CH	384	384	Linecard based (PoE+ or SFP+)
Dell	X4012		12	
Dell	S4048-ON		48	Up to 72 10GbE ports with breakout cables.
Commscope/Ruckus	ICX7550-24F		24	
Commscope/Ruckus	ICX7650-48F		24	

Commscope/Ruckus	ICX7750-48F		48	48 10GbE SFP+ ports and 6 40 GbE QSFP+ ports
Commscope/Ruckus	ICX7750-48C	48		48 10GbE RJ45 ports and 6 40 GbE QSFP+ ports
Cisco	Nexus 2348TQ	48	48	
Cisco	WS-C3580-48XS		48	48 10GbE SFP+ ports and 4 40GbE QSFP+ ports
Cisco Meraki	MS425-16		16	2x 40Gb QSFP+ ports
Cisco Meraki	MS425-32		32	2x 40Gb QSFP+ ports
Niveo	N10GSM24XP	24		24-port PoE+ with 2x 100G fiber trunk ports
Huawei	S6720-30C-EI-24S		24	24 10GbE SFP+ ports and 2 40 GbE QSFP+ ports
Huawei	S6720-54C-EI-24S		48	48 10GbE SFP+ ports and 2 40 GbE QSFP+ ports
Yamaha	SWX2322P-16MT	12	4	12 10Gbe RJ45 PoE+ ports and 4 fiber ports

Important Note

If using a Network Switch to provide PoE power to the ZyPer4K devices, it is important that the switch itself be protected against electrical surges that could be caused by something like a lightning strike. An appropriate surge protector should be placed between the Network Switch and AC power source.

Appendix 2: Switch Configuration Options - Generic

Some Switches will work directly out of the box with zero configuration required. Nearly all switches however will provide the user some ability to customize the configuration. The list below includes various switch configuration options that ZeeVee has encountered. Look for these or similar options when configuring your switch. (Netgear M4300 users please see Appendix 3)

1. Enable IGMP Snooping
    a. Must be enabled
2. Enable IGMP Snooping on VLAN used by ZyPer4K system
    a. Must be enabled when all ports default to VLAN used by ZyPer4K system
3. Filter/Drop unregistered Multicast traffic
    a. If not applied, the behavior of the switch will be to broadcast multicast packets if the switch has no known destination for that packet.
    b. Must be enabled if found
4. Unregistered Multicast Flooding
    a. Must be disabled if found
    b. Cisco switches – No IP IGMP Snooping TCN Flood
5. Filter Unregistered Multicast (different wording than number 4 above)
    a. Must be enabled if found
6. Disable IGMP Query (Except on Cisco switches)
7. Disable IGMP Query on VLAN used by ZyPer4K system
8. Set IGMP Version to IGMP V2
    a. Must be set if found
9. Enable FASTLEAVE on port X
    a. Should be enabled, if found
10. Enable FASTLEAVE for VLAN used by ZyPer4K system
    a. Should be enabled if found
11. Disable Multicast Storm Control on Netgear switches. *(Security-Traffic Control-Storm Control-Multicast Storm Control = Disable)*
12. IGMP Report Flood Mode
    a. Should be enabled if found

Important Notes:

1. If using switching/L2 network with IGMP snooping
    a. Cannot have a multicast router anywhere in the network
    b. If more than one switch, cannot have proxy querier running
    c. If using Netgear, then more than one switch is fine since it does not require a proxy querier
    d. If using Cisco, then can only have one switch since it requires a proxy querier to be running

2. If using multicast routing with PIM/Sparse-mode
    c. Each switch must be acting as a router, separate subnets/VLANS.
    d. Each switch needs to be a Rendezvous Point in order to ensure shortest-path routing.
    d. Devices will not be discovered automatically unless broadcast forwarding is enabled between subnets for the devices.
        i. Or, manually add devices using the API

Appendix 3: NETGEAR M4300 Switch Configuration

NETGEAR M4300 Series will work directly out of the box with zero configuration required. (Some of these settings are different than shown in Appendix 2. Please using settings below for Netgear M4300 series.)

Visit the Netgear website and update to the latest M4300 firmware prior to checking these settings. *Current version is 12.0.17.7 as of September 26, 2022.*

https://www.netgear.com/support/product/M4300-12X12F.aspx#download

Access the M4300 User Interface and navigate to “Switching => Multicast => IGMP Snooping”. The following are set as default:

Configuration:

IGMP Snooping Configuration

Admin Mode	○ Disable ◉ Enable
Multicast Control Frame Count	22835
Validate IGMP IP header	○ Disable ◉ Enable
Interfaces Enabled for IGMP Snooping	
Proxy Querier Mode	○ Disable ◉ Enable
Report Flood Mode	○ Disable ◉ Enable
Exclude Mrouter Interface Mode	○ Disable ◉ Enable
Fast Leave Auto-Assignment Mode	○ Disable ◉ Enable
Operational Mode	Enable
IGMP Plus Mode	○ Disable ◉ Enable

VLAN IDs Enabled for IGMP Snooping

1

IGMP Snooping VLAN Configuration:

IGMP VLAN Configuration

	VLAN ID	Admin Mode	Fast Leave	Membership Interval	Maximum Response Time	Multicast Router Expiry Time	Report Suppression	Proxy Querier	Report Flood Mode	Exclude Mrouter Interface Mode	IGMP Plus Mode
☐	1	Enable	Enable	600	120	300	Disable	Enable	Enable	Enable	Enable

Querier Configuration:

Querier Configuration

Querier Admin Mode	○ Disable ◉ Enable	
Snooping Querier Address	0.0.0.0	
IGMP Version	2	*(1 to 2)*
Query Interval(secs)	60	*(1 to 1800)*
Querier Expiry Interval(secs)	180	*(60 to 300)*

VLAN IDs Enabled for IGMP Snooping Querier

1

Querier VLAN Configuration:

IGMP Snooping Querier VLAN Configuration

	VLAN ID	Querier Election Participate Mode	Querier VLAN Address	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time
☐	1	Enable	0.0.0.0	Querier	2			120

If a second VLAN is added for ZyPer4K, be sure to copy the IGMP Snooping VLAN Configuration settings to the new VLAN:

IGMP VLAN Configuration

	VLAN ID	Admin Mode	Fast Leave	Membership Interval	Maximum Response Time	Multicast Router Expiry Time	Report Suppression	Proxy Querier	Report Flood Mode	Exclude Mrouter Interface Mode	IGMP Plus Mode
☐	1	Enable	Enable	600	120	300	Disable	Enable	Enable	Enable	Enable
☐	2	Enable	Enable	600	120	300	Disable	Enable	Enable	Enable	Enable

Appendix 4: Maximum Transmission Distance

The ZyPer4K product is offered in both Fiber and Copper Ethernet versions. The table below details the maximum transmission distance between either directly connected ZyPer4K units or between the ZyPer4K and a Network Switch.

Cable / Transmission Type	Maximum Distance
850nm Multi-mode Fiber (MMF) OM3/4	300m-400m (990 ft - 1320 ft)
1310nm Single-mode Fiber (SMF) 9/125	10km
1550nm Single-mode Fiber (SMF) 9/125	40km
Category 5	Not supported
Category 5e	Not supported
Category 6 UTP	55m (180 ft)
Category 6 STP	100m (330 ft)
Category 6A UTP	100m (330 ft)
Category 7	100m (330 ft)
Category 7A	100m (330 ft)

UTP = Unshielded Twisted Pair
STP = Shielded Twisted Pair

Important Note: If using PoE with ZyPer4K-XS or Wallplate units you must use shielded cable. (F/UTP for example) Additionally, if possible, any displays connected to decoders should be grounded. This grounding can be accomplished by making sure the connected HDMI display uses a 3-prong power connector.

Important Note:
If using a Network Switch to provide PoE power to the ZyPer4K devices, it is important that the switch itself be protected against electrical surges that could be caused by something like a lightning strike. An appropriate surge protector should be placed between the Network Switch and AC power source.

Note: To achieve maximum distances with Fiber cable it is critical to ensure use of proper Fiber Optic Transceivers and cable types.

ZeeVee Part #	Description	Distance
Z4KSFP10G85-3M	Fiber Optic Transceiver, SFP+ 10Gbps 850nm MMF	300-400m
Z4KSFP10G31-10K	Fiber Optic Transceiver, SFP+ 10Gbps 1310nm SMF	10km

Fiber Cable Type	Cable	Cable Distance Maximum
Single Mode fiber	OS2	10km
Multimode fiber	OM3	300m
Multimode fiber	OM4	400m
Multimode fiber	OM5	300m

Appendix 5: Netgear M4300-96x and M4500 Important Notes

When using the Netgear M4300-96x with 40G ports provided by the APM402XL module it is important to note that only specific 40G QSFP+ modules and fiber optic cable are supported.

For very short distances it is recommended to use a copper DAC cable such as the Netgear AXLC761 or Netgear AXLC763. (1M or 3M)

For distances longer than 3M, Netgear supports both Multimode and Single mode fiber options. For Single mode, Netgear supports the following QSFP+ modules from Cisco and Meraki:

Cisco part QSFP-40G-LR4-S or Meraki MA-QSFP-40G-LR4

For Multimode, Netgear supports the following QSFP+ modules with LC style connectors. Please note all this, is for duplex MMF (BiDi) - so LC and only two strands.

The supported modules are the Cisco QSFP-40G-SR-BD or Meraki MA-QSFP-40G-SR-BD

Netgear themselves does not provide multimode 40G QSFP+ modules and directs customers to the Cisco or Meraki modules above.

Netgear can be reached via email at ProAVDesign@netgear.com

When using the 100G ports on the Netgear M4500 series switches the following Netgear 100G DAC and QSFP+ modules are recommended.

Netgear Part #	Description
ACC761	100G Direct Attach QSFP28 to QSFP28 1 Meter Passive DAC Cable
ACC763	100G Direct Attach QSFP28 to QSFP28 3 Meter Passive DAC Cable
ACM761	100GBASE-SR4 MMF 100m MTP/MPO (4 duplex MMF links) 100m QSFP28 Transceiver
ACM762	100GBASE-LR4 LC SMF (one duplex SMF link) 10km QSFP28 Transceiver

Appendix 6: The Need for Shielded Ethernet Cables

Grounding is crucial for ensuring reliable operation in Power over Ethernet (PoE) systems. PoE technology enables both power and data transmission over Ethernet cables, which can lead to challenges related to electrical noise and voltage differentials. Proper grounding establishes a stable reference point for electrical signals, essential for device functionality and preventing disruptions.

In PoE systems, the convergence of power and data transmission increases the risk of interference. Without adequate grounding, electrical noise can compromise network performance. Furthermore, parasitic coupling phenomena can induce a 60V 60Hz signal onto the shielding of HDMI jackets, potentially leading to anomalous behaviors and PoE handshake failures. To combat these issues, proper grounding through shielded cable options such as F/UTP, S/UTP, F/FTP, S/FTP, SF/UTP, and SF/FTP is imperative.

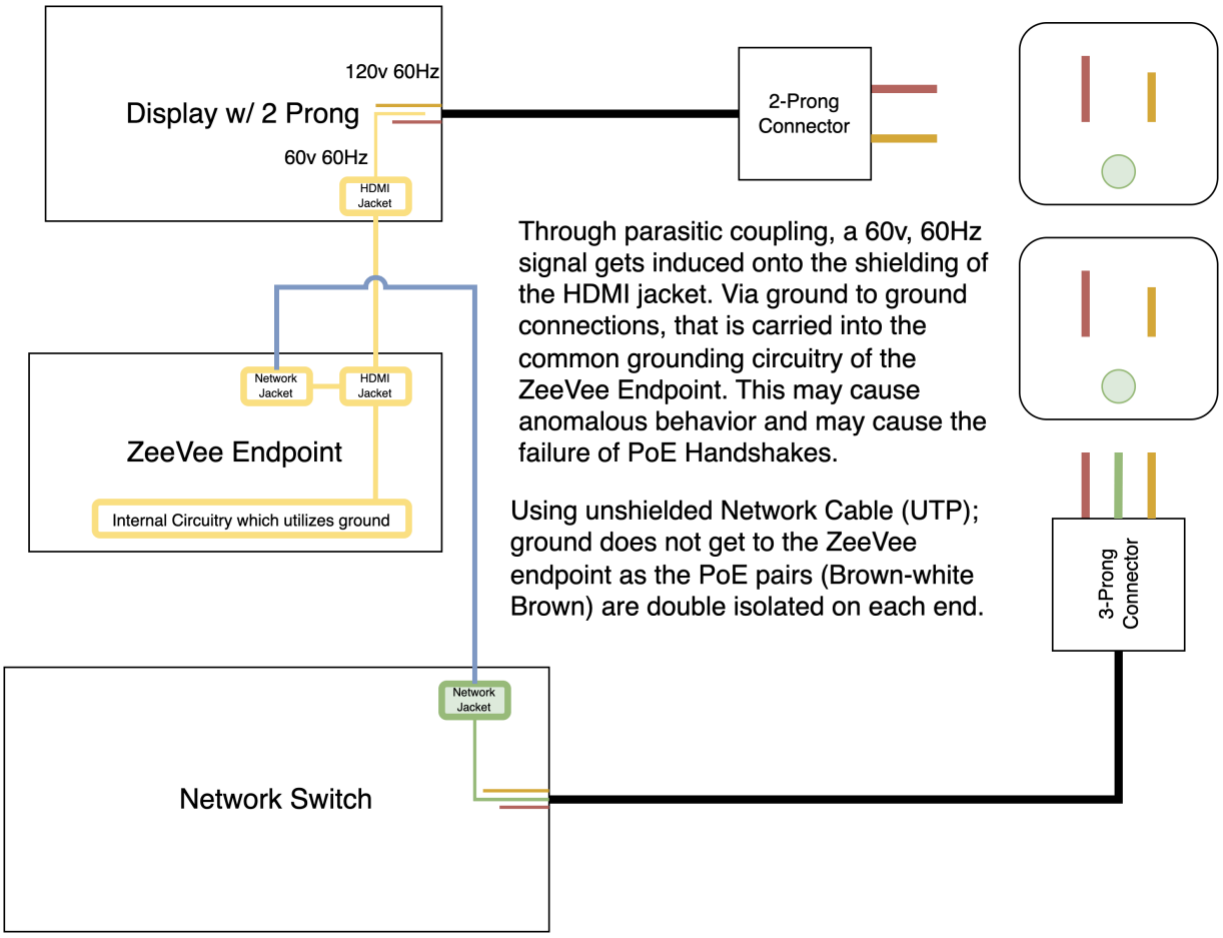
Inadequate grounding poses significant risks to the integrity of various signals in PoE systems. RS232 communication, for example, relies on a stable ground reference for accurate signal comparison. Without proper grounding, RS232 signals can become unreliable, leading to communication errors and system failures. Similarly, the operation of PoE relies on a solid ground connection to ensure efficient power delivery and data transmission. Any disruptions in grounding can result in PoE malfunctions or complete failure. Therefore, ensuring proper grounding is essential for maintaining the integrity and functionality of RS232, PoE, and internal components on a PoE powered AV over IP device.

In conclusion, proper grounding in PoE systems is paramount for maintaining reliability, performance, and signal integrity. By establishing a stable ground reference and mitigating electromagnetic interference, grounding ensures uninterrupted operation and safeguards against potential signal disruptions and equipment damage.

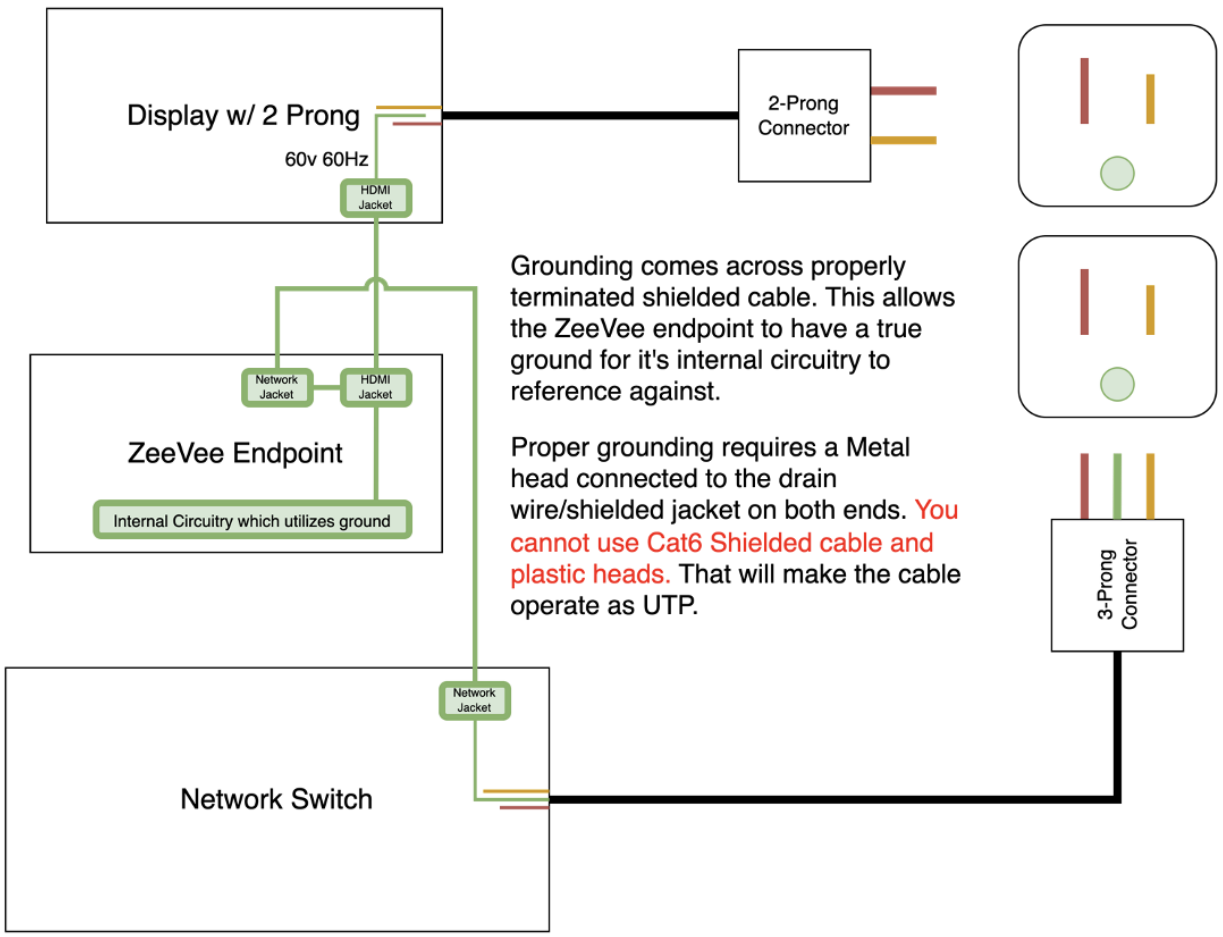
Examples

Shielded cable must be used with PoE systems to provide the ZyPer endpoint a path to ground when another path is not available. Shielded cable options include: F/UTP, S/UTP, F/FTP, S/FTP, SF/UTP and SF/FTP. (See Appendix)

Unshielded Example:



Shielded Example (F/UTP, S/UTP, F/FTP, S/FTP, SF/UTP or SF/FTP)



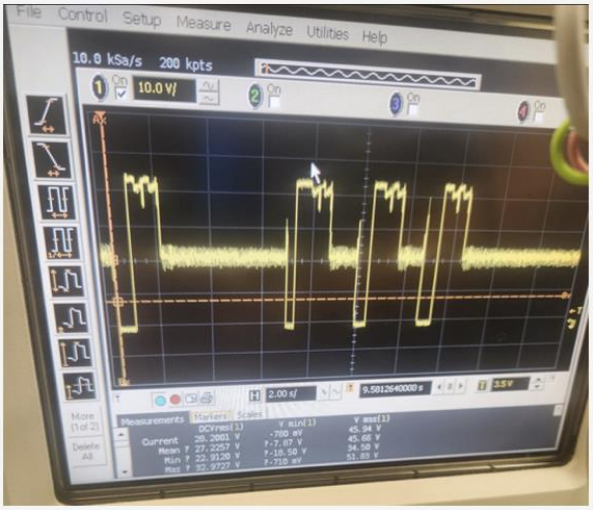
Recommended Cables:

ZeeVee has validated and can recommend Ethernet cables from Siemon Cable.

North America Link:
https://ecatalog.siemon.com/en/Copper/Cable/Category-6A-Shielded-Cable-North-America

International Link:
https://ecatalog.siemon.com/en/Copper/Cable/Category-6A-Shielded-Cable-International

Oscilloscope Traces

48V Input Signal with Shielded Cable	48V Input Signal with Unshielded Cable
	

In the *Shielded* case, all the pulses are the same length because they are successful on the first try. The *Unshielded* case has variable length pulses because the network switch keeps polling.

Disclaimers

ZeeVee has striven to ensure that this document is accurate and represents the described products fully. Although, ZeeVee assumes no responsibility for errors found, should any be found, please contact support@zeevee.com and corrections will be issued as appropriate.

Customers should always consult with qualified Network Engineers regarding all network designs. Design guidance provided by ZeeVee should be considered for reference only. It is up to the customer to validate and implement any network designs. ZeeVee cannot and will not be held responsible for network designs, equipment, cabling or other installation related network items.

ZeeVee hardware designs are property of ZeeVee.

Components, sub-assemblies, and methods utilized in the designs are free of any encumbrances or appropriate licenses and rights have been obtained by ZeeVee for the use in the described products in the intended manner.

ZeeVee software is the sole property of ZeeVee except within the restrictions and guidelines of any open-source or public-license component utilized. ZeeVee represents that normal usage of the product in a typical customer installation is fully within the granted rights and privileges of any licensed component. Visit www.zeevee.com for further details.

The specifications of the described products may change at any time without notice.

ZeeVee forbids unauthorized disassembly, reverse-engineering, duplication, or any other attempt to recreate all or portions of the hardware or software outside of any use explicitly authorized in writing by ZeeVee.

Trademarks

All trademarks are the property of their respective owners.

Copyright