

ZyPer4K Network Requirements & Security Considerations



ZeeVee, Inc.
295 Foster Street, Suite 200
Littleton, MA 01460 USA
May 25, 2018



Table of Contents

Basic elements of ZyPer4K communication.....	3
IP Address allocation.....	3
Ports.....	3
ZyPer Management Platform	3
Between ZyPer Management Platform and ZyPer4K Units	3
Video and Audio (multicast).....	3
Control: IR, RS-232 (unicast with some optional multicast and broadcast).....	4
Discovery (Broadcast)	4
The 1 Gb utility port.....	4
USB 2.0.....	4
Switch selection and network topology	4
Regarding trunk ports	5
Regarding “stackable switches”	5
Regarding “leaf-spine”	5
Multicast management.....	6
Multicast source addresses	6
Multicast routing management.....	7
Multicast Management Warnings	9
Network performance issues	9
Bandwidth management.....	9
The ZyPer4K 1 Gb port	11
USB switching	11
Typical USB Bandwidth.....	11
Bandwidth Use Summary.....	12
Security	13
Encryption between endpoints	13
High-bandwidth Digital Content Protection.....	13
Management Platform / MaestroZ.....	13
USB Ports.....	14
1Gb Ethernet utility port	14
10Gb Security	14
Appendix 1: Recommended Switches	15
Appendix 2: Switch Configuration Options.....	16
Appendix 3: Maximum Transmission Distance.....	17



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.

Ports

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

ZyPer Management Platform

Maestro (GUI): TCP port 80

Telnet: TCP port 23

SSH: TCP port 22

FTP: (default) TCP ports 20 and 21

FTP: (passive) TCP ports 21 and some port >1023

Between ZyPer Management Platform and ZyPer4K Units

General communications: UDP port 6969

RS232: UDP port 10001

USB: UDP port 6137 (Note USB support is optional)

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.

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, IGMP v2 with IGMP snooping and IGMP v2 fast-leave is required.

When IGMP v2 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.

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 that IGMP Query can be enabled on the Switch without causing any issues.

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.

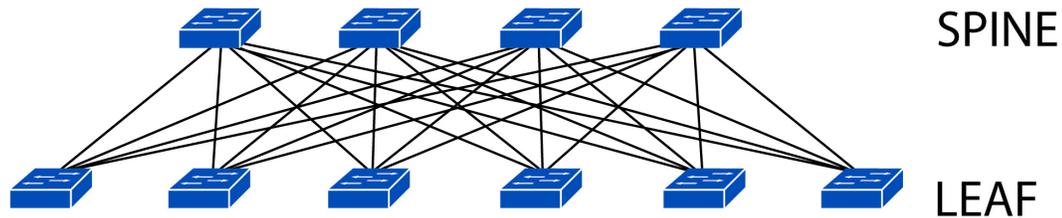


Figure: Illustration of leaf-spine topology

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 and is only supported with ZyPer4K units with HDMI 2.0 capability
- 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 224.1.3.255. This range must not be used by any other devices on the network.



Note that addresses 224.1.1.253 and 224.1.1.254 are reserved.

The method of assigning multicast addresses depends on the revision of firmware installed on the ZyPer4K encoder:

Firmware Version 2.10.5 and earlier:

By default, multicast addresses are assigned automatically by the ZyPer Management Platform. These addresses may be changed manually by the user to any available valid multicast address within the range detailed earlier. (Manual setting detailed below)

Firmware Version 2.11.X and newer:

Multicast addresses for each encoder must 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 send-ip-mcast-range 224.1.2.1 224.1.2.255
```

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

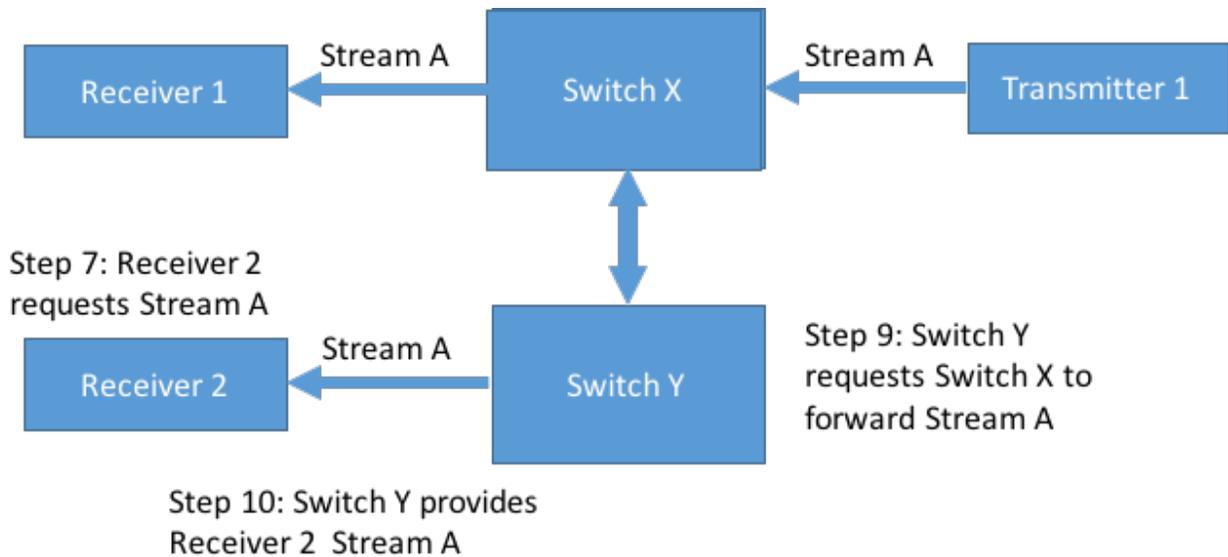
In a single switch environment, IGMP suffices to enable the switch to understand which traffic must be routed to which ports. In a ZyPer4K system, the switch will only route a transmitted video to those ports where a ZyPer4K receiver has requested a particular stream. In a multi-switch environment, higher-level 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.

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 in to 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 also 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	3.4	
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 13 Gbps



The ZyPer4K 1 Gb port

ZyPer4K products include a 1 Gb “courtesy 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:

- 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 of a 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 480 Mb/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)	13 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

Security and convenience are features with opposite requirements. You can do either in our system to whatever varying degrees satisfy your performance goals. 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.

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 / MaestroZ

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



Customers can modify this security with HTTPS/AJAX/JSON and secure the control system more tightly. This does add a layer of complexity to the implementation and should be done based on individual customer requirements.

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.

The API command is as follows:

```
set device <device:mac|name> ethernet-management-port enabled|disabled
```

Note: This feature is enabled in API version 1.5 and above.

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	M4300-24X	24	4 (shared)	Fully Managed Switch
Netgear	M4300-24x24F	24	24	Fully Managed Switch
Netgear	M4300-48X	48	4 (shared)	Fully Managed Switch
Netgear	M4300-96X	96	96	96 Max Ports. Configurable as mix of Copper/Fiber.
Arista	7050TX-48	32		
Arista	7050TX-64	48		
Arista	7050TX-128	96		
Arista	DCS-7504E	192		Linecard based
Arista	DCS-7508E	384		Linecard based
Arista	DCS-7512E	576		Linecard based
Arista	7150S-24		24	
Arista	7150S-52		52	
Arista	DCS-7504N		576	Linecard based
Arista	DCS-7508N		1152	Linecard based
Arista	DCS-7512N		1728	Linecard based
Dell	X4012		12	
Dell	S4048-ON		48	Up to 72 10GbE ports with breakout cables.
Brocade	ICX7500	48	4	
Brocade	ICX7750-48F		54*	48 10GbE SFP+ ports and 6 40 GbE QSFP+ ports
Brocade	ICX7750-48C	48	6	Fiber ports are 40 GbE QSFP+ ports
Cisco	Nexus 2348TQ	48	48	



Appendix 2: Switch Configuration Options

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.

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
5. Filter Unregistered Multicast (different wording than number 4 above)
 - a. Must be enabled if found
6. Disable IGMP Query
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 ProSafe XS708T**. (*Security-Traffic Control-Storm Control-Status=Disable*)



Appendix 3: 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 (990 ft)
1310nm Multi-mode Fiber (MMF) OM3/4	2km
1310nm Single-mode Fiber (SMF) 9/125	10km
1550nm Single-mode Fiber (SMF) 9/125	40km
Category 5	Not supported
Category 5e	55m (180 ft)
Category 6 UTP	55m (180 ft)
Category 6 STP	100m (330 ft)
Category 6A UTP	100m (330 ft)
Category 7	100m (330 ft)

UTP = Unshielded Twisted Pair

STP = Shielded Twisted Pair

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	300m
Z4KSFP10G31-2K	Fiber Optic Transceiver, SFP+ 10Gbps 1310nm MMF	2km
Z4KSFP10G31-10K	Fiber Optic Transceiver, SFP+ 10Gbps 1310nm SMF	10km